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

February 2021, top cyber risk and compliance related local news stories and world events

Dear readers,

At its meeting on 3 February 2021, the Federal Council approved the 2020 Foreign Policy Report. The report provides an overview of the priorities of Swiss foreign policy in the past year, most of which was marked by the COVID-19 pandemic. Other priorities were European policy and the implementation of the Foreign Policy Strategy 2020–23.

The COVID-19 pandemic also left its mark on Swiss foreign policy last year. The FDFA made an important contribution to the federal government's crisis management: its repatriation operation (FlyingHome) was the largest in the country's history, bringing a total of 7,255 people back to Switzerland. Thanks to a rapid and extensive reprogramming of existing SDC programmes, Switzerland also made important contributions to international crisis management.

The pandemic also affected the country's relations with the rest of Europe. For example, COVID patients from France were brought to Switzerland in

the spring for treatment. Switzerland's inclusion in the EU's crisis response and the close coordination of its crisis measures with the EU were important factors in the fight against the pandemic. It demonstrated how important secure access to the single market is for Switzerland. The European policy objective of the Federal Council therefore remains unchanged: conclude an institutional agreement with the EU to further consolidate the bilateral approach.

Swiss candidacy for Security Council on track.

Switzerland's international contributions to peace and security remain in demand. In the year under review, Switzerland provided support for 17 peace processes and also supported peace efforts in Libya, Cameroon and Ukraine, among others. Work progressed on Switzerland's candidacy for a non-permanent seat on the UN Security Council for the 2023–24 period. The final phase was launched with a virtual event in New York and Bern. In addition, the Federal Council approved a report on possible forms of parliamentary involvement.

As an open, export-oriented economy, Switzerland is dependent on the rules-based international trading system, particularly in the current economic crisis. As the ability of international organisations to act is also under pressure in the economic sphere, in 2020 Switzerland – together with 22 other WTO members – agreed to a provisional appeals procedure in the WTO dispute settlement mechanism. Switzerland was thus able to help bring stability to trade and in 2020 was also able to participate for the first time as a full guest country in all the work of the G-20.

Strategies consolidate Swiss foreign policy.

With a view to implementing the Foreign Policy Strategy 2020–23, the Federal Council adopted several sub-strategies. These included strategies for international cooperation, digital foreign policy, communication abroad and the MENA region.

On 13 January 2021, the Federal Council also adopted a strategy for sub-Saharan Africa. Further strategies are in development, notably for China, the Americas, arms control and disarmament. These strategies will further strengthen the coherence of Switzerland's foreign policy.

Despite the ongoing pandemic, overall the Federal Council is on track to meet the objectives of its Foreign Policy Strategy 2020–23.

Fraudsters love COVID, and they have been quick to adapt well-known fraud schemes to target citizens, businesses, and public organizations.

Experienced fraudsters are taking advantage of a *surge in dating app users*.

Yes, dating apps have done remarkably well during the pandemic, and have reported an important increase in downloads and subscribers from pre-COVID-19 levels. Fraudsters have become more creative: We have, an interesting *investment fraud via dating apps*.

In the initial stages, a romance is established via a dating app. Once communication becomes regular and a certain level of trust is established, criminals share *investment tips* with their victims and encourage them to join a scheme. Victims download a trading app and open an account, buy various financial products, and work their way up a so-called investment chain, all under the watchful eye of their new "friend". They are made to believe they can reach Gold or VIP status.

As is often the case with such fraud schemes, everything is made to look legitimate. Screenshots are provided, domain names are similar to real websites, and customer service agents pretend to help victims choose the right products.

One day, however, all contact stops, and victims are locked out of the account. They are left confused, hurt, and worried that they will never see their money again.

You can read more at number 2 below.

Voltaire believed that we must judge a man by his questions rather than his answers. *Johann Wolfgang von Goethe* has said that ignorant men raise questions that wise men answered a thousand years ago. But today we very much appreciate some answers to very important questions regarding suspicious activity reports (SARs) and anti-money laundering (AML) considerations.

The Financial Crimes Enforcement Network (FinCEN), jointly with the Federal Reserve, the FDIC, the NCUA and the OCC, are issuing answers to frequently asked questions.

Is a financial institution required to file a SAR based solely on negative news?
No. The existence of negative news related to a customer or other activity at a financial institution does not by itself indicate that the criteria

requiring the filing of a SAR have been met and does not automatically require the filing of a SAR by a financial institution.

A financial institution may review media reports, news articles and/or other references to assist in its performance of customer due diligence, as well as its evaluation of any transactions or activity it considers unusual or potentially suspicious.

For example, negative news may cause a financial institution to review customer activity as well as other related information, such as that of third parties with transactions involving the customer's account.

As with other identified unusual or potentially suspicious activity, financial institutions should comply with applicable regulatory requirements and follow their established policies, procedures, and processes to determine the extent to which it investigates and evaluates negative news, in conjunction with its review of transactions occurring by, at, or through the institution, to determine if a SAR filing is required.

It is good to know. According to *Francis Bacon,* who questions much, shall learn much, and retain much. But sometimes we ask many questions, but we receive no official answers. Not this time.

You can read more at number 7 below. Welcome to the top 10 list.

Welcome to our monthly newsletter.

Best regards,

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

Cyber Risk GmbH, Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341

Number 1 (Page 8)

Cybersecurity to the Rescue: Pseudonymisation for Personal Data Protection

ENISA's new report explores pseudonymisation techniques and use cases for healthcare and information sharing in cybersecurity.

Number 2 (Page 11)

Experienced fraudsters are taking advantage of a surge in dating app users.

Investment fraud via dating apps

Number 3 (Page 13)

The sovereign-bank-corporate nexus – virtuous or vicious?

Isabel Schnabel, Member of the Executive Board of the European Central Bank, at the LSE conference on Financial Cycles, Risk, Macroeconomic Causes and Consequences, Frankfurt am Main.

Number 4 (Page 15)

Fake apps responsible for rise in attacks targeting remote devices

Number 5 (Page 16)

2020 REPORT ON CSIRT-LE COOPERATION
A study of the roles and synergies among selected EU Member States/EFTA countries

Number 6 (Page 18)

Adopting Encrypted DNS in Enterprise Environments

Number 7 (Page 21)

Answers to Frequently Asked Questions Regarding Suspicious Activity Reporting and Other Anti-Money Laundering Considerations

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency

Number 8 (Page 23)

FETT Bug Bounty Helps Strengthen SSITH Hardware Defenses

DARPA's first bug bounty proves SSITH processors can thwart sophisticated attacks

Number 9 (Page 26)

WORLD'S MOST DANGEROUS MALWARE EMOTET DISRUPTED THROUGH GLOBAL ACTION

Number 10 (Page 30)

Recommended Options for Improving the Built Environment for Post-Earthquake Reoccupancy and Functional Recovery Time

Number 11 (Page 33)

Department of Justice Launches Global Action Against NetWalker Ransomware

NetWalker Defendant Charged, Dark Web Resource Disabled, Nearly $500,000 Seized

Number 12 (Page 36)

CYBER DIPLOMACY: State Should Use Data and Evidence to Justify Its Proposal for a New Bureau of Cyberspace Security and Emerging Technologies

GAO@100 U.S. GOVERNMENT ACCOUNTABILITY OFFICE
A Century of Non-Partisan Fact-Based Work
441 G St. N.W.
Washington, DC 20548

Number 13 (Page 39)

News and updates from the Project Zero team at Google. posted By Samuel Groß, Project Zero

A Look at iMessage in iOS 14

Project Zero

Number 14 (Page 41)

Precious metal investments: all that glitters is not gold

BaFin Federal Financial Supervisory Authority

Number 15 (Page 44)

Interactive map of national financial education websites

eiopa
European Insurance and Occupational Pensions Authority

Number 16 (Page 46)

New prompts to help people consider before they share

By Gina Hernandez, Product Manager, Trust & Safety

TikTok

Number 1 (Page 12)

Cybersecurity to the Rescue: Pseudonymisation for Personal Data Protection

ENISA's new report explores pseudonymisation techniques and use cases for healthcare and information sharing in cybersecurity.

Pseudonymisation is an established and accepted data protection measure that has gained additional attention following the adoption of the General Data Protection Regulation (GDPR) where it is both specifically defined and many times referenced as a safeguard.

ENISA, in its prior work on this field, has explored the notion and scope of data pseudonymisation, while presenting some basic technical methods and examples to achieve pseudonymisation in practice.

In this new report, ENISA complements its past work by discussing advanced pseudonymisation techniques, as well as specific use cases from the specific sectors of healthcare and cybersecurity.

