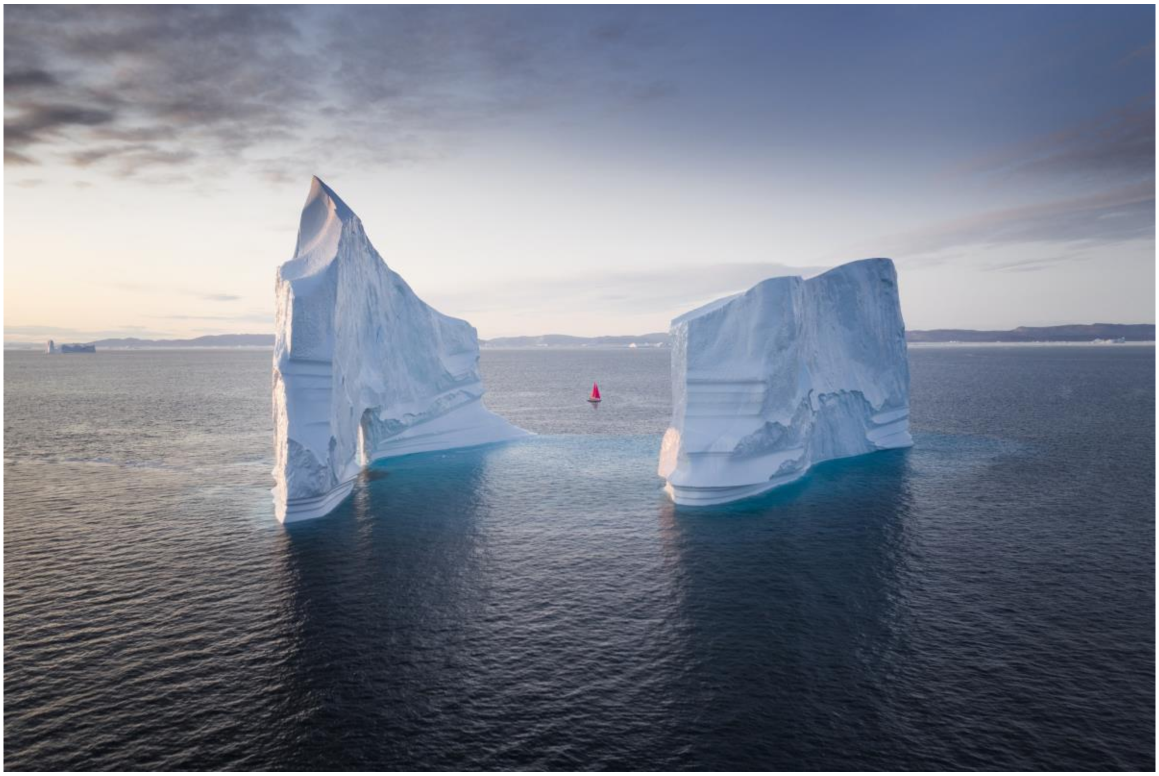
Cyber Risk GmbH
Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341
Dammstrasse 16, 8810 Horgen, Switzerland
Tel: +41 79 505 89 60 Web: https://www.cyber-risk-gmbh.com



March 2023, top cyber risk and compliance related local news stories and world events

Dear readers,

Confucius believed that “it is easy to hate, and it is difficult to love. All good things are difficult to achieve, and bad things are very easy to get.”

The compliance objectives in the EU these days are so difficult to achieve, and so difficult to love. Europe is running out of qualified compliance officers in certain difficult areas:

1. The Digital Services Act has been published in the Official Journal of the EU as of 27 October 2022, and shall apply from 17 February 2024.

In the context of the Russian military invasion in Ukraine, and the particular impact on the manipulation of online information, the Digital Services Act introduces a crisis response mechanism. This mechanism will make it possible to analyse the impact of the activities of very large online platforms (VLOPs) and very large online search engines (VLOSEs).

The Digital Services Act is the most important and most ambitious regulation in the world in the field of the protection of the digital space against the spread of illegal content. There is no other legislative act in the world having this level of ambition to regulate social media, online marketplaces, very large online platforms (VLOPs) and very large online search engines (VLOSEs).

After the Digital Services Act, platforms will not only have to be more transparent, but will also be held accountable for their role in disseminating illegal and harmful content.

Amongst other things, the DSA:

a. Lays down special obligations for online marketplaces in order to combat the online sale of illegal products and services;

b. Introduces measures to counter illegal content online and obligations for platforms to react quickly, while respecting fundamental rights;

c. Protects minors online by prohibiting platforms from using targeted advertising based on the use of minors' personal data as defined in EU law;

d. Imposes certain limits on the presentation of advertising and on the use of sensitive personal data for targeted advertising, including gender, race and religion;

e. Bans misleading interfaces known as 'dark patterns', and practices aimed at misleading.

2. The Digital Markets Act will enter into force in May 2023. It affects "gatekeeper platforms" like Google, Amazon and Meta, and covers the need for user consent before processing personal data for targeted advertising.

It is interesting that most of the companies that are affected by the EU Digital Markets Act and the EU Digital Services Act are based in the United States of America.

The DMA builds a digital level playing field with clear rights and rules for large online platforms ('gatekeepers'), and ensures that gatekeepers do not abuse their position. Most provisions of the regulation apply from 2 May 2023 (Article 54, Entry into force and application). Some provisions apply from 1 November 2022.

According to Article 2 of the Digital Markets Act (DMA), 'core platform service' means any of the following:

(a) online intermediation services;

(b) online search engines;

(c) online social networking services;

(d) video-sharing platform services;

(e) number-independent interpersonal communications services;

(f) operating systems;

(g) web browsers;

(h) virtual assistants;

(i) cloud computing services;

(j) online advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by an undertaking that provides any of the core platform services listed in points (a) to (i).

According to Article 3 of the Digital Markets Act (DMA), an undertaking shall be designated as a gatekeeper if:

1. (a) it has a significant impact on the internal market;

(b) it provides a core platform service which is an important gateway for business users to reach end users; and

(c) it enjoys an entrenched and durable position, in its operations, or it is foreseeable that it will enjoy such a position in the near future.

An undertaking shall be presumed to satisfy the respective requirements in paragraph 1:

(a) as regards paragraph 1, point (a), where it achieves an annual Union turnover equal to or above EUR 7,5 billion in each of the last three financial years, or where its average market capitalisation or its equivalent fair market value amounted to at least EUR 75 billion in the last financial year, and it provides the same core platform service in at least three Member States;

(b) as regards paragraph 1, point (b), where it provides a core platform service that in the last financial year has at least 45 million monthly active end users established or located in the Union and at least 10,000 yearly active business users established in the Union, identified and calculated in accordance with the methodology and indicators set out in the Annex;

3. The NIS 2 Directive is a major challenge for EU and non-EU companies. By 17 October 2024, Member States shall adopt and publish the measures necessary to comply with this Directive. They shall apply those measures from 18 October 2024.

According to Article 20 (Governance), the management bodies of essential and important entities must approve the cybersecurity risk-management measures taken by those entities, oversee its implementation and "can be held liable for infringements."

According to Article 20, Member States shall ensure that the "members of the management bodies of essential and important entities are required to follow training," and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

According to Article 21 (Cybersecurity risk-management measures), essential and important entities must take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Important note for Non-EU entities: Under Article 26 (Jurisdiction and territoriality), if an entity is not established in the EU, but offers services within the EU, it shall designate a representative in the EU.

The representative shall be established in one of those Member States where the services are offered. Such an entity shall be considered to fall under the jurisdiction of the Member State where the representative is established.

In the absence of a representative, any Member State in which the entity provides services may take legal actions against the entity for the infringement of this Directive.

4. The Critical Entity Resilience Directive (CER). By 17 October 2024, Member States shall adopt and publish the measures necessary to comply with this Directive. They shall apply those measures from 18 October 2024.

The new rules will strengthen the resilience of critical infrastructure to a range of threats, including natural hazards, terrorist attacks, insider threats, or sabotage.

11 sectors are covered: energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, public administration, space and food.

EU Member States will need to adopt a national strategy and carry out regular risk assessments to identify entities that are considered critical or vital for the society and the economy.

The above are just 4 out of many compliance challenges for EU and non-EU countries. In Cyber Risk GmbH we monitor the developments in 16 risk and compliance management areas in the EU, that are changed after EU legal Acts.
I feel guilty for not having the time to carefully study the regulation on markets in crypto-assets (MiCA).

We need patience and time.

Leo Tolstoy believed that the two most powerful warriors are patience and time. I really wonder how our so smart friends and good people (most of them), the Russians, made such a huge mistake with this war, that is changing Europe.

In the EU, they follow what Aristophanes believed: “Men of sense often learn from their enemies. It is from their foes, not their friends, that cities learn the lesson of building high walls and ships of war.”

Every time I read the word “resilience” these days, I leave everything else. Why? Well, we have the European Cyber Resilience Act (CRA), the Digital Operational Resilience Act (DORA), and the Critical Entities Resilience Directive (CER). There are firms that must implement all three, and it is not an easy task. And now, we have the Cyber resilience scenario testing (CyRST).

Lao Tzu has said: “Do the difficult things while they are easy.” Sorry Lao Tzu, no such thing there, this does not apply to the new regulatory landscape.

All jokes aside, I have been studying *all stress testing approaches, challenges and opportunities* at least since January 2009, when the Basel Committee on Banking Supervision released the “Principles for sound stress testing practices and supervision”.

The European Systemic Risk Board (ESRB) has just released an excellent paper, the “Advancing macroprudential tools for cyber resilience”, where we can read about the *Cyber resilience scenario testing (CyRST).* This is “an analytical tool for testing the capacity of the financial system to swiftly respond to and recover from a severe but plausible cyber scenario that causes a significant disruption and could affect financial and operational stability.”

The ability of the financial system to respond to and recover from such an event determines the extent to which it can support the continuity of key economic functions in a severe cyber scenario. This is assessed by designing a hypothetical cyber scenario and asking participating firms to:

- document the scenario’s impact,
- how they would respond to and recover from it, and
- the extent to which key economic functions could continue to operate under the scenario.

The test is used to evaluate the overall impact of the scenario *on financial and operational stability* and to identify areas where further work is required to mitigate risks.

CyRST can involve financial institutions, financial market infrastructures and other firms that support the operation of the financial system, including information and communications technology (ICT) third party service providers.

CyRST can complement other analytical tools. It should be viewed as one component of the overall framework for assessing system-wide cyber resilience.

In 2017, the Bank of England's Financial Policy Committee (FPC) set out its framework for building and maintaining *cyber resilience*.

Two of the elements of this framework involve setting clear baseline expectations for firms' resilience that reflect their importance for the financial system, and regular resilience testing by firms and supervisors.

Since then, the Bank of England has been working on the development of a new tool known as *"cyber stress testing"* which combines these two elements of the FPC's framework and focuses on the key cyber risks to the stability of the financial system.

The Bank of England is using its test to explore firms' capabilities and the potential impact on financial stability in a hypothetical scenario.

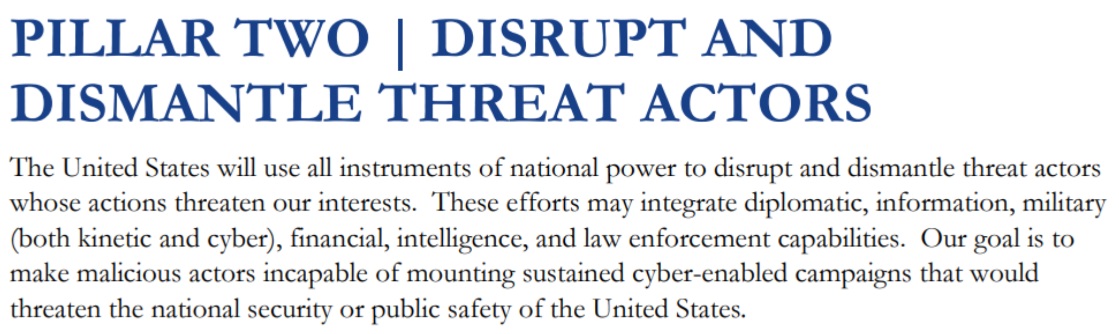
Following a successful pilot in 2019, the Bank of England carried out an exploratory cyber stress test in 2022 with several firms on a voluntary basis. The test had a data integrity incident as the disruption scenario and was intended to test firms' ability to meet the impact tolerance for payments in a severe but plausible scenario involving the retail payments system.

In June 2022, the Danish FSA announced the launch of its programme for strengthened operational resilience in the financial sector. The programme uses cyber stress testing to analyse the consequences of an extensive ICT disruption. The programme builds, among other things, on the work of the Danish Financial Sector forum for Operational Resilience (FSOR), which is chaired by Danmarks Nationalbank.

The cyber stress test, in which systemic firms will be required to participate, is being led by a team of information and cybersecurity supervisors assisted by core banking and resolution supervisors.

Read more about the CyRST at number 2 below.

I have just read for the second time the new US Cybersecurity Strategy of March 2023. There are some parts in this strategy that are very interesting. We read:



PILLAR TWO | DISRUPT AND DISMANTLE THREAT ACTORS

The United States will use all instruments of national power to disrupt and dismantle threat actors whose actions threaten our interests. These efforts may integrate diplomatic, information, military (both kinetic and cyber), financial, intelligence, and law enforcement capabilities. Our goal is to make malicious actors incapable of mounting sustained cyber-enabled campaigns that would threaten the national security or public safety of the United States.

“Using all instruments of national power, we will make malicious cyber actors incapable of threatening the national security or public safety of the United States, including by:

- Strategically employing all tools of national power to disrupt adversaries;

- Engaging the private sector in disruption activities through scalable mechanisms; and,

- Addressing the ransomware threat through a comprehensive Federal approach and in lockstep with our international partners.”

The phrase “Using all instruments of national power, we will make malicious cyber actors incapable of threatening ...” is very interesting, and it is the only way to achieve this objective.

Carl von Clausewitz (a Prussian general, author of “Vom Kriege” (On War), an expert on military strategy) had said: “Pursue one great decisive aim with force and determination.”

Isaac Newton believed that “An object in motion tends to remain in motion along a straight line unless acted upon by an outside force”. It is time to stop this object in motion, the cyber attacks against our societies, with all instruments of national power in each civilized country, to make malicious cyber actors incapable of threatening us.

Read more at number 6 below.

I could not resist the temptation, so I have just read the EU proposal for a Regulation on Markets in Crypto-assets (also called “MiCA”).

The European Commission believes that ‘crypto-assets’ and ‘distributed ledger technology’ should be defined *as widely as possible,* to capture all types of crypto-assets which currently fall *outside* the scope of EU legislation on financial services.

MiCA follows the recommendations of the Financial Action Task Force (FATF), and contributes to the objective of combating money laundering and the financing of terrorism.

Issuers of asset-referenced tokens should have robust *governance arrangements,* including a clear organisational structure with well-defined, transparent and consistent lines of responsibility and effective processes to identify, manage, monitor and report the risks to which they are or might be exposed.

The management body of such issuers and their shareholders should have good repute and sufficient expertise and be fit and proper for the purpose of anti-money laundering and combatting the financing of terrorism.

Issuers of asset-referenced tokens should also employ resources proportionate to the scale of their activities and should always ensure continuity and regularity in the performance of their activities.

For that purpose, issuers of asset-referenced tokens should establish a business continuity policy aimed at ensuring, in the case of an interruption to their systems and procedures, the performance of their core payment activities.

Issuers of asset-referenced tokens should also have a strong internal control and risk assessment mechanism, as well as a system that guarantees the integrity and confidentiality of information received. (I would not be surprised if they asked for Sarbanes-Oxley compliance too).

All jokes aside, this is an important development. The EU wants to avoid corporate governance failures like the one Sam Bankman-Fried had established in FTX. I know, crypto-assets were not exactly thought to work like that, but this is the obvious end of the road. MiCA is absolutely in line with FSB's framework for the regulation of crypto-asset activities. FSB asks for the principle of *"same activity, same risk, same regulation"*.

Where crypto-assets and intermediaries perform an equivalent economic function to one performed by instruments and intermediaries of the traditional "centralized" financial sector, they should be subject to equivalent regulation, even when they try (without much success) to become "decentralized".

Read more at number 15 below.

In Switzerland, according to the National Cyber Security Centre (NCSC), in CEO fraud attempts, attackers gather data from public sources in advance. They usually use company websites that list their employees and their functions. However, data on social media platforms can also be used for such fraud attempts, as shown by a case reported to the NCSC last week that targeted a company's HR department.

In addition to the classic variant, sub-variants have likewise been observed for some time now. One of these variants, also called the HR variant, targets HR managers. Here, too, the fraudsters partly use data from the company website. However, in these cases, data from social media platforms increasingly plays a more significant role, as a case reported to the NCSC last week demonstrated.

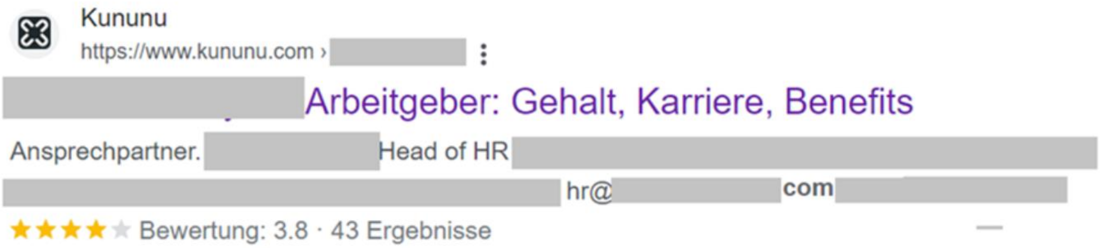
CEO fraudsters target HR

In the HR variant, an email is sent to the HR department by a purported employee requesting that their next salary payment be made to a different account. For this scam, the attacker must know the HR manager's name and email address, as well as an employee's name.

In the current case, however, these details were not visible on the website, which led to the initial suspicion that the attackers could have obtained the data from a hacking attempt against the company or against the employee. However, an extended search revealed that the fraudsters had gathered the data from social media channels in advance.

Platforms such as Xing or LinkedIn aim to connect professional contacts, and job titles are a central part of this. As a result, the name and function of the company's HR manager was also visible on Xing in the current case. In addition, other employees of the company are listed on Xing with their first and last names, job titles and direct links. The attackers focus on the employees with the highest salaries.

On another social media platform, the email address of the HR department is also listed. However, this address needs to be published, as it is usually used to submit job applications as well.



Kununu
https://www.kununu.com › [redacted] ⋮

[redacted] Arbeitgeber: Gehalt, Karriere, Benefits

Ansprechpartner. [redacted] Head of HR [redacted]

[redacted] hr@ [redacted] com [redacted]

★★★★☆ Bewertung: 3.8 · 43 Ergebnisse

Ban the use of social media?

At a time when social media is playing an increasingly important role, prohibiting employees from using such channels is clearly not a solution. Nevertheless, every company should also set guidelines on what information employees are allowed to disclose on social media channels and what not.

It is clear that the availability of such information will also lead to increased fraud. It is therefore particularly important to raise awareness of such fraud variants among all company employees who can initiate payments. HR departments should also be informed accordingly. Changes to salary bank accounts should only be made through verifiable channels or after personal consultation with the employees.

Cyber Security Centre (NCSC) Recommendations:

- Raise all employees' awareness of CEO fraud! Especially employees in finance divisions, in HR departments and in key positions must be informed about these possible methods of attack. In the case of associations, all presiding members and treasurers must receive training.

- Define a process which can be used to amend bank account details, even urgently. Typically, this should be done through a second channel (e.g. by phone).

- Define guidelines on what information employees are allowed to disclose about the company.

We have another interesting article from the Swiss National Cyber Security Centre (NCSC):

Computer disposed of – account hacked

Every computer eventually becomes outdated or breaks down, is replaced and has to be disposed of. This was the case with a computer that was reported to the NCSC last week. The person who reported the incident had handed in his MacBook at a disposal point. A few days later, however, he received a security warning that his MacBook had been activated and someone had tried to change his Apple account.

It is suspected that someone was indeed able to gain access to the disposed-of device and hence to the data stored on it, such as the victim's photo collection, emails and login details.

This report to the NCSC highlights the importance of completely erasing the hard drive in computers and notebooks, USB sticks, mobile phones or tablets, etc. before their disposal or resale.

Simply deleting data is not enough

It is important to be aware that simply deleting data is not sufficient. Electronic data remains on the storage medium even after deletion, or after emptying the recycle bin. Only the information in the internal "table of contents" about where the data is stored on the hard disk is deleted.

To delete data permanently, the storage location must be overwritten multiple times at random.

Special programs are available for this process, known as wiping. If used properly, the hard disk is permanently erased so that the data can no longer be recovered, even using recovery programmes.

Before wiping, you should also remove linked accounts from your device and log out of applications (email client, Office 365 account, etc.).

Nowadays, modern operating systems also include functions that reset notebooks and mobile phones and prepare them for disposal or resale. In the past, however, deficiencies have been found in these functions and the deleted data could still be recovered.

In order to reliably delete your data from a hard disk, it is therefore recommended to use a specialised program to randomly overwrite the hard disk several times.

In addition, the recovery partition, and with that the manufacturer's recovery function, should also be overwritten. Overwriting the data is the only option for older devices.

If a device is no longer to be used, the data carrier can also be physically destroyed. However, the storage media must first be removed from the device, which can be time-consuming.

MacOS and Windows

Apple has published instructions for its operating systems on what to do if the computer is to be disposed of, sold or given away. These allow the data to be deleted and the notebook to be restored to factory settings.

The current Windows operating systems also have functions that reset computers to factory settings. Microsoft has published the relevant instructions.
Smartphones and tablets

On both Android and Apple devices, the storage space is encrypted if the corresponding function is available and switched on. It is therefore sufficient to delete the associated key to prevent access to the data. This is done as part of the factory reset.

However, how secure this procedure is also depends on the encryption algorithm and key used by the manufacturer. Therefore, it makes sense to additionally overwrite the data. Overwriting the data is also the only option for older devices that do not have encrypted memory.

USB sticks, SIM cards with memory function, external hard disks, CDs/DVDs and other storage media

There are countless freely available tools on the internet for deleting data, known as shredder or wiper programs. However, it is sometimes unclear how effective a program is. If in doubt, specialists can provide information. Physical destruction must cause as much damage as possible.

In the case of SSD (solid state drive) memory, each individual memory chip must be physically damaged. Note that many types of storage media can shatter violently when destroyed.

Welcome to our monthly newsletter.

Best regards,

George Lekatis

George Lekatis
General Manager, Cyber Risk GmbH
Dammstrasse 16, 8810 Horgen
Phone: +41 79 505 89 60
Email: george.lekatis@cyber-risk-gmbh.com
Web: www.cyber-risk-gmbh.com

Number 1 (Page 16)

JP-23-01 - Sustained activity by specific threat actors

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

CERT-EU

Joint Publication
Structured Cooperation between CERT-EU and ENISA
TLP:CLEAR | 15/02/2023 | JP-23-01 | v1.0

Number 2 (Page 19)

Advancing macroprudential tools for cyber resilience

ESRB
European Systemic Risk Board
European System of Financial Supervision

Number 3 (Page 23)

DEV-1101 enables high-volume AiTM campaigns with open-source phishing kit

Microsoft Threat Intelligence

Microsoft

Number 4 (Page 27)

CISA Director Remarks at Carnegie Mellon University

Number 5 (Page 29)

Developing National Vulnerabilities Programmes

enisa European Network and Information Security Agency

Number 6 (Page 32)

The new US National Cybersecurity Strategy

THE WHITE HOUSE

Number 7 (Page 37)

Social Media Manipulation 2022/2023:
Assessing the Ability of Social Media Companies to Combat Platform Manipulation

NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE

Number 8 (Page 39)

Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA)
#StopRansomware: Royal Ransomware

JOINT CYBERSECURITY ADVISORY

Coauthored by:

Number 9 (Page 41)

The quick and the dead - building up cyber resilience in the financial sector
Fabio Panetta, Member of the Executive Board of the European Central Bank, at the meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures, Frankfurt am Main.

