June 2019, cyber risk and compliance in Switzerland

Top cyber risk and compliance related local news stories and world events

Dear readers,

According to the Reporting and Analysis Centre for Information Assurance (MELANI), *encryption trojans increasingly target corporate networks*.

We read: “Since the beginning of 2019, there is an increase of reports from SMEs and large companies in Switzerland and abroad which have been attacked by ransomware. In some cases, the attackers were able to encrypt the backup as well.

In the past, MELANI has consistently warned against ransomware and has already published recommendations in 2016.

Unfortunately, there are still cases where companies have completely lost their most valuable data because the chosen backup solution did not work or was not applied correctly and the attacker was able to delete or encrypt the backups.”

It is important to read MELANI’s recommendations:

“Due to the current situation, MELANI urgently warns Swiss companies against ransomware and recommends the following measures:

- Make regular backups of your data, for example on an external hard disk. Use a rotation scheme (grandfather-father-son [daily, weekly, monthly] / at least 2 generations). Make sure that you physically disconnect the backup media from the computer or network after the backup process. Otherwise, the attackers will also access the backup and encrypt or delete it.

- For cloud-based backup solutions, you should make sure that the provider has at least two generations analogue to the classic backup and that the backup is not accessible for a ransomware. It is

recommended to apply for example a two-factor authentication for critical operations.

- Operating systems and applications installed on computers and servers (e.g. Adobe Reader, Adobe Flash, Java etc.) must be consistently updated. If available, it is best to use the automatic update function.

- Protect resources which are accessible from the internet (for example Terminal-Server, RAS, VPN-Access) with a second factor.

- Block the receipt of dangerous email attachments at your email gateway. Detailed information you will find at the bottom of the following page: https://www.melani.admin.ch/against-ransomware"

To read more:
https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/verschluesselungstrojaner-greifen-vermehrt-gezielt-unternehmensn.html

---

This indictment is amazing. It could be used as training material. We read:

"In order to perpetrate the criminal scheme, the defendants utilized a network of co-conspirators who provided specialized technical skills and services used in furtherance of the conspiracy.

The specialized skills or services included, inter alia, the following:

1. Malware Developer: In the context of this Indictment, a "malware developer" was a conspirator involved in the creation, development, management, and leasing of malware for use by himself and/or others.

2. Crypter: In the context of this Indictment, a "crypter" was a conspirator involved in encrypting malware in such a way as to avoid detection by antivirus tools and software on victims' computers.

3. Spammer: In the context of this Indictment, a "spammer" was a conspirator involved in the mass distribution of malware through phishing emails.

The phishing emails were designed to appear legitimate to entice victim recipients into opening the emails and clicking on a link or attachment, which facilitated the downloading of malware onto the victims' computers.

4. Bulletproof Hoster: In the context of this Indictment, a "bulletproof hoster" was a conspirator involved in the hosting of malware campaigns on an intricate network of servers designed to thwart detection by law enforcement and cybersecurity researchers, thereby enabling the malware-related criminal activities to continue without disruption.

5. Casher / Account Takeover Specialist: In the context of this Indictment, a "casher" or "account takeover specialist' was a conspirator who used victims' stolen login credentials (obtained through GozNym malware infections) to access the victims' online bank accounts and steal, or attempt to steal, victims' funds through electronic funds transfers.

6. Cash-Out / Drop Master: In the context of this Indictment, a "cash-ouf' or "drop master" was a conspirator who provided "cashers / account takeover specialists" and other members of the conspiracy with access to bank accounts (also known as "drop accounts") to receive stolen funds in the form of electronic funds transfers from victims' online bank accounts.

"Drop masters" utilized money mules (also known as "drops") to open drop accounts, withdraw stolen fundi, or transfer stolen funds to other accounts for withdrawal."

Read more at Number 4 below.

I have just received a paper from the Irving Fisher Committee on Central Bank Statistics, IFC Bulletin No 50, *"The use of big data analytics and artificial intelligence in central banking"*. In 970 pages, there are many hidden gems.

At page 12, for example, we find an interesting approach from Okiriza Wibisono, Hidayah Dhini Ari, Anggraini Widjanarti, Alvin Andhika Zulen and Bruno Tissot:

"Another rapidly developing area of big data analytics is text-mining, ie analysis of semantic information – through the automated analysis of large quantities of natural language text and the detection of lexical or linguistic patterns with the aim of extracting useful insights.

While most empirical work in economics deals with numerical indicators, such as prices or sales data, a large and increasing amount of textual information is also generated by economic and financial activities – including internet-based activities (eg social media posts), but also the wider range of textual information provided by, say, company financial reports, media articles, public authorities' deliberations etc.

Analysing this unstructured information has become of key interest to policymakers, not least in view of the important role played by "soft" indicators such as confidence and expectations during the GFC.

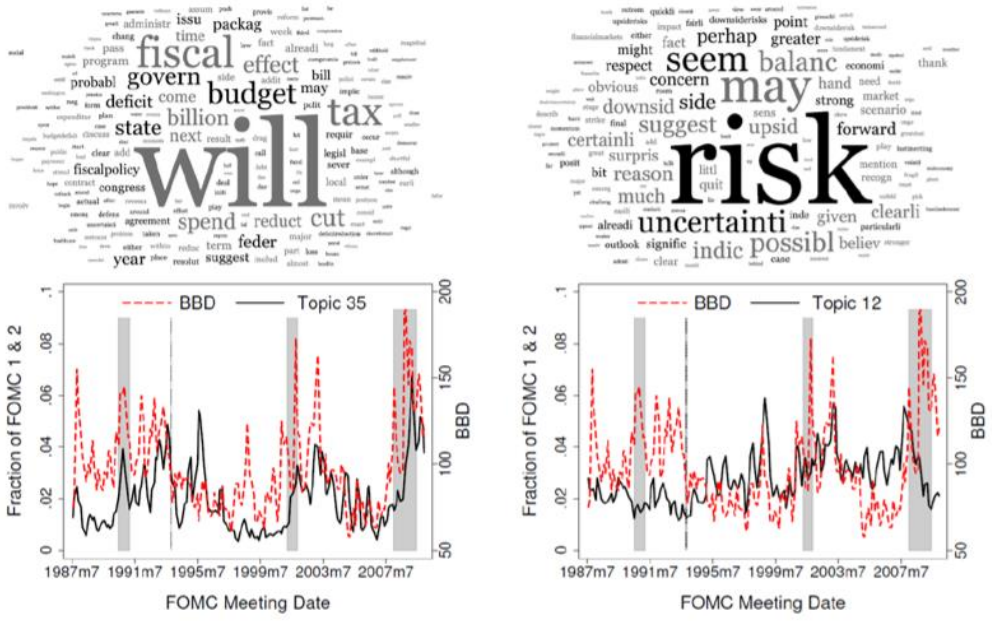
As illustrated in the lecture delivered by Stephen Hansen (University of Oxford), text-mining techniques can usefully be applied to dealing with these data in a structured, quantitative way.

Text analysis typically starts with some standard pre-processing steps, such as tokenisation (splitting text into words), stopword removal (discarding very frequent/non-topical words eg "a", "the", "to"), stemming or lemmatising (converting words into their root forms, for instance "prediction" and "predicted" into "predict"), and merging words within a common message (eg "Bank" and "Indonesia" grouped into "Bank Indonesia").