In particular, the report, building on the basic pseudonymisation techniques, examines advanced solutions for more complex scenarios that can be based on asymmetric encryption, ring signatures and group pseudonyms, chaining mode, pseudonyms based on multiple identifiers, pseudonyms with proof of knowledge and secure multi-party computation.

It then applies some of these techniques in the area of healthcare to discuss possible pseudonymisation options in different example cases, while also exploring the possible application of the data custodianship model.

Lastly, it examines the application of basic pseudonymisation techniques in common cybersecurity use cases, such as the use of telemetry and reputation systems.

Based on the analysis provided in the report, the following basic conclusions and recommendations for all relevant stakeholders are provided.

Defining the best possible technique

As it has been stressed also in past ENISA's reports, there is no fit-for-all pseudonymisation technique and a detailed analysis of the case in question is necessary in order to define the best possible option.

To do so, it is essential to take a critical to look into the semantics (the "full picture") before conducting data pseudonymisation.

In addition, pseudonymisation is only one possible technique and must be combined with a thorough security risk assessment for the protection of personal data.

Data controllers and processors should engage in data pseudonymisation, based on a security and data protection risk assessment and taking due account of the overall context and characteristics of personal data processing.

This may also comprise methods for data subjects to pseudonymise personal data on their side (e.g. before delivering data to the controller/processor) to increase control of their own personal data.

Regulators (e.g. Data Protection Authorities and the European Data Protection Board) should promote risk-based data pseudonymisation through the provision of relevant guidance and examples.

Advanced techniques for advanced scenarios

While the technical solution is a critical element for achieving proper pseudonymisation, one must not forget that the organisational model and its underlying structural architecture are also very important parameters of success.

Advanced techniques go together with advanced scenarios, such as the case of the data custodianship model.

Data controllers and processors should consider possible scenarios that can support advanced pseudonymisation techniques, based – among other – on the principle of data minimisation.

The research community should support data controllers and processors in identifying the necessary trust elements and guarantees for the advanced scenarios (e.g. data custodianship) to be functional in practice.

Regulators (e.g. Data Protection Authorities and the European Data Protection Board) should ensure that regulatory approaches, e.g. as regards new technologies and application sectors, take into account all possible entities and roles from the standpoint of data protection, while remaining technologically neutral.

Establishing the state-of-the-art

Although a lot of work is already in place, there is certainly more to be done in defining the state-of-the-art in data pseudonymisation.

To this end, research and application scenarios must go hand-in-hand, involving all relevant parties (researchers, industry, and regulators) to discuss joined approaches.

The European Commission, the relevant EU institutions, as well as Regulators (e.g. Data Protection Authorities and the European Data Protection Board) should support the establishment and maintenance of the state-of-the-art in pseudonymisation, bringing together all relevant stakeholders in the field (regulators, research community, and industry).

The research community should continue its efforts on advancing the existing work on data pseudonymisation, addressing special challenges appearing from emerging technologies, such as Artificial Intelligence.

The European Commission and the relevant EU institutions should support and disseminate these efforts.

Towards the broader adoption of data pseudonymisation

Recent developments, e.g. in international personal data transfers, show clearly the need to further advance appropriate safeguards for personal data protection.

This will only be intensified in the future by the use of emerging technologies and the need for open data access.

It is, thus, important to start today the discussion on the broader adoption of pseudonymisation in different application scenarios.

Regulators (e.g. Data Protection Authorities and the European Data Protection Board), the European Commission and the relevant EU institutions should disseminate the benefits of data pseudonymisation and provide for best practices in the field.

To read more: https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases

Number 2 (Page 12)

Experienced fraudsters are taking advantage of a surge in dating app users.

Investment fraud via dating apps

INTERPOL has issued a Purple Notice to its 194 member countries outlining a specific modus operandi on dating applications.

The threat involves taking advantage of people's vulnerabilities as they look for potential matches, and luring them into a sophisticated fraud scheme.

In the initial stages, an artificial romance is established via a dating app. Once communication becomes regular and a certain level of trust is established, criminals share investment tips with their victims and encourage them to join a scheme.

Victims download a trading app and open an account, buy various financial products and work their way up a so-called investment chain, all under the watchful eye of their new "friend". They are made to believe they can reach Gold or VIP status.

As is often the case with such fraud schemes, everything is made to look legitimate. Screenshots are provided, domain names are eerily similar to real websites, and customer service agents pretend to help victims choose the right products.

One day, however, all contact stops and victims are locked out of the account. They're left confused, hurt, and worried that they'll never see their money again.

INTERPOL's Financial Crimes unit has received reports from around the world of this scam and is encouraging dating app users to be vigilant, be skeptical and be safe when entering into online relationships.

This has become especially important as people turn to online interactions during the COVID-19 pandemic.

Here are some tips to make sure online dating remains fun and doesn't empty your bank account:

- Always be vigilant when you are approached by someone you don't know, especially if it leads to a request for money;

- Be skeptical: online investments with promises of fast, amazing returns are often too good to be true;

- Think twice before transferring money, however genuine the request might seem;

- Do your research: check reviews, double check the app, the domain name, the email address, etc;

- Don't disclose personal/confidential information;

If you realize you've been the victim of a fraud, report it.

Number 3 (Page 12)

The sovereign-bank-corporate nexus – virtuous or vicious?

Isabel Schnabel, Member of the Executive Board of the European Central Bank, at the LSE conference on Financial Cycles, Risk, Macroeconomic Causes and Consequences, Frankfurt am Main.

One year after the first cases were reported in Europe, the coronavirus (COVID-19) pandemic continues to take a tragic human toll and to pose enormous challenges to workers, firms, the financial system and policymakers in the euro area.

Without the forceful responses of fiscal, monetary and prudential authorities the economic and social costs of this crisis would have been significantly higher.

Governments, in particular, have stabilized aggregate demand and incomes by absorbing economic and financial risks of the private sector as the crisis unfolded.

Through the generous issuance of guarantee schemes, governments secured a continuous flow of credit to firms, which supported economic growth and protected financial stability.

Monetary policy has complemented these efforts by providing ample liquidity and restoring favourable financing conditions.

As a consequence, the policy response to the pandemic has visibly intensified the interdependencies between sovereigns, banks and firms. It has created a “sovereign-bank-corporate” nexus.

In my remarks today, I will argue that the extent to which such interdependencies may create challenges in the future depends, to a large extent, on the types of feedback loops they create.

Broad fiscal and monetary policy support today minimise the realisation of contingent liabilities in the future, and thus limit the scarring effects of the pandemic on the economy, creating a virtuous circle.

So, contrary to the vicious “sovereign-bank” nexus that plagued the euro area throughout most of the last decade, the current nexus, if managed

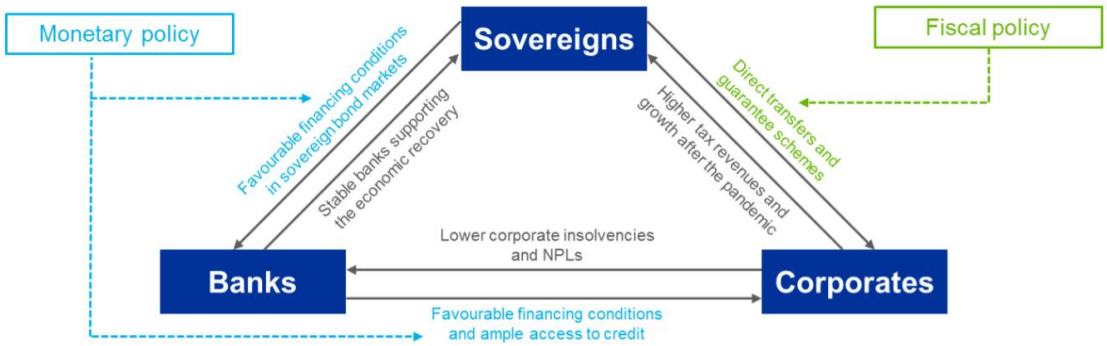
properly, can be an engine for a faster recovery, which also supports the ECB's price stability mandate.

A virtuous circle between sovereigns, banks and corporates

At the onset of the pandemic, the strict lockdown measures hit large parts of the corporate sector hard, raising its vulnerability to levels last seen during the global financial crisis (Chart 1).

Many firms saw their revenues collapse and were facing acute liquidity shortages that threatened to turn into solvency problems.

To read more: https://www.bis.org/review/r210129b.pdf



Source: ECB.

