Top cyber risk and compliance related news stories and world events, that (for better or for worse) shaped the month's agenda, and what is next

*July 2018, cyber risk and compliance in Switzerland*

Dear readers and friends,

The Financial Stability Board (FSB) has published a draft Cyber Lexicon for public consultation. It comprises a set of 50 core terms related to cyber security and cyber resilience in the financial sector.

The Cyber Lexicon is intended to support the work of the FSB, standard-setting bodies, authorities and private sector participants, e.g. financial institutions, and international standards organisations.

In my opinion, the draft lexicon, as it is today, does not meet the expectations of the industry. I will give some examples.

According to the draft Cyber Lexicon:

- Cyber Risk is "the combination of the probability of cyber events occurring and their consequences."

- Cyber Event is "any observable occurrence in an information system. Events sometimes provide indication that a cyber incident is occurring."

- Cyber Security is the "preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved."

The National Institute of Standards and Technology (NIST) gives a very different definition: Cyber Security is the "prevention of damage to, protection of, and restoration of computers, electronic communications

systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."

Having many different definitions of the same term is not going to help governments, standard setting bodies, firms and organizations.

The FSB developed the lexicon in response to a request from G20 Finance Ministers and Central Bank Governors at their October 2017 meeting. The FSB delivered a stocktake report to that meeting on existing publicly available regulations and supervisory practices with respect to cyber security in the financial sector.

Ministers and Governors asked that the FSB continue its work to protect financial stability against the malicious use of Information and Communication Technologies, noting that this work could be supported by a common lexicon of terms that are important in the work.

After considering the responses to this consultation, the FSB will finalise the lexicon for delivery to the G20 Leaders' Summit in Buenos Aires in November 2018.

---

Sun Tzu believed that the opportunity to secure ourselves against defeat, lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself.

This year's football World Cup is important for hundreds of millions of people, and this makes it an opportunity for the organized crime and State-sponsored "hackers".

Phishing campaigns and homograph attacks are taking advantage of the World Cup. A homograph is a word that shares the same written form as another word but has a different meaning.

One common effective attack starts with a homographic web link, where a character is replaced by a similar looking symbol, like Lloydsbank.co.uk and IIoydsbank.co.uk.

It could be worse. Unicode character U+0430 refers to the Cyrillic small letter "a". It looks identical to Unicode character U+0061 that refers to the Latin small letter "a", which is the lowercase "a" used in English.

So, www.apple com (the “a” is the Cyrillic letter) looks the same with apple.com (the “a” is the Latin letter). We cannot see the difference, but computers can, and send the persons that click these URLs to two different web sites.

The Cyrillic letters a, c, e, o, p, x and y have optical counterparts in the basic Latin alphabet. The Greek letter omicron “o” looks identical to the letter “o” of the Latin alphabet.

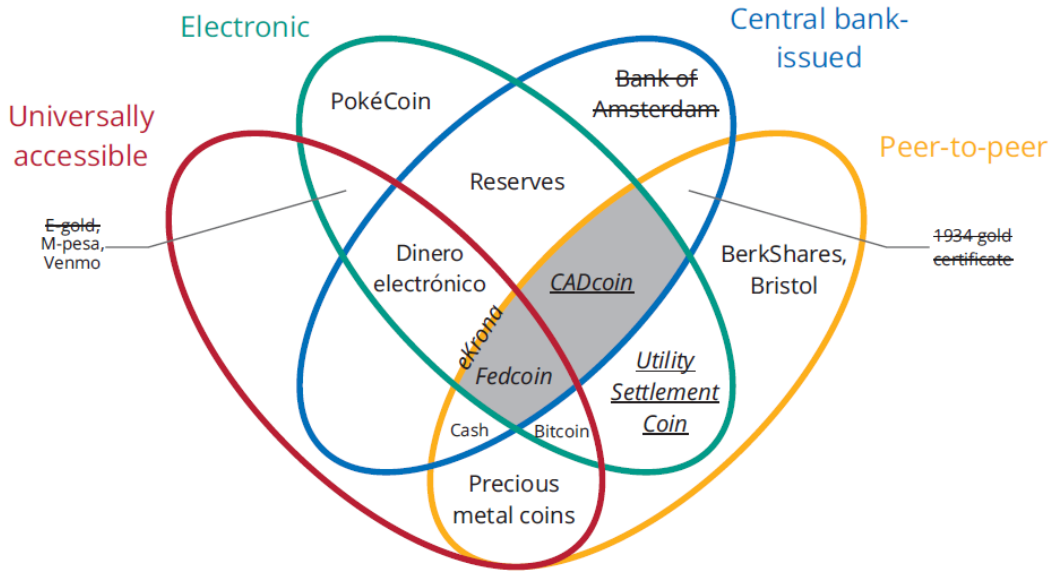
The moral of the story: Don’t click on URLs in emails. If you want to go to apple, open your browser and type www.apple.com

An attacker can register a domain name that looks similar or identical to a legitimate website, but in which one letter has been replaced by homographs in another alphabet. The victims may never notice the difference, until it is too late.

Francis Bacon was right: Opportunity makes a thief.

Read more at Number 3 below.

The money flower




A standard font indicates that a system is in operation; an *italic* font indicates a proposal; an *italic and underlined* font indicates experimentation; a ~~strikethrough~~ font indicates a defunct company or an abandoned project.

*Money Flower* is a South Korean television series. It tells the story of people who are driven by the illusion that they can control money.