Once this is done, the initial document can be transformed into a document-term matrix, which indicates for each specific text a term's degree of appearance (or non-appearance).

This vectoral text representation is made of numerical values that can then be analysed by quantitative algorithms; for example, to measure the degree of similarity between documents by comparing the related matrixes (Graph 3).

Graph 3: Topic distributions obtained from text-mining techniques[11]



Source: Hansen (2018).

One popular algorithm for working on textual information is the Latent Dirichlet Allocation (LDA). This assumes that documents are distributed by topics, which in turn are distributed by keywords.

For example, one document may combine, for a respective 20% and 80%, a "monetary" and an "employment" topic, based on the number of words reflecting this topic distribution (ie 20% of them related to words such as "inflation" or "interest rate", and the remaining 80% related to words such as "jobs" and "labour").

Based on these calculations, one can build an indicator measuring how frequently a specific topic appears over time, for instance, to gauge the frequency of the messages related to "recession" – providing useful insights when monitoring the state of the economy.

Besides quantitative algorithms, simpler dictionary-based methods can be also employed for analysing text data. A set of keywords can be selected that are relevant to the topic of interest – for example, a keyword related to "business confidence".

Then an index can be constructed based on how frequently these selected keywords appear in a given document, allowing the subject indicator to be assessed (eg the evolution of business sentiment).

A prominent example is the Economic Policy Uncertainty (EPU), which quantifies the degree of uncertainty based on the appearance of a set of economic-, policy-, and uncertainty-related keywords in news articles; by the end of 2018, more than 20 country-specific EPU indexes had been compiled."

Read more at Number 10 below. Welcome to our monthly newsletter.

Best regards,

George Lekatis
General Manager, Cyber Risk GmbH
Rebackerstrasse 7, 8810 Horgen
Phone: +41 43 810 43 61
Mobile: +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

Our catalog, in-house instructor-led training in Switzerland, Liechtenstein and Germany:
https://www.cyber-risk-gmbh.com/Cyber_Risk_GmbH_Catalog_2019.pdf

Number 1 (Page 10)

A handful of cyber - five key issues for international cooperation

Agustín Carstens, General Manager of the BIS, at the conference on "Cybersecurity: coordinating efforts to protect the financial sector in the global economy", Paris.

Number 2 (Page 15)

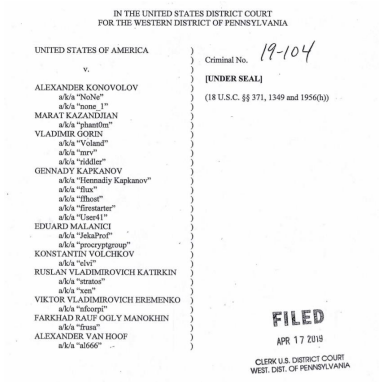
Flipboard
NOTICE OF SECURITY INCIDENT

Number 3 (Page 18)

Supplemental Tool: NPPD Resources to Support Vulnerability Assessments

Number 4 (Page 20)

Indictment



IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA
v.
ALEXANDER KONOVOLOV
a/k/a "NoNe"
a/k/a "none_1"
MARAT KAZANDJIAN
a/k/a "phant0m"
VLADIMIR GORIN
a/k/a "Voland"
a/k/a "mrv"
a/k/a "riddler"
GENNADY KAPKANOV
a/k/a "Hennadiy Kapkanov"
a/k/a "flux"
a/k/a "ffhost"
a/k/a "firestarter"
a/k/a "User41"
EDUARD MALANICI
a/k/a "JekaProf"
a/k/a "procryptgroup"
KONSTANTIN VOLCHKOV
a/k/a "slvt"
RUSLAN VLADIMIROVICH KATIRKIN
a/k/a "stratos"
a/k/a "tsm"
VIKTOR VLADIMIROVICH EREMENKO
a/k/a "nfcorpi"
FARKHAD RAUF OGLY MANOKHIN
a/k/a "frusa"
ALEXANDER VAN HOOF
a/k/a "al666"

Criminal No. 19-104
[UNDER SEAL]
(18 U.S.C. §§ 371, 1349 and 1956(h))

FILED
APR 17 2019
CLERK U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

Number 5 (Page 22)

INDUSTRY 4.0 CYBERSECURITY: CHALLENGES & RECOMMENDATIONS

Number 6 (Page 24)

Cyber Incident Response and Recovery: Progress Report to the G20 Finance Ministers and Central Bank Governors

Number 7 (Page 26)

Trends in international law for cyberspace

Number 8 (Page 28)

Our ongoing work to tackle hate

Number 9 (Page 31)

Modelling the Cognitive Work of Cyber Protection Teams

Colonel Stoney Trent, Dr. Robert R. Hoffman, Lieutenant Colonel David Merritt, Captain Sarah Smith

VOLUME 4 • NUMBER 1 SPRING 2019

THE CYBER DEFENSE REVIEW

Number 10 (Page 34)

Irving Fisher Committee on Central Bank Statistics, IFC Bulletin No 50

The use of big data analytics and artificial intelligence in central banking

Proceedings of the IFC – Bank Indonesia International Workshop and Seminar in Bali, May 2019

BIS

Number 11 (Page 36)

PATCH REMOTE DESKTOP SERVICES ON LEGACY VERSIONS OF WINDOWS

NATIONAL SECURITY AGENCY
CYBERSECURITY ADVISORY

Number 12 (Page 38)

NIST Infrared Frequency Comb Measures Biological Signatures

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

Number 13 (Page 40)

THE MISADVENTURES OF CYBER SAM

DoD CYBER EXCHANGE PUBLIC

Number 14 (Page 41)

Unsecured database exposes security logs of major hotel chains

National Cyber Security Centre

Number 15 (Page 42)

Dropping the password expiration policies

Microsoft | TechNet

Number 1

A handful of cyber - five key issues for international cooperation

Agustín Carstens, General Manager of the BIS, at the conference on "Cybersecurity: coordinating efforts to protect the financial sector in the global economy", Paris.

Introduction

Many thanks for inviting me to speak here today.

Cyber security is in the minds of all of us in the central banking community, and international cooperation is of the essence. As many of you here know, part of the BIS's mission is to foster international cooperation in serving central banks in their pursuit of monetary and financial stability.

Cyber security is a more recent concern for the BIS. However, as it has become increasingly important, our contribution to the central banking community's efforts has also grown.

We have convened many discussions with experts from the public and private sector and academia.

Cooperation is of course not an end in itself: the ultimate aim is to be better prepared for cyber attacks. I want to put five points on the table today.

Criminals are coordinating

First, criminals are mastering the art of international cooperation. Hacktivists, cyber criminals and nation states are coordinating with one another. This coordination is sophisticated and market-based. We have before us a very skilled set of adversaries.

Recent high-profile attacks have shown that attackers are also active in reconnaissance. They gather up seemingly harmless information (such as the online social media profiles of firms' staff) to better plan and execute attacks.

Moreover, sophisticated hacking tools can be acquired on the black market at low cost, lowering the level of technical skills required by criminal organisations.