Number 10 (Page 47)

NIST Internal Report, NIST IR 8432 ipd, 4 Initial Public Draft
Cybersecurity of Genomic Data

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Number 11 (Page 49)

US Federal Authorities Seize Internet Domain Selling Malware Used to Illegally Control and Steal Data from Victims' Computers

United States
Attorney's Office
Central District of California

Number 12 (Page 52)

Cyber criminals use Eurovision as the latest phishing lure

National Cyber
Security Centre

Number 13 (Page 54)

DARPA Seeks Input to Advance Hybrid Quantum/Classical Computers

DARPA
DEFENSE ADVANCED
RESEARCH PROJECTS AGENCY

Number 14 (Page 57)

Sanctions and Export Controls Compliance

Department of Commerce, Department of the Treasury, and Department of Justice Tri-Seal Compliance Note

Cracking Down on Third-Party Intermediaries Used to Evade Russia-Related Sanctions and Export Controls

Number 15 (Page 60)

Proposal for a regulation on Markets in Crypto-assets (MiCA)

EUROPEAN COMMISSION

Number 16 (Page 65)

NPSA is the UK Government's National Technical Authority for Physical and Personnel Protective Security.

Security Campaigns

National Protective
Security Authority

Number 17 (Page 68)

How Digital Twins Could Protect Manufacturers From Cyberattacks

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Number 18 (Page 72)

European Parliament resolution on the adequacy of the protection afforded by the EU-US Data Privacy Framework

European Parliament
2019-2024

Committee on Civil Liberties, Justice and Home Affairs

Number 19 (Page 78)

Office of the Director of National Intelligence

2023 Annual Threat Assessment of the U.S. Intelligence Community

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
UNITED STATES OF AMERICA

Number I

JP-23-01 - Sustained activity by specific threat actors

Joint Publication
Structured Cooperation between CERT-EU and ENISA
TLP:CLEAR | 15/02/2023 | JP-23-01 | v1.0

Summary

The EU Cybersecurity Agency (ENISA) and the CERT for the EU institutions, bodies and agencies (CERT-EU) would like to draw the attention of their respective audiences on particular Advanced Persistent Threats (APTs), known as APT27, APT30, APT31, Ke3chang, GALLIUM and Mustang Panda.

These threat actors have been recently conducting malicious cyber activities against business and governments in the Union.

On 19 July 2021, the EU has urged Chinese authorities to take actions against malicious cyber activities undertaken from their territory, and linked to APT31.

These malicious cyber activities, which had significant effects, targeted government institutions and political organisations in the EU and Member States, as well as key European industries.

On 18 July 2022, Belgium has also urged Chinese authorities to take action against malicious cyber activities undertaken by Chinese actors. These activities can be linked to the hacker groups known as APT 27, APT 30, APT 31, and GALLIUM.

Moreover, commercial firms indicated that Ke3chang and Mustang Panda are likely operating from the territory of China.

These threat actors present important and ongoing threats to the European Union. Recent operations pursued by these actors focused mainly on information theft, primarily via establishing persistent footholds within the network infrastructure of organisations of strategic relevance.

ENISA and CERT-EU call for all public and private sector organisations in the EU to apply the recommendations included in this document in a consistent and systematic manner.

These recommendations aim to reduce the risk of being compromised by the mentioned APTs, as well as substantially improve the cybersecurity posture and enhance the overall resilience of these organisations against cyberattacks.

Recommendations

All public and private sector organisations in the EU are strongly advised to follow common cyber hygiene recommendations.

Our previously published best practices and the corresponding security guidance provide a solid basis for mitigating cyberattacks.

CERT-EU

CERT-EU Security Guidance 22-001

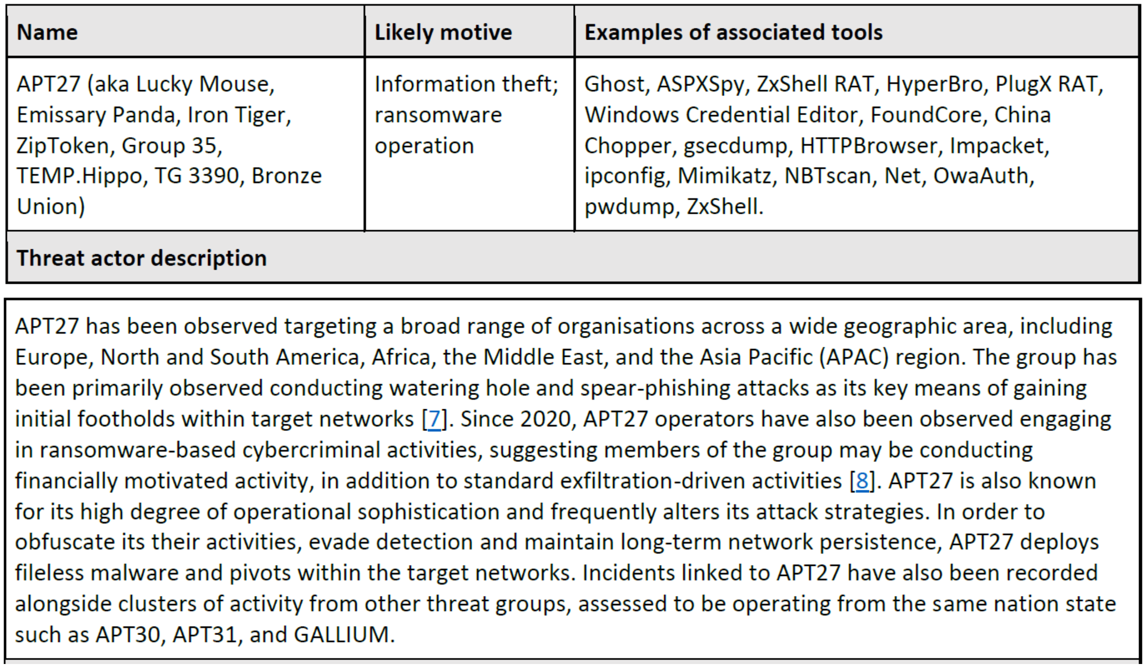
Cybersecurity mitigation measures against critical threats

You may visit: https://www.cert.europa.eu/static/WhitePapers/TLP-WHITE-CERT-EU_Security_Guidance-22-001_v1_0.pdf

Following the analysis of the available information on the aforementioned threat actors (see below) and of some of their major tactics, techniques, and procedures, ENISA and CERT-EU draw a number of complementary recommendations to foster the defensive capabilities of the intended audience.

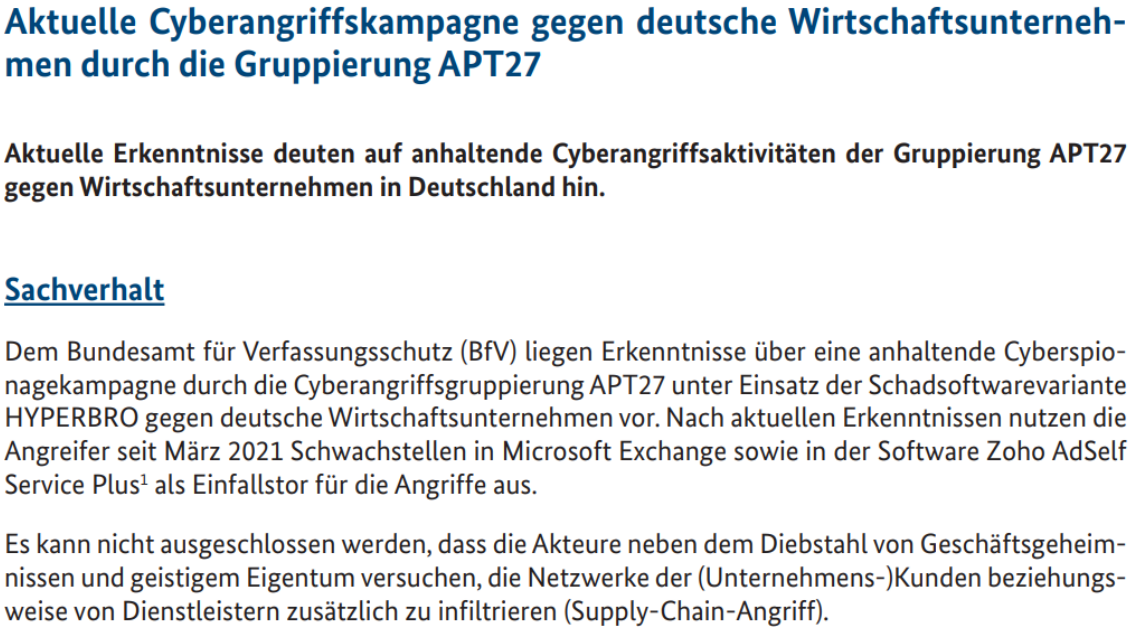
Each organisation which wants to apply these recommendations is fully responsible for the implementation, according to its business needs and priorities.

Additionally, CERT-EU and ENISA emphasise the importance of participating in information sharing communities and reviewing your national/governmental CSIRT's security guidance and public resources detailing tactics, techniques and procedures associated with the threat actors.



Name	Likely motive	Examples of associated tools
APT27 (aka Lucky Mouse, Emissary Panda, Iron Tiger, ZipToken, Group 35, TEMP.Hippo, TG 3390, Bronze Union)	Information theft; ransomware operation	Ghost, ASPXSpy, ZxShell RAT, HyperBro, PlugX RAT, Windows Credential Editor, FoundCore, China Chopper, gsecdump, HTTPBrowser, Impacket, ipconfig, Mimikatz, NBTscan, Net, OwaAuth, pwdump, ZxShell.
Threat actor description		

APT27 has been observed targeting a broad range of organisations across a wide geographic area, including Europe, North and South America, Africa, the Middle East, and the Asia Pacific (APAC) region. The group has been primarily observed conducting watering hole and spear-phishing attacks as its key means of gaining initial footholds within target networks [7]. Since 2020, APT27 operators have also been observed engaging in ransomware-based cybercriminal activities, suggesting members of the group may be conducting financially motivated activity, in addition to standard exfiltration-driven activities [8]. APT27 is also known for its high degree of operational sophistication and frequently alters its attack strategies. In order to obfuscate its their activities, evade detection and maintain long-term network persistence, APT27 deploys fileless malware and pivots within the target networks. Incidents linked to APT27 have also been recorded alongside clusters of activity from other threat groups, assessed to be operating from the same nation state such as APT30, APT31, and GALLIUM.



Aktuelle Cyberangriffskampagne gegen deutsche Wirtschaftsunternehmen durch die Gruppierung APT27

Aktuelle Erkenntnisse deuten auf anhaltende Cyberangriffsaktivitäten der Gruppierung APT27 gegen Wirtschaftsunternehmen in Deutschland hin.

Sachverhalt

Dem Bundesamt für Verfassungsschutz (BfV) liegen Erkenntnisse über eine anhaltende Cyberspionagekampagne durch die Cyberangriffsgruppierung APT27 unter Einsatz der Schadsoftwarevariante HYPERBRO gegen deutsche Wirtschaftsunternehmen vor. Nach aktuellen Erkenntnissen nutzen die Angreifer seit März 2021 Schwachstellen in Microsoft Exchange sowie in der Software Zoho AdSelf Service Plus[1] als Einfallstor für die Angriffe aus.

Es kann nicht ausgeschlossen werden, dass die Akteure neben dem Diebstahl von Geschäftsgeheimnissen und geistigem Eigentum versuchen, die Netzwerke der (Unternehmens-)Kunden beziehungsweise von Dienstleistern zusätzlich zu infiltrieren (Supply-Chain-Angriff).

To read more: https://www.enisa.europa.eu/publications/sustained-activity-by-specific-threat-actors-joint-publication

Number 2

Advancing macroprudential tools for cyber resilience

ESRB
European Systemic Risk Board
European System of Financial Supervision

The ESRB worked in 2022 within the context of a substantially heightened cyber threat environment across Europe.

The cyber activity resulting from Russia's invasion of Ukraine have affected both Ukraine and EU Member States directly and indirectly.

Furthermore, an increase in cyber attacks and the active sabotage of power and telecommunications infrastructure in EU Member States – which the financial sector relies on – present significant threats to financial stability.

The ESRB responded to this heightened cyber threat environment by:

1. Enhancing the exchange of information across jurisdictions and authorities.

2. Focusing on the tools and elements needed to advance cyber resilience and strengthen preparedness for potential cyber incidents.

3. Advancing a cyber resilience scenario testing (CyRST) approach: the ESRB completed further work on this approach, which could support authorities in:

(i) testing the response and recovery capacity of the financial system against severe but plausible scenarios involving a cyber incident,

(ii) evaluating their impact on financial and operational stability, and

(iii) identifying areas where further work is required to mitigate cyber risks.

4. Developing the concept for a systemic impact tolerance objective (SITO): the ESRB worked on developing SITOs, which can assist in identifying and measuring the impacts of cyber incidents on the financial system, and evaluating when they are likely to breach tolerance levels and cause significant disruption.

5. Reviewing current financial crisis management tools: the ESRB evaluated whether these tools are sufficient for adequately responding to system-wide cyber incidents.

The heightened cyber threat environment across Europe calls for a step change in enhancing system-wide cyber resilience.

The resistance and detection capabilities of individual entities constitute a first layer of defence against cyber incidents.

The Digital Operational Resilience Act (DORA) is part of an ongoing effort at the EU level to improve the cyber resilience of individual entities.

Threat-led penetration tests outlined by DORA, such as the European Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU), provide a way of testing this first layer of defence.

However, further layers of defence are needed to increase the resilience of the financial system as a whole against cyber incidents.

Against this background, the ESRB has three key areas of focus.

1. The ESRB encourages authorities to use the CyRST approach to pilot system-wide cyber resilience scenario testing as soon as possible.

Such pilots can complement other analytical tools that the authorities might be using and deepen their understanding of CyRST and of the risks to system-wide cyber resilience.

This is important and urgent, given the increased likelihood that a cyber attack will strike the European financial sector and because it will take time to pilot CyRST, identify the risks and implement appropriate mitigating measures.

The ESRB will continue to work in this area as a hub for sharing progress and good practice, and will update the conceptual approach based on what the authorities learn from their more detailed work in the pilots.

2. The ESRB advocates the use of SITOs and will continue to transition from a conceptual approach to a practical basis for implementing them.

Specifically, the ESRB will identify a key economic function3 where disruptions have cross-border implications and define appropriate SITOs at EU level so as to ensure consistency across the region/sector and authorities.

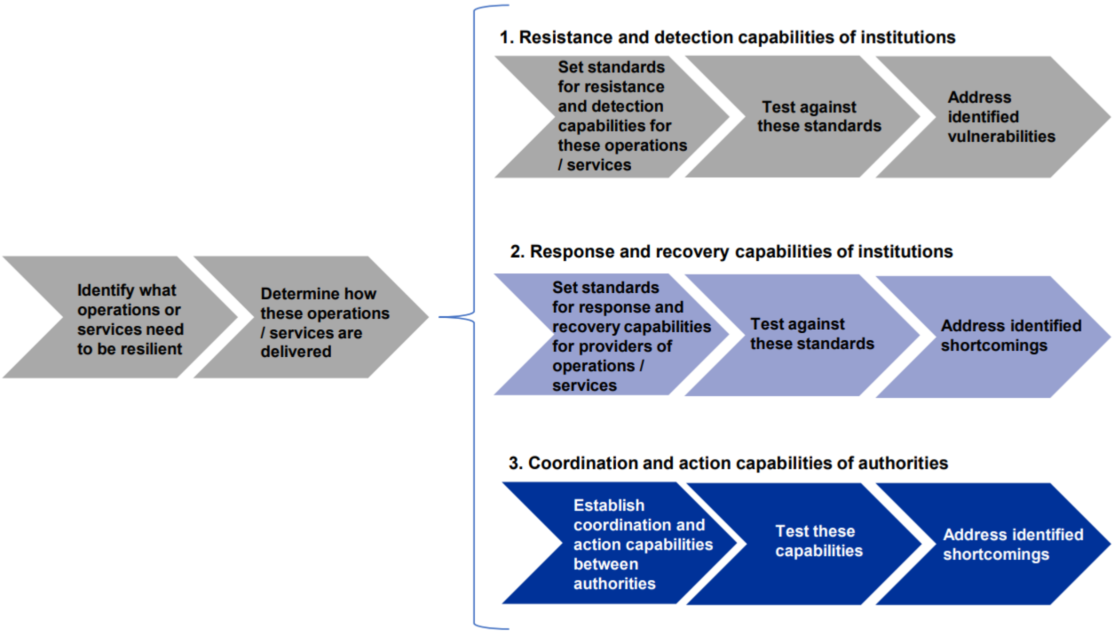
The ESRB will work with authorities across the EU to identify where a consistent approach is required and to decide on the approach for setting SITOs where there are crossborder implications.

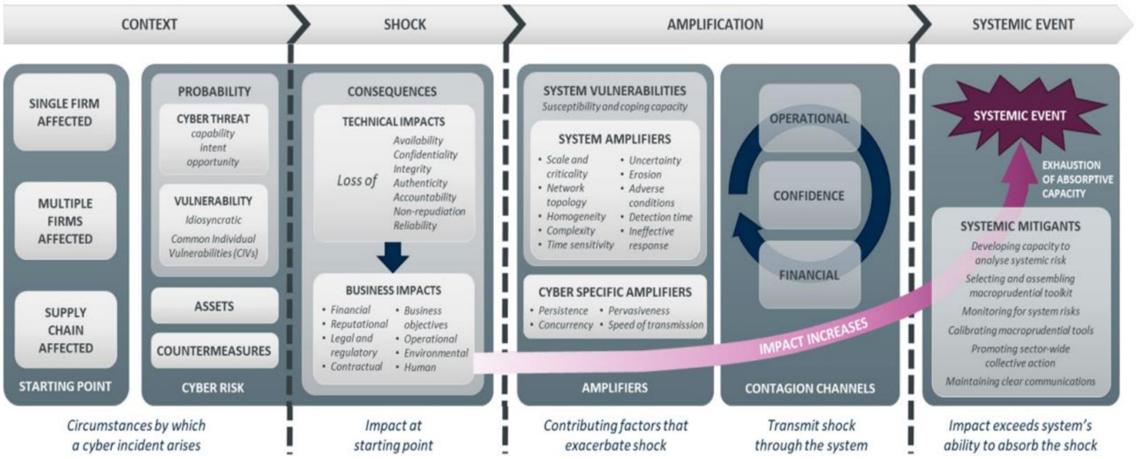
The ESRB recognises that where disruptions have no or few cross-border implications, SITOs may differ across jurisdictions to reflect national specificities.

3. The ESRB will consider which operational policy tools are most effective in responding to a system-wide cyber incident and identify gaps across operational and financial policy tools.

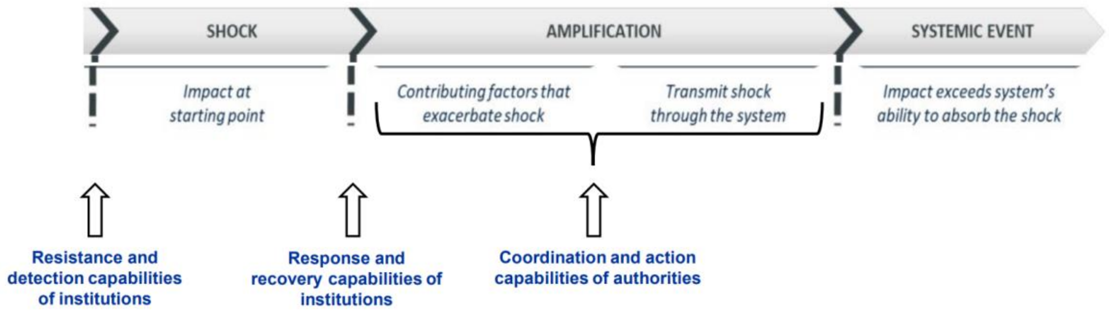
This work will build on the analysis of financial crisis management tools described in this report.

Designing, assessing and strengthening defences against systemic cyber risk

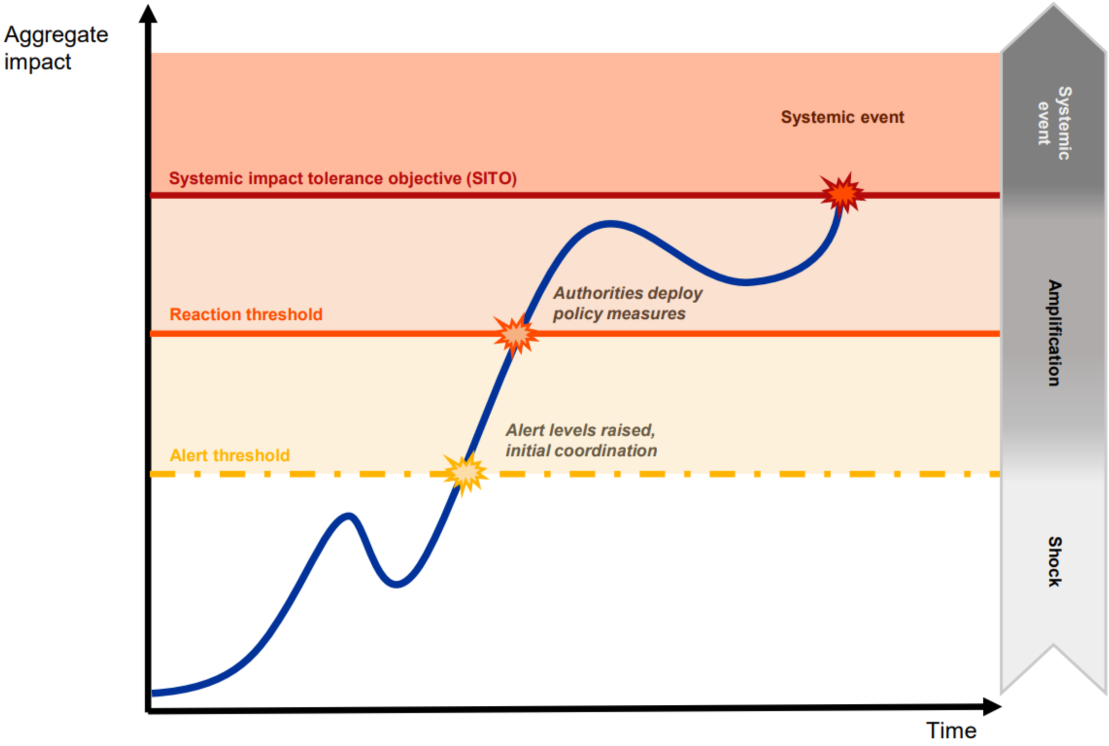

Identify what operations or services need to be resilient
Determine how these operations / services are delivered
1. Resistance and detection capabilities of institutions
Set standards for resistance and detection capabilities for these operations / services
Test against these standards
Address identified vulnerabilities
2. Response and recovery capabilities of institutions
Set standards for response and recovery capabilities for providers of operations / services
Test against these standards
Address identified shortcomings
3. Coordination and action capabilities of authorities
Establish coordination and action capabilities between authorities
Test these capabilities
Address identified shortcomings



Stylised representation of the layers of defence


SHOCK
AMPLIFICATION
SYSTEMIC EVENT
Impact at starting point
Contributing factors that exacerbate shock
Transmit shock through the system
Impact exceeds system's ability to absorb the shock
Resistance and detection capabilities of institutions
Response and recovery capabilities of institutions
Coordination and action capabilities of authorities

Cyber incident impact and tolerance for different impact levels



To read more:
https://www.esrb.europa.eu/pub/pdf/reports/esrb.macroprudentialtoolscyberresilience220214~984a5ab3a7.en.pdf?888a06fcb36d2c1ce41594efd67a4c88

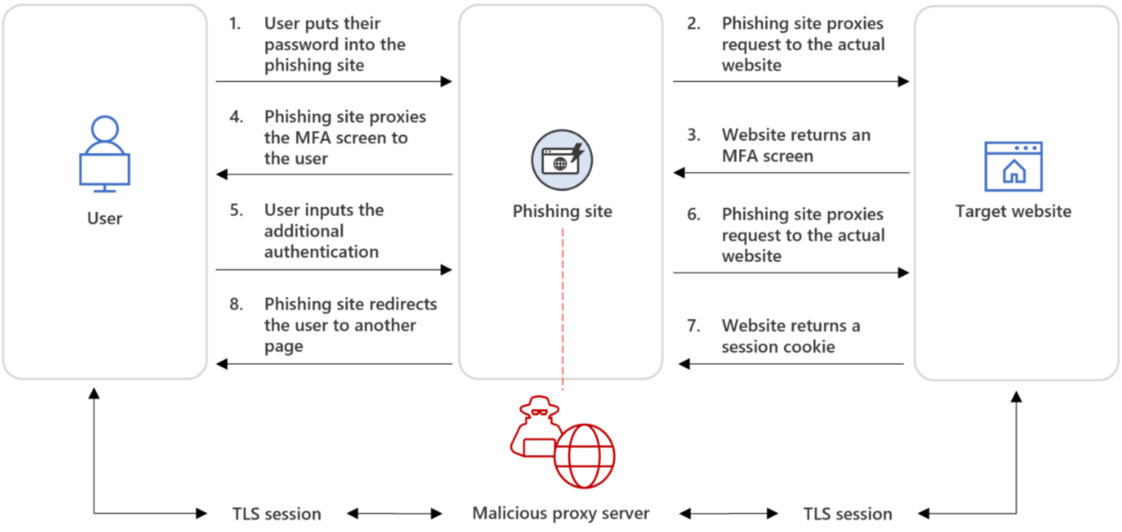
Number 3

DEV-1101 enables high-volume AiTM campaigns with open-source phishing kit

Microsoft Threat Intelligence

Adversary-in-the-middle (AiTM) phishing kits are part of an increasing trend that is observed supplanting many other less advanced forms of phishing.