Number 4 (Page 12)

Fake apps responsible for rise in attacks targeting remote devices

The number of organisations experiencing malware attacks on remote devices has increased over the past year since the COVID-19 global pandemic began, which is detailed in a recent Cloud Security Report by Wandera. You may visit: https://www.wandera.com/cloud-security-report-2021eapvoeasdasdasdcaz/wandera-cloud-security-report-2021/

Some of the attacks on remote workers involved targeting victims by using phishing emails, which if clicked on, tricked victims into downloading malicious applications, reporting to be tools to help with 'improving productivity at home' but instead allowed attackers to gain access to corporate devices.

It was reported that around a third of the devices compromised in this type of attack, continued to access work email and around 10% continued to access cloud services, which could potentially give the attackers even more access to corporate networks. You may visit: https://www.zdnet.com/article/fake-collaboration-apps-are-stealing-data-as-staff-struggle-with-home-working-security/

The NCSC's home working and mitigating malware and ransomware guidance explains how organisations can protect themselves against cyber attacks whilst working online. You may visit: https://www.ncsc.gov.uk/guidance/home-working

https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

Number 5 (Page 12)

2020 REPORT ON CSIRT-LE COOPERATION
A study of the roles and synergies among selected EU Member States/EFTA countries

The purpose of this report is to further explore and support the cooperation between computer security incident response teams (CSIRTs), in particular national and governmental (n/g) CSIRTs, and law enforcement agencies (LEAs) and their interactions with the judiciary (prosecutors and judges).

This report follows a number of previous reports published by the European Union Agency for Cybersecurity (ENISA), including Tools and methodologies to support cooperation between CSIRTs and law enforcement (ENISA, 2017), Improving cooperation between CSIRTs and law enforcement: legal and organisational aspects, Cooperation between CSIRTs and Law Enforcement: interaction with the Judiciary (ENISA, 2017a), An Overview on Enhancing Technical Cooperation between CSIRTs and LE (ENISA, 2019a) and Roadmap of the cooperation between CSIRTs and LE (ENISA, 2019b).

This report proposes a methodology to analyse the legal and organisational framework, the roles and duties of CSIRTs, LEAs and the judiciary, and their required competences, as well as synergies and potential interferences in their activities related to their responses to cyber incidents and fight against cybercrime, respectively.

In addition, this report aims to present a detailed analysis focusing on some Member States (MSs) and European Free Trade Association (EFTA) countries, namely Czechia, France, Germany, Luxembourg, Norway, Portugal, Romania and Sweden.

The data for this report were collected via desk research and interviews with subject-matter experts.

The data collected showed, among other things, that:

- The communities make efforts to avoid interferences where possible and attempt to create effective partnerships and take advantage of their synergies to support each other in the fight against cybercrime; however, some interferences might occur during incident handling and cybercrime investigations.

- There are examples of joint training activities, mainly involving two communities (CSIRTs and LEAs or LEAs and the judiciary, especially prosecutors) and, more rarely, involving all three communities, in particular in the form of joint exercises. These joint training activities help enhance overall the competences required to respond to cybercrime.

- There has been no significant impact of the coronavirus disease 2019 (COVID-19) pandemic on cooperation and interaction between the three communities and their ability to function. In some instances, interaction among the communities has increased, with even daily interactions, to ensure that each community is kept up to date. As the COVID-19 pandemic has continued, the use of online tools to facilitate meetings and events has become the norm.

  This report, the 2020 handbook and the 2020 toolset on CSIRT and LE (law enforcement) cooperation (ENISA, 2021) are a set of deliverables complementing each other as follows:

- The report analyses roles, duties, competences, synergies and potential interferences across the three communities (CSIRTs, LE and judiciary).

- The handbook helps a trainer explain these concepts through scenarios.

- The toolset contains exercises for trainees based on these scenarios.

To read more: https://www.enisa.europa.eu/publications/2020-report-on-csirt-le-cooperation

Number 6 (Page 12)

Adopting Encrypted DNS in Enterprise Environments

Use of the Internet relies on translating domain names (like “nsa.gov”) to Internet Protocol addresses. This is the job of the Domain Name System (DNS).

In the past, DNS lookups were generally unencrypted, since they have to be handled by the network to direct traffic to the right locations.

DNS over Hypertext Transfer Protocol over Transport Layer Security (HTTPS), often referred to as DNS over HTTPS (DoH), encrypts DNS requests by using HTTPS to provide privacy, integrity, and “last mile” source authentication with a client’s DNS resolver.

It is useful to prevent eavesdropping and manipulation of DNS traffic.

While DoH can help protect the privacy of DNS requests and the integrity of responses, enterprises that use DoH will lose some of the control needed to govern DNS usage within their networks unless they allow only their chosen DoH resolver to be used.

Enterprise DNS controls can prevent numerous threat techniques used by cyber threat actors for initial access, command and control, and exfiltration.

Using DoH with external resolvers can be good for home or mobile users and networks that do not use DNS security controls.

For enterprise networks, however, NSA recommends using only designated enterprise DNS resolvers in order to properly leverage essential enterprise cybersecurity defenses, facilitate access to local network resources, and protect internal network information.

The enterprise DNS resolver may be either an enterprise-operated DNS server or an externally hosted service.

Either way, the enterprise resolver should support encrypted DNS requests, such as DoH, for local privacy and integrity protections, but all other encrypted DNS resolvers should be disabled and blocked.

However, if the enterprise DNS resolver does not support DoH, the enterprise DNS resolver should still be used and all encrypted DNS should be disabled and blocked until encrypted DNS capabilities can be fully integrated into the enterprise DNS infrastructure.

This guidance explains the purpose behind the DoH design and the importance of configuring enterprise networks appropriately to add benefits to, but not hinder, their DNS security controls.

The following recommendations will assist enterprise network owners and administrators to balance DNS privacy and governance.

What is DoH?

Domain Name System (DNS) over Hypertext Transfer Protocol over Transport Layer Security (HTTPS), often referred to as DNS over HTTPS (DoH), encrypts DNS requests to provide privacy, integrity, and "last mile" source authentication for DNS transactions with a client's DNS resolver.

It is useful to prevent eavesdropping and manipulation of DNS traffic (T1040, T1565.002).

While DoH can help protect the privacy of DNS requests and the integrity of responses, enterprises that use DoH will lose some of the control needed to govern DNS usage within their networks unless they allow only their designated DoH resolver to be used.

These essential protective DNS controls can prevent numerous threat techniques used for initial access, command and control, and exfiltration, such as phishing links to malicious domains, connections using dynamic name resolution, and commands hidden in DNS traffic (TA0001, TA0011, TA0010, T1566.002, T1568, T1071.004).

The enterprise DoH resolver may be either an enterprise-operated DNS server or an external resolver from a protective DNS provider.

However, if the enterprise DNS resolver does not support DoH, the enterprise resolver should still be used and all encrypted DNS should be disabled and blocked until encrypted DNS capabilities can be fully integrated into the enterprise DNS infrastructure.

How do DNS and DoH work?

DNS translates domain names to their corresponding Internet Protocol (IP) addresses, allowing web users to more easily access websites.

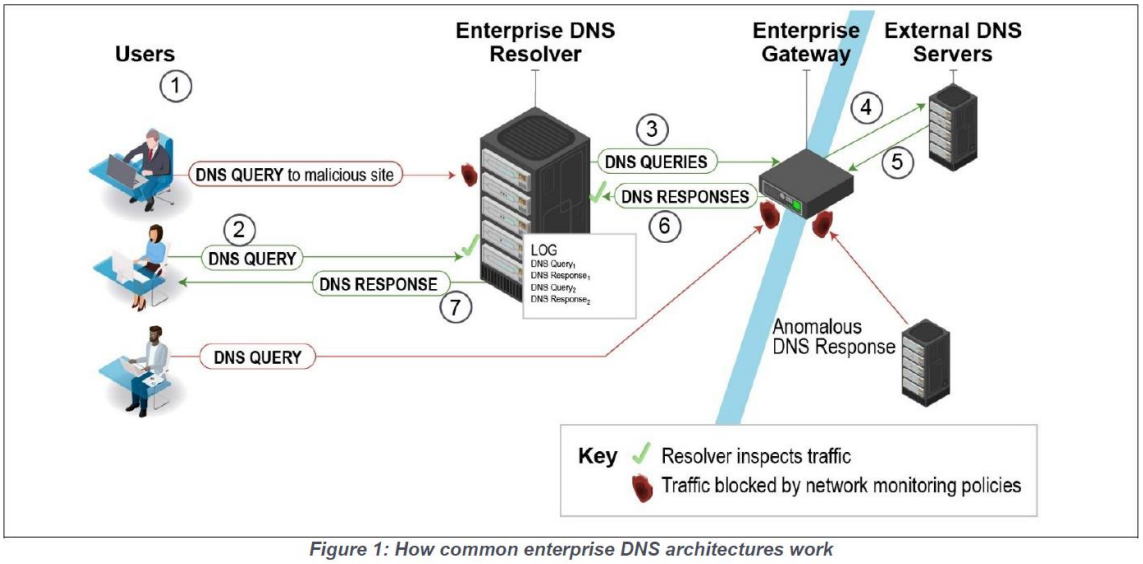


Figure 1: How common enterprise DNS architectures work

1. The user wants to visit a website they do not know is malicious and types the domain name into the web browser.
2. The request for the domain name is sent to the enterprise DNS resolver with a plaintext packet on port 53. Queries that violate DNS monitoring policies may generate alerts and/or be blocked.