This black market, together with the coordination it enables, is international. It brings together cyber criminals and nation states to execute targeted attacks for financial gain. If cyber criminals are embracing the benefits of cooperation, we need to embrace it as well.

International law is not up to speed

Second, international legal arrangements are not up to speed. Detecting criminal activity is not easy, and tracing it back to where it came from is even more difficult. Yet, even if a suspected criminal can be identified, international law may not support any action against them.

The current international legal framework for cooperation on cyber crime is fragmented.

Hacking is not necessarily a crime, for example. Differing domestic laws and regulations, uncertainty in establishing which jurisdictions are responsible for what, and ambiguity regarding evidential standards are a significant hurdle.

Harmonisation of laws defining criminal behaviour could help here, but laws are not enough on their own.

We also need international cooperation among the investigatory agencies. This cooperation would help prevent delays and loss of evidence. Only with cross-border cooperation is it possible to catch cross-border criminals.

There are a number of workstreams currently under way to address this and improve investigation and prosecutions between domestic authorities.

One example is the Council of Europe's Convention on Cybercrime - the Budapest Convention.

However, it is likely to be some time before current laws catch up with the internet age.

This makes adequate defences an even greater imperative.

If there is limited risk of being stopped by authorities, then preventing criminals from stealing is the most effective deterrent.

Compliance is not security

Third, compliance is not security. The standard-setting bodies are prioritising cyber. The Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions led the way with their cyber guidance some years ago; the Basel Committee on Banking Supervision (BCBS) recently published a report on a range of cyber resilience practices; and the Financial Stability Board is currently also working on aspects of resilience and recovery.

Supplementing this work, there are a number of best practice cyber resilience frameworks available, including ISO27000 and the NIST framework.

However, "compliance" is different for cyber. Getting the basics right makes a significant difference. An accurate IT inventory and a strong patching process are the cornerstones of any defence. "Basic" does not imply that this is an easy or simple task. The complexity and diversity of most modern networks create significant challenges.

However, at the same time, most of the organisations that have experienced highly publicised breaches were in compliance with some form of control framework. So while compliance is clearly necessary, it is not sufficient for security. Even with every box ticked, an organisation can still be vulnerable. A list of controls simply cannot keep pace with threat developments.

An organisation needs a "cultural shift", driven by a strong governance framework that learns and evolves, to go beyond compliance. An example of this is a cyber security department's engagement with the other staff in an organisation.

Users need to be part of the security of an organisation. To achieve this, organisations need to innovate in how they communicate and engage with staff to make them feel like they are the ones tasked with defending their organisation - not that it is someone else's responsibility to do so on their behalf.

For defence, bigger is better

Fourth, to be effective, cyber defence needs scale and it needs to cross borders. The threats we face are international and the financial system we defend is global, and interconnected. We need to cooperate.

One aspect of cooperation is sharing information on threats and incidents. Beyond vulnerabilities, we all have an interest in broad cooperation in this

area. Progress is reportedly being made. A BCBS survey found that 75% of banks have mandatory or voluntary cyber risk information-sharing arrangements in place. However, only 30% of their regulators had equivalent arrangements. We need to do more.

Another cooperative aspect is in the services, tools and software provided for cyber security. We cannot all be the best at everything. Even larger international companies can struggle to do everything themselves. We need to learn from one another, and we need to know who we can trust to provide services for us. The current pool of service providers is international.

Sophisticated IT or security companies do not operate purely domestically, even in the largest countries. Yet the accreditation schemes to help guide people towards the best service are currently domestic. Extending the schemes currently provided by some national governments or agencies internationally could help.

It is also worth noting that economies of scale in this area are not a one-way street. There are challenges to putting all our eggs in one basket. For example, while cloud computing may bring significant efficiency and security benefits, we need to cooperate to ensure that arrangements are safe.

Cyber is not going away

Finally, cyber risk is here to stay. Many risks can be tied to an economic or business cycle, but cyber is not one of them. It will not disappear overnight or be "solved". Therefore we can engage in some longer-term thinking about how to tackle it, and plan for the future.

Central banks realise this, and also appreciate that we need more technical cyber expertise. Yet cyber experts are hard to find and, once hired, they need to keep up to date.

Significant training and experience are required to transform new recruits into cyber security professionals.

However, this is not a new problem. We had a similar issue with bank supervisors, which was one of the driving factors behind setting up the Financial Stability Institute at the BIS, which celebrated its 20th anniversary last year.

Now that we are in a similar situation, the BIS is again helping to coordinate international central bank efforts to train and develop the next generation of central bank staff.

Concluding thought

I close with this thought: Coordinating our efforts is important, but we cannot coordinate work that is not shared. There can be no sharing without trust. That is why central banks - institutions that are experts in trust - have such a vital role to play in bringing people together. Many thanks to our hosts, the Bank of France, who are demonstrating this today.

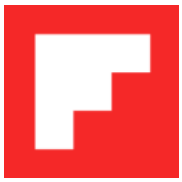
The Convention on Cybercrime of the Council of Europe (CETS No.185), known as the Budapest Convention:
https://www.coe.int/en/web/cybercrime/the-budapest-convention

To read more:
https://www.bis.org/cpmi/publ/d146.htm

https://www.bis.org/bcbs/publ/d454.htm

Number 2

Flipboard
NOTICE OF SECURITY INCIDENT



Flipboard recently identified and addressed a security incident involving a subset of user data. We know transparency is important to our community, and we have created this page to share what we have learned from our investigation, measures we have taken, and what steps users can take in response.

What happened

We recently identified unauthorized access to some of our databases containing certain Flipboard users' account information, including account credentials. In response to this discovery, we immediately launched an investigation and an external security firm was engaged to assist.

Findings from the investigation indicate an unauthorized person accessed and potentially obtained copies of certain databases containing Flipboard user information between June 2, 2018 and March 23, 2019 and April 21 – 22, 2019.

What information was involved

The databases involved contained some of our users' account information, including name, Flipboard username, cryptographically protected password and email address.

Flipboard has always cryptographically protected passwords using a technique known by security experts as "salted hashing".

The benefit of hashing passwords is that we never need to store the passwords in plain text. Moreover, using a unique salt for each password in combination with the hashing algorithms makes it very difficult and requires significant computer resources to crack these passwords.

If users created or changed their password after March 14, 2012, it is hashed with a function called bcrypt. If users have not changed their password since then, it is uniquely salted and hashed with SHA-1.

Additionally, if users connected their Flipboard account to a third-party account, including social media accounts, then the databases may have contained digital tokens used to connect their Flipboard account to that third-party account.

We have not found any evidence the unauthorized person accessed third-party account(s) connected to users' Flipboard accounts. As a precaution, we have replaced or deleted all digital tokens.

Importantly, we do not collect from users, and this incident did not involve, Social Security numbers or other government-issued IDs, bank account, credit card, or other financial information.

What we are doing

As a precaution, we have reset all users' passwords, even though the passwords were cryptographically protected and not all users' account information was involved. You can continue to use Flipboard on devices from which you are already logged in.

When you access your Flipboard account from a new device, or the next time you log into Flipboard after logging out of your account, you will be asked to create a new password.