The following diagram illustrates the AiTM phishing attack chain:



1. User puts their password into the phishing site
2. Phishing site proxies request to the actual website
3. Website returns an MFA screen
4. Phishing site proxies the MFA screen to the user
5. User inputs the additional authentication
6. Phishing site proxies request to the actual website
7. Website returns a session cookie
8. Phishing site redirects the user to another page

Figure 8. AiTM phishing attack diagram

AiTM phishing is capable of circumventing multifactor authentication (MFA) through reverse-proxy functionality.

DEV-1101 is an actor tracked by Microsoft responsible for the development, support, and advertising of several AiTM phishing kits, which other cybercriminals can buy or rent.

The availability of such phishing kits for purchase by attackers is part of the industrialization of the cybercriminal economy and lowers the barrier of entry for cybercrime.

DEV-1101 offers an open-source kit that automates setting up and launching phishing activity and provides support services to attackers.

The threat actor group began offering their AiTM phishing kit in 2022, and since then has made several enhancements to their kit, such as the capability to manage campaigns from mobile devices, as well as evasion features like CAPTCHA pages.

These attributes make the kit attractive to many different actors who have continually put it to use since it became available in May 2022. Actors using this kit have varying motivations and targeting and might target any industry or sector.

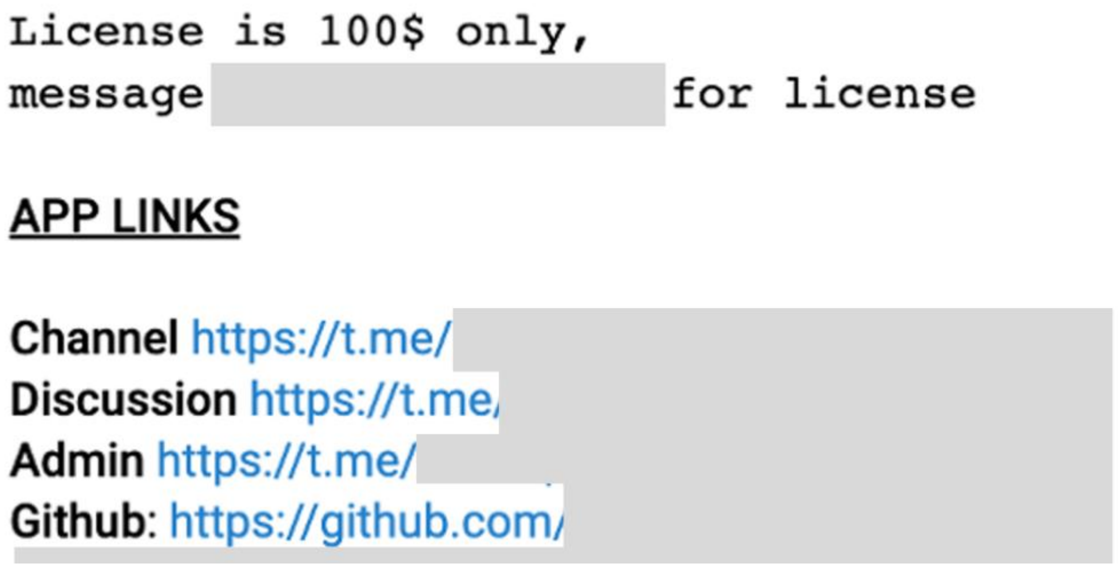
Microsoft 365 Defender detects suspicious activities related to AiTM phishing attacks and follow-on activities, such as session cookie theft and attempts to use the stolen cookies to sign in.

In this blog post, we share information on DEV-1101, the tool they offer, and details on related AiTM campaigns. We also share best practices and detection details to further protect organizations from AiTM phishing attacks.

AiTM tool promotion

DEV-1101 began advertising their AiTM kit around May 2022 through a Telegram channel and an advertisement in exploit[.]in, a popular cybercrime forum.

The advertisement describes the AiTM kit as a phishing application written in NodeJS with PHP reverse-proxy capabilities, automated setup, detection evasion through an antibot database, management of phishing activity through Telegram bots, and a wide range of ready-made phishing pages mimicking services such as Microsoft Office or Outlook.



License is 100$ only,
message [redacted] for license

APP LINKS

Channel https://t.me/
Discussion https://t.me/
Admin https://t.me/
Github: https://github.com/
[redacted]

On June 12, 2022, DEV-1101 announced that the kit would be open source with a $100 monthly licensing fee. The actor also provided links to additional Telegram channels and a now-defunct GitHub page.

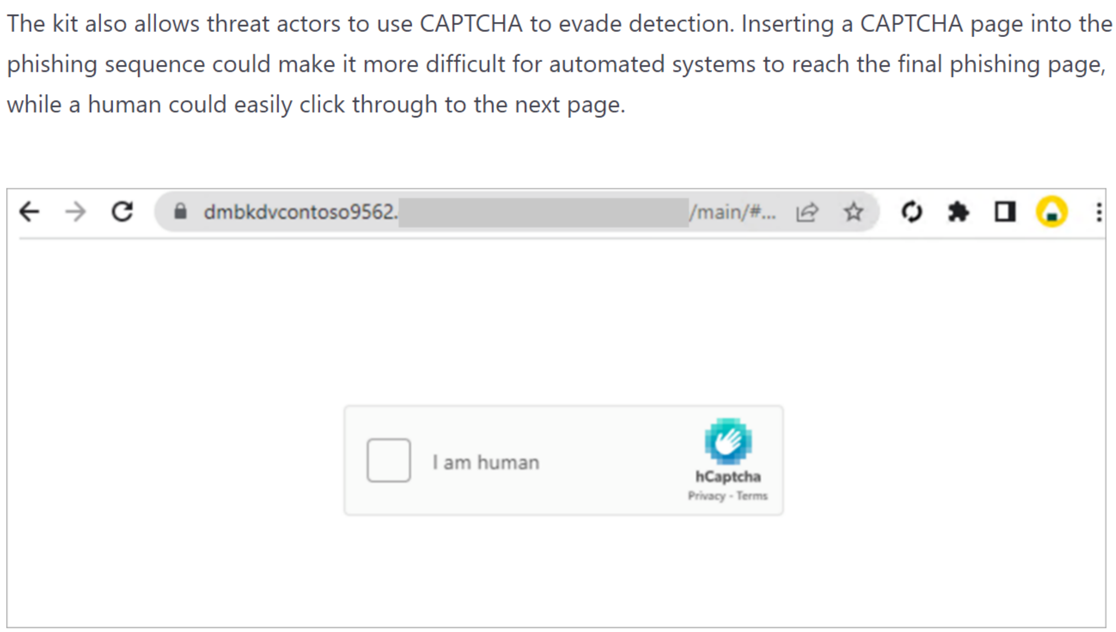
In September 2022, DEV-1101 added the ability to manage servers running their kit through a Telegram bot rather than requiring the use of cPanel, further facilitating phishing activities and letting their customers manage campaigns from mobile devices.

DEV-1101 was able to increase the price of their tool multiple times due to the rapid growth of their user base from July through December 2022. This allowed DEV-1101 to dedicate themselves fully to the development and support of their tool.

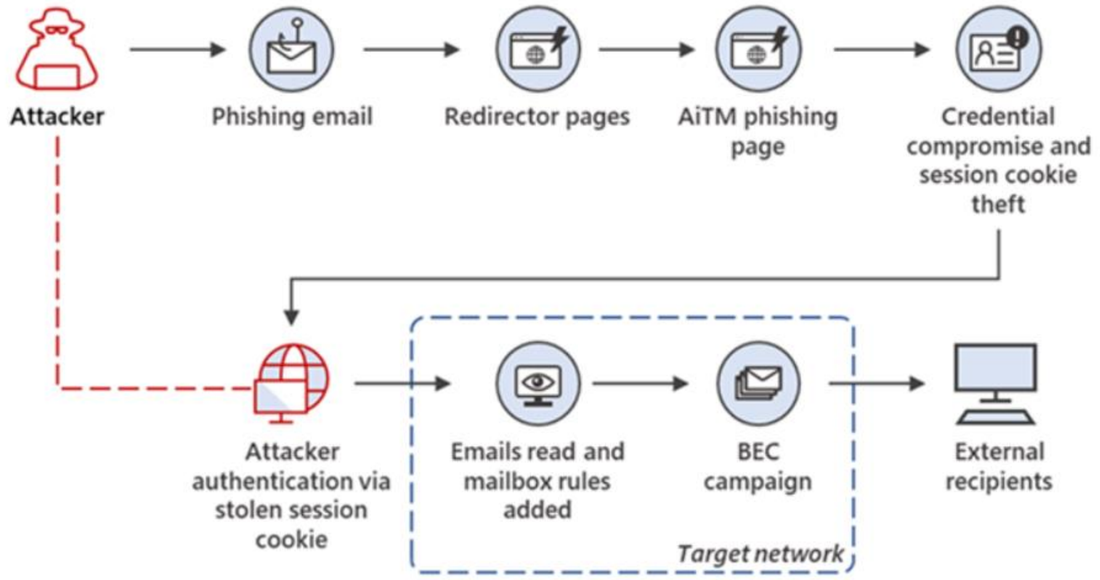
As of this writing, DEV-1101 offers their tool for $300, with VIP licenses at $1,000. Legacy users were permitted to continue purchasing licenses at $200 prior to January 1, 2023.

Microsoft observed several high-volume phishing campaigns from various actors using the tool offered by DEV-1101, comprising millions of phishing emails per day.

DEV-0928, an actor Microsoft has tracked since September 2022, is one of DEV-1101's more prominent patrons and was observed launching a phishing campaign involving over one million emails.



The kit also allows threat actors to use CAPTCHA to evade detection. Inserting a CAPTCHA page into the phishing sequence could make it more difficult for automated systems to reach the final phishing page, while a human could easily click through to the next page.


Attacker
Phishing email
Redirector pages
AiTM phishing page
Credential compromise and session cookie theft
Attacker authentication via stolen session cookie
Emails read and mailbox rules added
BEC campaign
External recipients
Target network

To read more: https://www.microsoft.com/en-us/security/blog/2023/03/13/dev-1101-enables-high-volume-aitm-campaigns-with-open-source-phishing-kit/

Number 4

CISA Director Remarks at Carnegie Mellon University

Good morning. Thank you to President Jahanian for that warm introduction and to everyone for joining me today on this Monday morning. It's wonderful to start the week off with this incredible community.

I can't think of a more fitting location for this discussion than Pittsburgh, a city built on innovation, imagination, and technological transformation; and Carnegie Mellon University, one of the world's most renowned educational institutions, home to one of our nation's top undergraduate computer science programs and top engineering programs, but also, to so much more. Let me share a few of my own favorites:

- The first smile in an email was created by research Professor Scott Fahlman, which launched the emoticon craze

- CAPTCHAs—or completely automated public Turing tests to tell computers and humans apart— (how many of you knew what that stood for?) were developed here by Professor Luis von Ahn and his colleagues, used to help prevent cybercrime

- Wireless research conducted at CMU laid the foundation for now ubiquitous wi-fi

- CMU is home to the nation's first robotics lab; and of course, home to the Software Engineering Institute, the first Federal Lab dedicated to software engineering. SEI established the first Computer Emergency Response Team, or CERT, in response to the Morris worm—that became the model for CERTs around the globe, and of course was a key partner in the creation of US-CERT in 2003, the precursor to CISA's Cybersecurity Division.

But the partnership between CMU and CISA goes well beyond technical capability – to what I consider the most important aspect of technology – People.

The CISA team is full of amazing CMU alumni like Karen Miller who leads our vulnerability evaluation work and Dr. Jono Spring, who is on the front lines of our vulnerability management work – both are here with me today.

Finally, I wanted to come here because CISA and CMU share a common set of values—collaboration, innovation, inclusion, empathy, impact, and service. And of course, a shared passion for our work.

So, now that you know why I am here, I want to start with a story.

At 2:39 pm on a chilly but sunny Saturday, just six miles off the coast of South Carolina, an F-22 fighter jet from Langley Air Force Base fired a Sidewinder air-to-air missile to take down a balloon—the size of three school buses—that had drifted across the United States.

The deliberate action came after a tense public standoff with Beijing and intense media scrutiny about the Chinese "spy balloon."

The response and surrounding attention to the issue, reinforced for me a major challenge we face in the field of cybersecurity—raising national attention to issues much less visible but in many ways far more dangerous.

Our country is subject to cyber intrusions every day from the Chinese government, but these intrusions rarely make it into national news.

Yet these intrusions can do real damage to our nation—leading to theft of our intellectual property and personal information; and even more nefariously: establishing a foothold for disrupting or destroying the cyber and physical infrastructure that Americans rely upon every hour of every day—for our power, our water, our transportation, our communication, our healthcare, and so much more.

China's massive and sophisticated hacking program is larger than that of every other major nation – combined. This is hacking on an enormous scale, but unlike the spy balloon, which was identified and dealt with, these threats more often than not go unidentified and undeterred.

The Speech: https://www.cisa.gov/cisa-director-easterly-remarks-carnegie-mellon-university

Watch the Speech:
https://www.kaltura.com/index.php/extwidget/preview/partner_id/2612992/uiconf_id/49325582/entry_id/1_s80j6080/embed/dynamic

Number 5

Developing National Vulnerabilities Programmes

Based on the experiences and perspectives gathered from industry players and national governments, as well as on the documentation developed by multiple actors involved with national vulnerability initiatives and programmes, the EU Coordinated Vulnerability Disclosure (CVD) ecosystem remains fragmented.

Although interesting approaches and initiatives are taking place in some EU Member States, yet further steps can be done towards an integrated EU vision and action.

This report shows that, despite recent efforts by national governments in developing CVD policies, some industry players have taken the lead and developed vulnerability policies and programmes at organisation level.

Nevertheless, among the top industry expectations is that the development of a national or European level CVD policy could help organisations and public administrations to set vulnerability management as a priority and further encourage security practices.

In addition, the alignment of such policies with existing international standards, can greatly help in promoting harmonization.

As far as vulnerability initiatives are concerned, Bug Bounties Programmes (BBP) is an area that grew remarkably over the past few years.

BBPs have considerably adapted their business models in offering different type of services, hence different coverages of IT systems and levels of involvement in vulnerability management processes.

Today, BBPs platform providers are now cooperating with key public institutions to run customised programmes adapted to their needs and IT infrastructures.

Further expansion is expected as long as the community can continue relying on BBPs (i.e., confidentiality of internal information and data protection) and ensuring trust between the stakeholders involved. In terms of human capital, researchers play a fundamental role in the disclosure of vulnerabilities.

Accordingly, it is interesting to understand motivations, incentives and challenges influencing researchers' contribution.

From their perspective, reputation remains as a one of the key incentives to legally report vulnerabilities, as it leads to fame and recognition.

However, legal protection is also highly considered, especially because the absence, uncertainty or non-clarity of legal conditions can push to illegal channels.

Collaborative challenges arise in the use of tools to improve vulnerability disclosure processes.

For example, when looking into vulnerabilities related to open-source software (OSS) and considering how intertwined commercial and OSS are today, a need to further improve coordination between OSS developers and private vendors was identified.

Aspects such as OSS vulnerability handling, responsibility and accountability are not yet clearly defined and among actors involved across the IT product supply chains, which may hinder coordination efforts.

Challenges related to technical and technological issues also constitute a key area of discussion and analysis.

A forward-looking perspective on the use of automation as an enabler to efficiently manage vulnerability identification, sourcing and classification is also provided by this report.

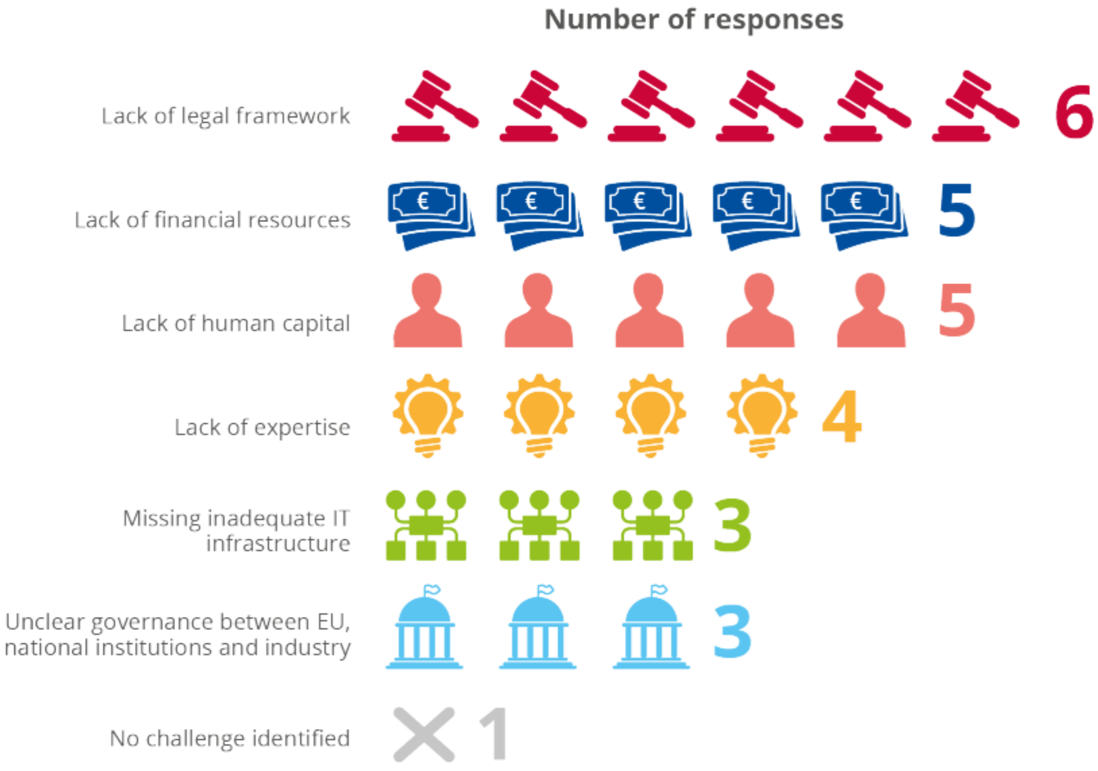
It is observed that, as vulnerability analysis and treatment still require human expertise, the risk of deskilling experts due to automated processes may be minimised.

Finally, alignment across different legislation as well as cooperation between industry players and governments are needed to avoid silos.

Harmonisation of CVD practices, coordination and international cooperation among players are essential priorities both from a legal and technical perspectives.

In this regard, ENISA will continue offering advice, publishing guidelines, promoting information sharing, raising awareness, and coordinating CVD-related activities at national and EU level.

Figure 3: Challenges encountered by stakeholders involved in coordinated vulnerability disclosure policy development and implementation



Source: Findings from interviews, Q3) What are the main challenges regarding the vulnerability policies' development and implementation? Interviewees (N=9).

To read more: https://www.enisa.europa.eu/publications/developing-national-vulnerabilities-programmes

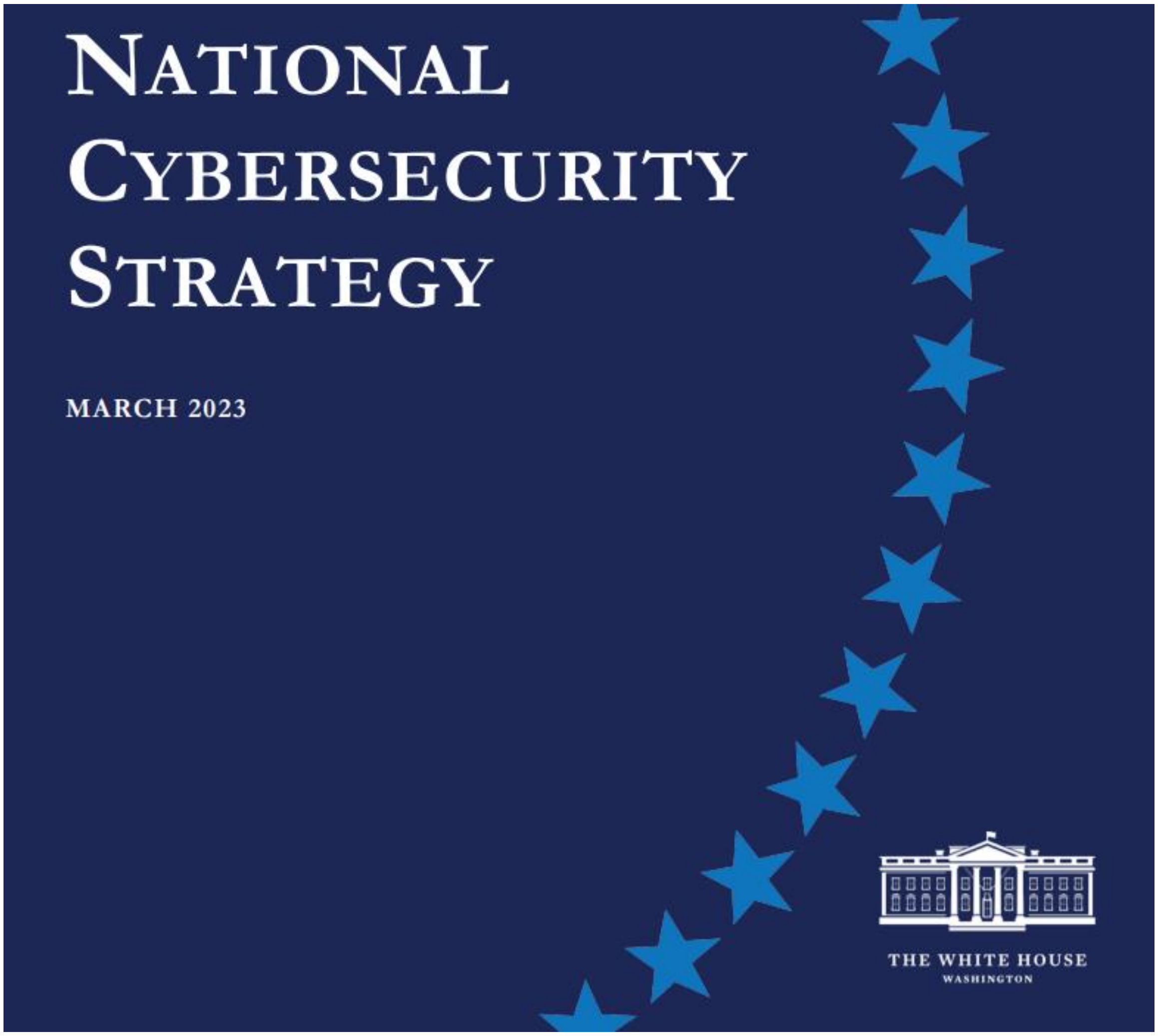
Number 6

The new US National Cybersecurity Strategy

THE WHITE HOUSE

The Biden-Harris Administration released the National Cybersecurity Strategy to secure the full benefits of a safe and secure digital ecosystem for all Americans.

In this decisive decade, the United States will reimagine cyberspace as a tool to achieve our goals in a way that reflects our values: economic security and prosperity; respect for human rights and fundamental freedoms; trust in our democracy and democratic institutions; and an equitable and diverse society. To realize this vision, we must make fundamental shifts in how the United States allocates roles, responsibilities, and resources in cyberspace.