I was surprised to see the phrase "money flower" in the annual report of the Bank for International Settlements (BIS), which is a very effective and efficient entity, and has no illusions.

We read: "As private DLT-based cryptocurrencies mushroomed in 2017, the growing hype prompted debate about whether central banks should issue their own digital currencies. A special feature in the September BIS Quarterly Review (https://www.bis.org/publ/qtrpdf/r_qt1709f.htm) provides a taxonomy of money that identifies two types of central bank digital currency (CBDC) – retail and wholesale – and differentiates them from other forms of central bank money, such as cash and reserves.

The "money flower" establishes a way to classify different types of money and understand how past, present and potential future forms relate to each other."

According to the annual report, the BIS evolution includes communicating better with all stakeholders and also the broader public. In my opinion, using the word flower just after the word money has definitely been approved by communications experts.

After all, Christian Dior has said that after women, flowers are the most lovely thing God has given the world. Sigmund Freud has said that flowers are restful to look at. They have neither emotions nor conflicts.

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:
www.cyber-risk-gmbh.com/Cyber_Risk_GmbH_Catalog_2018.pdf

*Number 1 (Page 11)*

## Freedom before security

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Monitoring major digital projects has once again been the focus activity for the Federal Data Protection and Information Commissioner (FDPIC). The E-ID Act as the basis for using a SwissID, the risk report on using the OASI number as a universal personal identifier or the conditions that must be met by e-ticketing or public transport apps underline this prioritisation.

As a supervisory authority, the Commissioner had to intervene to prevent the processing of data on compulsory health insurance and had to deal with data leaks at several large companies.

*Number 2 (Page 14)*

École Polytechnique Fédérale de Lausanne

## Making opaque materials totally transparent

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

EPFL researchers have found a way to make materials that are normally opaque to sound waves completely transparent.

Their system involves placing acoustic relays at strategic locations so that sound waves can propagate at a constant amplitude – regardless of what may lie in their path.

This method could eventually be used to make it possible to hide objects like submarines.

Most naturally occurring materials have a disordered atomic structure that interferes with the propagation of both sound and electromagnetic waves.

*Number 3 (Page 17)*

## Football or Phishing?

At least two phishing campaigns are taking advantage of this year's football World Cup.

National Cyber Security Centre
a part of GCHQ

Fraudsters are attempting to exploit fans' eagerness to *keep up* with the games and the results in the expectation that fans might click on links more readily.

Phishing emails are reported to be sending fixture schedules and results mappers to fans, but the links are loaded with adware and malware.

In another example, fraudsters are offering a pair of Adidas shoes in exchange for completing a survey. The victim is then redirected to a fake Adidas website asking them to pay a small fee to receive the shoes (and an ongoing monthly charge, which is hidden in the small print).

*Number 4 (Page 18)*

## Identity and travel document fraud

INTERPOL

## The different types of document fraud

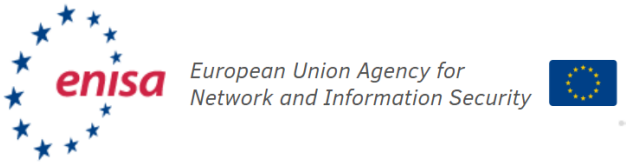
Counterfeit – a document that constitutes an unauthorized reproduction of a genuine document. These documents are not legitimately manufactured, nor issued or recognized by an official authority.

Forgery – these are typically based on a genuine document, a part of which has been added or altered in order to give misleading information about the person who presents it.

Pseudo document – a document produced with no authority and which is not officially recognized. They can occur in various forms and may have the physical appearance of a passport or an ID card.

*Number 5 (Page 20)*

## VPNFilter, a Nation State Operation




The recent disclosure of a sophisticated malware affecting 500,000 networking devices is making headlines around the world.

It followed several warnings made by manufacturers, security researchers and law enforcement concerning a malicious operation classified as a state sponsored. The malware dubbed VPNFilter - initially affecting Ukrainian hosts - is now spreading over 54 countries at an alarming rate.

Researchers attributed this malware to a Russian state-sponsored hacking group Sofacy (also known as Fancy Bear and APT28) just weeks after the discovery of "Lojack" attack, attributed to the same group.

*Number 6 (Page 25)*

Legal Working Paper Series

## The Eurosystem and the Single Supervisory Mechanism: institutional continuity under constitutional constraints


This paper analyses regulatory solutions that have been adopted to address constitutional constraints imposed on the functioning of the Single Supervisory Mechanism (SSM), in which the ECB's exclusive supervisory competence is carried out.
It argues that the operational framework governing the functioning of the SSM has assimilated, to a certain extent, three specific regulatory solutions underpinning the workings of the ESCB/Eurosystem.

*Number 7 (Page 26)*

Justice Department

## Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices

Additional action necessary worldwide to remediate the botnet.

The Justice Department has announced an effort to disrupt a global botnet of hundreds of thousands of infected home and office (SOHO) routers and other networked devices under the control of a group of actors known as the "Sofacy Group" (also known as "apt28," "sandworm," "x-agent," "pawn storm," "fancy bear" and "sednit").

The group, which has been operating since at least in or about 2007, targets government, military, security organizations, and other targets of perceived intelligence value.