As another precautionary step, we disconnected tokens used to connect to all third-party accounts, and in collaboration with our partners, we replaced all digital tokens or deleted them where applicable.

Additionally, to help prevent something like this from happening in the future, we implemented enhanced security measures and continue to look for additional ways to strengthen the security of our systems. We also notified law enforcement.

What you can do

You can continue to use Flipboard without further action. However, next time you log into your account, you will notice your Flipboard account password needs to be updated.

You will find instructions on our support page (linked below) explaining how to create a new password.

Also, if you use the same username and password you created for Flipboard for any other online service, we recommend you change your password there, too.

If you connected your Flipboard account to a third-party account to see its content, you may notice in some cases that you need to reconnect it. On our support page you will also find instructions for how to do this.

To learn more: https://about.flipboard.com/support-information-incident-May-2019/

Number 3

Supplemental Tool: NPPD Resources to Support Vulnerability Assessments

NPPD Resources to Support Vulnerability Assessments

Assessing vulnerabilities of critical infrastructure is an important step in developing security solutions and managing critical infrastructure risk.

The Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD) works with owners and operators to conduct vulnerability assessments of select critical infrastructure to inform its internal risk management processes and provide technical assistance to its State, local, tribal, and territorial (SLTT) and private sector partners to enable their own risk assessments and security plans.

NPPD provides additional resources, typically in the form of informational material on known vulnerabilities, to help owners and operators understand vulnerabilities at a more general level.

The Homeland Security Act of 2002 and Presidential Policy Directive 21 (PPD-21) direct the DHS Secretary to conduct comprehensive assessments of the vulnerabilities of the Nation's critical infrastructure, in coordination with the Sector-Specific Agencies (SSAs) and in collaboration with SLTT entities and critical infrastructure owners and operators.

This supplement provides information on Federal resources that are used by DHS and available to SLTT governments and critical infrastructure owners and operators to identify and assess critical infrastructure vulnerabilities.

Cyber Resilience Review (CRR)

The DHS Office of Cybersecurity and Communications conducts voluntary assessments to help evaluate and enhance cybersecurity capacities and capabilities within the critical infrastructure sectors and SLTT governments through its CRR process.

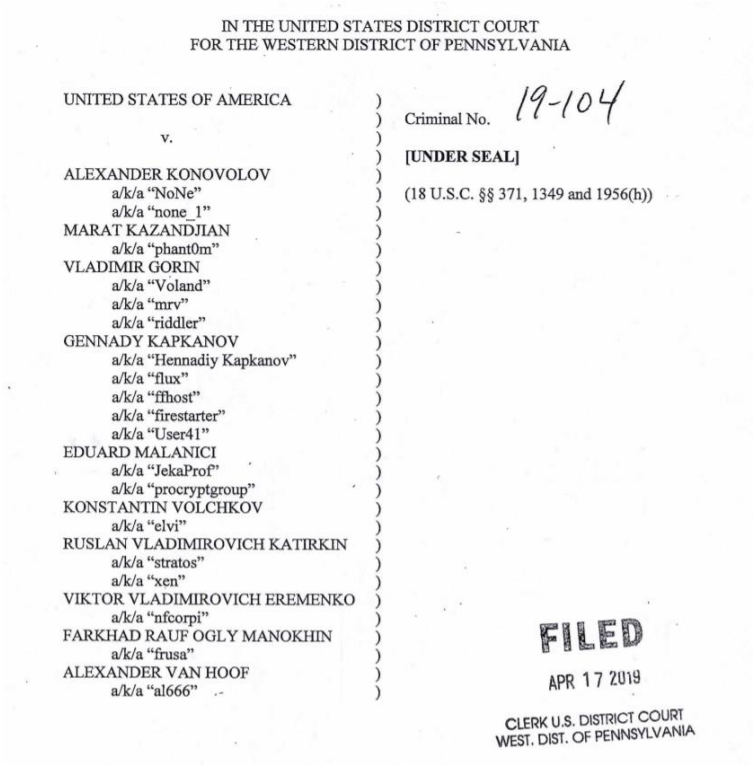
The goal of the CRR is to understand and measure key cybersecurity capabilities and provide meaningful maturity indicators of an organization's operational resilience and ability to manage cyber risk to its critical services during normal operations and times of

operational stress and crisis.

To read more:
https://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-NPPD-Resources-to-Support-VAs-508.pdf

Number 4

Indictment



IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA)
v.)
ALEXANDER KONOVOLOV)
a/k/a "NoNe")
a/k/a "none_1")
MARAT KAZANDJIAN)
a/k/a "phant0m")
VLADIMIR GORIN)
a/k/a "Voland")
a/k/a "mrv")
a/k/a "riddler")
GENNADY KAPKANOV)
a/k/a "Hennadiy Kapkanov")
a/k/a "flux")
a/k/a "ffhost")
a/k/a "firestarter")
a/k/a "User41")
EDUARD MALANICI)
a/k/a "JekaProf")
a/k/a "procryptgroup")
KONSTANTIN VOLCHKOV)
a/k/a "elvi")
RUSLAN VLADIMIROVICH KATIRKIN)
a/k/a "stratos")
a/k/a "xen")
VIKTOR VLADIMIROVICH EREMENKO)
a/k/a "nfcorpi")
FARKHAD RAUF OGLY MANOKHIN)
a/k/a "frusa")
ALEXANDER VAN HOOF)
a/k/a "al666")

Criminal No. 19-104

[UNDER SEAL]

(18 U.S.C. §§ 371, 1349 and 1956(h))

FILED
APR 17 2019
CLERK U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

The objectives of the conspiracy included:

(a) infecting victims' computers with GozNym malware designed to capture victims' online banking login credentials;

(b) using the captured login credentials to gain unauthorized access to victims' online bank accounts at U.S. financial institutions; and

(c) stealing funds from victims' U.S. bank accounts and laundering those funds using U.S. and foreign beneficiary bank accounts provided and controlled by conspirators.

Manner and Means of the Conspiracy

The manner and means used to accomplish the objectives of the conspiracy are set forth in paragraphs 28 through 55 of this Indictment.

In order to infect victims' computer with GozNym malware, the defendants and conspirators known and unknown to the grand jury crafted and transmitted through the Internet in interstate and foreign commerce phishing emails containing malicious hyperlinks or attachments which, when clicked, downloaded GozNym malware onto victims' computers without the victims' knowledge or consent.

The phishing emails were falsely designed to appear as legitimate business emails from companies and fir1anqial institutions in order to deceive victim recipients into opening the emails.

The malicious hyperlinks and attachments were falsely represented to be legitimate links and attachments, such as business invoices, in order to fraudulently entice the victim recipients to click on them. GozNym malware captured the victims' online banking login credentials.

To read more:
https://www.justice.gov/file/1163056/download?utm_medium=email&utm_source=govdelivery

Number 5

INDUSTRY 4.0 CYBERSECURITY: CHALLENGES & RECOMMENDATIONS

The ENISA study on "Good Practices for Security of IoT in the context of Smart Manufacturing" focuses on addressing the security and privacy challenges related to the evolution of industrial systems and services precipitated by the introduction of IoT innovations.