NATIONAL CYBERSECURITY STRATEGY

MARCH 2023

THE WHITE HOUSE
WASHINGTON

1. We must rebalance the responsibility to defend cyberspace by shifting the burden for cybersecurity away from individuals, small businesses, and

local governments, and onto the organizations that are most capable and best-positioned to reduce risks for all of us.

2. We must realign incentives to favor long-term investments by striking a careful balance between defending ourselves against urgent threats today and simultaneously strategically planning for and investing in a resilient future.

The Strategy recognizes that government must use all tools of national power in a coordinated manner to protect our national security, public safety, and economic prosperity.

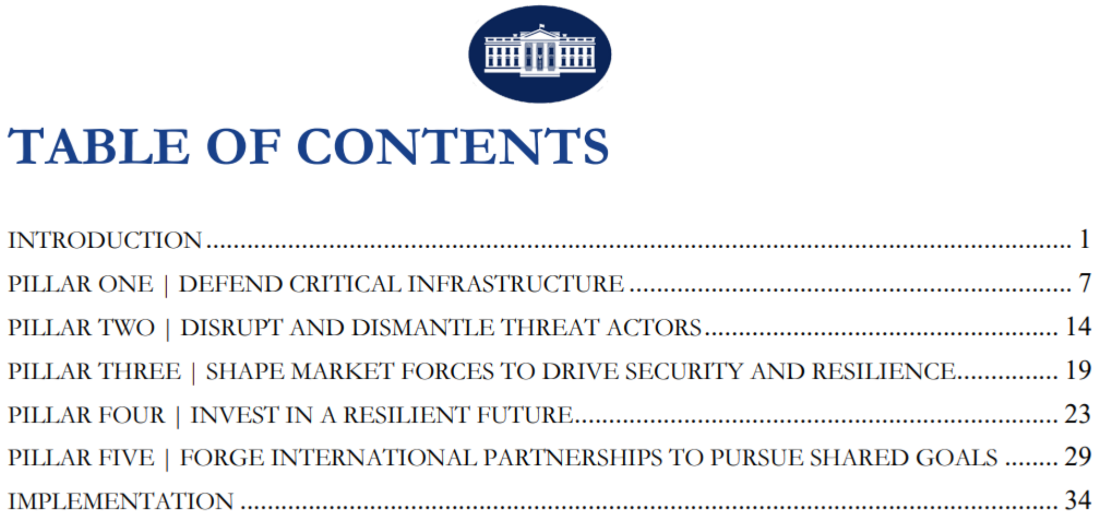


TABLE OF CONTENTS

VISION

Our rapidly evolving world demands a more intentional, more coordinated, and more well-resourced approach to cyber defense. We face a complex threat environment, with state and non-state actors developing and executing novel campaigns to threaten our interests. At the same time, next-generation technologies are reaching maturity at an accelerating pace, creating new pathways for innovation while increasing digital interdependencies.

This Strategy sets out a path to address these threats and secure the promise of our digital future. Its implementation will protect our investments in rebuilding America’s infrastructure, developing our clean energy sector, and re-shoring America’s technology and manufacturing base. Together with our allies and partners, the United States will make our digital ecosystem:

- **Defensible,** where cyber defense is overwhelmingly easier, cheaper, and more effective;

- **Resilient,** where cyber incidents and errors have little widespread or lasting impact; and,

- **Values-aligned,** where our most cherished values shape—and are in turn reinforced by— our digital world.

The Administration has already taken steps to secure cyberspace and our digital ecosystem, including the National Security Strategy, Executive Order 14028 (Improving the Nation's Cybersecurity), National Security Memorandum 5 (Improving Cybersecurity for Critical Infrastructure Control Systems), M-22-09 (Moving the U.S. Government Toward Zero-Trust Cybersecurity Principles), and National Security Memorandum 10 (Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems). Expanding on these efforts, the Strategy recognizes that cyberspace does not exist for its own end but as a tool to pursue our highest aspirations.

APPROACH

This Strategy seeks to build and enhance collaboration around five pillars:

1. **Defend Critical Infrastructure** – We will give the American people confidence in the availability and resilience of our critical infrastructure and the essential services it provides, including by:

- Expanding the use of minimum cybersecurity requirements in critical sectors to ensure national security and public safety and harmonizing regulations to reduce the burden of compliance;

- Enabling public-private collaboration at the speed and scale necessary to defend critical infrastructure and essential services; and,

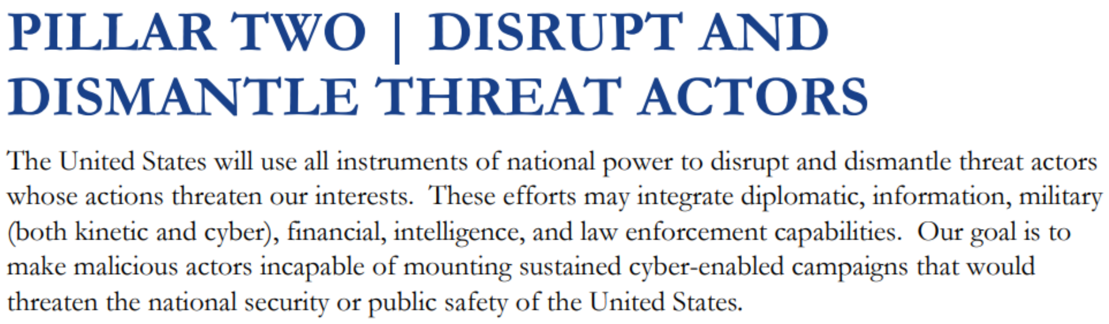
- Defending and modernizing Federal networks and updating Federal incident response policy

2. **Disrupt and Dismantle Threat Actors** – Using all instruments of national power, we will make malicious cyber actors incapable of threatening the national security or public safety of the United States, including by:

- Strategically employing all tools of national power to disrupt adversaries;

- Engaging the private sector in disruption activities through scalable mechanisms; and,

- Addressing the ransomware threat through a comprehensive Federal approach and in lockstep with our international partners.



PILLAR TWO | DISRUPT AND DISMANTLE THREAT ACTORS

The United States will use all instruments of national power to disrupt and dismantle threat actors whose actions threaten our interests. These efforts may integrate diplomatic, information, military (both kinetic and cyber), financial, intelligence, and law enforcement capabilities. Our goal is to make malicious actors incapable of mounting sustained cyber-enabled campaigns that would threaten the national security or public safety of the United States.

3. **Shape Market Forces to Drive Security and Resilience** – We will place responsibility on those within our digital ecosystem that are best positioned to reduce risk and shift the consequences of poor cybersecurity away from the most vulnerable in order to make our digital ecosystem more trustworthy, including by:

- Promoting privacy and the security of personal data;

- Shifting liability for software products and services to promote secure development practices; and,

- Ensuring that Federal grant programs promote investments in new infrastructure that are secure and resilient.

4. **Invest in a Resilient Future** – Through strategic investments and coordinated, collaborative action, the United States will continue to lead the world in the innovation of secure and resilient next-generation technologies and infrastructure, including by:

- Reducing systemic technical vulnerabilities in the foundation of the Internet and across the digital ecosystem while making it more resilient against transnational digital repression;

- Prioritizing cybersecurity R&D for next-generation technologies such as postquantum encryption, digital identity solutions, and clean energy infrastructure; and,

- Developing a diverse and robust national cyber workforce

5. **Forge International Partnerships to Pursue Shared Goals** – The United States seeks a world where responsible state behavior in cyberspace is expected and reinforced and where irresponsible behavior is isolating and costly, including by:

- Leveraging international coalitions and partnerships among like-minded nations to counter threats to our digital ecosystem through joint preparedness, response, and cost imposition;

- Increasing the capacity of our partners to defend themselves against cyber threats, both in peacetime and in crisis; and,

- Working with our allies and partners to make secure, reliable, and trustworthy global supply chains for information and communications technology and operational technology products and services.

Coordinated by the Office of the National Cyber Director, the Administration's implementation of this Strategy is already underway.

To read more: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Number 7

Social Media Manipulation 2022/2023:

Assessing the Ability of Social Media Companies to Combat Platform Manipulation

NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE

In this report—the fourth version of our social media manipulation experiment—we show that social media companies remain unable to prevent commercial manipulators from undermining platform integrity.

Overall, no platform has improved compared to 2021 and, taken together, their ability to prevent manipulation has decreased.

Buying manipulation remains cheap. The percentage of accounts identified and removed by the platforms dropped. We demonstrate that the manipulation providers have circumvented sanctions imposed in response to Russia's full-scale invasion of Ukraine.

It remains easy to pay for manipulation services with both Visa and Apple Pay. The platforms' ability to combat manipulation by slowing the speed of delivery has declined.

Today, 89 per cent of purchased inauthentic behaviour is delivered within one day. The vast majority of the inauthentic engagement remained active across all social media platforms four weeks after purchasing.

Thus, the platforms' moderation decisions appear to be only minimally responsive to user notifications.

Social media manipulation services hence continue to outperform social media platforms. With the quality of transparency reporting unchanged, the gap between platform performance in countering inauthentic engagement and the quality of platform reporting is widening.

Platforms have found it expedient to focus less on preventing commercial manipulators from accessing the platform, and more on reducing the reach and impact of their posts.

However, our research shows that commercial accounts are exploiting flaws in platforms, and pose a structural threat to the integrity of platforms.

More data is required to assess whether the platforms' approach adequately mitigates the systemic risk posed by platform manipulators.

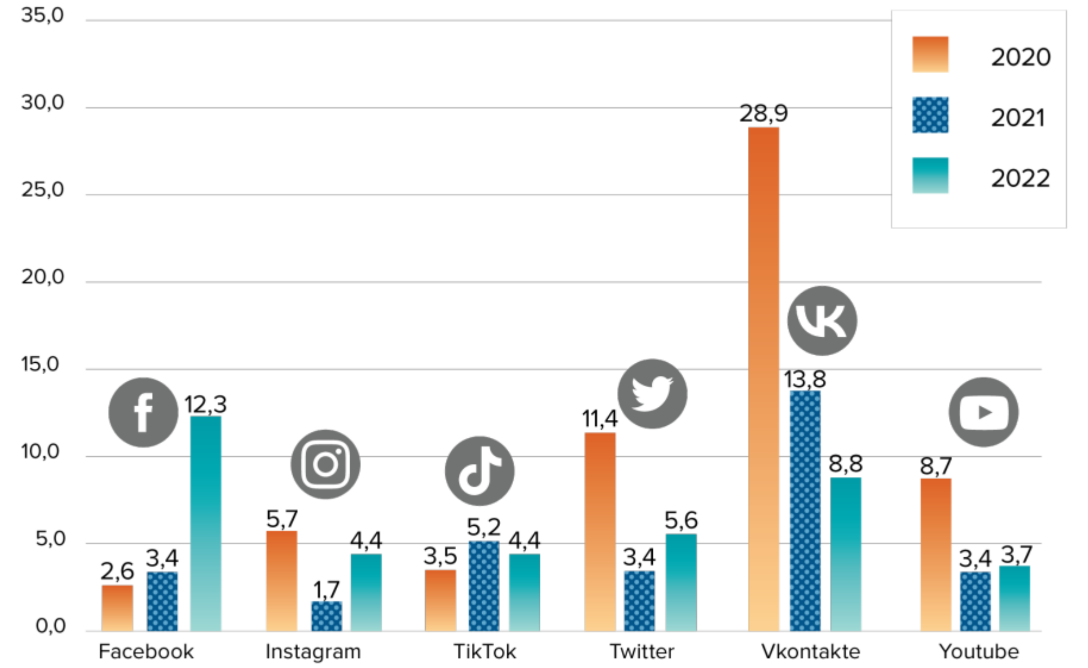


Figure 1: Cost (euro cents) of purchasing fake accounts by platform over time

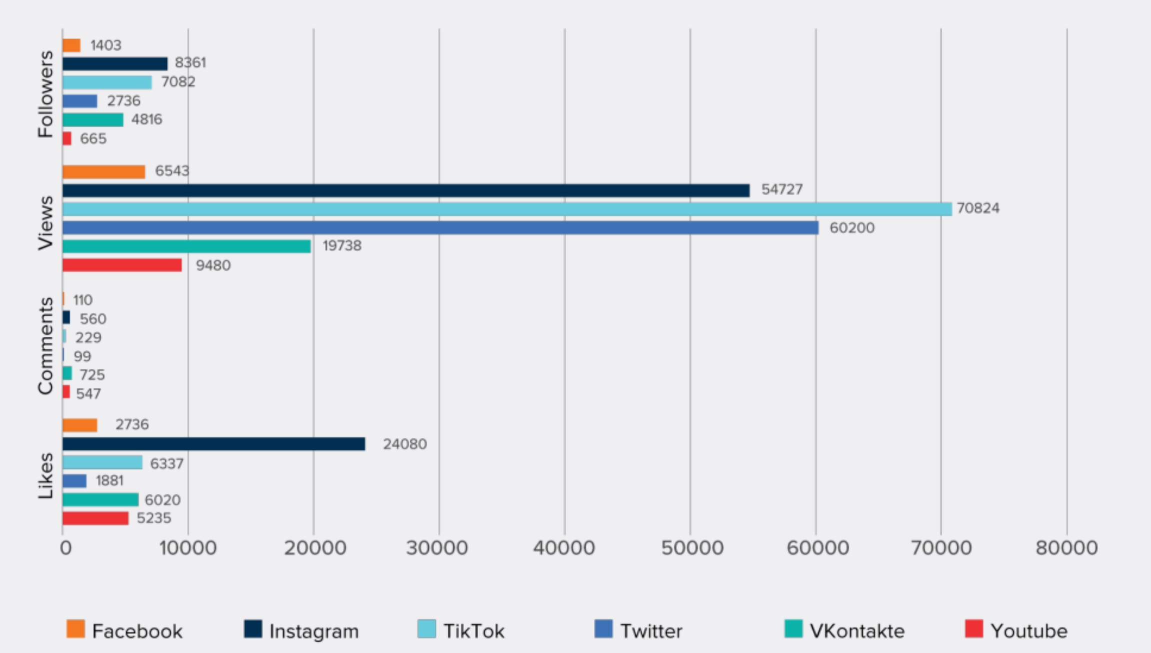


Figure 4. The amount of manipulation that can be bought for €10

To read more: https://stratcomcoe.org/publications/social-media-manipulation-20222023-assessing-the-ability-of-social-media-companies-to-combat-platform-manipulation/272

Number 8

Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA)

#StopRansomware: Royal Ransomware

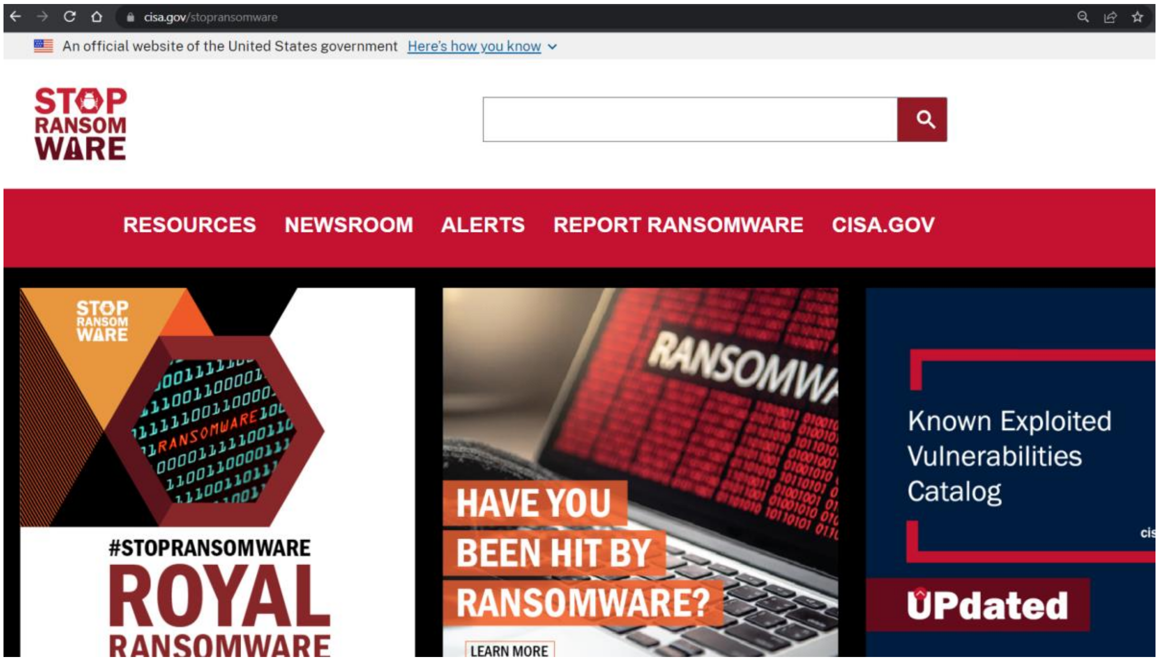
JOINT CYBERSECURITY ADVISORY

Coauthored by:

This joint Cybersecurity Advisory (CSA) is part of an ongoing effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors.

These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware.

Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.



cisa.gov/stopransomware

An official website of the United States government Here's how you know

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint CSA to disseminate known Royal ransomware IOCs and TTPs identified through FBI threat response activities as recently as January 2023.

Since approximately September 2022, cyber criminals have compromised U.S. and international organizations with a Royal ransomware variant.

FBI and CISA believe this variant, which uses its own custom-made file encryption program, evolved from earlier iterations that used "Zeon" as a loader.

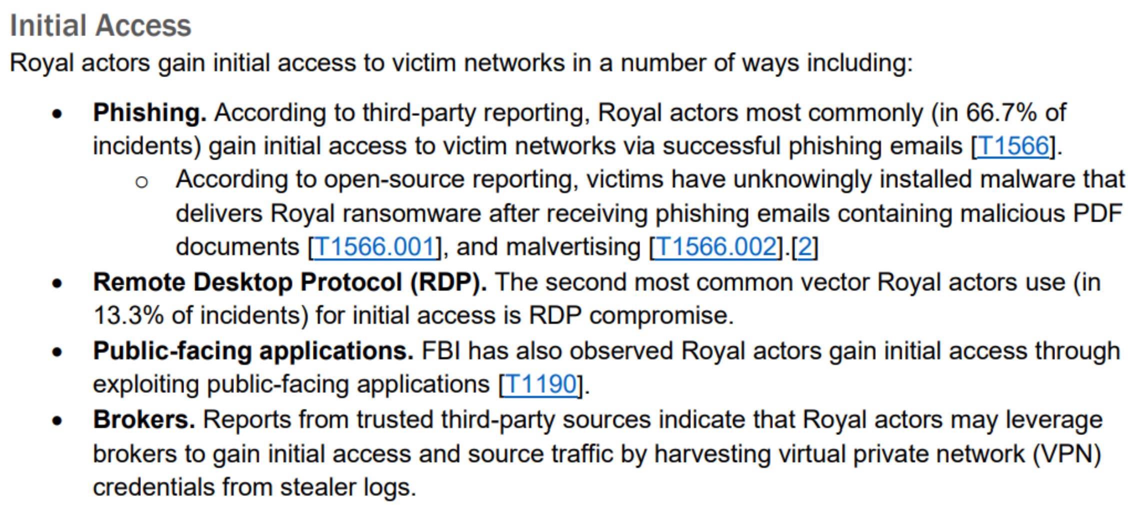
After gaining access to victims' networks, Royal actors disable antivirus software and exfiltrate large amounts of data before ultimately deploying the ransomware and encrypting the systems.

Royal actors have made ransom demands ranging from approximately $1 million to $11 million USD in Bitcoin.

In observed incidents, Royal actors do not include ransom amounts and payment instructions as part of the initial ransom note.

Instead, the note, which appears after encryption, requires victims to directly interact with the threat actor via a .onion URL (reachable through the Tor browser).

Royal actors have targeted numerous critical infrastructure sectors including, but not limited to, Manufacturing, Communications, Healthcare and Public Healthcare (HPH), and Education.



Initial Access

Royal actors gain initial access to victim networks in a number of ways including:

- **Phishing.** According to third-party reporting, Royal actors most commonly (in 66.7% of incidents) gain initial access to victim networks via successful phishing emails [T1566].
  - According to open-source reporting, victims have unknowingly installed malware that delivers Royal ransomware after receiving phishing emails containing malicious PDF documents [T1566.001], and malvertising [T1566.002].[2]
- **Remote Desktop Protocol (RDP).** The second most common vector Royal actors use (in 13.3% of incidents) for initial access is RDP compromise.
- **Public-facing applications.** FBI has also observed Royal actors gain initial access through exploiting public-facing applications [T1190].
- **Brokers.** Reports from trusted third-party sources indicate that Royal actors may leverage brokers to gain initial access and source traffic by harvesting virtual private network (VPN) credentials from stealer logs.

To read more: https://www.cisa.gov/sites/default/files/2023-03/aa23-061a-stopransomware-royal-ransomware.pdf

Number 9

The quick and the dead - building up cyber resilience in the financial sector

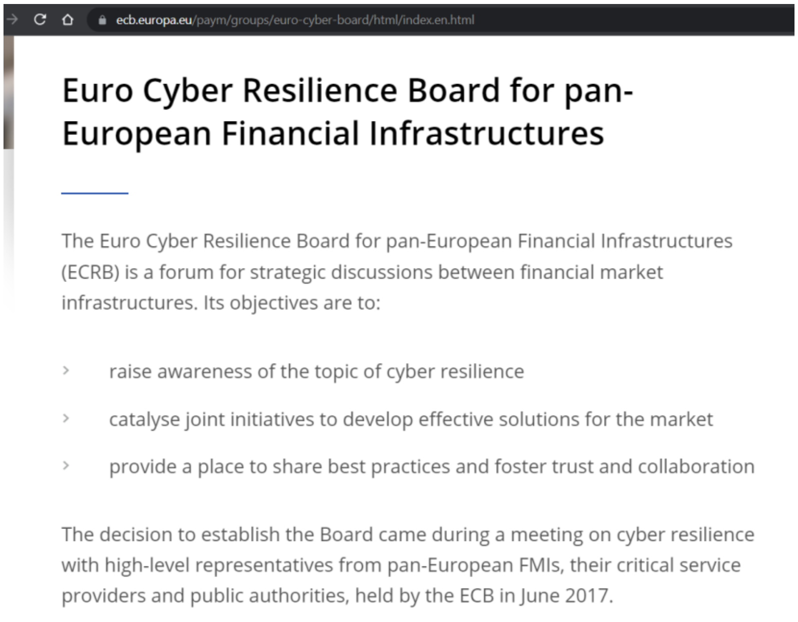
Fabio Panetta, Member of the Executive Board of the European Central Bank, at the meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures, Frankfurt am Main.

The proliferation of cyber threat actors combined with an increase in remote working and greater digital interconnectedness is raising the risk, frequency and severity of cyberattacks.

Increasingly, cyber criminals are launching ransomware attacks and demanding payment in crypto. Cyberattacks related to geopolitical developments – Russia's aggression against Ukraine in particular – have also become a more common feature of the cyber-threat landscape.

The Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB) has played a key role in protecting the security and integrity of the financial system from these threats.

Our note: You may visit: https://www.ecb.europa.eu/paym/groups/euro-cyber-board/shared/pdf/ECRB_mandate.pdf


ecb.europa.eu/paym/groups/euro-cyber-board/html/index.en.html

Euro Cyber Resilience Board for pan-European Financial Infrastructures

The Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB) is a forum for strategic discussions between financial market infrastructures. Its objectives are to:

- raise awareness of the topic of cyber resilience
- catalyse joint initiatives to develop effective solutions for the market
- provide a place to share best practices and foster trust and collaboration

The decision to establish the Board came during a meeting on cyber resilience with high-level representatives from pan-European FMIs, their critical service providers and public authorities, held by the ECB in June 2017.

The last three years have shown that we can work under adverse conditions towards a common goal. Our financial infrastructures have proven their resilience to cyber threats. But this does not mean we can become complacent or any less vigilant in the face of cyber threats. We simply cannot afford to fall behind the curve: cybersecurity must be the backbone of digital finance.

Today I will take stock of the ECRB's work. I will then discuss current cyber threats and emerging risks before outlining the implications for our work in the future.

The contribution of the Euro Cyber Resilience Board

The ECRB brings together private and public stakeholders across pan-European financial infrastructures, critical service providers, central banks and other authorities.