*Number 8 (Page 29)*

## SP 800-71 (DRAFT)
## Recommendation for Key Establishment Using Symmetric Block Ciphers

Draft NIST Special Publication (SP) 800-71, Recommendations for Key Establishment Using Symmetric Block Ciphers, addresses key establishment techniques that use symmetric key cryptography algorithms to protect symmetric keying material.
The objective is to provide recommendations for reducing exposure to the unauthorized disclosure of the keying material and detecting its unauthorized modification, substitution, insertion or deletion.

## Number 9 (Page 30)

### FBI's Tech Tuesday: Building a Digital Defense Against Online Sale Frauds

Welcome to the Oregon FBI's Tech Tuesday segment. This week: building a digital defense against online sale frauds.

Summer is upon us – and if you are like me, this is the best time to get rid of all that extra stuff sitting in your garage. Who couldn't use a few extra bucks for that summer vacation, right?

You can do it the old fashioned way – sitting outside for hours on end, hoping someone drives up and offers you big money for your cast-offs. Or, you can sell on platforms like Craigslist and Facebook. Those are great options – if you are smart about how you do business.

## Number 10 (Page 33)

### A letter to Google

Congress of the United States
Washington, DC 20515

A bipartisan group of lawmakers sent a letter to Google expressing concerns over the company's partnership with the Chinese phone maker Huawei.

*Number 1*

## Freedom before security

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Monitoring major digital projects has once again been the focus activity for the Federal Data Protection and Information Commissioner (FDPIC). The E-ID Act as the basis for using a SwissID, the risk report on using the OASI number as a universal personal identifier or the conditions that must be met by e-ticketing or public transport apps underline this prioritisation.

As a supervisory authority, the Commissioner had to intervene to prevent the processing of data on compulsory health insurance and had to deal with data leaks at several large companies.

As the Freedom of Information Commissioner, the FDPIC succeeded in achieving a substantial increase in the efficiency of his arbitration procedures and welcomed the National Council's unanimous commitment to guaranteeing transparency in connection with public procurement – thus ensuring that the principle of freedom of information does not become a farce.

The phenomena of digital reality, such as Big Data and algorithms, e-commerce, e-health, mobility and digital identification remain the focus of supervision. Against this background, the transitional period before the delayed total revision of the Data Protection Act (FADP) is completed poses a particular challenge.

Whereas the data protection authorities in EU member states were given powers to issue orders and impose sanctions, not to mention considerable additional resources before the EU General Data Protection Regulation (GDPR) came into force, for the time being the FDPIC only has the power granted in the FADP of 1993 to issue recommendations and the same resources as in 2005, two years before the first smartphones came on the market.

However, he will continue to do everything in his power to support Swiss companies in their application of the GDPR by providing advice and assistance. Switzerland's residents and businesses deserve an up-to-date

data protection system. The total revision of the FADP should therefore be dealt with as quickly as possible.

## Data leaks and informal rights to decide for oneself in major digital projects

In the report year, the Commissioner was called on to deal with several cases of data leaks, such as those at Swisscom or at the international debt collection company EOS. He also had to intervene in connection with a bonus programme run by the Helsana health insurance company.

The FDPIC took legal action against the latter, which had rejected his recommendations. People are being subjected to increasing surveillance in public spaces.

The FDPIC is therefore monitoring numerous major digital projects, such as the creation of an electronic identity (E-ID) or e-ticketing applications for public transport, where anonymous and non-discriminatory travel must remain possible even when ticket machines have been phased out for good.

## Freedom before security

In the light of the worldwide availability of inexpensive face recognition technologies, the Commissioner warns of developments that are evolving in authoritarian states into the blanket surveillance and identification of the population and thus the loss of any privacy and independence.

In any democratic state governed by the rule of law, the constitutional right to freedom must always take precedence over maintaining security; the Commissioner is concerned by the growing trend towards expanding data processing by security services in Switzerland to cover largely unspecific groups of persons such as ‘potential attackers’.

Given the flurry of special federal legislation that has been issued on policing matters, which is likely to be exacerbated by further laws, such as that on police counter-terrorism measures, the FDPIC is calling, not before time, for an easily understandable federal act on policing to be introduced.

Once the federal government has done this job, one the cantons finished long ago, citizens will also be able to gain an overview of the many police information systems operating at federal level.

## Information service before the federal elections in 2019

The unauthorised use by the British company Cambridge Analytica of personal data belonging to unsuspecting Facebook users in the run-up to the US presidential elections in 2017 and the Brexit referendum sparked international outrage. Ahead of the federal elections in 2019, the FDPIC and the cantonal data protection commissioners (Privatim), supported by a contact group of experts, will keep the public up-to-date on digital personal data processing methods that might be used to shape political opinion at national and cantonal levels.

The content of this information service provided by the data protection authorities to the public will be limited to data protection matters.

## FoIA: Efficient arbitration procedures and transparency in public procurement projects

As part of a year-long trial, on 1 January 2017 the FDPIC introduced an accelerated summary procedure with oral arbitration hearings. As the trial proved successful and resulted in all pending cases being dealt with and more amicable solutions being reached, this new working method has become the permanent procedure.

In the final week of the summer session of 2018, the National Council in its debate on the total revision of the Federal Act on Public Procurement (PPA) expressed its unanimous support for the principle of freedom of information in public procurement matters, thus rejecting the Federal Council's proposal not to apply the principle of freedom of information in such cases.

The Freedom of Information Commissioner hopes that the Council of States will now follow this decision so that transparency remains guaranteed in public procurement.

The complete 25th Annual Report 2017/2018 is available in German and French at www.derbeauftragte.ch (under Documentation).