With traditional enterprise DNS architectures, once a client submits a DNS query, it will first go to the enterprise recursive DNS resolver, often assigned via Dynamic Host Configuration Protocol (DHCP).

The enterprise DNS resolver will either return the answered query from its cache or forward the query through the enterprise gateway to the external authoritative DNS servers.

The DNS response will return through the enterprise gateway, to the enterprise DNS resolver, and then finally to the client.

During this exchange, both the enterprise DNS resolver and the enterprise gateway can see the plaintext query and response and log it for analysis or block it if it seems malicious or violates enterprise policies

To read more: https://media.defense.gov/2021/Jan/14/2002564889/-1/-1/0/CSI_ADOPTING_ENCRYPTED_DNS_U_OO_102904_21.PDF

Number 7 (Page 12)

Answers to Frequently Asked Questions Regarding Suspicious Activity Reporting and Other Anti-Money Laundering Considerations

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency

BOARD OF GOVERNORS
OF THE FEDERAL RESERVE SYSTEM
WASHINGTON, D.C. 20551

The Financial Crimes Enforcement Network (FinCEN), jointly with the Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), and the Office of the Comptroller of the Currency (OCC) (collectively, the Federal banking agencies), and in consultation with the staff of certain other federal functional regulators, is issuing answers to frequently asked questions (FAQs) regarding suspicious activity reports (SARs) and other anti-money laundering (AML) considerations for financial institutions covered by SAR rules.

The answers to these FAQs clarify the regulatory requirements related to SARs to assist such financial institutions with their compliance obligations, while enabling financial institutions to focus resources on activities that produce the greatest value to law enforcement agencies and other government users of Bank Secrecy Act (BSA) reporting.

The answers to these FAQs neither alter existing BSA/AML legal or regulatory requirements, nor establish new supervisory expectations; they were developed in response to recent Bank Secrecy Act Advisory Group (BSAAG) recommendations, as described in more detail in FinCEN's Advance Notice of Proposed Rulemaking (ANPRM) on Anti-Money Laundering Program Effectiveness, published in September 2020.

Question 1: Requests by Law Enforcement for Financial Institutions to Maintain Accounts

Can a financial institution maintain an account or customer relationship for which it has received a written "keep open" request from law enforcement, even though the financial institution has identified suspicious or potentially illicit activity?

Yes. Law enforcement may have an interest in ensuring that certain accounts and customer relationships remain open notwithstanding suspicious or potential criminal activity in connection with the account. A

financial institution may decide to maintain an account based on a written "keep open" request from a law enforcement agency, however, it is not obligated to do so.

The written request should be specific and indicate both that the law enforcement agency has requested that the financial institution maintain the account, as well as the purpose and duration of the request.

Keeping such an account open as requested may be highly useful to law enforcement and may further efforts to identify and combat money laundering, terrorist financing, and other illicit financial activities.

A financial institution should not be criticized solely for its decision to maintain an account relationship at the request of law enforcement or for its decision to close the account. Ultimately, the decision to maintain or close an account should be made by a financial institution in accordance with its own policies, procedures, and processes.

It may be useful for financial institutions to maintain documentation of "keep open" requests, including after a request has expired.

If financial institutions keep such an account open as requested by law enforcement, they are still required to comply with all applicable BSA requirements, including requirements to conduct ongoing risk-based monitoring, and as appropriate, file SARs, including continuing activity SARs consistent with FinCEN guidance.

To read more:
https://www.federalreserve.gov/supervisionreg/srletters/SR2102a1.pdf

Number 8 (Page 12)

FETT Bug Bounty Helps Strengthen SSITH Hardware Defenses

DARPA's first bug bounty proves SSITH processors can thwart sophisticated attacks

After three months of reviewing more than 13,000 hours of hacking exploits conducted by more than 580 cybersecurity researchers, DARPA today announced that its Finding Exploits to Thwart Tampering (FETT) Bug Bounty successfully proved the value of the secure hardware architectures developed under its System Security Integration Through Hardware and Firmware (SSITH) program while pinpointing critical areas to further harden defenses.

From July-October 2020, DARPA held its first ever bug bounty program – a crowdsourced, red team exercise used to evaluate and analyze a technology's defenses.

DARPA partnered with the Department of Defense's Defense Digital Service (DDS), a self-described SWAT team within the Department of Defense, and Synack, a crowdsourced security platform on this effort.

More than 980 SSITH processors were tested by Synack's existing community of researchers and 10 valid vulnerabilities were discovered across all of the secure architecture implementations.

FETT leveraged Synack's penetration testing process to conduct the bug bounty and facilitate communications about the discovered weaknesses.

FETT is part of the "Hack the Pentagon" crowdsourced digital defense program operated by DDS.

The SSITH program aims to develop security architectures and tools that protect electronic systems against common classes of hardware vulnerabilities exploited through software.

To help test and evaluate their research efforts, the teams working on SSITH integrated their novel hardware security protections into FPGA-based emulated systems with RISC-V processor cores.

Full software stacks were built on top of each system, which were populated with vulnerable applications that could be exploited on unprotected processors.

These emulated systems were then provided to the Synack Red Team (SRT) – the organization's cohort of security researchers – via Amazon Web Services (AWS) EC2 F1 cloud.

Once live, the SRT had several months to virtually access the secure processor technology and devise exploit mechanisms to challenge their defenses.

"Knowing that virtually no system is unhackable, we expected to discover bugs within the processors but FETT really showed us that the SSITH technologies are quite effective at protecting against classes of common software-based hardware exploits," said Keith Rebello, the DARPA program manager leading SSITH and FETT.

"The majority of the bug reports did not come from exploitation of the vulnerable software applications that we provided to the researchers, but rather from our challenge to the researchers to develop any application with a vulnerability that could be exploited in contradiction with the SSITH processors' security claims. We're clearly developing hardware defenses that are raising the bar for attackers."

FETT ran for three months and during that time only 10 vulnerabilities were disclosed by the SRT – seven were considered "critical" and three were considered "high" by Common Vulnerability Scoring System 3.0 standards.

A majority of the critical vulnerabilities identified during FETT resulted in weaknesses introduced by interactions between the SSITH hardware, SSITH firmware, and the operating system software.

This signals that there is an opportunity to investigate approaches for hardware/software co-design and verification approaches that span the hardware-firmware-software boundary to better secure the system.

During the course of the FETT bug bounty, four of the discovered vulnerabilities were patched and validated by the SRT. The SSITH research teams are expected to mitigate the remaining vulnerabilities during the third phase of the program, or outside of the funded effort.

"FETT challenged performers and greatly matured the architectures in development," noted Rebello. "Several of the research teams were driven to document the use and benefits of their security frameworks in a rigorous and understandable way, which will ultimately help third parties understand and adopt these secure processors for operational use. Further, the FETT bug reports provided actionable information that is helping to drive Phase 3 development on SSITH."

In addition to enhancing the effectiveness of the SSITH secure hardware architectures, a critical outcome of FETT was the development of a scalable, virtualized platform for remotely testing and evaluating secure processor prototypes.

The platform was developed by Galois and provides a means of virtually crowdsourcing the analysis of future processor technologies beyond SSITH and FETT. “To date, similar platforms have just focused on software code analysis and verification. What FETT has developed is first of its kind,” said Rebello.

The SSITH program is now in its third and final phase. Research teams are focused on further improving the performance of their technologies as they push for even greater security protections.

In the final phase of the program, researchers are expected to fabricate a silicon system-on-chip (SoC) and are working to apply SSITH security approaches to other instruction set architectures, such as ARM and x86.

Number 9 (Page 12)

WORLD'S MOST DANGEROUS MALWARE EMOTET DISRUPTED THROUGH GLOBAL ACTION

Law enforcement and judicial authorities worldwide have this week disrupted one of most significant botnets of the past decade: EMOTET. Investigators have now taken control of its infrastructure in an international coordinated action.

This operation is the result of a collaborative effort between authorities in the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada and Ukraine, with international activity coordinated by Europol and Eurojust. This operation was carried out in the framework of the European Multidisciplinary Platform Against Criminal Threats (EMPACT).