This offers a unique prism through which the ECRB can identify and fix any weaknesses which cyberattacks could potentially exploit in order to propagate, which in turn would cause systemic ripples throughout the European financial ecosystem.

Let me give three examples of why the ECRB is such a useful forum for cooperation.

First, in the area of information sharing, the ECRB's Cyber Information and Intelligence Sharing Initiative (CIISI-EU) allows members to exchange information about cyber threats and mitigation in a secure and trusted group environment.

Second, the ECRB has established a crisis coordination protocol that facilitates cooperation and coordination, allowing members to exchange and respond to major cyber threats and incidents.

Third, in the area of training and awareness, the ECRB conducts joint assessments and training sessions to increase common knowledge and understanding.

A key pillar of the ECB's cyber strategy for financial infrastructures is the TIBER-EU framework for threat-led penetration testing, also known as red teaming. In June 2022 the ECRB organised a dedicated roundtable on TIBER-EU where members shared their experience of these kinds of exercises.

In view of their systemic role in the financial system, we will continue to focus on pan-European financial infrastructures. Nonetheless, financial infrastructures are increasingly interdependent through horizontal and vertical links and common participants.

They are also reliant on information and communication technology and on third-party service providers. As a result, these infrastructures are exposed to common risks and vulnerabilities through which cyberattacks could propagate swiftly if they are not rigorously managed. The ECRB allows us to join forces to address these risks on a sector-wide level.

Adapting to a constantly changing cyber threat landscape

Let me now turn to the cyber threat landscape.

Threats are becoming increasingly complex. Recent attacks call for constant vigilance at an operational level, and the continuous reassessment of regulatory and oversight frameworks to see whether they need to be updated. Significant but unpredictable shifts can occur at any time. We must therefore be prepared to understand them and to adapt quickly in order to mitigate the financial ecosystem's susceptibility to cyberattacks.

The ECRB has identified supply chain attacks and ransomware as key threats in the current environment, and artificial intelligence (AI) as an emerging threat. We have also witnessed how geopolitical developments, most recently Russia's aggression against Ukraine, have weaponised cyberspace. The most prominent examples are distributed denial-of-service (DDoS) attacks against government and financial entities.

Let me discuss the key current and emerging threats in more detail.

Supply chain attacks

The financial ecosystem's reliance on third-party products and services is a key risk, especially when financial entities outsource critical functions to them. An attack on these third parties or on their products and services can disrupt and harm the financial infrastructures that rely on them, with spillovers to interconnected entities.

When such third-party products and services are widely used in the financial ecosystem, a cyberattack can have widespread, possibly systemic effects by having an impact on multiple financial entities at once. That is why cyber threat actors target these third parties. In so doing, they can compromise numerous financial entities simultaneously.

The recent cyberattack on the third-party provider ION Cleared Derivatives shows how an attack on one software provider may cascade onto their clients. In this specific case, the disruptions to the trading and clearing of financial derivatives remained limited, but we cannot ignore scenarios where the attacks could have propagated quickly, disrupting the financial system.

This case signalled the need for financial entities to review their third-party providers, the providers of these third-parties, their cyber resilience levels and the systemic impact that may ensue from a cyberattack on any of these providers.

In particular, it is vital to assess critical service dependencies on third-party products and services which could be disrupted or even terminated as a result of a cyberattack. Mitigating measures need to be put in place.

Against this background, the G7 recently updated its Fundamental Elements for Third-Party Cyber Risk Management in the Financial Sector. In addition, the ECRB set up a working group in 2022 to support third-party cyber risk management.

We must have a cyber resilience mindset at all times. The question we must ask is not if a cyberattack will happen, but whether we are ready to respond when it happens.

Over the past year, the ECRB has worked on a conceptual model for how the financial infrastructure ecosystem could manage such a crisis if it occurred. It has also developed protocols and networks aimed at supporting a collective, consistent and comprehensive response to a cyber crisis by stakeholders.

Ransomware

The proliferation of ransomware is one of the most significant challenges currently facing financial entities. Not only may ransomware attacks result in financial loss, they may also severely disrupt operations.

Even after a ransom is paid, there is no guarantee the decryption key will actually work or that the stolen data will not be publicly disclosed or further misused to extort victims' customers, for example.

Ransomware attacks are growing more sophisticated and damaging, which in turn may enable ransomware threat actors to obtain even more resources. 2022 was one of the most active years for ransomware activity.

However, it was also the first year that the majority of victims of ransomware attacks decided not to pay up, which indicates that the approach towards ransomware attacks is changing.

Authorities globally are stepping up their efforts to counter ransomware. For instance, the G7 issued Fundamental Principles on Ransomware Resilience in October 2022.

We need to tackle ransomware attacks from various angles.

First, every firm must be ready to repel ransomware attacks, either through the use of proper cyber hygiene practices or by ensuring that data is backed up regularly and is kept up-to-date and tamper-proof.

Second, enforcement agencies need to conduct forensic analyses, locate attackers and join forces to prosecute them.

Third, crypto-assets – especially unbacked crypto-assets, which are used to make ransomware payments owing to the anonymity and money laundering possibilities they offer – need to be strictly regulated. Similarly, crypto-asset transfers must be traceable.

The proposed EU Regulation for Markets in Crypto-Assets (MiCA) and revision to the Regulation on information accompanying transfers of funds, which extends the "travel rule" to crypto-assets, are important steps. However, to be effective and prevent regulatory arbitrage, regulation must be stepped up globally.

Implementation of the Financial Action Task Force (FATF) guidance for crypto-assets and its enforcement at international level are therefore crucial.

In addition, all firms need to have the highest level of cyber controls in place to prevent attacks from being successful and to detect and recover from ransomware attacks.

Moreover, insurance firms can lend their support by obtaining assurances from their clients that they have high-level cyber resilience plans in place before providing cyber risk insurance policies, thus ensuring that these very same policies do not lower firms' incentives to prepare for cyberattacks.

Artificial Intelligence (AI)

Even if we do not realise it, the use of artificial intelligence (AI) is already widespread. We use AI every day, including on our phones, in our homes and at the workplace. And firms use it to harness big data.

AI can help to strengthen cybersecurity, for instance, by improving the detection of highly sophisticated cyberattacks through its ability to identify abnormal system behaviour compared with an established baseline. This is the kind of potential that we need to leverage.

But AI can also multiply cyber risks by, for instance, helping malicious individuals, even those who have limited or no technical skills, draft very convincing phishing emails or identify topics that will achieve the maximum engagement from those being targeted.

To make matters worse, AI can even create and fix code that can be used to exploit and compromise the endpoint.

This opens up new possibilities for malicious individuals to use AI to launch cyberattacks. Although AI development firms try to install safeguards to prevent its unethical use, they can be circumvented.

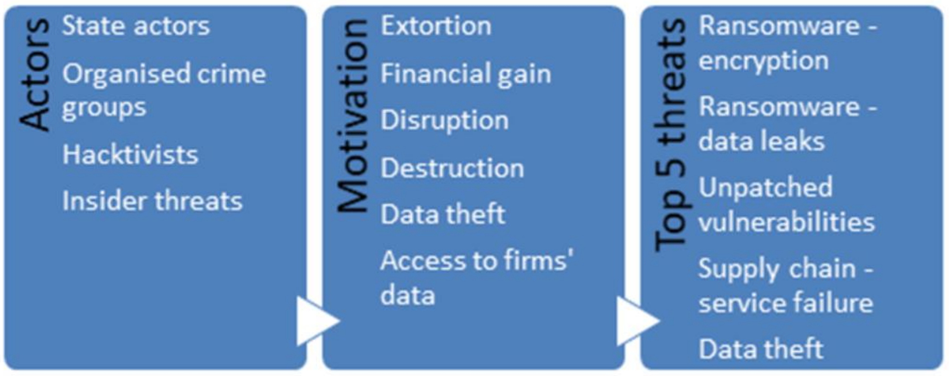
The risks from AI need to be clearly understood and addressed through regulation and oversight.

By exchanging information among its members and organising roundtables and training, the ECRB is in a strong position to raise awareness of risks at an early stage and accumulate knowledge of these types of threats.

For its part, the European Commission has proposed a Regulation on artificial intelligence that aims to address some of the key risks associated with AI.

Chart 1

Cyber threat landscape for financial market infrastructures in Europe



Actors

State actors

Organised crime groups

Hacktivists

Insider threats

Motivation

Extortion

Financial gain

Disruption

Destruction

Data theft

Access to firms' data

Top 5 threats

Ransomware - encryption

Ransomware - data leaks

Unpatched vulnerabilities

Supply chain - service failure

Data theft

Note: Threats are arranged in descending order of estimated severity.

To read more:
https://www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230308~92211cd1f5.en.html

Number 10

NIST Internal Report, NIST IR 8432 ipd, 4 Initial Public Draft

Cybersecurity of Genomic Data

Genomic data has enabled the rapid growth of the U.S. bioeconomy and is valuable to the individual, industry, and government due to intrinsic properties that, in combination, make it different from other types of high-value data which possess only a subset of these properties.

The characteristics of genomic data compared to other high value datasets raises some correspondingly unique cybersecurity and privacy challenges that are inadequately addressed with current policies, guidance, and technical controls.

This report describes current practices in risk management, cybersecurity, and privacy management for protecting genomic data, as well as the associated challenges and concerns.

It identifies gaps in protection practices across the genomic data lifecycle and proposes solutions to address real-life use cases occurring at various stages of the genomic data lifecycle.

This report also is intended to provide areas for regulatory/policy enactment or further research.

Cybersecurity and Privacy Concerns

Cyber attacks targeted at genomic data include attacks against the confidentiality of the data, its integrity, and its availability.

Cyber attacks against the confidentiality of the data can threaten our economy through theft of the intellectual property owned by the U.S. biotechnology industry, allowing competitors to gain an unfair economic advantage by accessing U.S. held genomic data.

Attacks against the integrity of the data can disrupt biopharmaceutical output, agricultural food production, and bio-manufacturing activity.

Attacks against the availability of the data include encrypting for ransom, deletion of data, and disabling critical automated equipment used in research, development, and manufacturing.

The potential harms of cyber attacks on genomic data threaten our national security as well, including enabling the development of biological weapons and the surveillance, oppression, and extortion of our citizens, military, and intelligence personnel based on their genomic data.

Cyber attacks targeted at genomic data can also harm individuals by enabling blackmail, discrimination based on disease risk, and privacy loss from the revealing of hidden consanguinity or phenotypes including health, emotional stability, mental capacity, appearance, and physical abilities.

In addition to the privacy risks that can arise because of a cyber attack, privacy risks unrelated to cybersecurity can arise when processing genomic data. These risks can arise when there is insufficient predictability, manageability, and disassociability in the genomic data processing.

Insufficient predictability in data processing can result in privacy problems if individuals are surprised by what is happening with their genomic data.

Insufficient manageability in data processing can arise when the capabilities are not in place to allow for appropriately granular administration of genomic data, for example, individuals may need to be able to have some or all their genomic data deleted from a dataset.

Permitting access to raw genomic data, instead of using appropriate privacy-enhancing technologies to extract only the necessary insights (without revealing the raw data), introduces privacy risks from insufficient disassociability in data processing.

Each of these areas of privacy risks can disrupt the ability to realize the benefits of processing genomic data.

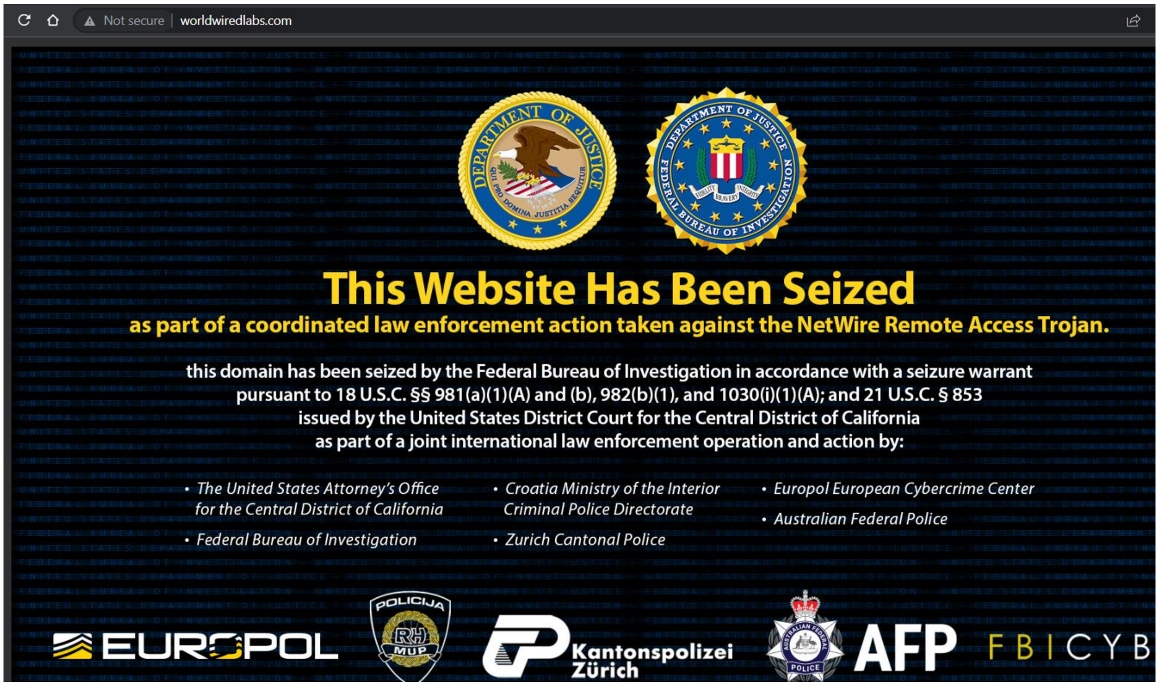
To read more:
https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8432.ipd.pdf

Number 11

US Federal Authorities Seize Internet Domain Selling Malware Used to Illegally Control and Steal Data from Victims’ Computers

United States
Attorney’s Office
Central District of California

As part of an international law enforcement effort, federal authorities in Los Angeles this week seized an internet domain that was used to sell computer malware used by cybercriminals to take control of infected computers and steal a wide array of information.



This Website Has Been Seized

as part of a coordinated law enforcement action taken against the NetWire Remote Access Trojan.

this domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (b), 982(b)(1), and 1030(i)(1)(A); and 21 U.S.C. § 853 issued by the United States District Court for the Central District of California as part of a joint international law enforcement operation and action by:

- *The United States Attorney’s Office for the Central District of California*
- *Federal Bureau of Investigation*
- *Croatia Ministry of the Interior Criminal Police Directorate*
- *Zurich Cantonal Police*
- *Europol European Cybercrime Center*
- *Australian Federal Police*

A seizure warrant approved by a United States Magistrate Judge on March 3 and executed on Tuesday led to the seizure of www.worldwiredlabs.com, which offered the NetWire remote access trojan (RAT), a sophisticated program capable of targeting and infecting every major computer operating system.

“A RAT is a type of malware that allows for covert surveillance, allowing a ‘backdoor’ for administrative control and unfettered and unauthorized remote access to a victim’s computer, without the victim’s knowledge or permission,” according to court documents filed in Los Angeles.

As part of this week’s law enforcement action, authorities in Croatia on Tuesday arrested a Croatian national who allegedly was the administrator of the website.

This defendant will be prosecuted by Croatian authorities. Additionally, law enforcement in Switzerland on Tuesday seized the computer server hosting the NetWire RAT infrastructure.

The FBI in Los Angeles in 2020 opened an investigation into worldwidelabs, the only known online distributor of NetWire.

Undercover investigators with the FBI created an account on the website, paid for a subscription plan, and "constructed a customized instance of the NetWire RAT using the product's Builder Tool," according to the affidavit in support of the seizure warrant.

While the website marketed NetWire as a legitimate business tool to maintain computer infrastructure, the affidavit states that NetWire is a malware used for malicious purposes, the software was advertised on hacking forums, and numerous cyber security companies and government agencies have documented instances of the NetWire RAT being used in criminal activity.

"Today's action is a testament to the innovation and flexibility necessary to fighting cybercriminals who operate without borders," said United States Attorney Martin Estrada.

"Our office will continue to forge international alliances to protect our communities from cyber threats. Criminals used NetWire on a global scale, and we have responded by dismantling the infrastructure that has caused untold harm to victims around the world."

"By removing the Netwire RAT, the FBI has impacted the criminal cyber ecosystem," said Donald Alway, the Assistant Director in Charge of the FBI's Los Angeles Field Office.

"The global partnership that led to the arrest in Croatia also removed a popular tool used to hijack computers in order to perpetuate global fraud, data breaches and network intrusions by threat groups and cyber criminals."

This matter is the result of the United States' strong law enforcement cooperation with Croatia and other global partners. The FBI's Los Angeles Field Office; the Croatia Ministry of the Interior, Criminal Police Directorate; Zurich Cantonal Police in Switzerland; the Europol European Cybercrime Center; and the Australian Federal Police conducted the investigation in this matter.

Assistant United States Attorneys Lisa Feldman of the Cyber and Intellectual Property Crimes Section and Maxwell Coll of the Asset

Forfeiture and Recovery Section obtained the seizure warrant for the internet domain.

The Office of International Affairs in the Justice Department's Criminal Division provided substantial assistance during the investigation.

To read more: https://www.justice.gov/usao-cdca/pr/federal-authorities-seize-internet-domain-selling-malware-used-illegally-control-and

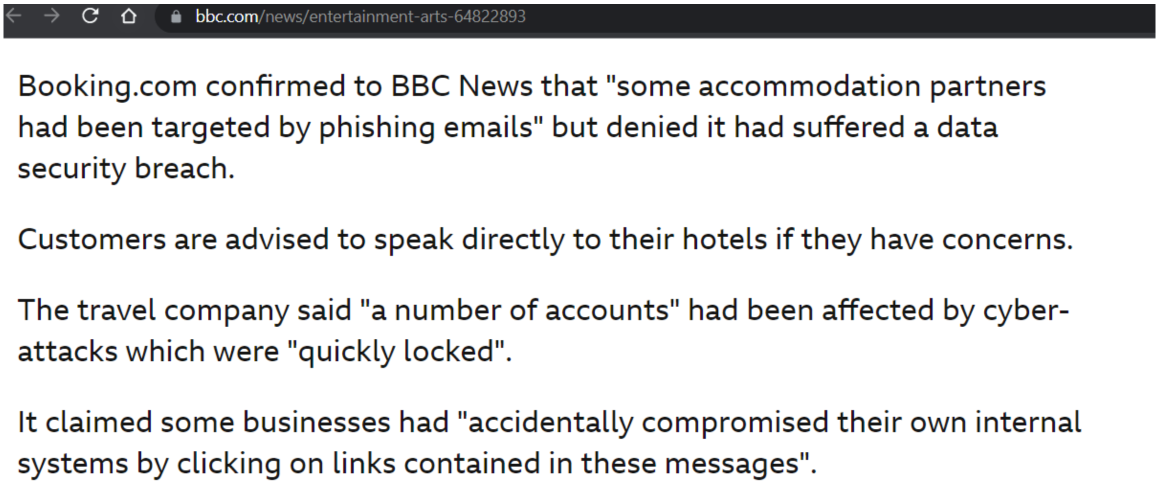
Number 12

Cyber criminals use Eurovision as the latest phishing lure

National Cyber Security Centre

Cyber criminals are targeting hotels hosting people travelling to Liverpool for the Eurovision song contest event in May.

The online travel agent booking.com has confirmed to the BBC they have seen evidence of “some accommodation partners being targeted by phishing emails.”



Booking.com confirmed to BBC News that "some accommodation partners had been targeted by phishing emails" but denied it had suffered a data security breach.

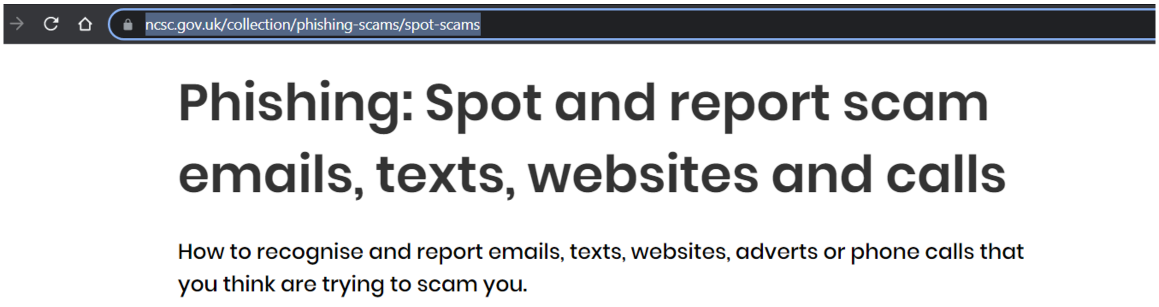
Customers are advised to speak directly to their hotels if they have concerns.

The travel company said "a number of accounts" had been affected by cyber-attacks which were "quickly locked".

It claimed some businesses had "accidentally compromised their own internal systems by clicking on links contained in these messages".

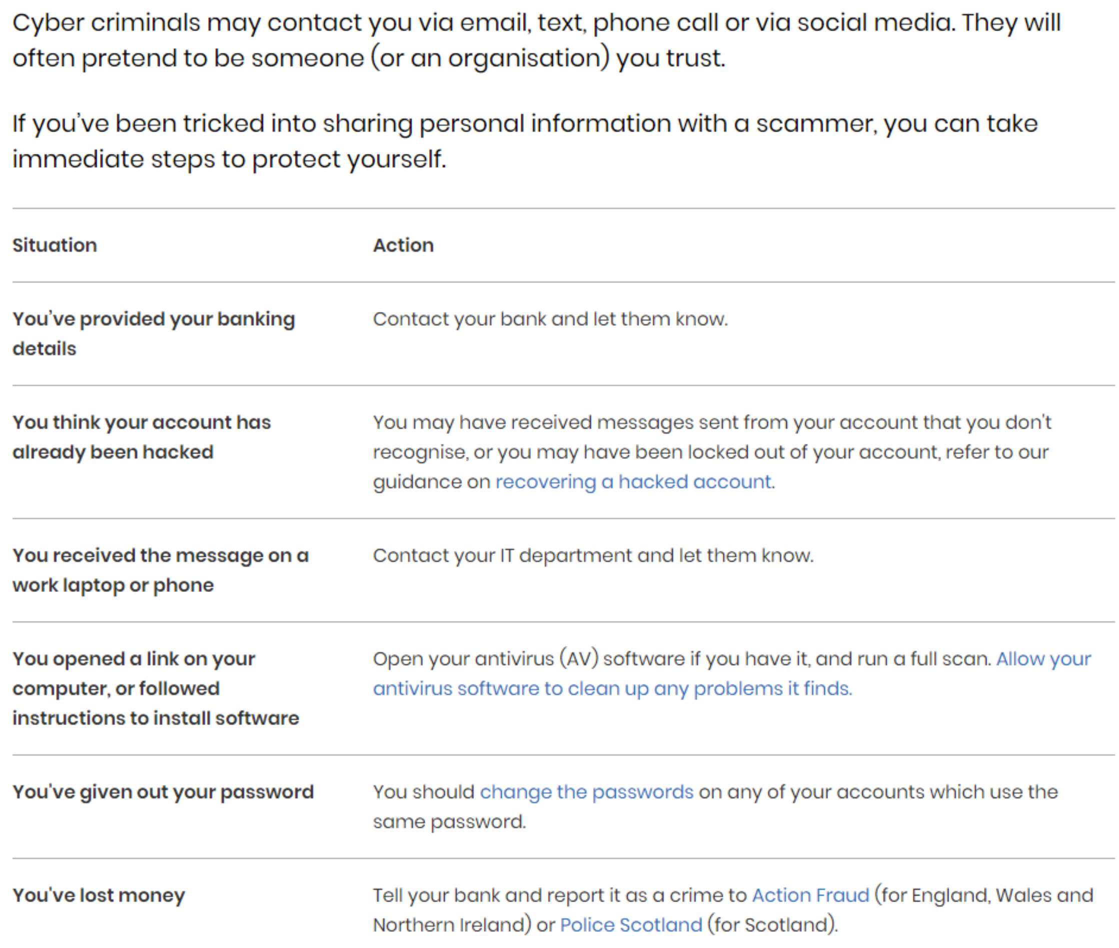
Cyber criminals often take advantage of news and topical events to scam customers.