*Number 2*

École Polytechnique Fédérale de Lausanne

## Making opaque materials totally transparent


EPFL researchers have found a way to make materials that are normally opaque to sound waves completely transparent.

Their system involves placing acoustic relays at strategic locations so that sound waves can propagate at a constant amplitude – regardless of what may lie in their path.

This method could eventually be used to make it possible to hide objects like submarines.

Most naturally occurring materials have a disordered atomic structure that interferes with the propagation of both sound and electromagnetic waves.

When the waves come into contact with these materials, they bounce around and disperse – and their energy dissipates according to a highly complex interference pattern, diminishing in intensity.

That means it's virtually impossible to transmit data or energy intact across wave-scattering media and fully leverage the potential of wave technology.

For an example, you need look no further than your smartphone – the geolocation function works less well inside buildings where radiofrequency waves scatter in all directions.

Other potential applications include biomedical imaging and geological surveying, where it's important to be able to send waves across highly disordered media.

A team of researchers from two labs at EPFL's School of Engineering, working in association with TU Wien and the University of Crete, has developed a system that allows sound waves to travel across such media with no distortion.

It uses tiny speakers as acoustic relays to offset the wave scattering, and has been successfully tested on a real acoustic system. Their work has just been published in Nature Physics.

## Using speakers to eliminate obstacles

In the researchers' system, the tiny speakers can be controlled to amplify, attenuate or shift the phase of the sound waves.

That lets them offset the diffusion that results when the waves hit obstacles, and thereby reproduce the original sound exactly on the other side of the disordered medium.

How does it work? "We realized that our acoustic relays had to be able to change the waves' amplitudes and phases at strategic locations, to either magnify or attenuate them," says Romain Fleury, head of EPFL's Laboratory of Wave Engineering (LWE) and a co-author of the study.

The researchers tested their system by building a 3,5 meters long air-filled tube and placing various kinds of obstacles such as walls, porous materials and chicanes into it, in order to create a highly disordered medium through which no sound waves could pass.

They then placed their tiny speakers between the obstacles and set up electronic controls to adjust the speakers' acoustic properties.

"We've been working on using controlled speakers as active sound absorbers for years, so it made sense to use them for this new application too," says Hervé Lissek, head of the acoustics research group at EPFL's Signal Processing Laboratory 2 (LTS2) and a co-author of the study.

"Until now, we only needed to attenuate sound waves. But here we had to develop a new control mechanism so we could also amplify them, like how we can already amplify optical waves with lasers," adds Etienne Rivet, another co-author at EPFL who wrote a thesis on the subject.

Their new method – the only one of its kind in acoustics – uses programmable circuits to control several speakers simultaneously and in real time.

## Making objects invisible

The researchers' method for active acoustic control is similar to that used in noise cancelling headphones and could potentially be used for sounds containing common ambient frequencies.

It could also be used to eliminate the waves that bounce off objects like submarines, making them undetectable by sonar.

Moreover, the theory underlying their work is universal and could have parallel applications in optics or radiofrequencies, to make objects invisible or to take images through opaque materials.

*Number 3*

## Football or Phishing?

At least two phishing campaigns are taking advantage of this year's football World Cup.

National Cyber Security Centre
a part of GCHQ

Fraudsters are attempting to exploit fans' eagerness to *keep up* with the games and the results in the expectation that fans might click on links more readily.

Phishing emails are reported to be sending fixture schedules and results mappers to fans, but the links are loaded with adware and malware.

In another example, fraudsters are offering a pair of Adidas shoes in exchange for completing a survey. The victim is then redirected to a fake Adidas website asking them to pay a small fee to receive the shoes (and an ongoing monthly charge, which is hidden in the small print).

The fake Adidas site uses homographic web links, where a character is replaced by a similar looking symbol:

Example 1: www. thisisarealwebsite .org.com
Example 2: www. thisisarea|website .org.com

The letter 'l' in the second website name is a symbol, but at a quick glance it is not immediately obvious. Fraudsters are increasingly using this technique and we advise readers to study web links carefully before clicking on them.

The NCSC has further information on how to protect yourself from phishing scams at: https://www.ncsc.gov.uk/guidance/avoiding-phishing-attacks

*Number 4*

# Identity and travel document fraud


## The different types of document fraud

Criminals and terrorists often make fraudulent use of identity and travel documents in order to carry out their illegal activities.

Both false and genuine documents are used to perpetrate a variety of frauds, which can be classified as follows:

## False documents

Counterfeit – a document that constitutes an unauthorized reproduction of a genuine document. These documents are not legitimately manufactured, nor issued or recognized by an official authority.

Forgery – these are typically based on a genuine document, a part of which has been added or altered in order to give misleading information about the person who presents it.

Pseudo document – a document produced with no authority and which is not officially recognized. They can occur in various forms and may have the physical appearance of a passport or an ID card.

## Genuine documents

Fraudulently obtained genuine document – an authentic identity or travel document obtained through deception by submission of either false or counterfeit documents, cooperation of a corrupt official or impersonation of the rightful holder of a genuine document.

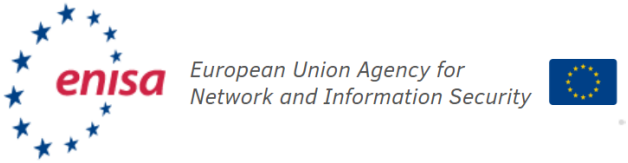
Misuse of a genuine document through deception by a person who knowingly misrepresents him or herself by using someone else's identity or travel document.