The main objectives are to collect good practices to ensure security of IoT in the context of Industry 4.0/Smart Manufacturing, while mapping the relevant security and privacy challenges, threats, risks and attack scenarios.

Building on this work, this document provides the results of a gap analysis conducted in order to identify main challenges to the adoption of the security measures and security of Industry 4.0 and Industrial IoT.

Moreover, ENISA lists high-level recommendations to different stakeholder groups in order to promote Industry 4.0 cybersecurity and facilitate wider take-up of relevant innovations in a secure manner.

The adoption of the high-level recommendations proposed by ENISA aims at contributing to the enhancement of Industry 4.0 cybersecurity across the European Union and at laying the foundations of the relevant forthcoming work, as well as at serving as a basis for future developments.

In this short paper, ENISA follows a holistic and comprehensive approach to the issues related to cybersecurity in Industry 4.0, whereby challenges and recommendations are associated with one of the following categories: People, Processes, and Technologies. This ensures consistency with the relevant ENISA study.

Additionally, recommendations are also categorised in terms the target audience groups to which they are addressed (the icons for the 5 stakeholder groups identified below may be used as a guidance, i.e. the presence of an icon next to a recommendation indicates that a particular set of recommendations is aimed at the corresponding stakeholder group).

To read more: https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations

Number 6

Cyber Incident Response and Recovery: Progress Report to the G20 Finance Ministers and Central Bank Governors

FSB FINANCIAL STABILITY BOARD

This progress report, delivered to G20 Finance Ministers and Central Bank Governors ahead of their meetings in Fukuoka on 8-9 June, provides an update on the FSB's work on developing effective practices for financial institutions' response to and recovery from a cyber incident.

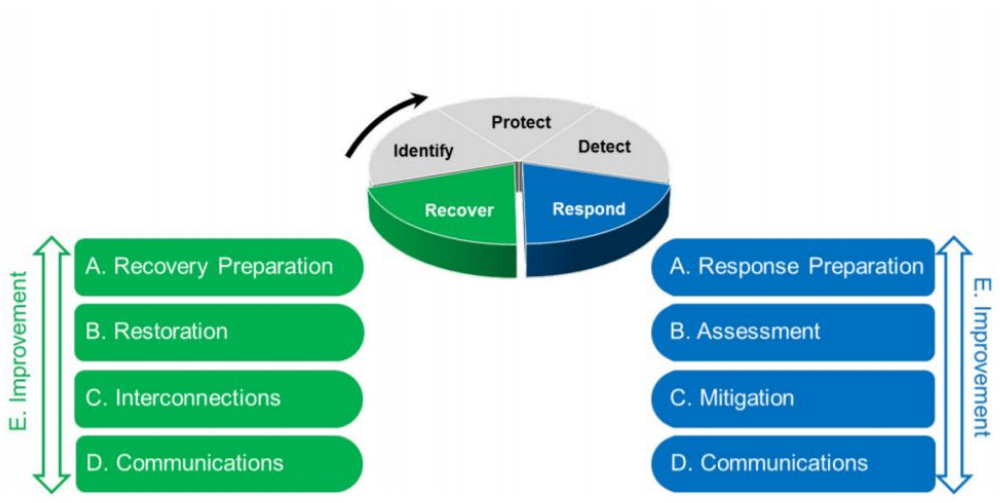
As part of its work programme to enhance the cyber resilience of financial institutions, the FSB is developing a toolkit of effective practices relating to a financial institution's response to, and recovery from, a cyber incident.

The toolkit also aims to help supervisors and other relevant authorities in supporting financial institutions before, during and after a cyber incident.

This project seeks to mitigate the implications of cyber incidents on financial stability, by taking into account their cross-border and cross-sectoral nature.

It will also leverage the shared experience and diversity of perspectives gathered in the course of this work.

Components of the Respond and Recover functions[8]



The development of effective practices will incorporate a stocktake of publicly released guidance from national authorities and international bodies, a review of case studies on past cyber incidents and various engagements with external stakeholders.

As part of its outreach, the FSB will launch an online survey in July which will help to identify effective practices at financial institutions.

A public consultation on the report will be launched in early 2020, with a view to finalising the toolkit of effective practices in late 2020.

The report:
https://www.fsb.org/wp-content/uploads/P280519-1.pdf

Number 7

Trends in international law for cyberspace

This paper is a collaborative view of the NATO CCDCOE Law Branch experts, demarcating the latest trends in international law and envisioning their evolution over the next few years.

It is an independent product of the CCDCOE and does not represent the official policy or position of NATO or any of its Sponsoring Nations.

We do not assert this to be a complete catalogue of trends, neither is the list presented in any particular order. Also, while we have made every effort to describe globally relevant legal developments, we acknowledge that the list stems from a Euro-Atlantic geopolitical perspective, and that the division between political developments and trends in law is not always clear-cut.

1. Maturing consensus that international law applies in cyberspace, but continued debate on how it applies

a. It is now generally held that international law applies to cyberspace: this has been confirmed inter alia by UN GGE 2013 and 2015 consensus reports; in statements of regional organisations (NATO, EU, OAS SCO, etc.); by (joint) statements of States; and by States in the Tallinn Manual 2.0 (TM 2.0) State consultation process.

However, such a conclusion does not warrant overconfidence, as States like Russia and China have been walking back their commitment even to the broad notion of the applicability of existing international law in cyberspace.

b. The legal debate has shifted to how international law applies in cyberspace.

This process is neither predetermined nor singular; it evolves through State practice and political statements (individually and collectively via international organisations and fora), and by scholarly legal discussion.

Furthermore, it involves a number of different issues of varied specificity.

c. Acceptance of particular legal rules to cyberspace varies. Certain rules are generally accepted, such as prohibition of intervention (Rules 66–67 of TM 2.0) and the right to self-defence (Rules 71–75 of TM 2.0).

Others, in particular the exercise of (territorial) sovereignty (Rules 1–5 of TM 2.0) and due diligence (Rules 6–7 of TM 2.0) in cyberspace, have received mixed reactions on their scope and content, even from countries which do not question the relevance of existing international law to cyberspace.

d. States are likewise divided on whether existing treaty and customary law is adequate (as maintained by the West) or whether new treaty instruments are needed; the SCO States are the most prominent proponents of the latter.

e. The conceptual difference in approaches 'cybersecurity vs. information security' also persists, as does the practice of applying national sovereignty over 'information space' (China and Russia as prime examples).

The paper: https://ccdcoe.org/uploads/2019/05/Trends-Intlaw_a4_final.pdf

Number 8

Our ongoing work to tackle hate

YouTube
Official Blog

Over the past few years, we've been investing in the policies, resources and products needed to live up to our responsibility and protect the YouTube community from harmful content.

This work has focused on four pillars: removing violative content, raising up authoritative content, reducing the spread of borderline content and rewarding trusted creators.

Thanks to these investments, videos that violate our policies are removed faster than ever and users are seeing less borderline content and harmful misinformation.

As we do this, we're partnering closely with lawmakers and civil society around the globe to limit the spread of violent extremist content online.

We review our policies on an ongoing basis to make sure we are drawing the line in the right place: In 2018 alone, we made more than 30 policy updates. One of the most complex and constantly evolving areas we deal with is hate speech.