EMOTET has been one of the most professional and long lasting cybercrime services out there. First discovered as a banking Trojan in 2014, the malware evolved into the go-to solution for cybercriminals over the years.

The EMOTET infrastructure essentially acted as a primary door opener for computer systems on a global scale. Once this 26nauthorized access was established, these were sold to other top-level criminal groups to deploy further illicit activities such data theft and extortion through ransomware.

Spread via Word documents

The EMOTET group managed to take email as an attack vector to a next level. Through a fully automated process, EMOTET malware was delivered to the victims' computers via infected e-mail attachments.

A variety of different lures were used to trick unsuspecting users into opening these malicious attachments. In the past, EMOTET email campaigns have also been presented as invoices, shipping notices and information about COVID-19.

All these emails contained malicious Word documents, either attached to the email itself or downloadable by clicking on a link within the email itself. Once a user opened one of these documents, they could be prompted to "enable macros" so that the malicious code hidden in the Word file could run and install EMOTET malware on a victim's computer.

Attacks for hire

EMOTET was much more than just a malware. What made EMOTET so dangerous is that the malware was offered for hire to other cybercriminals to install other types of malware, such as banking Trojans or ransomwares, onto a victim's computer.

This type of attack is called a 'loader' operation, and EMOTET is said to be one of the biggest players in the cybercrime world as other malware operators like TrickBot and Ryuk have benefited from it.

Its unique way of infecting networks by spreading the threat laterally after gaining access to just a few devices in the network made it one of the most resilient malware in the wild.

Disruption of EMOTET's infrastructure

The infrastructure that was used by EMOTET involved several hundreds of servers located across the world, all of these having different functionalities in order to manage the computers of the infected victims, to spread to new ones, to serve other criminal groups, and to ultimately make the network more resilient against takedown attempts.

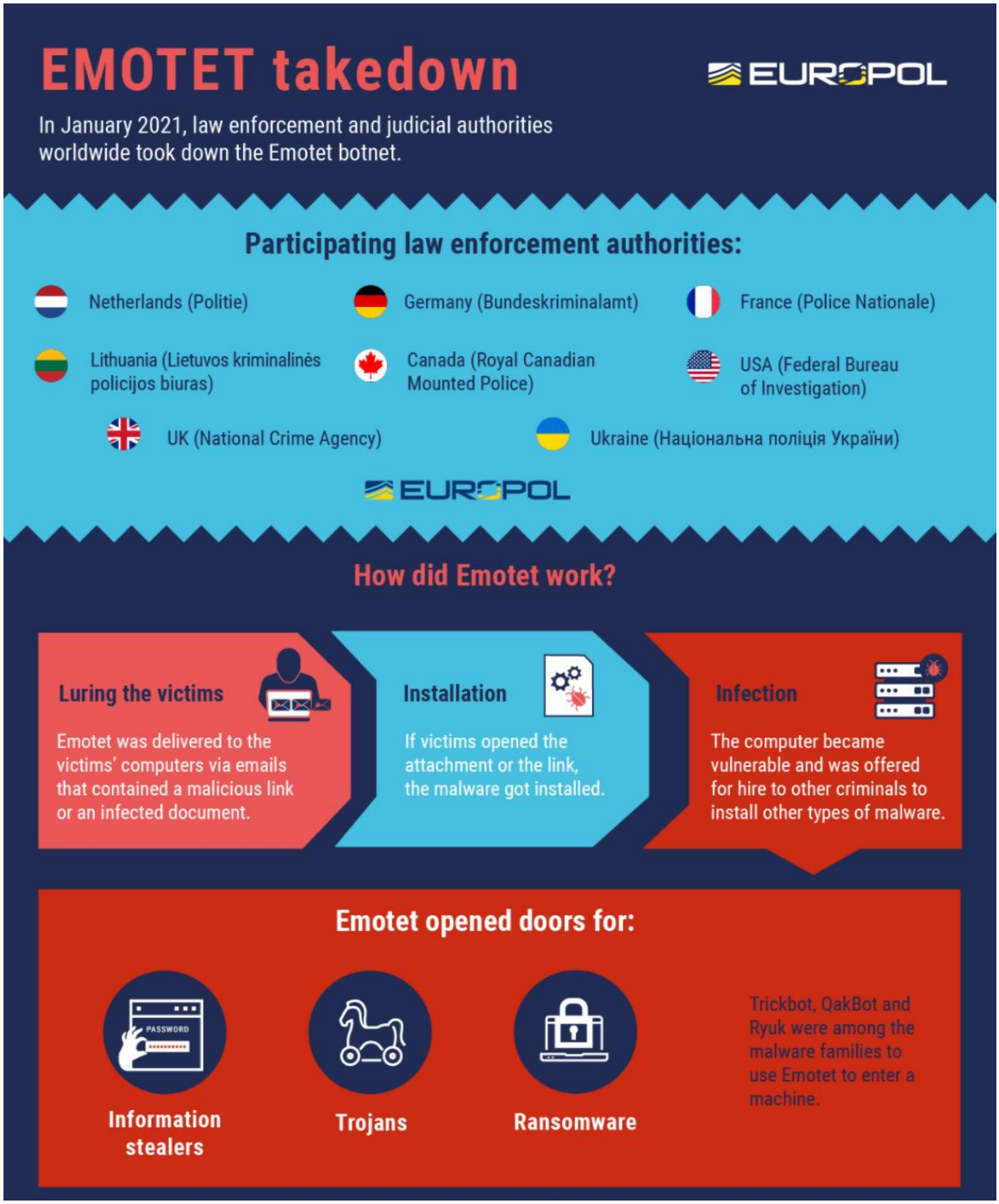
To severely disrupt the EMOTET infrastructure, law enforcement teamed up together to create an effective operational strategy. It resulted in this week's action whereby law enforcement and judicial authorities gained control of the infrastructure and took it down from the inside. The infected machines of victims have been redirected towards this law enforcement-controlled infrastructure. This is a unique and new approach to effectively disrupt the activities of the facilitators of cybercrime.

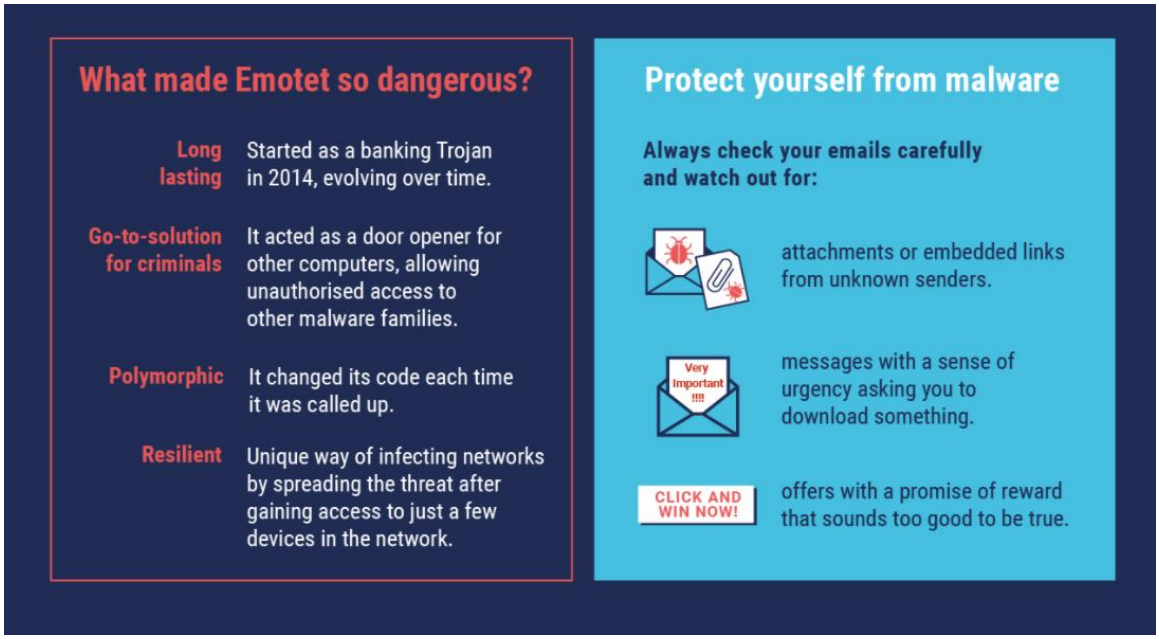
How to protect oneself against loaders

Many botnets like EMOTET are polymorphic in nature. This means that the malware changes its code each time it is called up. Since many antivirus programmes scan the computer for known malware codes, a code change may cause difficulties for its detection, allowing the infection to go initially undetected.