Often, the biographical details and photograph resemble the impostor, helping him or her to pass as the rightful bearer.

To read more:
https://www.interpol.int/News-and-media/Publications2/Fact-sheets2

*Number 5*

# VPNFilter, a Nation State Operation




## Introduction

The recent disclosure of a sophisticated malware affecting 500,000 networking devices is making headlines around the world.

It followed several warnings made by manufacturers, security researchers and law enforcement concerning a malicious operation classified as a state sponsored. The malware dubbed VPNFilter - initially affecting Ukrainian hosts - is now spreading over 54 countries at an alarming rate.

Researchers attributed this malware to a Russian state-sponsored hacking group Sofacy (also known as Fancy Bear and APT28) just weeks after the discovery of "Lojack" attack, attributed to the same group.

Researchers were conclusive determining this as a global, broadly deployed threat that is actively seeking to increase its footprint.

## Contextual Information

The research of the VPNFilter threat has been ongoing since 2016 leading to a stage where researchers agreed to disclose before concluding it.

The versatile and persistent behaviour of this malware on networking devices is generating great concern among security professionals and authorities around the world.

In its multi-stage and modular capabilities is able to support the collection of intelligence, misattribution and destructive cyberattack operations.

Moreover, it has a range of capabilities including data exfiltration, spying on traffic and ultimately rendering the infected device unbootable.

According to the researcher, the malware code overlaps with versions of the BlackEnergy malware, which was responsible for multiple large-scale attacks that targeted devices in Ukraine.

## Known VPNFilter capabilities

- Adopts a multi-stage architecture, in which some of the more complex functionality runs only in the memory of the infected devices;

- Contains a payload capable of self-destructing by overwriting critical portions of the device's firmware and rendering the infected device unbootable. This capability can be triggered individually or en masse, and has the potential of cutting off internet access for hundreds of thousands of victims worldwide;

- Allows C2 anonymous communication over TOR network or SSL-encrypted connections, meaning it will be hard to notice on regular network traffic checks.

- Include typical workhorse intelligence-collection capabilities such as traffic monitoring, file collection, command execution, data exfiltration and device management.

- Modify non-volatile configuration memory (NVRAM) values to add itself to the device crontab (Linux job scheduler) to achieve persistence.

- Downloads images from a gallery (Photobucket) to extract the download server IP address from the GPS six-integer value stored in the EXIF information, to achieve persistence.

- Use the infected device as a hop point before connecting to a final victim obfuscating the true point of origin.

## VPNFilter attack vector

VPNFilter attack vector is based on the exploitation of SOHO/NAS network devices vulnerabilities to gain initial access to the targets.

Once the malware gains control over the device, is capable of executing a variety of malicious actions and deploy additional payload in a persistent way.

Researchers were not able to confirm if the exploit of zero-day vulnerabilities is involved in spreading this threat.

## VPNFilter Kill-Chain

Installation – The attacker injects malware into devices running firmware version based on Busybox and Linux.
The main purpose is to gain a persistent foothold and enable the download and deployment of additional malware in a persistent way.

Command & Control - Utilizes multiple redundant C2 mechanisms to discover the IP address of deployment servers, making this malware extremely robust and capable of dealing with unpredictable C2 infrastructure changes.

Actions on Objectives – The attack is executed using a variety of capabilities such file collection, command execution, data exfiltration, device management and firmware overwrite among others. Additionally, the malware introduce multiple modules serving as plugins providing additional functionality.

The researcher identified two plugin modules: a packet sniffer for collecting traffic that passes through the device including theft of website credentials and monitoring of Modbus SCADA protocols, and a communications module over the TOR network.

## Affected devices

While the research is still ongoing, the current estimated number of infected devices is ca. 500,000 spread over 54 countries. The known device models affected by VPNFilter range from different manufacturers naming Linksys, MikroTik, NETGEAR and TP-Link in the small and home office (SOHO) space, as well at QNAP network-attached storage (NAS) devices. An updated list of affected devices can be found at the researcher's web site.

## Mitigation challenges

The targeted devices are frequently found on network perimeters, with no intrusion protection system (IPS) in place, and typically have no available host-based protection system making it more difficult to protect.

Furthermore, affected manufacturers published recommendations to device owners but failed to provide assurance for older versions that have known public exploits and default credentials making the compromise relatively easy. To mitigate this risk, victims are required to hold technical knowledge that in most cases they do not have.

Internet service providers (ISP) play an important role in mitigating this threat. Service providers typically supply these type of devices as part of an internet subscription package, and in some cases, remotely manage them. In this case, ISPs are required to assess which customers are using affected devices and advise on a course of action.

Recent reports reveal that law enforcement agencies such as the FBI, are seizing domains such as “toknowall.com” and “photobucket.com” used by the malware. Researchers and authorities believe that these domains are linked to the Russian group Sofacy, also known by the names “APT28,” “Sandworm,” “X-agent,” “Pawn storm,” “Fancy bear” and “Sednit”. These actions will help containing the incident temporarily, but will not resolve the underlying problem.

## Recommendations

- Users of SOHO routers and/or NAS devices to reset them to factory defaults and reboot them in order to remove the potentially destructive, non-persistent malware.

- Ensure that the device is up to date with the most recent firmware/software version by contacting manufacturer.

- Avoid using the default password for the administrator account.

- If possible, install a malware remover tool and run a full scan.