We've been taking a close look at our approach towards hateful content in consultation with dozens of experts in subjects like violent extremism, supremacism, civil rights, and free speech. Based on those learnings, we are making several updates:

Removing more hateful and supremacist content from YouTube

YouTube has always had rules of the road, including a longstanding policy against hate speech.

In 2017, we introduced a tougher stance towards videos with supremacist content, including limiting recommendations and features like comments and the ability to share the video.

This step dramatically reduced views to these videos (on average 80%). Today, we're taking another step in our hate speech policy by specifically prohibiting videos alleging that a group is superior in order to justify

discrimination, segregation or exclusion based on qualities like age, gender, race, caste, religion, sexual orientation or veteran status.

This would include, for example, videos that promote or glorify Nazi ideology, which is inherently discriminatory. Finally, we will remove content denying that well-documented violent events, like the Holocaust or the shooting at Sandy Hook Elementary, took place.

We recognize some of this content has value to researchers and NGOs looking to understand hate in order to combat it, and we are exploring options to make it available to them in the future.

And as always, context matters, so some videos could remain up because they discuss topics like pending legislation, aim to condemn or expose hate, or provide analysis of current events.

We will begin enforcing this updated policy today; however, it will take time for our systems to fully ramp up and we'll be gradually expanding coverage over the next several months.

Reducing borderline content and raising up authoritative voices

In addition to removing videos that violate our policies, we also want to reduce the spread of content that comes right up to the line.

In January, we piloted an update of our systems in the U.S. to limit recommendations of borderline content and harmful misinformation, such as videos promoting a phony miracle cure for a serious illness, or claiming the earth is flat.

We're looking to bring this updated system to more countries by the end of 2019. Thanks to this change, the number of views this type of content gets from recommendations has dropped by over 50% in the U.S.

Our systems are also getting smarter about what types of videos should get this treatment, and we'll be able to apply it to even more borderline videos moving forward.

As we do this, we'll also start raising up more authoritative content in recommendations, building on the changes we made to news last year.

For example, if a user is watching a video that comes close to violating our policies, our systems may include more videos from authoritative sources (like top news channels) in the "watch next" panel.

Continuing to reward trusted creators and enforce our monetization policies

Finally, it's critical that our monetization systems reward trusted creators who add value to YouTube.

We have longstanding advertiser-friendly guidelines that prohibit ads from running on videos that include hateful content and we enforce these rigorously. And in order to protect our ecosystem of creators, advertisers and viewers, we tightened our advertising criteria in 2017.

In the case of hate speech, we are strengthening enforcement of our existing YouTube Partner Program policies. Channels that repeatedly brush up against our hate speech policies will be suspended from the YouTube Partner program, meaning they can't run ads on their channel or use other monetization features like Super Chat.

The openness of YouTube's platform has helped creativity and access to information thrive. It's our responsibility to protect that, and prevent our platform from being used to incite hatred, harassment, discrimination and violence.

We are committed to taking the steps needed to live up to this responsibility today, tomorrow and in the years to come.

Number 9

Modelling the Cognitive Work of Cyber Protection Teams

Colonel Stoney Trent, Dr. Robert R. Hoffman, Lieutenant Colonel David Merritt, Captain Sarah Smith

VOLUME 4 • NUMBER 1 SPRING 2019

THE CYBER DEFENSE REVIEW

Cyber Protection Teams (CPTs) defend our Nation's critical military networks. While Cyber Security Service Providers are responsible for the continuous monitoring and vulnerability patching of particular networks, CPTs perform threat-oriented missions to defeat adversaries within and through cyberspace.

Each 39-person CPT must be able to work with network security teams and other CPTs to counter cyber threat actors. When fully operational, the Cyber Mission Force will include 68 CPTs, which will be manned, trained and equipped by the Military Service Departments.

Within the Cyber Mission Force, CPTs are allocated to an operational command and aligned with one of four mission areas: Combatant Command (CCMD), Service Department (Army, Navy, Air Force, and Marine Corps), Department of Defense Information Network (DODIN), and National Threats.

To maximize flexibility, these teams must be able to perform reliably as well as be interchangeable and interoperable.

CPTs must be able to perform three basic types of missions.

1. Survey: Short duration assessments that provide the supported organization with recommended mitigations based on an assessment of network vulnerabilities.

2. Secure: Harden and defend cyber key terrain; and

3. Protect: Time-sensitive deployments that include Survey and Secure tasks, but also include helping an organization recover from the effects of a cyber intrusion.

The research we report here provides a descriptive workflow of cyber defense in CPTs as well as a prescriptive work model that all CPTs should

be capable of executing. Work models, such as the one described here, provide a foundation for improvements to work processes.