A combination of both updated cybersecurity tools (antivirus and operating systems) and cybersecurity awareness is essential to avoid falling victim to sophisticated botnets like EMOTET. Users should carefully check their email and avoid opening messages and especially attachments from unknown senders. If a message seems too good to be true, it likely is and emails that implore a sense of urgency should be avoided at all costs.

As part of the criminal investigation conducted by the Dutch National Police into EMOTET, a database containing e-mail addresses, usernames and passwords stolen by EMOTET was discovered. You can check if your e-mail address has been compromised. As part of the global remediation strategy, in order to initiate the notification of those affected and the cleaning up of the systems, information was distributed worldwide via the network of so-called Computer Emergency Response Teams (CERTs).




What made Emotet so dangerous?
Long lasting
Started as a banking Trojan in 2014, evolving over time.
Go-to-solution for criminals
It acted as a door opener for other computers, allowing unauthorised access to other malware families.
Polymorphic
It changed its code each time it was called up.
Resilient
Unique way of infecting networks by spreading the threat after gaining access to just a few devices in the network.
Protect yourself from malware
Always check your emails carefully and watch out for:
attachments or embedded links from unknown senders.
Very Important !!!!
messages with a sense of urgency asking you to download something.
CLICK AND WIN NOW!
offers with a promise of reward that sounds too good to be true.

Number 10 (Page 12)

Recommended Options for Improving the Built Environment for Post-Earthquake Reoccupancy and Functional Recovery Time

The most recent reauthorization of the National Earthquake Hazards Reduction Program (NEHRP), P.L. 115-307, includes a heightened focus on achieving community resilience and a new requirement for the National Institute of Standards and Technology (NIST) and the Federal Emergency Management Agency (FEMA) to jointly convene a Committee of Experts to assess and recommend options for improving the built environment and critical infrastructure to reflect performance goals stated in terms of post-earthquake reoccupancy and functional recovery time.

To comply with this mandate, NIST and FEMA developed a plan of action in which FEMA funded a Project Technical Panel, responsible for report development, and NIST funded a Project Review Panel, responsible for report review.

The Committee of Experts consisted of the Project Technical Panel, with 17 outside experts and representation from all interest groups named in the reauthorization, and the Project Review Panel, with 10 outside experts and similar representation.

To facilitate national-level stakeholder interaction, NIST hosted five stakeholder workshops that were used to gather additional information and feedback.

This report provides a set of options in the form of recommendations, tasks, and alternatives for improving the built environment, which have been developed and assessed by the Committee of Experts.

It describes community resilience, defines the concepts of reoccupancy and functional recovery, and explains the relationship among these three ideas.

It explains why reoccupancy and functional recovery concepts are needed, describes a target performance state, and identifies potential cost and benefits associated with implementing enhanced seismic design.

To fulfill the Congressional mandate, this report addresses the issue of functional recovery for seismic hazard.

Although this report does not discuss the unique challenges associated with improving functional recovery for other hazards, recommendations in this report could be leveraged and adapted for other natural hazards.

The motivation for this report is the risk that the United States faces each year from all forms of natural hazards, including hurricanes, floods, wildfires, and earthquakes.

Natural hazard events can affect communities through damage that results in injury and loss of life, interruption of lifeline services, displacement of residents and businesses, and economic and socio-cultural impacts.

Almost half of the U.S. population – 150 million people – reside in portions of 42 states that are at risk of experiencing a damaging earthquake within the next 50 years.

Earthquakes have caused disastrous impacts in the past and are expected to cause more in the future.

In regions of high seismic risk where an earthquake hasn't occurred for some time, scenario studies predict deaths in the thousands, injuries in the tens of thousands, and hundreds of billions of dollars in direct economic losses, along with long-term, destabilizing impacts to community function.

In all cases, whether historic or scenario-based, the loss of life and property, and the negative impacts to the economy, were a direct result of the inability of the built environment to withstand the effects of earthquakes and other natural hazards.

Because federal, state, and local, governments have critical functions in disaster recovery, they all can play an important role in facilitating the process to reduce the costs of recovery.

To protect U.S. communities and taxpayers against future losses on the scale of those experienced in Hurricane Katrina, or predicted in earthquake scenario studies, a change in building codes, building practices, and societal values is needed.

To support resilience goals at the community level, there is a need to establish a link between the design, construction, and retrofit of individual buildings and lifeline infrastructure systems, and community resilience, as measured by time to recovery of function; but this link is currently missing.

The concepts of reoccupancy and functional recovery have been introduced to serve as this link, defined as follows:

- Reoccupancy is a post-earthquake performance state in which a building is maintained, or restored, to allow safe re-entry for the purposes of providing shelter or protecting building contents.

- Functional recovery is a post-earthquake performance state in which a building or lifeline infrastructure system is maintained, or restored, to safely and adequately support the basic intended functions associated with the pre-earthquake use or occupancy of a building, or the pre-earthquake service level of a lifeline infrastructure system.

To read more:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1254.pdf

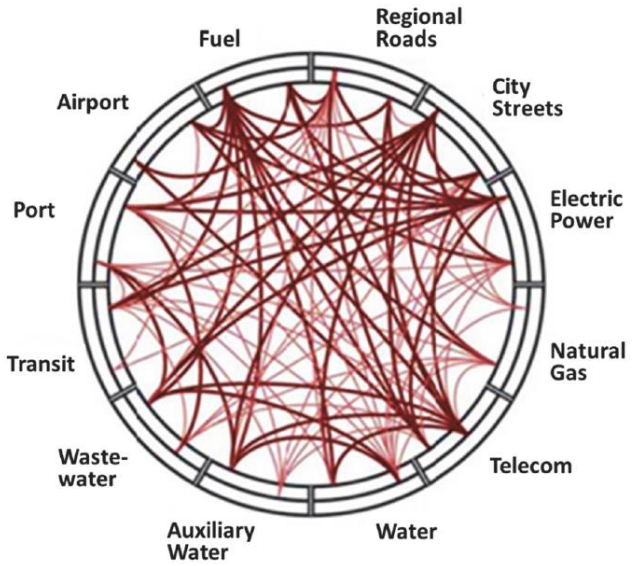


Figure 4-1 **Interdependencies of lifeline infrastructure systems in San Francisco (ABAG, 2014); connection points on the outer ring show which systems rely on the designated operator, and connection points on the inner ring show which systems the designated operator relies upon.**

Number 11 (Page 12)

Department of Justice Launches Global Action Against NetWalker Ransomware

NetWalker Defendant Charged, Dark Web Resource Disabled, Nearly $500,000 Seized

The Department of Justice today announced a coordinated international law enforcement action to disrupt a sophisticated form of ransomware known as NetWalker.

NetWalker ransomware has impacted numerous victims, including companies, municipalities, hospitals, law enforcement, emergency services, school districts, colleges, and universities.

Attacks have specifically targeted the healthcare sector during the COVID-19 pandemic, taking advantage of the global crisis to extort victims.

“We are striking back against the growing threat of ransomware by not only bringing criminal charges against the responsible actors, but also disrupting criminal online infrastructure and, wherever possible, recovering ransom payments extorted from victims,” said Acting Assistant Attorney General Nicholas L. McQuaid of the Justice Department’s Criminal Division. “Ransomware victims should know that coming forward to law enforcement as soon as possible after an attack can lead to significant results like those achieved in today’s multi-faceted operation.”

The NetWalker action includes charges against a Canadian national in relation to NetWalker ransomware attacks in which tens of millions of dollars were allegedly obtained, the seizure of approximately $454,530.19 in cryptocurrency from ransom payments, and the disablement of a dark web hidden resource used to communicate with NetWalker ransomware victims.

“This action reflects the resolve of the U.S. Attorney’s Office for the Middle District of Florida to target and disrupt sophisticated, international cybercrime schemes,” said U.S. Attorney Maria Chapa Lopez for the Middle District of Florida. “While these individuals believe they operate anonymously in the digital space, we have the skill and tenacity to identify

and prosecute these actors to the full extent of the law and seize their criminal proceeds."

According to court documents, NetWalker operates as a so-called ransomware-as-a-service model, featuring "developers" and "affiliates."

Developers are responsible for creating and updating the ransomware and making it available to affiliates. Affiliates are responsible for identifying and attacking high-value victims with the ransomware, according to the affidavit. After a victim pays, developers and affiliates split the ransom.

"This case illustrates the FBI's capabilities and global partnerships in tracking ransomware attackers, unmasking them, and holding them accountable for their alleged criminal actions," said Special Agent in Charge Michael F. McPherson of the FBI's Tampa Field Office. "If you are a victim of ransomware, contact your local FBI field office or submit a tip to tips.fbi.gov. You can also file a complaint with the FBI's Internet Crime Complaint Center at www.ic3.gov."