- If the device is not maintained by a service provider, access the device admin page and turn off the remote management option in the advanced settings.

- Internet service providers that remotely maintain SOHO routers to reboot and update the firmware on their customers' behalf.

- ISPs and/or device owners to replace the equipment, if in the list of affected devices.

## Closing Remarks

Several factors are determining the seriousness of the VPNFilter threat: the different capabilities that this malware presents, its fast and wide spread and the difficulties in mitigating the risks due to technical and human challenges.

Much is still to uncover while researchers investigate the threat, assess the impact and better understand the malicious actor motivations.

Users, industry, ISPs and law enforcement have a critical role in providing adequate response to this incident, that if not properly contained, may configure a similar or even higher scale to what was observed last year with the WannaCry and NotPetya aggressive outbreaks.

*Number 6*

Legal Working Paper Series

## The Eurosystem and the Single Supervisory Mechanism: institutional continuity under constitutional constraints


This paper analyses regulatory solutions that have been adopted to address constitutional constraints imposed on the functioning of the Single Supervisory Mechanism (SSM), in which the ECB's exclusive supervisory competence is carried out.

It argues that the operational framework governing the functioning of the SSM has assimilated, to a certain extent, three specific regulatory solutions underpinning the workings of the ESCB/Eurosystem:

1) the (legislative) allocation of certain tasks and responsibilities between ECB internal administrative bodies and structures;

2) the possibility of internal delegation of decision-making powers; and

3) the decentralised exercise of certain of the Union's tasks.

Such a design of the SSM reflects institutional continuity concerning a political choice on how to achieve stage one of a genuine Economic and Monetary Union.

It concludes that the Union operates at its best when centralised decision-making on substantial policy issues is combined with a decentralised operational framework allowing for the meaningful involvement of national administrations in the exercise of Union exclusive competences.

To read more:
https://www.ecb.europa.eu/pub/pdf/scplps/ecb.lwp17.en.pdf?b39bee753107db68032c7238e711ae91

*Number 7*

Justice Department

## Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices

Additional action necessary worldwide to remediate the botnet.

The Justice Department has announced an effort to disrupt a global botnet of hundreds of thousands of infected home and office (SOHO) routers and other networked devices under the control of a group of actors known as the "Sofacy Group" (also known as "apt28," "sandworm," "x-agent," "pawn storm," "fancy bear" and "sednit").

The group, which has been operating since at least in or about 2007, targets government, military, security organizations, and other targets of perceived intelligence value.

Assistant Attorney General for National Security John C. Demers, U.S. Attorney Scott W. Brady for the Western District of Pennsylvania, Assistant Director Scott Smith for the FBI's Cyber Division, FBI Special Agent in Charge Robert Johnson of the Pittsburgh Division and FBI Special Agent in Charge David J. LeValley of the Atlanta Division made the announcement.

"The Department of Justice is committed to disrupting, not just watching, national security cyber threats using every tool at our disposal, and today's effort is another example of our commitment to do that," said Assistant Attorney General Demers. "This operation is the first step in the disruption of a botnet that provides the Sofacy actors with an array of capabilities that could be used for a variety of malicious purposes, including intelligence gathering, theft of valuable information, destructive or disruptive attacks, and the misattribution of such activities."

"The United States Attorney's Office will continue to aggressively fight against threats to our national security by criminals, no matter who they work for" said U.S. Attorney Brady. "This court-ordered seizure will assist in the identification of victim devices and disrupts the ability of these

hackers to steal personal and other sensitive information and carry out disruptive cyber attacks. We will be relentless in protecting the people of Western Pennsylvania - from international corporations to local businesses to the elderly - from these threats."

"Today's announcement highlights the FBI's ability to take swift action in the fight against cybercrime and our commitment to protecting the American people and their devices," said Assistant Director Scott Smith. "By seizing a domain used by malicious cyber actors in their botnet campaign, the FBI has taken a critical step in minimizing the impact of the malware attack. While this is an important first step, the FBI's work is not done. The FBI, along with our domestic and international partners, will continue our efforts to identify and expose those responsible for this wave of malware."

"The FBI will not allow malicious cyber actors, regardless of whether they are state-sponsored, to operate freely," said FBI Special Agent in Charge Bob Johnson. "These hackers are exploiting vulnerabilities and putting every American's privacy and network security at risk. Although there is still much to be learned about how this particular threat initially compromises infected routers and other devices, we encourage citizens and businesses to keep their network equipment updated and to change default passwords."

"This action by the FBI, DOJ, and our partners should send a clear message to our adversaries that the U.S. Government will take action to mitigate the threats posed by them and to protect our citizens and our allies even when the possibility of arrest and prosecution may not be readily available," said FBI Special Agent in Charge David J. LeValley. "As our adversaries' technical capabilities evolve, the FBI and its partners will continue to rise to the challenge, placing themselves between the adversaries and their intended victims."

The botnet, referred to by the FBI and cyber security researchers as "VPNFilter," targets SOHO routers and network-access storage (NAS) devices, which are hardware devices made up of several hard drives used to store data in a single location that can be accessed by multiple users. The VPNFilter botnet uses several stages of malware. Although the second stage of malware, which has the malicious capabilities described above, can be cleared from a device by rebooting it, the first stage of malware persists through a reboot, making it difficult to prevent reinfection by the second stage.