There are some good ways you can prepare yourself and spot potential scams on the NCSC website, as well as guidance on what to do next if you are a victim of phishing. You may visit: https://www.ncsc.gov.uk/collection/phishing-scams/spot-scams



Phishing: Spot and report scam emails, texts, websites and calls

How to recognise and report emails, texts, websites, adverts or phone calls that you think are trying to scam you.



Cyber criminals may contact you via email, text, phone call or via social media. They will often pretend to be someone (or an organisation) you trust.

If you've been tricked into sharing personal information with a scammer, you can take immediate steps to protect yourself.

Situation	Action
You've provided your banking details	Contact your bank and let them know.
You think your account has already been hacked	You may have received messages sent from your account that you don't recognise, or you may have been locked out of your account, refer to our guidance on recovering a hacked account.
You received the message on a work laptop or phone	Contact your IT department and let them know.
You opened a link on your computer, or followed instructions to install software	Open your antivirus (AV) software if you have it, and run a full scan. Allow your antivirus software to clean up any problems it finds.
You've given out your password	You should change the passwords on any of your accounts which use the same password.
You've lost money	Tell your bank and report it as a crime to Action Fraud (for England, Wales and Northern Ireland) or Police Scotland (for Scotland).

To read more: https://www.ncsc.gov.uk/report/threat-report-10th-march-2023

Number 13

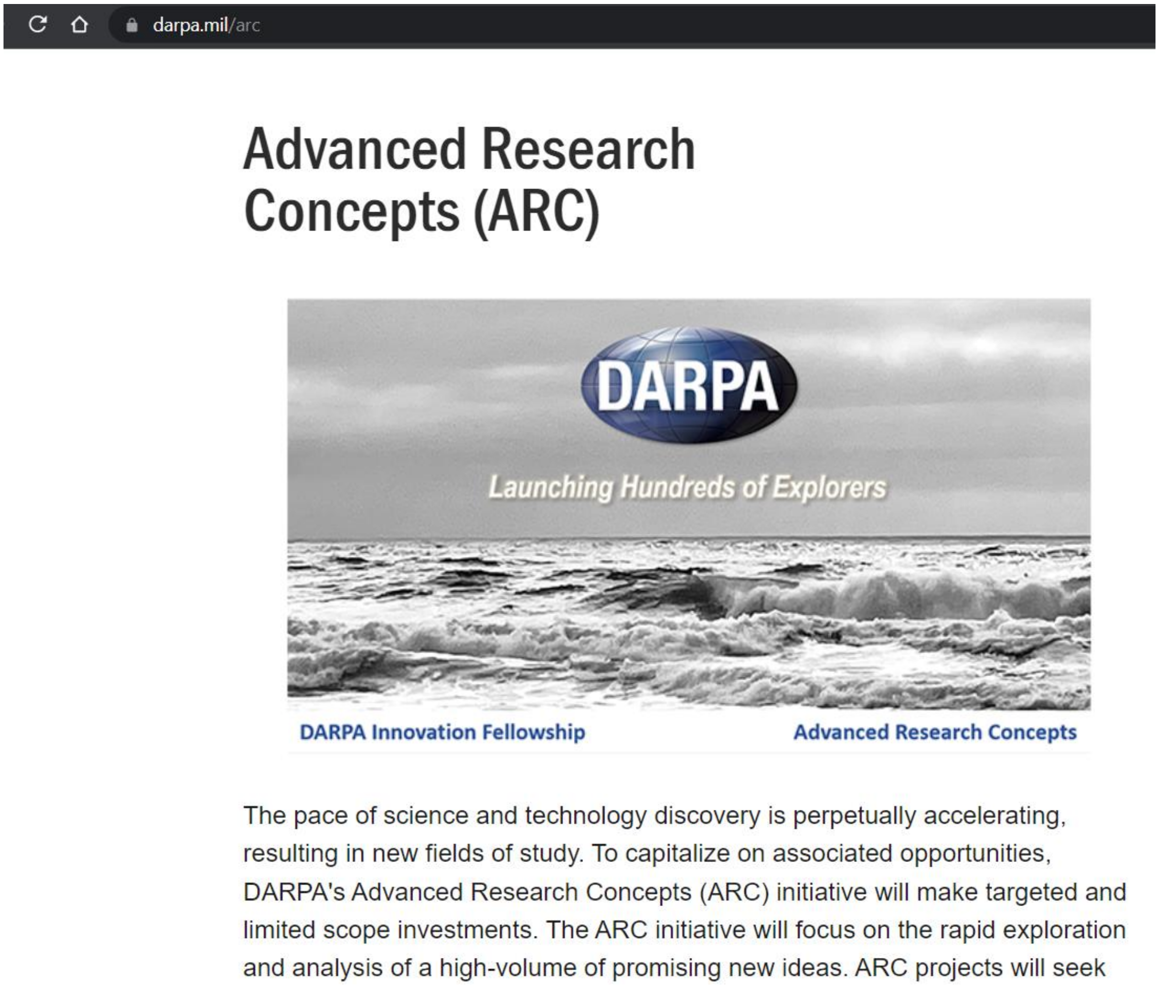
DARPA Seeks Input to Advance Hybrid Quantum/Classical Computers

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Although fault-tolerant quantum computers are projected to be years to decades away, processors made from tens to hundreds of quantum bits have made significant progress in recent years, especially when working in tandem with a classical computer.

These hybrid quantum/classical systems could enable technical disruption soon by superseding the best classical-only supercomputers in solving difficult optimization challenges and related problems of interest to defense, security, and industry.

DARPA is sponsoring a live webinar on Tuesday, April 11, 2023, to highlight an Advanced Research Concept (ARC) topic called Imagining Practical Applications for a Quantum Tomorrow (IMPAQT).



Advanced Research Concepts (ARC)

DARPA Innovation Fellowship

Advanced Research Concepts

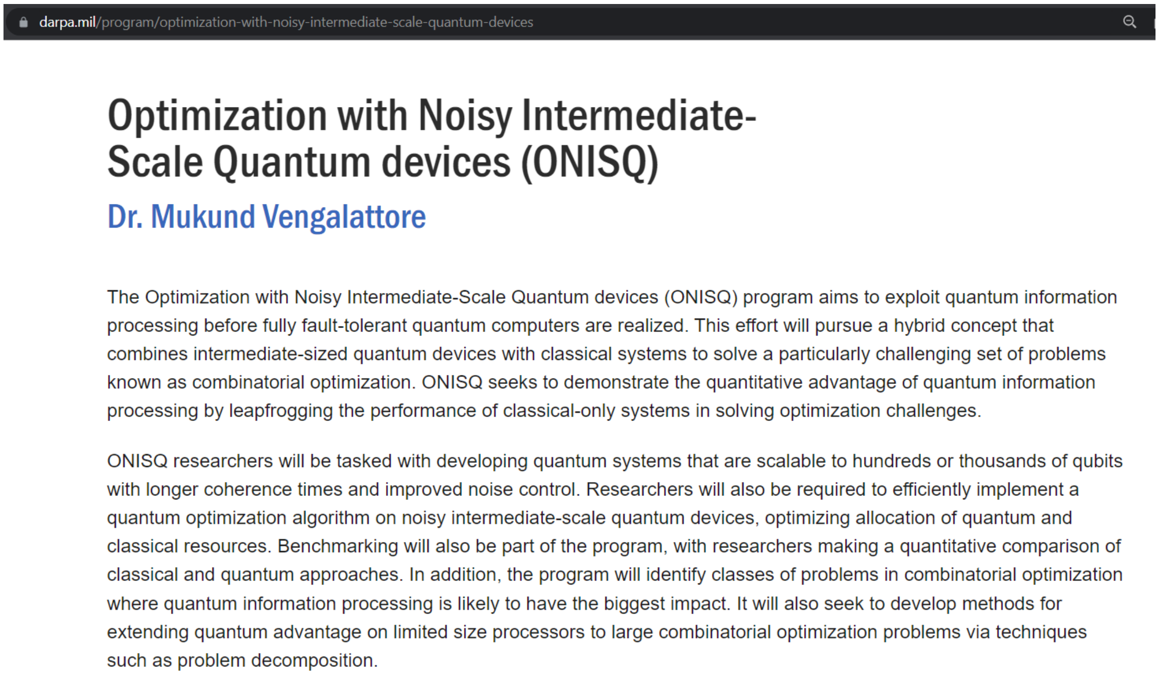
The pace of science and technology discovery is perpetually accelerating, resulting in new fields of study. To capitalize on associated opportunities, DARPA's Advanced Research Concepts (ARC) initiative will make targeted and limited scope investments. The ARC initiative will focus on the rapid exploration and analysis of a high-volume of promising new ideas. ARC projects will seek

Registrants will have the opportunity to hear from government experts, university professors, and industry-leading quantum hardware providers as well as participate in live question-and-answer sessions.

“We’re billing the webinar as a help day for quantum algorithmists,” said DARPA Innovation Fellow Alex Place, who is leading the event.

“Building on successes of DARPA’s ONISQ (Optimization with Noisy Intermediate-Scale Quantum devices) program, the webinar’s goal is to spark innovative ideas and discuss new concepts for making near-term intermediate scale quantum computers, as well as sought-after fault tolerant processors, practical and useful for solving real problems.

We’re encouraging teams from academia and industry who have expertise in quantum algorithms or a practical problem that could be mapped to a quantum processor to engage with IMPAQT.”



darpa.mil/program/optimization-with-noisy-intermediate-scale-quantum-devices

Optimization with Noisy Intermediate-Scale Quantum devices (ONISQ)

Dr. Mukund Vengalattore

The Optimization with Noisy Intermediate-Scale Quantum devices (ONISQ) program aims to exploit quantum information processing before fully fault-tolerant quantum computers are realized. This effort will pursue a hybrid concept that combines intermediate-sized quantum devices with classical systems to solve a particularly challenging set of problems known as combinatorial optimization. ONISQ seeks to demonstrate the quantitative advantage of quantum information processing by leapfrogging the performance of classical-only systems in solving optimization challenges.

ONISQ researchers will be tasked with developing quantum systems that are scalable to hundreds or thousands of qubits with longer coherence times and improved noise control. Researchers will also be required to efficiently implement a quantum optimization algorithm on noisy intermediate-scale quantum devices, optimizing allocation of quantum and classical resources. Benchmarking will also be part of the program, with researchers making a quantitative comparison of classical and quantum approaches. In addition, the program will identify classes of problems in combinatorial optimization where quantum information processing is likely to have the biggest impact. It will also seek to develop methods for extending quantum advantage on limited size processors to large combinatorial optimization problems via techniques such as problem decomposition.

IMPAQT is the first of many anticipated DARPA ARC topics. The ARC initiative is designed to speed the pace of innovation by rapidly exploring and analyzing a high volume of promising new ideas.

For more information about ARC, to view the open IMPAQT solicitation, and to see new topics as they become available, visit www.darpa.mil/arc.

The ARC topics are managed by DARPA’s innovation fellows, who include recent Ph.D. graduates (within five years of receiving a doctorate) and active-duty military with STEM degrees.

To learn more about the DARPA Innovation Fellowship, current fellows, and how you can apply to become a fellow visit:
www.darpa.mil/innovationfellowship

To read more: https://www.darpa.mil/news-events/2023-03-07

Number 14

Sanctions and Export Controls Compliance

Department of Commerce, Department of the Treasury, and Department of Justice Tri-Seal Compliance Note

Cracking Down on Third-Party Intermediaries Used to Evade Russia-Related Sanctions and Export Controls

Over the year following Russia's illegal and unprovoked war against Ukraine, the U.S. government has used its economic tools to degrade Russia's economy and war machine.

Along with international partners and allies, the Department of the Treasury's Office of Foreign Assets Control (OFAC) and the Department of Commerce's Bureau of Industry and Security (BIS) have imposed sanctions and export controls of an unprecedented scope and scale in an effort to degrade Russia's ability to wage its unjust war and to prevent it from taking military action elsewhere.

The Department of Justice (DOJ) has matched these unprecedented restrictions with equally unprecedented enforcement efforts to aggressively prosecute those who violate U.S. sanctions and export control laws, led by the work of Task Force KleptoCapture.

Despite these efforts, malign actors continue to try to evade Russia-related sanctions and export controls.

One of the most common tactics is the use of third-party intermediaries or transshipment points to circumvent restrictions, disguise the involvement of Specially Designated Nationals and Blocked Persons (SDNs) or parties on the Entity List in transactions, and obscure the true identities of Russian end users.

This Note highlights several of these tactics to assist the private sector in identifying warning signs and implementing appropriate compliance measures.

DETECTING SANCTIONS AND EXPORT CONTROL EVASION

It is critical that financial institutions and other entities conducting business with U.S. persons or within the United States, or businesses dealing in U.S.-origin goods or services or in foreignorigin goods otherwise subject to U.S. export laws, be vigilant against efforts by individuals or entities to evade sanctions and export control laws.

Effective compliance programs employ a risk-based approach to sanctions and export controls compliance by developing, implementing, and routinely updating a compliance program, depending on an organization's size and sophistication, products and services, customers and counterparties, and geographic locations.

Companies such as manufacturers, distributors, resellers, and freight forwarders are often in the best position to determine whether a particular dealing, transaction, or activity is consistent with industry norms and practices, and they should exercise heightened caution and conduct additional due diligence if they detect warning signs of potential sanctions or export violations.

Equally important is the maintenance of effective, risk-based compliance programs that entities can adopt to minimize the risk of evasion. These compliance programs should include management commitment (including through appropriate compensation incentives), risk assessment, internal controls, testing, auditing, and training.

These efforts empower staff to identify and report potential violations of U.S. sanctions and export controls to compliance personnel such that companies can make timely voluntary disclosures to the U.S. government.

Optimally, compliance programs should include controls tailored to the risks the business faces, such as diversion by third-party intermediaries.

Common red flags can indicate that a third-party intermediary may be engaged in efforts to evade sanctions or export controls, including the following:

1. Use of corporate vehicles (i.e., legal entities, such as shell companies, and legal arrangements) to obscure (i) ownership, (ii) source of funds, or (iii) countries involved, particularly sanctioned jurisdictions;

2. A customer's reluctance to share information about the end use of a product, including reluctance to complete an end-user form;

3. Use of shell companies to conduct international wire transfers, often involving financial institutions in jurisdictions distinct from company registration;

4. Declining customary installation, training, or maintenance of the purchased item(s);

5. IP addresses that do not correspond to a customer's reported location data;

6. Last-minute changes to shipping instructions that appear contrary to customer history or business practices;

7. Payment coming from a third-party country or business not listed on the End-User Statement or other applicable end-user form;

8. Use of personal email accounts instead of company email addresses;

9. Operation of complex and/or international businesses using residential addresses or addresses common to multiple closely-held corporate entities;

10. Changes to standard letters of engagement that obscure the ultimate customer;

11. Transactions involving a change in shipments or payments that were previously scheduled for Russia or Belarus;

12. Transactions involving entities with little or no web presence; or

13. Routing purchases through certain transshipment points commonly used to illegally redirect restricted items to Russia or Belarus. Such locations may include China (including Hong Kong and Macau) and jurisdictions close to Russia, including Armenia, Turkey, and Uzbekistan.

Further, entities that use complex sales and distribution models may hinder a company's visibility into the ultimate end-users of its technology, services, or products.

To rear more:
https://home.treasury.gov/system/files/126/20230302_compliance_note.pdf

Number 15

Proposal for a regulation on Markets in Crypto-assets (MiCA)

EUROPEAN COMMISSION

This proposal seeks to provide legal certainty for crypto-assets not covered by existing EU financial services legislation and establish uniform rules for crypto-asset service providers and issuers at EU level. The proposed Regulation will replace existing national frameworks applicable to crypto-assets not covered by existing EU financial services legislation and also establish specific rules for so-called 'stablecoins', including when these are e-money. The proposed Regulation is divided into nine Titles.

Title I sets the subject matter, the scope and the definitions. Article 1 sets out that the Regulation applies to crypto-asset service providers and issuers, and establishes uniform requirements for transparency and disclosure in relation to issuance, operation, organisation and governance of crypto-asset service providers, as well as establishes consumer protection rules and measures to prevent market abuse.

Article 2 limits the scope of the Regulation to crypto-assets that do not qualify as financial instruments, deposits or structured deposits under EU financial services legislation.

Article 3 sets out the terms and definitions that are used for the purposes of this Regulation, including 'crypto-asset', 'issuer of crypto-assets', 'asset-referenced token' (often described as 'stablecoin'), 'e-money token' (often described as 'stablecoin'), 'crypto-asset service provider', 'utility token' and others.

Article 3 also defines the various crypto-asset services. Importantly, the Commission may adopt delegated acts to specify some technical elements of the definitions, to adjust them to market and technological developments.

Title II regulates the offerings and marketing to the public of crypto-assets other than asset-referenced tokens and e-money tokens.

It indicates that an issuer shall be entitled to offer such crypto-assets to the public in the Union or seek an admission to trading on a trading platform for such crypto-assets if it complies with the requirements of Article 4, such as the obligation to be established in the form of a legal person or the obligation to draw up a crypto-asset white paper in accordance with Article 5 (with Annex I) and the notification of such a crypto-asset white paper to the competent authorities (Article 7) and its publication (Article 8).

Once a whitepaper has been published, the issuer of crypto-assets can offer its crypto-assets in the EU or seeks an admission of such crypto-assets to trading on a trading platform (Article 10).

Article 4 also includes some exemptions from the publication of a whitepaper, including for small offerings of crypto-assets (below €1 million within a twelve-month period) and offerings targeting qualified investors as defined by the Prospectus Regulation (Regulation EU 2017/1129).

Article 5 and Annex I of the proposal set out the information requirements regarding the crypto-asset white paper accompanying an offer to the public of crypto-assets or an admission of crypto-assets to a trading platform for crypto-assets, while Article 6 imposes some requirements related to the marketing materials produced by the issuers of crypto-assets, other than asset-referenced tokens or e-money tokens.

The crypto-asset white paper will not be subject to a pre-approval process by the national competent authorities (Article 7). It will be notified to the national competent authorities with an assessment whether the crypto-asset at stake constitutes a financial instrument under the Markets in Financial Instruments Directive (Directive 2014/65/EU), in particular.

After the notification of the crypto-asset white paper, competent authorities will have the power to suspend or prohibit the offering, require the inclusion of additional information in the crypto-asset white paper or make public the fact that the issuer is not complying with the Regulation (Article 7).

Title II also includes specific provisions on the offers of crypto-assets that are limited in time (Article 9), the amendments of an initial crypto-asset white paper (Article 11), the right of withdrawal granted to acquirers of crypto-assets (Article 12), the obligations imposed on all issuers of crypto-assets (Article 13) and on the issuers' liability attached to the crypto-asset white paper (Article 14).

Title III, Chapter 1 describes the procedure for authorisation of asset-referenced token issuers and the approval of their crypto-asset white paper by national competent authorities (Articles 16 to 19 and Annexes I and II). To be authorised to operate in the Union, issuers of asset-referenced tokens shall be incorporated in the form of a legal entity established in the EU (Article 15).

Article 15 also indicates that no asset-referenced tokens can be offered to the public in the Union or admitted to trading on a trading platform for crypto-assets if the issuer is not authorised in the Union and it does not publish a crypto-asset white paper approved by its competent authority.

Article 15 also includes exemptions for small-scale asset-referenced tokens and for asset-referenced tokens that are marketed, distributed and exclusively held by qualified investors. Withdrawal of an authorisation is detailed in Article 20 and Article 21 sets out the procedure for modifying the crypto-asset white paper.

Title III, Chapter 2 sets out the obligations for issuers of asset-referenced tokens. It states they shall act honestly, fairly and professionally (Article 23). It lays down the rules for the publication of the crypto-asset white paper and potential marketing communications (Article 24) and the requirements for these communications (Article 25). Further, issuers are subject to ongoing information obligations (Article 26) and they are required to establish a complaint handling procedure (Article 27).

They shall also comply with other requirements, such as rules on conflicts of interest (Article 28), notification on changes to their management body to its competent authority (Article 29), governance arrangements (Article 30), own funds (Article 31), rules on the reserve of assets backing the asset-referenced tokens (Article 32) and requirements for the custody of the reserve assets (Article 33).

Article 34 explains that an issuer shall only invest the reserve assets in assets that are secure, low risk assets. Article 35 also imposes on issuers of asset-referenced tokens the disclosure of the rights attached to the asset-referenced tokens, including any direct claim on the issuer or on the reserve of assets. Where the issuer of asset-referenced tokens does not offer direct redemption rights or claims on the issuer or on the reserve assets to all holders of asset-reference tokens, Article 35 provides holders of asset-referenced tokens with minimum rights. Article 36 prevents issuers of asset-referenced tokens and crypto-asset service providers from granting any interest to holders of asset-referenced tokens.

Title III, Chapter 4, sets out the rules for the acquisition of issuers of asset-referenced tokens, with Article 37 detailing the assessment of an intended acquisition, and Article 38 the content of such an assessment.

Title III, Chapter 5, Article 39 sets out the criteria that EBA shall use when determining whether an asset-referenced token is significant. These criteria are: the size of the customer base of the promoters of the asset-referenced tokens, the value of the asset-referenced tokens or their market capitalisation, the number and value of transactions, size of the reserve of assets, significance of the issuers' cross-border activities and the interconnectedness with the financial system.

Article 39 also includes an empowerment for the Commission to adopt a delegated act in order to specify further the circumstances under which and thresholds above which an issuer of asset-referenced tokens will be considered significant. Article 39 includes some minimum thresholds that the delegated act shall in any case respect.

Article 40 details the possibility for an issuer of an asset-referenced token to classify as significant at the time of applying for an authorisation on their own initiative. Article 41 lists the additional obligations applicable to issuers of significant asset-referenced tokens, such as additional own funds requirements, liquidity management policy and interoperability.

Tittle III, Chapter 6, Article 42 obliges the issuer to have a procedure in place for an orderly wind-down of their activities.

Title IV, Chapter 1 describes the procedure for authorisation as an issuer of e-money tokens. Article 43 describes that no e-money tokens shall be offered to the public in the Union or admitted to trading on a crypto-asset trading platform unless the issuer is authorised as a credit institution or as an 'electronic money institution' within the meaning of Article 2(1) of Directive 2009/110/EC. Article 43 also states that 'e-money tokens' are deemed electronic money for the purpose of Directive 2009/110/EC.

Article 44 describes how holders of e-money tokens shall be provided with a claim on the issuer: e-money tokens shall be issued at par value and on the receipt of funds, and upon request by the holder of e-money tokens, the issuers must redeem them at any moment and at par value. Article 45 prevents issuers of e-money tokens and crypto-asset service providers from granting any interest to holders of e-money tokens.

Article 46 and Annex III sets out the requirements for the crypto-asset white paper accompanying the issuance of e-money tokens, for example: description of the issuer, detailed description of the issuer's project, indication of whether it concerns an offering of e-money tokens to the public or admission of these to a trading platform, as well as information on the risks relating to the e-money issuer, the e-money tokens and the implementation of any potential project.

Article 47 includes provision on the liability attached to such crypto-asset white paper related to e-money tokens. Article 48 sets requirements for potential marketing communications produced in relation to an offer of e-money tokens and Article 49 states that any funds received by an issuer in exchange for e-money tokens, shall be invested in assets denominated in the same currency as the one referenced by the e-money token.

Title IV, Chapter 2, Article 50 states that the EBA shall classify e-money tokens as significant on the basis of the criteria listed in Article 39. Article 51 details the possibility of an issuer of an e-money token to classify as significant at the time of applying for an authorisation on their own initiative. Article 52 contains the additional obligations applicable to issuers of significant e-money tokens. Issuers of significant e-money tokens must apply Article 33 on the custody of the reserve assets and Article 34 on the investment of these assets instead of Article 7 of Directive 2009/110/EC, Article 41, paragraphs 1, 2, and 3 on remuneration, interoperability and liquidity management, Article 41, paragraph 4 instead of Article 5 of Directive 2009/110/EC and Article 42 on an orderly wind-down of their activities.