According to the affidavit, once a victim's computer network is compromised and data is encrypted, actors that deploy NetWalker deliver a file, or ransom note, to the victim. Using Tor, a computer network designed to facilitate anonymous communication over the internet, the victim is then provided with the amount of ransom demanded and instructions for payment.

Actors that deploy NetWalker commonly gain unauthorized access to a victim's computer network days or weeks prior to the delivery of the ransom note. During this time, they surreptitiously elevate their privileges

within the network while spreading the ransomware from workstation to workstation.

They then send the ransom note only once they are satisfied that they have sufficiently infiltrated the victim's network to extort payment, according to the affidavit.

According to an indictment unsealed today, Sebastien Vachon-Desjardins of Gatineau, a Canadian national, was charged in the Middle District of Florida. Vachon-Desjardins is alleged to have obtained at least over $27.6 million as a result of the offenses charged in the indictment.

The Justice Department further announced that on Jan. 10, law enforcement seized approximately $454,530.19 in cryptocurrency, which was comprised of ransom payments made by victims of three separate NetWalker ransomware attacks.

This week, authorities in Bulgaria also seized a dark web hidden resource used by NetWalker ransomware affiliates to provide payment instructions and communicate with victims.

Visitors to the resource will now find a seizure banner that notifies them that it has been seized by law enforcement authorities. The investigation was led by the FBI's Tampa field office.

Trial Attorneys S. Riane Harper and Brian Mund of the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorneys Carlton C. Gammons and Suzanne Nebesky of the U.S. Attorney's Office for the Middle District of Florida are prosecuting the case against Vachon-Desjardins.

Substantial assistance was provided by the Department of Justice's Office of International Affairs. Additionally, the Bulgarian National Investigation Service and General Directorate Combating Organized Crime provided substantial assistance in the seizure of the dark web hidden resource.

An indictment is merely an allegation. A defendant is presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

Number 12 (Page 12)

CYBER DIPLOMACY: State Should Use Data and Evidence to Justify Its Proposal for a New Bureau of Cyberspace Security and Emerging Technologies

GAO@100 U.S. GOVERNMENT ACCOUNTABILITY OFFICE
A Century of Non-Partisan Fact-Based Work
441 G St. N.W.
Washington, DC 20548

The United States and its allies are facing expanding foreign cyber threats, as international trade, communication, and critical infrastructure become increasingly dependent on cyberspace.

The United States also faces challenges to build consensus within international organizations on setting standards for how to govern the internet and cultivating norms for acceptable government behavior in cyberspace.

The Department of State (State) leads U.S. government international efforts to advance the full range of U.S. interests in cyberspace.

In January 2019, members of Congress introduced the Cyber Diplomacy Act of 2019, which would have established a new office to lead State's international cyberspace efforts that would consolidate cross-cutting efforts on international cybersecurity, digital economy, and internet freedom, among other cyber diplomacy issues.

In June 2019, State notified Congress of its intent to establish a new Bureau of Cyberspace Security and Emerging Technologies (CSET).

In contrast to the proposed legislation discussed above, State intended that its new bureau would focus more narrowly on cyberspace security and the security aspects of emerging technologies.

According to State officials, Members of Congress raised objections to State's plan.

On January 7, 2021, State announced that the Secretary had approved the creation of CSET and directed the department to move forward with establishing the bureau. However, as of the date of this report, State had not created CSET.

We reported in September 2020 that State did not involve federal agency partners in its plan to establish CSET. In the report, we recommended State involve federal agencies that contribute to cyber diplomacy to obtain their views and identify any risks, such as unnecessary fragmentation,

overlap, and duplication of efforts, as it implements its plan to establish CSET.

State did not agree with our recommendation, noting that it was unaware that these agencies had consulted with State before reorganizing their own cyberspace security capabilities and organizations.

We stand by the recommendation and maintain that it is important for State, as the leader of U.S. government international efforts to advance U.S. interests in cyberspace, to incorporate leading practices to ensure the successful implementation of its reorganization effort and to reduce the potential for any unwarranted overlap and duplication in its efforts.

You asked us to review State's efforts to advance U.S. interests in cyberspace. This report examines the extent to which State used data and evidence to develop and justify its proposal to establish CSET.

To address this objective, we interviewed State officials and reviewed documentation from State on its planning process for establishing the new bureau.

We assessed State's documentation against the key practice of using data and evidence in the development of the proposed agency reforms, drawn from our June 2018 report on government reorganization.

To address this practice, we analyzed State's activities leading to the development of the June 2019 Congressional Notification on its proposal for establishing CSET.

We also consulted our prior work on agencies' efforts to develop and use evidence to support their decision-making, which highlights decision makers' need for using evidence to help address pressing governance challenges faced by the federal government.

We conducted this performance audit from July 2019 to January 2021 in accordance with generally accepted government auditing standards.

Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives.

We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To read more: https://www.gao.gov/assets/720/712040.pdf

GAO@100 U.S. GOVERNMENT ACCOUNTABILITY OFFICE
A Century of Non-Partisan Fact-Based Work

441 G St. N.W.
Washington, DC 20548

January 28, 2021

The Honorable Gregory W. Meeks
Chairman
The Honorable Michael T. McCaul
Ranking Member
Committee on Foreign Affairs
House of Representatives

CYBER DIPLOMACY: State Should Use Data and Evidence to Justify Its Proposal for a New Bureau of Cyberspace Security and Emerging Technologies

Number 13 (Page 12)

News and updates from the Project Zero team at Google. posted By Samuel Groß, Project Zero

A Look at iMessage in iOS 14

Project Zero

Note: Formed in 2014, Project Zero is a team of security researchers at Google who study zero-day vulnerabilities in the hardware and software systems that are depended upon by users around the world.

Our mission is to make the discovery and exploitation of security vulnerabilities more difficult, and to significantly improve the safety and security of the Internet for everyone.

We perform vulnerability research on popular software like mobile operating systems, web browsers, and open source libraries.

We use the results from this research to patch serious security vulnerabilities, to improve our understanding of how exploit-based attacks work, and to drive long-term structural improvements to security.

On December 20, Citizenlab published “The Great iPwn”, detailing how “Journalists [were] Hacked with Suspected NSO Group iMessage ‘Zero-Click’ Exploit”.

Of particular interest is the following note: “We do not believe that [the exploit] works against iOS 14 and above, which includes new security protections".

Given that it is also now almost exactly one year ago since we published the Remote iPhone Exploitation blog post series, in which we described how an iMessage 0-click exploit can work in practice and gave a number of suggestions on how similar attacks could be prevented in the future, now seemed like a great time to dig into the security improvements in iOS 14 in more detail and explore how Apple has hardened their platform against 0-click attacks.

The content of this blog post is the result of a roughly one-week reverse engineering project, mostly performed on a M1 Mac Mini running macOS 11.1, with the results, where possible, verified to also apply to iOS 14.3, running on an iPhone XS. Due to the nature of this project and the limited timeframe, it is possible that I have missed some relevant changes or made mistakes interpreting some results.

Where possible, I've tried to describe the steps necessary to verify the presented results, and would appreciate any corrections or additions.

The blog post will start with an overview of the major changes Apple implemented in iOS 14 which affect the security of iMessage.

Afterwards, and mostly for the readers interested in the technical details, each of the major improvements is described in more detail while also providing a walkthrough of how it was reverse engineered.

At least for the technical details, it is recommended to briefly review the blog post series from last year for a basic introduction to iMessage and the exploitation techniques used to attack it.

To read more: https://googleprojectzero.blogspot.com/2021/01/a-look-at-imessage-in-ios-14.html

Number 14 (Page 12)

Precious metal investments: all that glitters is not gold

BaFin Federal Financial Supervisory Authority

Four in ten investors have either already invested in gold or other precious metals or could imagine doing so in future. However, investments in precious metals are risky and speculative.