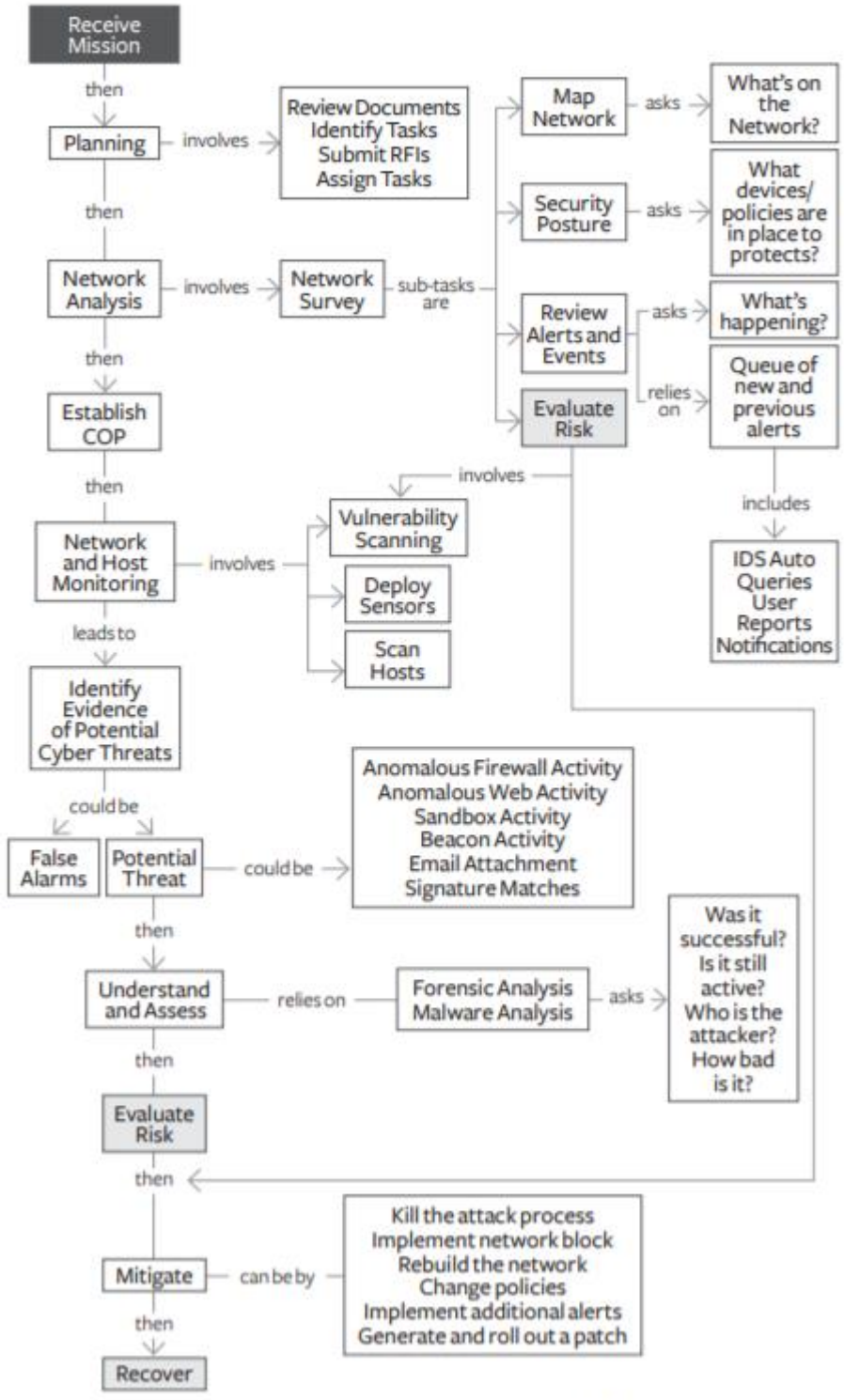


Figure 1. Initial Workflow model

As an illustration of required or desired workflows, work models provide a bridge to common ground between researchers and practitioners, particularly when the work domain is difficult to access, or is esoteric.

The model in this report has multiple purposes.

The first purpose is to inform the design of experiments to assess current and emerging technologies for operational fit.

The second is to educate developers, who may have limited knowledge of CPT work, about the tasks that require technical support.

The third is to inform revisions to operational doctrine.

Finally, this model is meant to provide the basis for operational and strategic planning of defensive cyberspace operations.

To read more (at page 127) you may visit:
https://cyberdefensereview.army.mil/Portals/6/CDR_V4N1_FULL_WEB.pdf?ver=2019-04-30-102349-643

Number 10

Irving Fisher Committee on Central Bank Statistics, IFC Bulletin No 50

The use of big data analytics and artificial intelligence in central banking

Proceedings of the IFC – Bank Indonesia International Workshop and Seminar in Bali, May 2019

BIS

Executive summary

Information and internet technology has fostered new web-based services that affect every facet of today's economic and financial activity.

This creates enormous quantities of "big data" – defined as "the massive volume of data that is generated by the increasing use of digital tools and information systems" (FSB (2017)).

Such data are produced in real time, in differing formats, and by a wide range of institutions and individuals.

For their part, central banks face a surge in "financial big data sets", reflecting the combination of new, rapidly developing electronic footprints as well as large and growing financial, administrative and commercial records.

This phenomenon has the potential to strengthen analysis for decision-making, by providing more complete, immediate and granular information as a complement to "traditional" macroeconomic indicators.

To this end, a number of techniques are being developed, often referred to as "big data analytics" and "artificial intelligence" (AI).

These promise faster, more holistic and more connected insights, as compared with traditional statistical techniques and analyses.

An increasing number of central banks have launched specific big data initiatives to explore these issues.

They are also sharing their expertise in collecting, working with, and using big data, especially in the context of the BIS's Irving Fisher Committee on Central Bank Statistics (IFC); see IFC (2017).

Getting the most out of these new developments is no trivial task for policymakers.

Central banks, like other public authorities, face numerous challenges, especially in handling these new data and using them for policy purposes.

In particular, significant resources are often required to handle large and complex data sets, while the benefits of such investments are not always clear-cut.

For instance, to what extent should sophisticated techniques be used to deal with this type of information?

What is the added value over more traditional approaches, and how should the results be interpreted?

How can the associated insights be integrated into current decision-making processes and be communicated to the public?

And, lastly, what are the best strategies for central banks seeking to realise the full potential of new big data information and analytical tools, considering in particular resource constraints and other priorities?

To read the paper:
https://www.bis.org/ifc/publ/ifcb50.pdf

Number II

PATCH REMOTE DESKTOP SERVICES ON LEGACY VERSIONS OF WINDOWS

The National Security Agency is urging Microsoft Windows administrators and users to ensure they are using a patched and updated system in the face of growing threats.

Recent warnings by Microsoft stressed the importance of installing patches to address a vulnerability in older versions of Windows. (https://blogs.technet.microsoft.com/msrc/2019/05/30/a-reminder-to-update-your-systems-to-prevent-a-worm).

Microsoft has warned that this flaw is potentially "wormable," meaning it could spread without user interaction across the internet.

We have seen devastating computer worms inflict damage on unpatched systems with wide-ranging impact, and are seeking to motivate increased protections against this flaw.

CVE-2019-0708, dubbed "BlueKeep," is a vulnerability in Remote Desktop Services (RDS) on legacy versions of the Windows® operating system.

The following versions of Windows are affected:

- Windows® XP
- Windows Server® 2003
- Windows® Vista
- Windows Server® 2008
- Windows® 7
- Windows Server® 2008 R2

Although Microsoft has issued a patch, potentially millions of machines are still vulnerable. This is the type of vulnerability that malicious cyber actors frequently exploit through the use of software code that specifically targets the vulnerability.

For example, the vulnerability could be exploited to conduct denial of service attacks. It is likely only a matter of time before remote exploitation tools are widely available for this vulnerability. NSA is concerned that

malicious cyber actors will use the vulnerability in ransomware and exploit kits containing other known exploits, increasing capabilities against other unpatched systems.

To read more: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csa-bluekeep_20190604.pdf?ver=2019-06-04-123329-617

Number 12

NIST Infrared Frequency Comb Measures Biological Signatures

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

Researchers at the National Institute of Standards and Technology (NIST) and collaborators have demonstrated a compact frequency-comb apparatus that rapidly measures the entire infrared band of light to detect biological, chemical and physical properties of matter.

Infrared light travels in waves longer than visible light and is most familiar as the radiation associated with heat.

The NIST setup, which occupies just a few square feet of table space, has potential applications such as disease diagnosis, identification of chemicals used in manufacturing, and biomass energy harvesting.

The work is described in Science Advances at: https://advances.sciencemag.org/content/5/6/eaaw8794.

Optical frequency combs measure exact frequencies, or colors, of light. Various comb designs have enabled the development of next-generation atomic clocks and show promise for environmental applications such as detecting methane leaks.

Biological applications have been slower to develop, in part because it's been hard to directly generate and measure the relevant infrared light.

To showcase biological applications, the NIST team used the new apparatus to detect "fingerprints" of NIST's monoclonal antibody reference material, a protein made of more than 20,000 atoms that is used by the biopharmaceutical industry to ensure the quality of treatments.

"For the first time our frequency combs have simultaneous coverage across the entire infrared molecular fingerprint region," project leader Scott Diddams said. "Other key advantages are speed, resolution and dynamic range in acquiring data."

Mid-infrared light is an especially useful research probe because molecules usually rotate and vibrate at these frequencies. But until now it's been difficult to probe this region due to a lack of broadband or tunable light sources and efficient detectors such as those available for visible and near-infrared light, the part of the infrared spectrum closest to visible light.