To read more: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0593&from=EN

Number 16

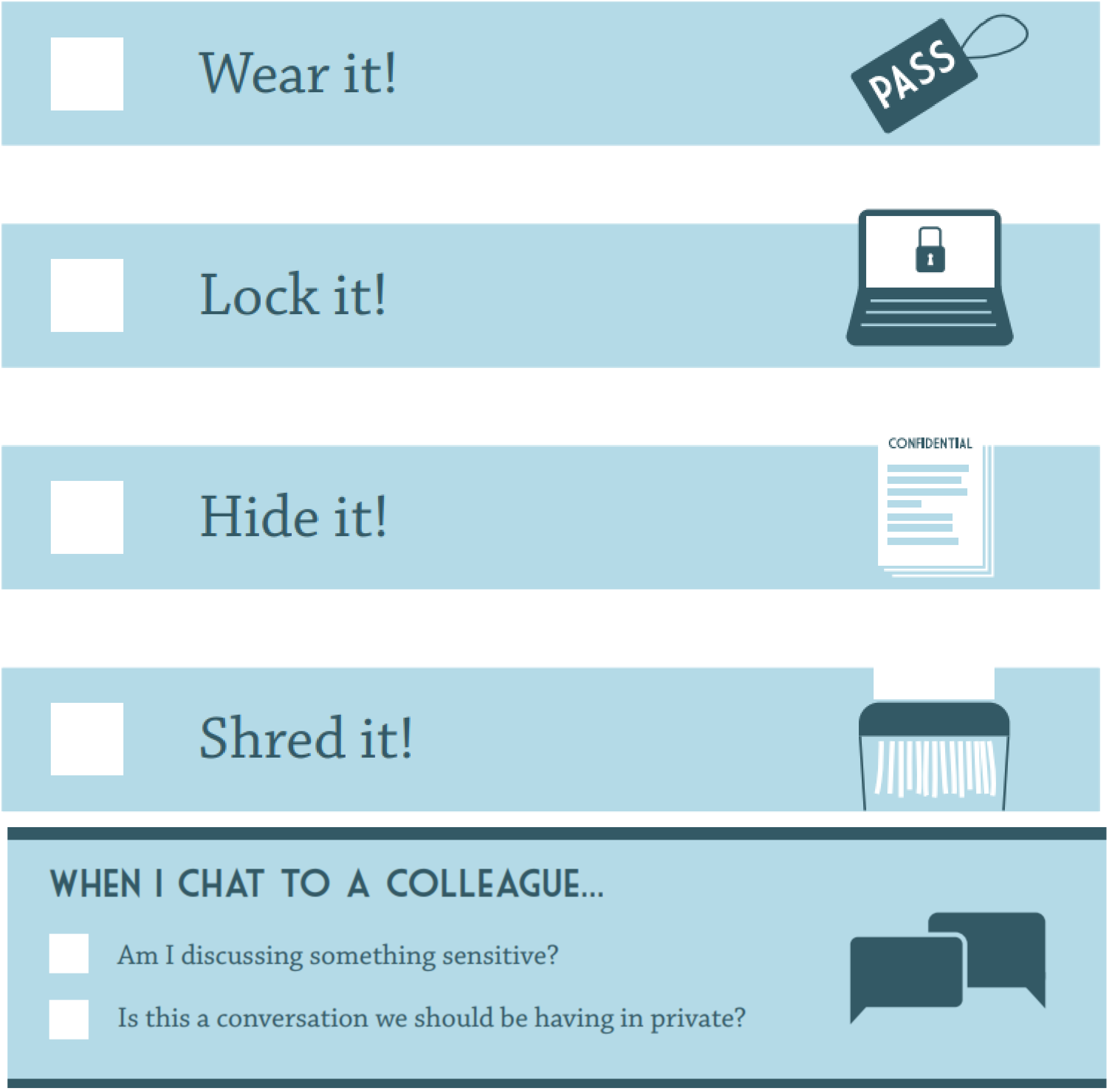
NPSA is the UK Government's National Technical Authority for Physical and Personnel Protective Security.

Security Campaigns

National Protective Security Authority

The NPSA works with partners in government, police, industry and academia to reduce the vulnerability of the national infrastructure.

NPSA has developed a series of security awareness campaigns, designed to provide organisations with a complete range of materials they need.



□ Wear it!

□ Lock it!

□ Hide it!

□ Shred it!

WHEN I CHAT TO A COLLEAGUE...

□ Am I discussing something sensitive?

□ Is this a conversation we should be having in private?

3.What would you do if you overheard a discussion, which you knew to be about some highly sensitive and confidential information, being held in a corridor where external visitors often pass through?

A – Approach the individuals and ask them to stop the discussion immediately – they risk compromising the security of highly sensitive information.

B – Point out where the nearest vacant meeting room is and politely suggest they continue their conversation privately in there.

C – Not say anything at the time, but make a note of the individuals involved, what they discussed, before informing either your line manager, their line manager or a security representative.

D – Remind the individuals that visitors frequent the corridor and suggest they continue their discussion elsewhere or at another time.

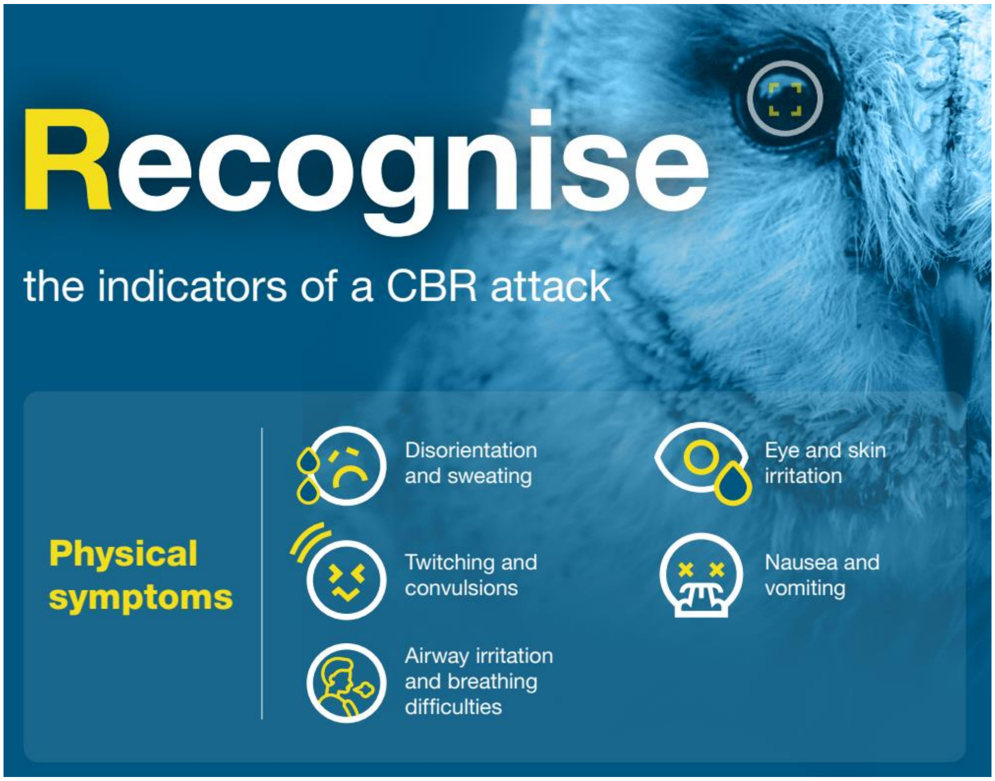
6. You notice that a colleague is unusually quiet at work, and frequently ignores basic security procedures (e.g. they send sensitive information inappropriately to a supplier over email). What would you do?

A – Let your colleague know they've been breaking security protocol and brief them on how to handle sensitive information on email.

B – Check the current security policy to ensure your colleague is deviating from this. If so, send them and others concerned a reminder of the policy. Offer to help if they are unclear what to do with certain information.

C – Keep an eye on your colleague and share your observations about their change in character and recent security lapses with a line manager. Together you can discuss a way forward.

D – Invite your colleague for an informal catch-up to ask how they are. Use this as an opportunity to also tactfully let them know that you've noticed they're not following security policy, and remind them that it's important to do so.

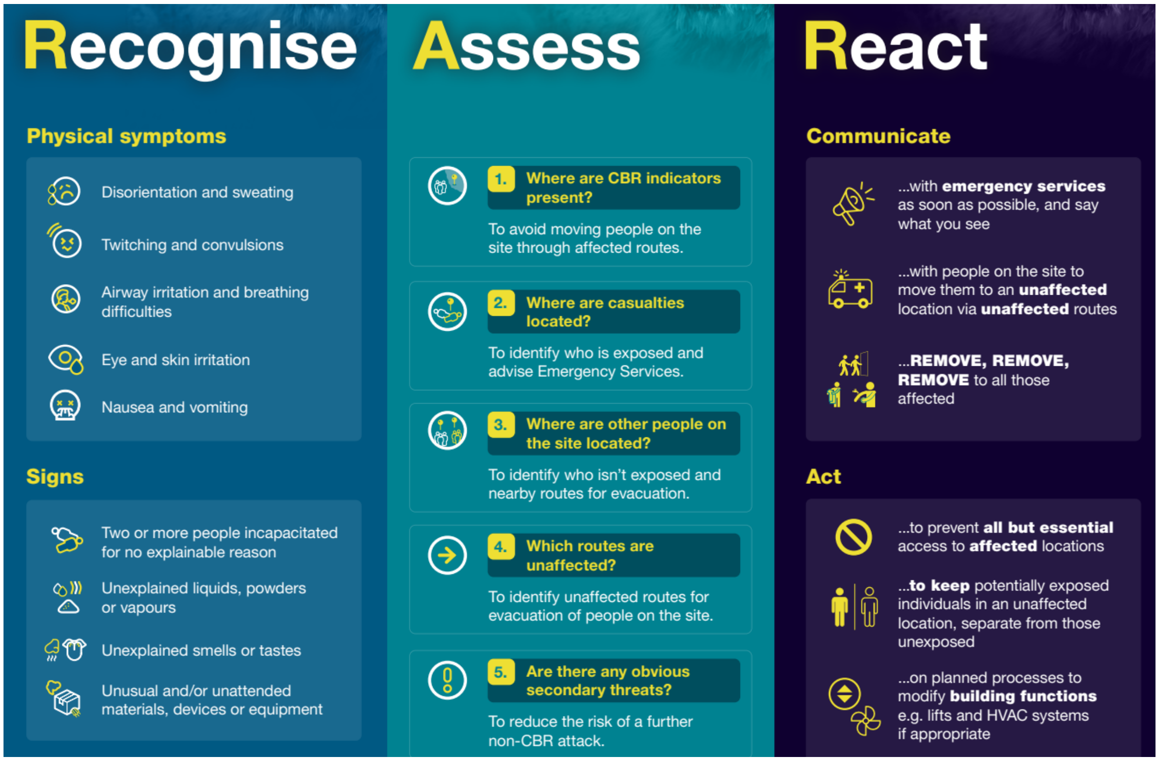


Recognise

the indicators of a CBR attack

Physical symptoms

- Disorientation and sweating
- Twitching and convulsions
- Airway irritation and breathing difficulties
- Eye and skin irritation
- Nausea and vomiting



Recognise

Physical symptoms

- Disorientation and sweating
- Twitching and convulsions
- Airway irritation and breathing difficulties
- Eye and skin irritation
- Nausea and vomiting

Signs

- Two or more people incapacitated for no explainable reason
- Unexplained liquids, powders or vapours
- Unexplained smells or tastes
- Unusual and/or unattended materials, devices or equipment

Assess

1. Where are CBR indicators present?

To avoid moving people on the site through affected routes.

2. Where are casualties located?

To identify who is exposed and advise Emergency Services.

3. Where are other people on the site located?

To identify who isn't exposed and nearby routes for evacuation.

4. Which routes are unaffected?

To identify unaffected routes for evacuation of people on the site.

5. Are there any obvious secondary threats?

To reduce the risk of a further non-CBR attack.

React

Communicate

- ...with **emergency services** as soon as possible, and say what you see
- ...with people on the site to move them to an **unaffected** location via **unaffected** routes
- ...**REMOVE, REMOVE, REMOVE** to all those affected

Act

- ...to prevent **all but essential** access to **affected** locations
- ...**to keep** potentially exposed individuals in an unaffected location, separate from those unexposed
- ...on planned processes to modify **building functions** e.g. lifts and HVAC systems if appropriate

You may visit: https://www.npsa.gov.uk/security-campaigns

Number 17

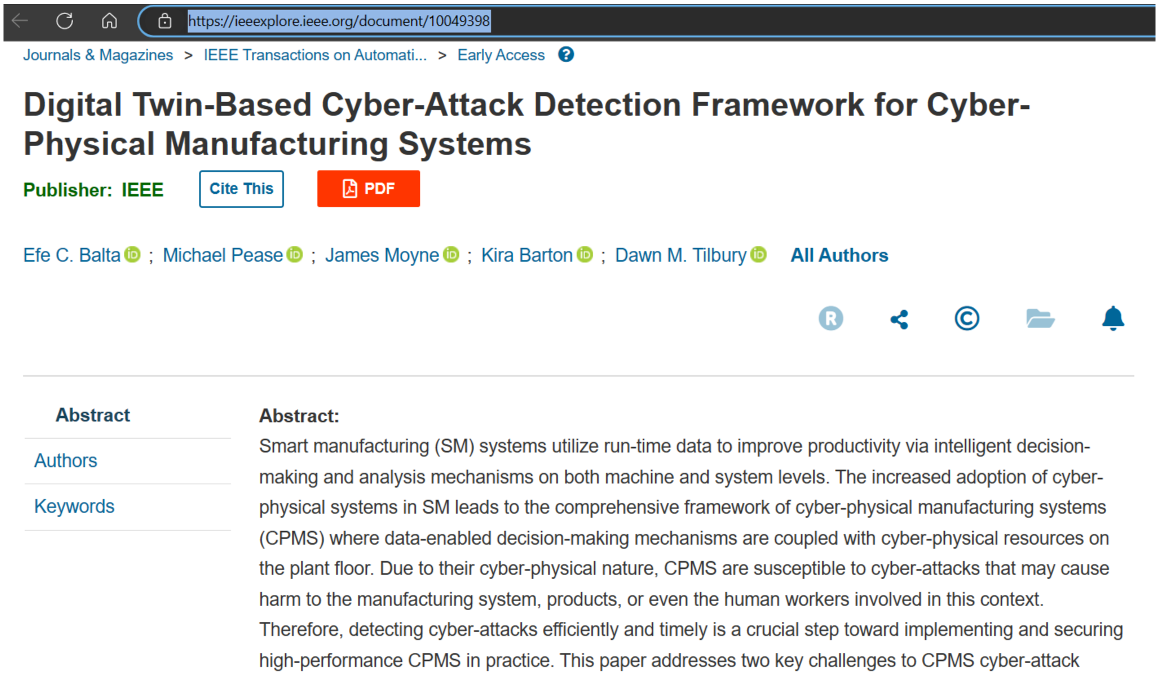
How Digital Twins Could Protect Manufacturers From Cyberattacks

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Detailed virtual copies of physical objects, called digital twins, are opening doors for better products across automotive, health care, aerospace and other industries. According to a new study, cybersecurity may also fit neatly into the digital twin portfolio.

As more robots and other manufacturing equipment become remotely accessible, new entry points for malicious cyberattacks are created. To keep pace with the growing cyber threat, a team of researchers at the National Institute of Standards and Technology (NIST) and the University of Michigan devised a cybersecurity framework that brings digital twin technology together with machine learning and human expertise to flag indicators of cyberattacks.

In a paper published in IEEE Transactions on Automation Science and Engineering, the NIST and University of Michigan researchers demonstrated the feasibility of their strategy by detecting cyberattacks aimed at a 3D printer in their lab. They also note that the framework could be applied to a broad range of manufacturing technologies. You may visit: https://ieeexplore.ieee.org/document/10049398


https://ieeexplore.ieee.org/document/10049398
Journals & Magazines > IEEE Transactions on Automati... > Early Access
Cite This
PDF
All Authors
Abstract
Authors
Keywords

Digital Twin-Based Cyber-Attack Detection Framework for Cyber-Physical Manufacturing Systems

Publisher: IEEE

Efe C. Balta ; Michael Pease ; James Moyne ; Kira Barton ; Dawn M. Tilbury

Abstract:

Smart manufacturing (SM) systems utilize run-time data to improve productivity via intelligent decision-making and analysis mechanisms on both machine and system levels. The increased adoption of cyber-physical systems in SM leads to the comprehensive framework of cyber-physical manufacturing systems (CPMS) where data-enabled decision-making mechanisms are coupled with cyber-physical resources on the plant floor. Due to their cyber-physical nature, CPMS are susceptible to cyber-attacks that may cause harm to the manufacturing system, products, or even the human workers involved in this context. Therefore, detecting cyber-attacks efficiently and timely is a crucial step toward implementing and securing high-performance CPMS in practice. This paper addresses two key challenges to CPMS cyber-attack

Cyberattacks can be incredibly subtle and thus difficult to detect or differentiate from other, sometimes more routine, system anomalies.

Operational data describing what is occurring within machines — sensor data, error signals, digital commands being issued or executed, for instance — could support cyberattack detection. However, directly accessing this kind of data in near real time from operational technology (OT) devices, such as a 3D printer, could put the performance and safety of the process on the factory floor at risk.

“Typically, I have observed that manufacturing cybersecurity strategies rely on copies of network traffic that do not always help us see what is occurring inside a piece of machinery or process,” said NIST mechanical engineer Michael Pease, a co-author of the study. “As a result, some OT cybersecurity strategies seem analogous to observing the operations from the outside through a window; however, adversaries might have found a way onto the floor.”

Without looking under the hood of the hardware, cybersecurity professionals may be leaving room for malicious actors to operate undetected.

Taking a Look in the Digital Mirror

Digital twins aren’t your run-of-the-mill computer models. They are closely tied to their physical counterparts, from which they extract data and run alongside in near real time. So, when it’s not possible to inspect a physical machine while it’s in operation, its digital twin is the next best thing.

In recent years, digital twins of manufacturing machinery have armed engineers with an abundance of operational data, helping them accomplish a variety of feats (without impacting performance or safety), including predicting when parts will start to break down and require maintenance.

In addition to spotting routine indicators of wear and tear, digital twins could help find something more within manufacturing data, the authors of the study say.

“Because manufacturing processes produce such rich data sets — temperature, voltage, current — and they are so repetitive, there are opportunities to detect anomalies that stick out, including cyberattacks,” said Dawn Tilbury, a professor of mechanical engineering at the University of Michigan and study co-author.

To seize the opportunity presented by digital twins for tighter cybersecurity, the researchers developed a framework entailing a new strategy, which they tested out on an off-the-shelf 3D printer.

The team built a digital twin to emulate the 3D printing process and provided it with information from the real printer. As the printer built a part (a plastic hourglass in this case), computer programs monitored and analyzed continuous data streams including both measured temperatures from the physical printing head and the simulated temperatures being computed in real time by the digital twin.

The researchers launched waves of disturbances at the printer. Some were innocent anomalies, such as an external fan causing the printer to cool, but others, some of which caused the printer to incorrectly report its temperature readings, represented something more nefarious.

So, even with the wealth of information at hand, how did the team's computer programs distinguish a cyberattack from something more routine? The framework's answer is to use a process of elimination.

The programs analyzing both the real and digital printers were pattern-recognizing machine learning models trained on normal operating data, which is included in the paper, in bulk. In other words, the models were adept at recognizing what the printer looked like under normal conditions, also meaning they could tell when things were out of the ordinary.

If these models detected an irregularity, they passed the baton off to other computer models that checked whether the strange signals were consistent with anything in a library of known issues, such as the printer's fan cooling its printing head more than expected. Then the system categorized the irregularity as an expected anomaly or a potential cyber threat.

In the last step, a human expert is meant to interpret the system's finding and then make a decision.

"The framework provides tools to systematically formalize the subject matter expert's knowledge on anomaly detection. If the framework hasn't seen a certain anomaly before, a subject matter expert can analyze the collected data to provide further insights to be integrated into and improve the system," said lead-author Efe Balta, a former mechanical engineering graduate student at the University of Michigan and now a postdoctoral researcher at ETH Zurich.

Generally speaking, the expert would either confirm the cybersecurity system's suspicions or teach it a new anomaly to store in the database. And then as time goes on, the models in the system would theoretically learn more and more, and the human expert would need to teach them less and less.

In the case of the 3D printer, the team checked its cybersecurity system's work and found it was able to correctly sort the cyberattacks from normal anomalies by analyzing physical and emulated data.

But despite the promising showing, the researchers plan to study how the framework responds to more varied and aggressive attacks in the future, ensuring the strategy is reliable and scalable. Their next steps will likely also include applying the strategy to a fleet of printers at once, to see if the expanded coverage either hurts or helps their detection capabilities.

"With further research, this framework could potentially be a huge win-win for both maintenance as well as monitoring for indications of compromised OT systems," Pease said.

To read more: https://www.nist.gov/news-events/news/2023/02/how-digital-twins-could-protect-manufacturers-cyberattacks

Number 18

European Parliament resolution on the adequacy of the protection afforded by the EU-US Data Privacy Framework

European Parliament
2019-2024

Committee on Civil Liberties, Justice and Home Affairs

DRAFT MOTION FOR A RESOLUTION, to wind up the debate on the statement by the Commission pursuant to Rule 132(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP))
Juan Fernando López Aguilar, on behalf of the Committee on Civil Liberties, Justice and Home Affairs

The European Parliament,

– having regard to the Charter of Fundamental Rights of the European Union (‘the Charter’), in particular Articles 7, 8, 16, 47 and 52 thereof,

– having regard to the judgment of the Court of Justice of 6 October 2015 in Case C-362/14 Maximillian Schrems v Data Protection Commissioner (‘Schrems I’),

– having regard to the judgment of the Court of Justice of 16 July 2020 in Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (‘Schrems II’),

– having regard to its enquiry into the revelations made by Edward Snowden on the electronic mass surveillance of EU citizens, including the findings in its resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens’ fundamental rights and on transatlantic cooperation in Justice and Home Affairs,

– having regard to its resolution of 26 May 2016 on transatlantic data flows,

– having regard to its resolution of 6 April 2017 on the adequacy of the protection afforded by the EU-US Privacy Shield,

– having regard to its resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield,

– having regard to its resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 – Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (‘Schrems II’), Case C-311/18,

– having regard to the Commission draft Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework,

– having regard to President of the United States’ Executive Order 14086 of 7 October 2022 on Enhancing Safeguards For United States Signals Intelligence Activities,

– having regard to the Regulation on the Data Protection Review Court issued by the US Attorney General (‘AG Regulation’),

– having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (‘GDPR’), in particular Chapter V thereof,

– having regard to the Commission proposal of 10 January 2017 for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (COM(2017)0010), to the decision to enter into interinstitutional negotiations confirmed by Parliament’s plenary on 25 October 2017, and to the Council’s general approach adopted on 10 February 2021 (6087/21),

– having regard to the European Data Protection Board (EDPB) Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, and to the EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures,

– having regard to the EDPB Opinion of [to be added],

– having regard to Rule 132(2) of its Rules of Procedure,

A. whereas in the ‘Schrems I’ judgment, the Court of Justice of the European Union (CJEU) invalidated the Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US

Department of Commerce, and pointed out that indiscriminate access by intelligence authorities to the content of electronic communications violates the essence of the fundamental right to confidentiality of communications provided for in Article 7 of the Charter;

B. whereas in the ‘Schrems II’ judgment, the CJEU invalidated Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield and concluded that it did not provide sufficient legal remedies against mass surveillance for non-US nationals and that this violates the essence of the fundamental right to a legal remedy as provided for in Article 47 of the Charter;

C. whereas on 7 October 2022, the President of the United States of America signed Executive Order 14086 on Enhancing Safeguards For United States Signals Intelligence Activities (‘EO’);

D. whereas on 13 December 2022 the Commission launched the process to adopt an adequacy decision for the EU-US Data Privacy Framework;

E. whereas, when examining the level of protection afforded by a third country, the Commission is obliged to assess the content of the rules applicable in that country deriving from its domestic law or its international commitments, as well as the practice designed to ensure compliance with those rules;

F. whereas the ability to transfer personal data across borders has the potential to be a key driver of innovation, productivity and economic competitiveness; whereas these transfers should be carried out in full respect for the right to the protection of personal data and the right to privacy; whereas one of the fundamental objectives of the EU is the protection of fundamental rights, as enshrined in the Charter;

G. whereas the GDPR applies to all companies processing the personal data of data subjects in the EU, where the processing activities are related to the offering of goods or services to such data subjects in the Union, or the monitoring of their behaviour as far as their behaviour takes place within the Union;