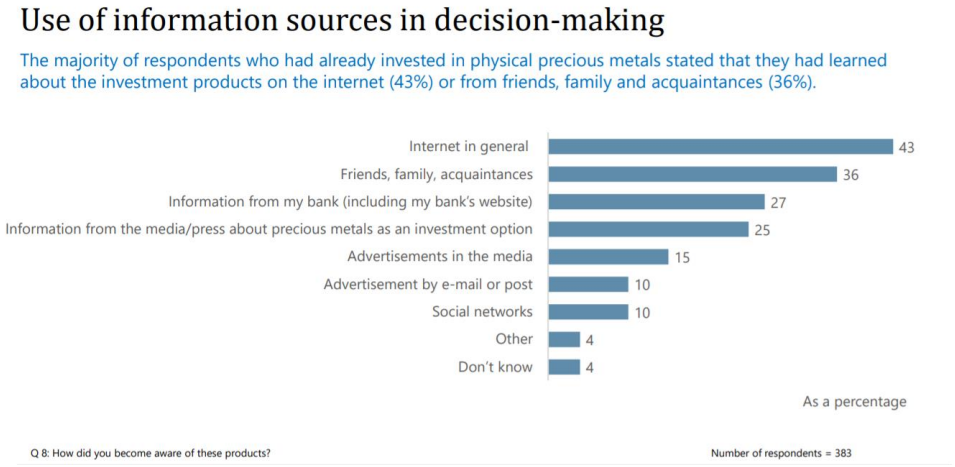
Gold glitters, and its reputation as a secure capital investment is equally dazzling.

There are two reasons for this: in a survey conducted on behalf of BaFin, 83% of those who had purchased or are considering purchasing precious metals believed this to be a secure investment. And in the current low interest rate environment, investments in gold, silver or platinum seem not only safe, but also lucrative. The risks and the costs of such investments are evidently being underestimated.

At a glance - Precious metals survey

In August 2020, on behalf of BaFin, the company OmniQuest Gesellschaft für Beratungsprojekte GmbH surveyed 1,000 consumers over the age of 18 that are resident in Germany about their attitudes towards physical precious metals as a capital investment.

The answers to the 18 questions included in the representative survey provided BaFin with insights into the form of investment favoured by investors, the sources of information they use most, their motivations for investing, and their views regarding the costs of purchasing precious metals.



To read more:
https://www.bafin.de/SharedDocs/Downloads/EN/dl_Edelmetallumfrage_2020_en.html;jsessionid=2F0DC3A4934AD2CE5981CE83AD429CE5.2_cid392?nn=8813520

Certain credit institutions and other providers use the positive properties customers associate with gold to advertise investments. The websites BaFin analysed alongside the precious metal study often claim that gold is timeless, crisis-proof and that its value is stable.

Where investors purchase precious metals

Of the 1,000 respondents, 259 had already purchased precious metals and 124 could imagine doing so in future.

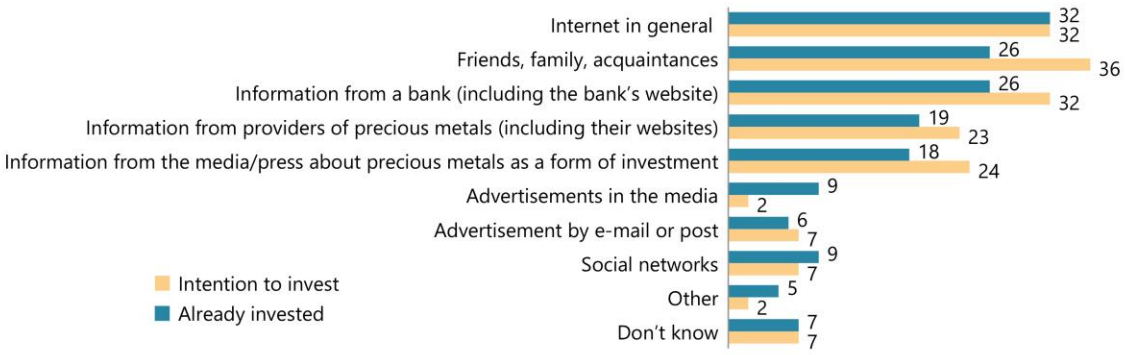
47% of investors purchased their precious metals from banks, whilst 53% used other providers.

63% of respondents who had purchased precious metals from a bank reported that their bank advisor had recommended the investment.

For 26%, information obtained from the bank was the most important factor in their decision to purchase precious metals. 32% of respondents who had not yet invested in precious metals but were interested in doing so in future believed information they received from their bank would influence their investment decision the most.

For investors, only other websites (32%) were reported as a more important source of information than banks.

Those interested in investing in future stated that information from friends, family and acquaintances would be most important (36%) (see Figure 1).



To read more:
https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2020/fa_bj_2012_Edelmetallumfrage_en.html

Number 15 (Page 12)

Interactive map of national financial education websites

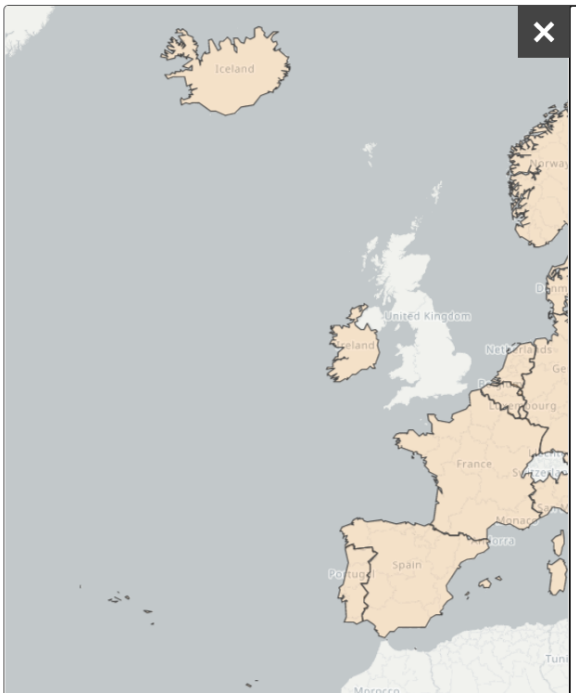
The European Insurance and Occupational Pensions Authority (EIOPA) launched today an interactive European map of national financial education websites.

The map is targeted to consumers who will have the opportunity to explore information about financial education in an interactive way.

The websites typically include practical information about insurance and pensions products, warnings about public scams and unauthorised practices, provide answers to frequently asked questions or contacts where consumers can turn to in case of complaints.

The interactive map will help consumers to learn about key concepts about insurance and pensions in different EU Member States. At the same time, it is an important step in promoting EIOPA's mandate in the area of financial education and literacy.

The map: https://www.eiopa.europa.eu/interactive-map_en



Germany

Financial education websites: BaFin information for consumers & Voice of Consumer

The Federal Financial Supervisory Authority (BaFin) which brings together under one roof the supervision of banks and financial services providers, insurance undertakings and securities trading has a dedicated comprehensible consumer portal on its website (https://www.bafin.de/EN/Verbraucher/verbraucher_node_e The specific area for consumers puts together a range of information specifically relevant for consumers. The information provided covers information regarding and supervisory activities relevant for consumers as well as information for financial education for example regarding products, investment advice. The area also holds a list of Q&As and links to more in-depth information for example through expert articles. Almost all information is available in German and English.

Number 16 (Page 12)

New prompts to help people consider before they share

By Gina Hernandez, Product Manager, Trust & Safety

TikTok

People come to TikTok to be creative, find community, and have fun. Being authentic is valued by our community, and we take the responsibility of helping counter inauthentic, misleading, or false content to heart.

We remove misinformation as we identify it, and in the UK we now partner with Logically, a technology company with one of the world's largest dedicated fact-checking teams, who are supporting our efforts to determine whether content shared on the platform is false, misleading or misinformation.

If fact checks confirm content to be false, we'll remove the video from our platform.

Sometimes fact checks are inconclusive or content is not able to be confirmed, especially during unfolding events.

In these cases, a video may become ineligible for recommendation into anyone's For You feed to limit the spread of potentially misleading information.

Today, we're taking that a step further to inform viewers when we identify a video with unsubstantiated content in an effort to reduce sharing.

Here's how it works: First, a viewer will see a banner on a video if the content has been reviewed but cannot be conclusively validated.

The video's creator will also be notified that their video was flagged as unsubstantiated content.

If a viewer attempts to share the flagged video, they'll see a prompt reminding them that the video has been flagged as unverified content.

This additional step requires a pause for people to consider their next move before they choose to "cancel" or "share anyway."

We love that our community's creativity encourages people to share TikTok videos with others who might enjoy them – both within our platform and beyond – but we've designed this feature to help our users be mindful about what they share.

In fact, when we tested this approach we saw viewers decrease the rate at which they shared videos by 24%, while likes on such unsubstantiated content also decreased by 7%.

This feature will be rolling out globally over the coming weeks, starting today in the US and Canada and reaching UK users from 22 February.

It was designed and tested with Irrational Labs, a behavioral science lab.

This is just the latest step we've taken to counter misinformation.

Last summer, we signed up to the EU Code of Practice on Disinformation, and throughout the Covid-19 global pandemic, we've ensured that our community has access to trustworthy and authoritative public health information.

We'll continue to invest in product features, partnerships and other strategies that help promote an authentic and welcoming community.

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.