In order to identify infected devices and facilitate their remediation, the U.S. Attorney's Office for the Western District of Pennsylvania applied for and obtained court orders, authorizing the FBI to seize a domain that is part of the malware's command-and-control infrastructure. This will redirect attempts by stage one of the malware to reinfect the device to an FBI-controlled server, which will capture the Internet Protocol (IP) address of infected devices, pursuant to legal process. A non-profit partner organization, The Shadowserver Foundation, will disseminate the IP addresses to those who can assist with remediating the VPNFilter botnet, including foreign CERTs and internet service providers (ISPs).

Owners of SOHO and NAS devices that may be infected should reboot their devices as soon as possible, temporarily eliminating the second stage malware and causing the first stage malware on their device to call out for instructions. Although devices will remain vulnerable to reinfection with the second stage malware while connected to the Internet, these efforts maximize opportunities to identify and remediate the infection worldwide in the time available before Sofacy actors learn of the vulnerability in their command-and-control infrastructure.

The FBI and the Department of Homeland Security have also jointly notified trusted ISPs. The Department and the FBI also encourage users and administrators to review the Cisco blog post on VPNFilter, for recommendations and to ensure that their devices are updated with the latest patches.

The efforts to disrupt the VPNFilter botnet were led by the FBI's Pittsburgh and Atlanta Offices; FBI Cyber Division; Trial Attorney Matthew Chang of the National Security Division's Counterintelligence and Export Control Section; and Assistant U.S. Attorneys Charles Eberle and Soo C. Song of the Western District Pennsylvania. Critical assistance was also provided by Richard Green of the Criminal Division's Computer Crime and Intellectual Property Section and The Shadowserver Foundation.

*Number 8*

## SP 800-71 (DRAFT)
## Recommendation for Key Establishment Using Symmetric Block Ciphers

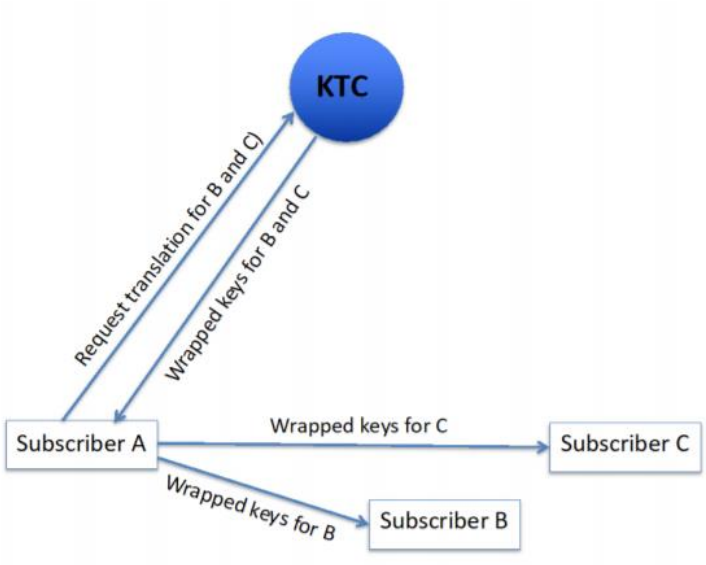
NIST
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

Draft NIST Special Publication (SP) 800-71, Recommendations for Key Establishment Using Symmetric Block Ciphers, addresses key establishment techniques that use symmetric key cryptography algorithms to protect symmetric keying material.

The objective is to provide recommendations for reducing exposure to the unauthorized disclosure of the keying material and detecting its unauthorized modification, substitution, insertion or deletion.

The Recommendation also addresses recovery in the event of detectable errors during the key-distribution process. Wrapping mechanisms are specified for encrypting keys, binding key control information to the keys and protecting the integrity of this information.

To read the paper:
https://csrc.nist.gov/CSRC/media/Publications/sp/800-71/draft/documents/sp800-71-draft.pdf



*Number 9*

## FBI's Tech Tuesday: Building a Digital Defense Against Online Sale Frauds

Welcome to the Oregon FBI's Tech Tuesday segment. This week: building a digital defense against online sale frauds.

Summer is upon us – and if you are like me, this is the best time to get rid of all that extra stuff sitting in your garage. Who couldn't use a few extra bucks for that summer vacation, right?

You can do it the old fashioned way – sitting outside for hours on end, hoping someone drives up and offers you big money for your cast-offs. Or, you can sell on platforms like Craigslist and Facebook. Those are great options – if you are smart about how you do business.

I have some personal examples to share with you. Recently, I posted several items for sale… a bed, a barbecue, and a few other things. Usually within the first 24 hours of a new posting I received at least one suspicious inquiry, either by e-mail or text.

In many cases, the seller said he or she needed to have a mover or shipper pick up the item. The seller proposed sending me a larger-than-requested payment by cashier's check or electronic transfer, with the caveat that I would use those extra funds to pay the shipper when he arrives to pick up my item.

This is a version of an overpayment scam. Let's say you get that check and cash it. The shipper takes the item, and eventually the bank figures out the cashier's check is bogus. The bank is going to come after you for the missing funds and could even pursue criminal charges.

Electronic transfers are not necessarily safer. In a couple cases, the fraudster proposed making a payment via PayPal or a funds transfer. Had I pursued this option, the person would have likely ended up asking for

personal information – including bank routing numbers – to push the payment through.

Here are some warning signs to watch for if you are trying to sell online this summer:

- Look for out-of-area phone numbers. All of the suspicious inquiries I received came from area codes nowhere near Oregon. It is possible for scammers to spoof phone numbers, of course, so make sure to proceed cautiously even when you receive an inquiry from a local number.