H. whereas mass surveillance, including the bulk collection of data, by state actors is detrimental to the trust of European citizens and businesses in digital services and, by extension, in the digital economy;

I. whereas controllers should always be accountable for compliance with data protection obligations, including demonstrating compliance for any data processing whatever its nature, scope, context, purposes and risks for data subjects;

J. whereas there is no federal privacy and data protection legislation in the United States (US); whereas the EU and the US have differing definitions of key data protection concepts such as principles of necessity and proportionality;

1. Recalls that privacy and data protection are legally enforceable fundamental rights enshrined in the Treaties, the Charter and the European Convention of Human Rights, as well as in laws and case-law; emphasises that they must be applied in a manner that does not unnecessarily hamper trade or international relations, but can be balanced only against other fundamental rights and not against commercial or political interests;

2. Acknowledges the efforts made in the EO to lay down limits on US Signals Intelligence Activities, by referring to the principles of proportionality and necessity, and providing a list of legitimate objectives for such activities; points out, however, that these principles are long-standing key elements of the EU data protection regime and that their substantive definitions in the EO are not in line with their definition under EU law and their interpretation by the CJEU; points out, furthermore, that for the purposes of the EU-US Data Privacy Framework, these principles will be interpreted solely in the light of US law and legal traditions; points out that the EO requires that signals intelligence must be conducted in a manner proportionate to the ‘validated intelligence priority’, which appears to be a broad interpretation of proportionality;

3. Regrets the fact that the EO does not prohibit the bulk collection of data by signals intelligence, including the content of communications; notes that the list of legitimate national security objectives can be expanded by the US President, who can determine not to make the relevant updates public;

4. Points out that the EO does not apply to data accessed by public authorities via other means, for example through the US Cloud Act or the US Patriot Act, by commercial data purchases, or by voluntary data sharing agreements;

5. Points out that the decisions of the Data Protection Review Court (‘DPRC’) will be classified and not made public or available to the complainant; points out that the DPRC is part of the executive branch and not the judiciary; points out that a complainant will be represented by a ‘special advocate’ designated by the DPRC, for whom there is no

requirement of independence; points out that the redress process provided by the EO is based on secrecy and does not set up an obligation to notify the complainant that their personal data has been processed, thereby undermining their right to access or rectify their data; notes that the proposed redress process does not provide for an avenue for appeal in a federal court and therefore, among other things, does not provide any possibility for the complainant to claim damages; concludes that the DPRC does not meet the standards of independence and impartiality of Article 47 of the Charter;

6. Notes that, while the US has provided for a new mechanism for remedy for issues related to public authorities' access to data, the remedies available for commercial matters under the adequacy decision are insufficient; notes that these issues are largely left to the discretion of companies, which can select alternative remedy avenues such as dispute resolution mechanisms or the use of companies' privacy programmes;

7. Notes that European businesses need and deserve legal certainty; stresses that successive data transfer mechanisms, which were subsequently repealed by the CJEU, created additional costs for European businesses; notes that continuing uncertainty and the need to adapt to new legal solutions is particularly burdensome for micro, small and medium-sized enterprises;

8. Points out that, unlike all other third countries that have received an adequacy decision under the GDPR, the US still does not have a federal data protection law; points out that the EO is not clear, precise or foreseeable in its application, as it can be amended at any time by the US President; is therefore concerned about the absence of a sunset clause which could provide that the decision would automatically expire four years after its entry into force;

9. Emphasises that adequacy decisions must include clear and strict mechanisms for monitoring and review in order to ensure that decisions are future proof and that EU citizens' fundamental right to data protection is guaranteed;

Conclusions

10. Recalls that, in its resolution of 20 May 2021, Parliament called on the Commission not to adopt any new adequacy decision in relation to the US, unless meaningful reforms were introduced, in particular for national security and intelligence purposes;

11. Concludes that the EU-US Data Privacy Framework fails to create actual equivalence in the level of protection; calls on the Commission to continue negotiations with its US counterparts with the aim of creating a mechanism that would ensure such equivalence and which would provide the adequate level of protection required by Union data protection law and the Charter as interpreted by the CJEU; urges the Commission not to adopt the adequacy finding;

12. Instructs its President to forward this resolution to the Council, the Commission and the President and Congress of the United States of America.

Number 19

Office of the Director of National Intelligence

2023 Annual Threat Assessment of the U.S. Intelligence Community

This annual report of worldwide threats to the national security of the United States responds to Section 617 of the Intelligence Authorization Act (Pub. L. No. 116-260).

This report reflects the collective insights of the Intelligence Community (IC), which is committed every day to providing the nuanced, independent, and unvarnished intelligence that policymakers, warfighters, and domestic law enforcement personnel need to protect American lives and America's interests anywhere in the world.

This assessment focuses on the most direct, serious threats to the United States during the next year. The order of the topics presented in this assessment does not necessarily indicate their relative importance or the magnitude of the threats in the view of the IC.

All require a robust intelligence response, including those where a near-term focus may help head off greater threats in the future.

Information available as of 18 January was used in the preparation of this assessment.

China, Cyber

China probably currently represents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks.

China's cyber pursuits and its industry's export of related technologies increase the threats of aggressive cyber operations against the U.S. homeland, suppression of the free flow of information in cyberspace—such as U.S. web content—that Beijing views as threatening to the CCP's hold on power, and the expansion of technology-driven authoritarianism globally.

If Beijing feared that a major conflict with the United States were imminent, it almost certainly would consider undertaking aggressive cyber operations against U.S. homeland critical infrastructure and military assets worldwide.

Such a strike would be designed to deter U.S. military action by impeding U.S. decisionmaking, inducing societal panic, and interfering with the deployment of U.S. forces.

- China almost certainly is capable of launching cyber attacks that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines, and rail systems.

China leads the world in applying surveillance and censorship to monitor its population and repress dissent. Beijing conducts cyber intrusions that are targeted to affect U.S. and non-U.S. citizens beyond its borders—including journalists, dissidents, and individuals it views as threats—to counter views it considers critical of CCP narratives, policies, and actions.

- China's cyber espionage operations have included compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations.

China, malign influence operations

Beijing will continue expanding its global intelligence and covert influence posture to better support the CCP's political, economic, and security goals.

China is attempting to sow doubts about U.S. leadership, undermine democracy, and extend Beijing's influence, particularly in East Asia and the western Pacific, which Beijing views as its sphere of influence.

Beijing largely concentrates its U.S.-focused influence efforts on shaping U.S. policy and the U.S. public's perception of China in a positive direction, but has shown a willingness to meddle in select election races that involved perceived anti-China politicians.

- Beijing uses a sophisticated array of covert, overt, licit, and illicit means to try to soften U.S. criticism, shape U.S. power centers' views of China, and influence policymakers at all levels of government.

PRC leaders probably believe that a U.S. bipartisan consensus against China is impeding their efforts to directly influence U.S. national-level policy regarding China.

Beijing has adjusted by redoubling its efforts to build influence at the state and local level to shift U.S. policy in China's favor because of Beijing's belief that local officials are more pliable than their federal counterparts.

PRC actors have become more aggressive with their influence campaigns, probably motivated by their view that antiChina sentiment in the United States is threatening their international image, access to markets, and technological expertise.

Beijing's growing efforts to actively exploit perceived U.S. societal divisions using its online personas move it closer to Moscow's playbook for influence operations.

- Beijing is intensifying efforts to mold U.S. public discourse—particularly by trying to shape U.S. views of sensitive or core sovereignty issues, such as Taiwan, Xinjiang, Tibet, and Hong Kong—and pressure perceived political opponents.

As part of efforts to stifle anti-Beijing criticism, the PRC monitors overseas Chinese students for dissident views, mobilizes Chinese student associations to conduct activities on behalf of Beijing, and influences research by U.S. academics and think tank experts.

These activities have included pressuring family members in China, denying or canceling visas, blocking access to China's archives and resources, and disrupting or withdrawing funding for exchange programs.

- China is rapidly expanding and improving its artificial intelligence (AI) and big data analytics capabilities, which could expand beyond domestic use.

Russia, Cyber

The Ukraine war was the key factor in Russia's cyber operations prioritization in 2022.

Although its cyber activity surrounding the war fell short of the pace and impact we had expected, Russia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities.

Russia views cyber disruptions as a foreign policy lever to shape other countries' decisions.

- Russia is particularly focused on improving its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries, because compromising such infrastructure improves and demonstrates its ability to damage infrastructure during a crisis.

Russia, malign influence operations

Russia presents one of the most serious foreign influence threats to the United States, because it uses its intelligence services, proxies, and wide-ranging influence tools to try to divide Western alliances and increase its sway around the world, while attempting to undermine U.S. global standing, sow discord inside the United States, and influence U.S. voters and decisionmaking.

Moscow probably will build on these approaches to try to undermine the United States as opportunities arise.

Russia and its influence actors are adept at capitalizing on current events in the United States to push Moscow-friendly positions to Western audiences.

Russian officials, including Putin himself, and influence actors routinely inject themselves into contentious U.S. issues, even if that causes the Kremlin to take a public stand on U.S. domestic political matters.

- Moscow views U.S. elections as opportunities for malign influence as part of its larger foreign policy strategy. Moscow has conducted influence operations against U.S. elections for decades, including as recently as the U.S. midterm elections in 2022. It will try to strengthen ties to U.S. persons in the media and politics in hopes of developing vectors for future influence operations.

- Russia’s influence actors have adapted their efforts to increasingly hide their hand, laundering their preferred messaging through a vast ecosystem of Russian proxy websites, individuals, and organizations that appear to be independent news sources.

Moscow seeds original stories or amplifies preexisting popular or divisive discourse using a network of state media, proxy, and social media influence actors and then intensifies that content to further penetrate the Western information environment.

These activities can include disseminating false content and amplifying information perceived as beneficial to Russian influence efforts or conspiracy theories.

DEVELOPMENTS IN TECHNOLOGY

New technologies—particularly in the fields of AI and biotechnology—are being developed and are proliferating faster than companies and governments can shape norms, protect privacy, and prevent dangerous outcomes.

The convergence of emerging technologies is likely to create potentially breakthrough technologies not foreseeable by examining narrow science and technology areas, which could lead to the rapid development of asymmetric threats to U.S. interests.

- The convergence of capabilities in high-performance computing, big data, and machine learning—each a critical enabler across multiple domains—could have broad yet unidentified consequences across military, commercial, and basic research applications with relevance to national defense, economic security, and political stability.

- Large-scale simulation and the accumulation and analysis of massive amounts of data are revolutionizing many areas of science and engineering research with the potential to influence the future battlefield and shape political discourse through disinformation operations.

Our adversaries increasingly view data as a strategic resource. They are focused on acquiring and analyzing data—from personally identifiable information on U.S. citizens to commercial and government data—that can make their espionage, influence, kinetic and cyber attack operations more effective; advance their exploitation of the U.S. economy; and give them strategic advantage over the United States.

- Foreign intelligence services are adopting cutting-edge technologies — from advanced cyber tools to unmanned systems to enhanced technical surveillance equipment—that improve their capabilities and challenge U.S. defenses. Much of this technology is available commercially, providing a shortcut for previously unsophisticated services to become legitimate threats.

The global pandemic, which spurred unprecedented collection of genetic and health data worldwide, along with technological advances in genetic engineering, genome sequencing, and DNA modification, are driving new lines of effort in biotech research.

- Several countries, universities, and private companies have or are creating centralized genetic or genomic databases to collect, store, process, and analyze genetic data, albeit at the risk of potentially compromising health and genetic data privacy, and are ripe targets for cyber attack and theft.

• China has been collecting genetic and health data from its entire population, bolstering the state's surveillance and security apparatus, and its ability to try to monitor, manage, and control society in real-time. Beijing also has collected U.S. health and genomic data through its acquisitions and investments in U.S. companies, as well as cyber breaches.

Advances in semiconductors and high-performance computing are driving military and technological breakthroughs, but also are heightening the risk of technology surprise because high-performance computers will help address longstanding research and development hurdles.

Our adversaries' advances in semiconductors and high-performance computing could result in future challenges to our military and technological sectors.

• China may now have two exascale systems using older generation, domestically designed processors— neither of which have been officially acknowledged or subject to independent benchmarks—and plans to build more by 2025.

Exascale computers are capable of solving massive scientific challenges that would have been impossible with previous generation supercomputers.

• As of June 2022, China had 173 of the world's most powerful supercomputers, a third more than the United States, which accounted for 128 supercomputers.

TRENDS IN DIGITAL AUTHORITARIANISM AND MALIGN INFLUENCE

Globally, foreign states' malicious use of digital information and communication technologies will become more pervasive, automated, targeted, and complex during the next few years, further threatening to distort publicly available information and probably will outpace efforts to protect digital freedoms.

The exploitation of U.S. citizens' sensitive data and illegitimate use of technology, including commercial spyware and surveillance technology, probably will continue to threaten U.S. interests.

Authoritarian governments usually are the principal offenders of digital repression, but some democratic states have engaged in similar approaches, contributing to democratic backsliding and erosion.

Many foreign governments have become adept at the tools of digital repression, employing censorship, misinformation and disinformation, mass surveillance, and invasive spyware to suppress freedom.

During the next several years, governments are likely to grow more sophisticated in their use of existing technologies, and learn quickly how to exploit new and more intrusive technologies for repression, particularly automated surveillance and identity resolution techniques.

• Digital repression is occurring against the backdrop of broader digital influence operations that many autocrats are conducting globally to try to shape how foreign publics view their regimes, create social and political upheaval in some democracies, shift policies, and sway voters' perspectives and preferences.

Various technologies now constitute an important component of many governments' repressive toolkits, extending states' power to stifle dissent beyond traditional means—such as censoring print media or physically harming dissidents—which repressive regimes continue to employ.

Firms around the world sell capabilities and expertise that facilitate governments' internal and extraterritorial monitoring and repression.

• The commercial spyware industry—which makes tools that allow users to hack digital devices such as mobile telephones to surveil users—grew rapidly during the past decade and is now estimated to be worth $12 billion.

While some states use such spyware tools and lawful intercept programs to target criminals and terrorists, governments also are increasingly using spyware to target political opposition and dissidents.

• Authoritarian states use spyware and other digital means to conduct transnational repression against individual critics and diaspora communities to limit their influence over domestic audiences.

Monitoring and threats against these communities limit freedom of speech wherever they reside, including in the United States and other liberal democracies.

• Beijing has demonstrated its willingness to enlist the aid of China-based commercial enterprises to help surveil and censor PRC critics abroad, and China's technology industry is a key global supplier of advanced surveillance technologies to foreign governments.

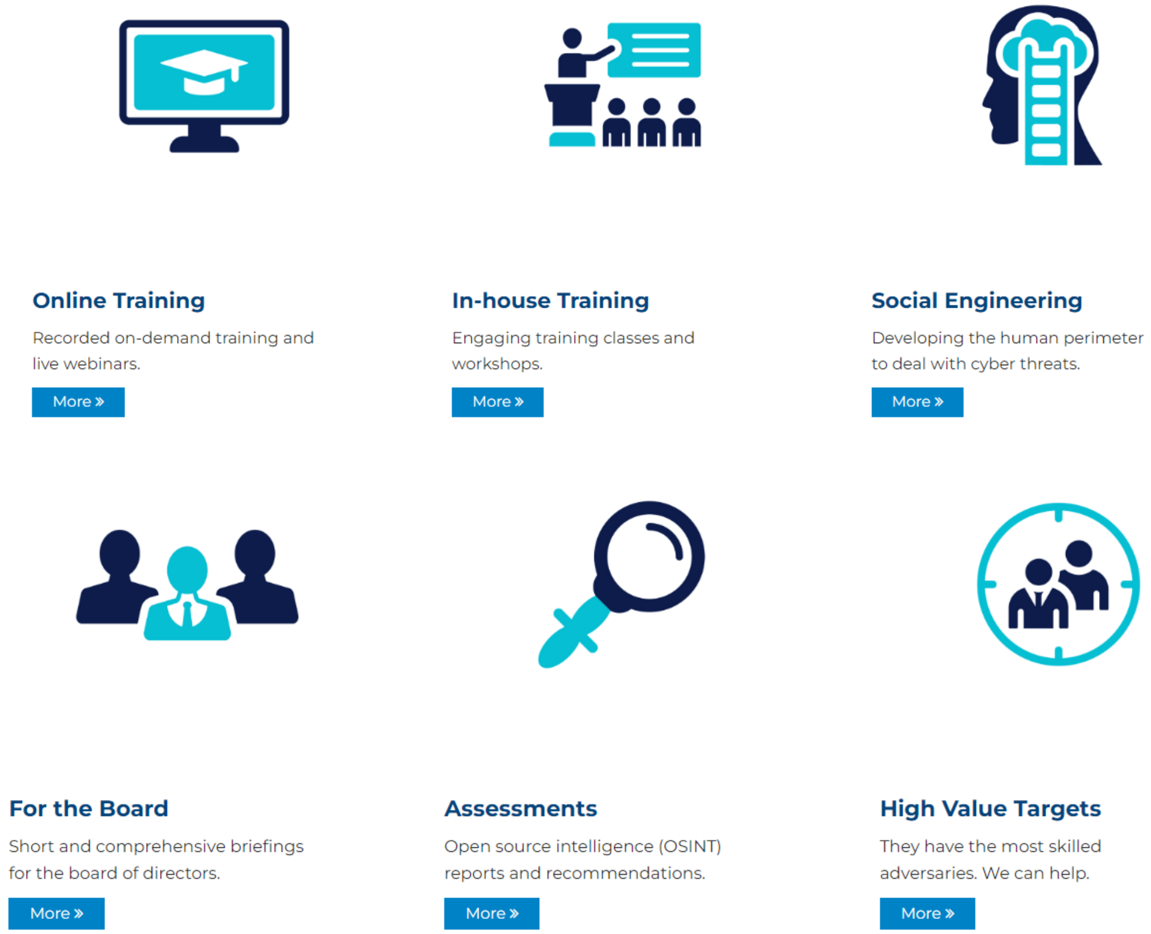
The report:
https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

ANNUAL THREAT ASSESSMENT
OF THE U.S. INTELLIGENCE COMMUNITY

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Cyber Risk GmbH

Cyber Risk GmbH has been established in Horgen, Switzerland, by George Lekatis, a well-known expert in risk management and compliance.



Online Training

Recorded on-demand training and live webinars.

More »

In-house Training

Engaging training classes and workshops.

More »

Social Engineering

Developing the human perimeter to deal with cyber threats.

More »

For the Board

Short and comprehensive briefings for the board of directors.

More »

Assessments

Open source intelligence (OSINT) reports and recommendations.

More »

High Value Targets

They have the most skilled adversaries. We can help.

More »

Cyber security training

Overview

The world of cyber security and privacy is constantly changing. Today, effective cyber security programs involve the entire organization and not only the IT or the information security teams. Employees that have access to critical assets of an organization, have become primary targets of cyber attacks. Those that have access to technology and organizational assets are also responsible for the protection of those assets. Are they fit and proper to handle this responsibility? Do they have the awareness and skills necessary to meet these expectations?

Our training programs have the objective to help managers and employees not only understand the cyber security threats, but also their responsibility towards protecting the assets they handle. We explain how to proactively apply good cyber security practices, how to identify threats and attacks, and what to do to protect themselves and their organizations. Cyber security is a shared responsibility.

Duration

We tailor each program to the needs of each client. We can provide trainings as short as one hour, but we can also deep dive into our topics for one or two days. The duration depends entirely on the needs, the agreed content of the program, and the case studies.

Our Education Method

In the core of our training approach is to ensure that our delivery is relatable, engaging, and interesting. We always make cyber security training an exciting adventure for our attendees. Our instructors have trained thousands of employees across the globe and have the skills and experience necessary to ensure that our attendees will enjoy the process while they learn. Our training programs may have workshop elements that get everyone involved.

Our Instructors

They are working professionals that have the necessary knowledge and experience in the fields in which they teach. They can lead full-time, part-time, and short-form programs that are tailored to your needs. You will always know up front who the instructor of the training program will be.

Our websites include:

a. Sectors and Industries.

1. Cyber Risk GmbH - https://www.cyber-risk-gmbh.com

2. Social Engineering Training - https://www.social-engineering-training.ch

3. Healthcare Cybersecurity - https://www.healthcare-cybersecurity.ch

4. Airline Cybersecurity - https://www.airline-cybersecurity.ch

5. Railway Cybersecurity - https://www.railway-cybersecurity.com

6. Maritime Cybersecurity - https://www.maritime-cybersecurity.com

7. Transport Cybersecurity - https://www.transport-cybersecurity.com

8. Transport Cybersecurity Toolkit - https://www.transport-cybersecurity-toolkit.com

9. Hotel Cybersecurity - https://www.hotel-cybersecurity.ch

10. Sanctions Risk - https://www.sanctions-risk.com

11. Travel Security - https://www.travel-security.ch

b. Understanding Cybersecurity.

1. What is Disinformation? - https://www.disinformation.ch

2. What is Steganography? - https://www.steganography.ch

3. What is Cyberbiosecurity? - https://www.cyberbiosecurity.ch

4. What is Synthetic Identity Fraud? - https://www.synthetic-identity-fraud.com

5. What is a Romance Scam? - https://www.romance-scams.ch

6. What is Cyber Espionage? - https://www.cyber-espionage.ch

7. What is Sexspionage? - https://www.sexspionage.ch

c. Understanding Cybersecurity in the European Union.

1. The NIS 2 Directive - https://www.nis-2-directive.com

2. The European Cyber Resilience Act - https://www.european-cyber-resilience-act.com

3. The Digital Operational Resilience Act (DORA) - https://www.digital-operational-resilience-act.com

4. The Critical Entities Resilience Directive (CER) - https://www.critical-entities-resilience-directive.com

5. The Digital Services Act (DSA) - https://www.eu-digital-services-act.com

6. The Digital Markets Act (DMA) - https://www.eu-digital-markets-act.com

7. The European Health Data Space (EHDS) - https://www.european-health-data-space.com

8. The European Chips Act - https://www.european-chips-act.com

9. The European Data Act - https://www.eu-data-act.com

10. European Data Governance Act (DGA) - https://www.european-data-governance-act.com

11. The Artificial Intelligence Act - https://www.artificial-intelligence-act.com

12. The European ePrivacy Regulation - https://www.european-eprivacy-regulation.com

13. The European Cyber Defence Policy - https://www.european-cyber-defence-policy.com

14. The Strategic Compass of the European Union - https://www.strategic-compass-european-union.com

15. The EU Cyber Diplomacy Toolbox - https://www.cyber-diplomacy-toolbox.com

You may contact:

George Lekatis
General Manager, Cyber Risk GmbH
Dammstrasse 16, 8810 Horgen
Phone: +41 79 505 89 60
Email: george.lekatis@cyber-risk-gmbh.com
Web: www.cyber-risk-gmbh.com

Disclaimer

Despite the great care taken to prepare this newsletter, we cannot guarantee that all information is current or accurate. If errors are brought to our attention, we will try to correct them, and we will publish the correct information to the LinkedIn and Facebook pages of Cyber Risk GmbH.

Readers will make their own determination of how suitable the information is for their usage and intent. Cyber Risk GmbH expressly disclaims all warranties, either expressed or implied, including any implied warranty of fitness for a particular purpose, and neither assumes nor authorizes any other person to assume for it any liability in connection with the information or training programs provided.

Cyber Risk GmbH and its employees will not be liable for any loss or damages of any nature, either direct or indirect, arising from use of the information provided on this newsletter, or our web sites.

We are not responsible for opinions and information posted by others. The inclusion of links to other web sites does not necessarily imply a recommendation or endorsement of the views expressed within them. Links to other web sites are presented as a convenience to users. Cyber Risk GmbH does not accept any responsibility for the content, accuracy, reliability, or currency found on external web sites.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;

- should not be relied on in the particular context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the association has no control and for which the association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of interpretative;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts. It is our goal to minimize disruption caused by technical errors. However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

Readers that are interested in a specific topic covered in the newsletter, must download the official papers, must find more information, and must ask for legal and technical advice, before making any business decisions.

General Terms and Conditions for all visitors to the Cyber Risk GmbH websites, and all legal transactions made through the Cyber Risk GmbH websites (hereinafter "GTC"):
https://www.cyber-risk-gmbh.com/Impressum.html