The new NIST apparatus overcomes these problems. Simple fiber lasers generate light spanning the entire range used to identify molecules—that is, mid-infrared to far-infrared wavelengths of 3-27 micrometers (frequencies of approximately 10-100 terahertz).

The amounts of light absorbed at specific frequencies provide a unique signature of a molecule. The new system is innovative in detecting the electric fields of the absorbed light using photodiodes (light detectors) operating in the near-infrared range.

“A unique feature is that we detect signals in real time by rapidly sampling the infrared electric field with a near-infrared laser,” Diddams explained. “This has two advantages: It shifts the detection from the infrared to the near-infrared where we can use inexpensive telecommunications photodiodes, and we no longer suffer from the limitations of infrared detectors, which require cryogenic (liquid nitrogen) cooling.”

The researchers detected signature vibrations of three bands of amides (chemical groups containing carbon, oxygen, nitrogen and hydrogen) in the monoclonal antibody reference material.

Amide bands in proteins are used to determine the folding, unfolding and aggregating mechanisms. Specific features of the detected bands indicated that the protein has a sheet structure, agreeing with previous studies. Sheets connect chemical groups in a flat arrangement.

In addition to biological applications, the new apparatus might be used to detect interactions between infrared light and condensed matter for quantum computing approaches that store data in molecular vibrations or rotations.

In addition, when combined with novel imaging techniques, the tabletop system could obtain nanometer-scale images of samples that currently require the use of a much larger synchrotron facility.

Coauthors of the new paper include researchers from the University of Campinas, in Brazil, and the Institute of Photonic Sciences, in Spain. Funding was provided by the Defense Advanced Research Projects Agency, the National Research Council and the Air Force Office of Scientific Research.

Number 13

THE MISADVENTURES OF CYBER SAM

DoD CYBER EXCHANGE PUBLIC

As technology has changed, the environment that we work in has changed and we have become more reliant upon computers in all aspect of life.

Our utilization of these systems has made even the most mundane tasks enjoyable and easier to accomplish.

Unfortunately, the use of these systems and technologies can be influenced by cyber threats that can manipulate, steal, and/or deny their use.

Through this comic strip we introduce our hero and cyber expert, Cyber Sam.

Cyber Sam will lead you through his struggles to protect, defend, and educate his organization and their Information Technology networks, while introducing them to a whole new world of Operational Technologies (OT) and their vulnerabilities.

You may visit: https://public.cyber.mil/cyber-sam/

Number 14

Unsecured database exposes security logs of major hotel chains

Security researchers have discovered an unsecured database that exposed the security logs - and therefore potential cyber security weaknesses - of major hotels managed by the Pyramid Hotel Group.

Pyramid Hotel Group manages hotels in the US, Hawaii, the Caribbean, Ireland, and the UK, including Marriott, Sheraton and Hilton properties.

The unsecured server allowed unrestricted access to security audit logs generated by an open-source intrusion detection system.

This resulted in the exposure of information regarding their operating systems, security policies, internal networks, and application logs, in addition to sensitive employee data.

In total, 85.4GB of security audit logs were exposed.

Any would-be attacker using the database would have the ability to monitor the hotels' network, gather valuable information about administrators and other users, and build an attack vector targeting the weakest links in the security chain.

The issue was uncovered on May 27th 2019, while using port scanners to map areas of the Internet. Access to the database was closed shortly after Pyramid was made aware of the incident.

The NCSC recommends that organisations take care to keep security-sensitive logs private.

To read more: https://www.vpnmentor.com/blog/pyramid-hotel-group-data-leak/

Number 15

Dropping the password expiration policies

Microsoft | TechNet

There's no question that the state of password security is problematic and has been for a long time. When humans pick their own passwords, too often they are easy to guess or predict.

When humans are assigned or forced to create passwords that are hard to remember, too often they'll write them down where others can see them.

When humans are forced to change their passwords, too often they'll make a small and predictable alteration to their existing passwords, and/or forget their new passwords.

When passwords or their corresponding hashes are stolen, it can be difficult at best to detect or restrict their unauthorized use.

Recent scientific research calls into question the value of many long-standing password-security practices such as password expiration policies, and points instead to better alternatives such as enforcing banned-password lists (a great example being Azure AD password protection) and multi-factor authentication.

While we recommend these alternatives, they cannot be expressed or enforced with our recommended security configuration baselines, which are built on Windows' built-in Group Policy settings and cannot include customer-specific values.

This reinforces a larger important point about our baselines: while they are a solid foundation and should be part of your security strategy, they are not a complete security strategy.

In this particular case, the small set of ancient password policies enforceable through Windows' security templates is not and cannot be a complete security strategy for user credential management.

Removing a low-value setting from our baseline and not compensating with something else in the baseline does not mean we are lowering security standards.

It simply reinforces that security cannot be achieved entirely with baselines.

Why are we removing password-expiration policies?

First, to try to avoid inevitable misunderstandings, we are talking here only about removing password-expiration policies – we are not proposing changing requirements for minimum password length, history, or complexity.

Periodic password expiration is a defense only against the probability that a password (or hash) will be stolen during its validity interval and will be used by an unauthorized entity.

If a password is never stolen, there's no need to expire it. And if you have evidence that a password has been stolen, you would presumably act immediately rather than wait for expiration to fix the problem.

If it's a given that a password is likely to be stolen, how many days is an acceptable length of time to continue to allow the thief to use that stolen password? The Windows default is 42 days.

Doesn't that seem like a ridiculously long time? Well, it is, and yet our current baseline says 60 days – and used to say 90 days – because forcing frequent expiration introduces its own problems. And if it's not a given that passwords will be stolen, you acquire those problems for no benefit.

Further, if your users are the kind who are willing to answer surveys in the parking lot that exchange a candy bar for their passwords, no password expiration policy will help you.

Our baselines are intended to be usable with minimal if any modification by most well-managed, security-conscious enterprises. They are also intended to serve as guidance for auditors.

So, what should the recommended expiration period be? If an organization has successfully implemented banned-password lists, multi-factor authentication, detection of password-guessing attacks, and detection of anomalous logon attempts, do they need any periodic password expiration? And if they haven't implemented modern mitigations, how much protection will they really gain from password expiration?

The results of baseline compliance scans are usually measured by how many settings are out of compliance: "How much red do we have on the chart?"

It is not unusual for organizations during audit to treat compliance numbers as more important than real-world security.

If a baseline recommends 60 days and an organization with advanced protections opts for 365 days – or no expiration at all – they will get dinged in an audit unnecessarily and might be compelled to adhere to the 60-day recommendation.

Periodic password expiration is an ancient and obsolete mitigation of very low value, and we don't believe it's worthwhile for our baseline to enforce any specific value.

By removing it from our baseline rather than recommending a particular value or no expiration, organizations can choose whatever best suits their perceived needs without contradicting our guidance.

At the same time, we must reiterate that we strongly recommend additional protections even though they cannot be expressed in our baselines.

To read more:
https://blogs.technet.microsoft.com/secguide/2019/05/23/security-baseline-final-for-windows-10-v1903-and-windows-server-v1903/

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.