- Look for bad spelling, stilted language, random capitalizations, and chunks of text that are obviously cut-and-pasted from your post.

- Look for those who try to justify why they can't meet in person. In one case, I had a fraudster claim to be a cabin steward on a major cruise line… which, he said, required an electronic payment and a shipping service. Really? Why does someone who works on a cruise ship need a large barbecue?

## FBI Tech Tuesday: Building a Digital Defense Against Online Sale Frauds (Part 2)

Welcome to the Oregon FBI's Tech Tuesday segment. This week, building a digital defense against online sale frauds—part 2!

Last week we talked about how to avoid being scammed by overpayment fraud schemes while trying to sell items on sites such as Craigslist and Facebook. This week—some other common frauds that can come with launching virtual garage sales.

Using platforms like these are easy, and they can generate some extra cash for you and your family. But, fraudsters also know how to take advantage of your good will.

I recently posted some items online and almost immediately started receiving suspicious texts and e-mails. They often included bad spellings, bad grammar, lots of extra capital letters, or text just cut-and-pasted from my online ad.

One, though, was a bit different. This person texted me from an out-of-state number with a request to e-mail him back. He didn't even mention the item I was selling—just a generic request about my "appliance."

This is a perfect set-up for an unsuspecting seller to click on the e-mail link.

The fraudster may be "phishing"—sending out thousands of such non-specific texts hoping to get a few people to respond.

Clicking on that link could download malware onto my phone or computer—or it could give the fraudster a heads-up that I am a willing victim. He could then try to lure me into an overpayment or non-payment scam, wire or credit card fraud, or ID theft situation.

In other situations, a fraudster may send you an official-looking, but fake, e-mail from what purports to be a third-party company offering to guarantee that the sale is legit. Don't fall for it. Transactions should happen directly between the seller and the buyer when you are dealing in these forums. Don't count on anyone else to guarantee the sale.

Other warning signs to watch for:

- Don't accept or send money via wire transfer. Same thing goes for cashier's checks and money orders. Cash is best.

- Don't deal with people who live out-of-town or people who require shippers or movers. Deals should happen face-to-face. For your own personal safety, consider making the deal in a public place—such as outside a police station—when possible.

- Be concerned if the buyer won't talk to you on the phone. Most scammers prefer text and e-mail.

- Watch for buyers who offer an online escrow service. Don't do it. Again, meet in person and deal in cash.

- Never give out personal details, including bank or PayPal account information.

- Don't click on links, even if the link appears to go back to your own listing.

Remember—if the deal seems too easy, too fast and too good to pass up—it is probably a scam.

*Number 10*

## A letter to Google

Congress of the United States
Washington, DC 20515

A bipartisan group of lawmakers sent a letter to Google expressing concerns over the company's partnership with the Chinese phone maker Huawei.

Congress of the United States
Washington, DC 20515

June 20, 2018

Mr. Sundar Pichai
Chief Executive Officer
Google LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043

Dear Mr. Pichai,

We write to express our concerns about Google's "strategic partnership" with Huawei Technologies. Chinese telecommunications companies, such as Huawei, have extensive ties with the Chinese Communist Party. As a result, this partnership between Google and Huawei could pose a serious risk to U.S. national security and American consumers.

Since the House Permanent Select Committee on Intelligence released its investigative report on the national-security issues posed by Chinese telecommunications firms in 2012, U.S. officials have publicly raised concerns about Huawei's ties to the Chinese government. During a February 2018 hearing of the Senate Select Committee on Intelligence, the heads of six U.S. intelligence agencies warned American citizens not to use Huawei products or services. At the same hearing, Federal Bureau of Investigation (FBI) Director Christopher Wray testified that he was "deeply concerned about the risks of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications networks." The concerns of the Intelligence Community are well founded: recent reports indicate that a former U.S. intelligence officer charged with spying for the Chinese government used Huawei technology to communicate with his handlers.

In fact, Congress is considering a number of bipartisan measures to address the threat posed by Huawei. Earlier this year, we introduced the Defending U.S. Government Communications Act, which would prohibit the U.S. government from purchasing or leasing telecommunications equipment or services from Huawei or other Chinese telecommunications companies. Both chambers of Congress have included elements of this bill in the fiscal year 2019 National Defense Authorization Act. In addition, the Federal Communications Commission (FCC) has proposed a measure that would bar the use of the FCC's Universal Service Fund to purchase equipment or services from companies deemed a national-security risk, including Huawei. Over the coming months, the federal government will likely take further measures to defend U.S. telecommunications networks from Huawei and companies like it.

We urge you to reconsider Google's partnership with Huawei, particularly since your company recently refused to renew a key research partnership, Project Maven, with the Department of Defense. This project uses artificial intelligence to improve the accuracy of U.S. military targeting, not least to reduce civilian casualties. While we regret that Google did not want to continue a long and fruitful tradition of collaboration between the military and technology companies, we are even more disappointed that Google apparently is more willing to support the Chinese Communist Party than the U.S. military.

Thank you for your time and consideration. We look forward to your response, including the rationale for your decision to partner with Huawei but not the U.S. military, as well as your plans to mitigate the grave risks of working with Huawei.

Sincerely,

TOM COTTON
United States Senator

K. MICHAEL CONAWAY
Member of Congress

MARCO RUBIO
United States Senator

LIZ CHENEY
Member of Congress

DUTCH RUPPERSBERGER
Member of Congress

## 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.*