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

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

Dear readers,

The Swiss National Cyber Security Centre (NCSC) has published the first semi-annual report that deals with the most important cyberincidents of the second half of 2020 in Switzerland and internationally. It replaces the former MELANI semi-annual report.

According to the report, hospitals and other healthcare providers are exposed to the same cyberthreats as all companies that have an internet connection and work with computers.

For this reason, access to data and systems in the healthcare sector must also be secured with multi-factor authentication, if possible, and malware infections must be prevented or at least detected and remedied promptly.

Another important protective measure is to raise employee awareness regarding the secure use of IT resources and to highlight cyberthreats such as social engineering.

While the threats are very similar or even the same in most sectors, the consequences of successful attacks in the healthcare sector do have some specific characteristics.

On the one hand, data leaks usually affect unalterable and sensitive personal data, and on the other hand, functional failures of IT systems or even temporary unavailability of data can endanger people's health or even their lives.

For several years now, encryption Trojans (ransomware) have proliferated as a successful criminal business model that is also used against hospitals. Nowadays, the perpetrators download as much data as possible before encrypting the files on the victims systems in order to have an additional means of extortion.

At a psychotherapy company in Finland, extortionists unsuccessfully tried to get money from the company to prevent the publication of patient data and details of therapy sessions. The criminals subsequently tried to blackmail the patients in question directly.

During a pandemic, cases of illness can soar in a short period of time, stretching the healthcare system to its capacity limits. If cyberincidents then occur that lead to functional restrictions for healthcare providers, this may have life-threatening consequences.

The case of Düsseldorf University Hospital, which was affected by ransomware in September 2020, attracted worldwide attention.

The Hirslanden Group fell victim to ransomware in the summer of 2020. However, it was possible to restore the encrypted data with the help of backups, and patient care was reportedly not at risk at any time.

At two other hospitals in Switzerland, infections with the Emotet Trojan were detected and remedied at an early stage.

During a pandemic, healthcare workers are under extraordinary strain and often overworked. People are more likely to fall for social engineering methods when they are already under pressure due to external circumstances.

A key feature of social engineering involves creating a sense of urgency. The accumulation of real and artificially created pressure increases the chances of such attacks succeeding. The risk of clicking on a malicious link in an email or opening a harmful attachment rises when people are in a hurry. In addition to implementing technical measures, all employees should be made aware of the dangers of social engineering.

Administrative processes should be established to detect fraud attempts and other social engineering attacks.

To read the report:
https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/berichte/lageberichte/halbjahresbericht-2020-2.html

---

According to the Swiss National Cyber Security Centre (NCSC), fake support calls have been observed for several years: a caller pretends to be an employee of an IT company (typically Microsoft) and tells the victim that their computer is infected and needs to be repaired.

The purported support callers have no idea whatsoever of the configuration of the computers of the people they are calling. The attackers want to persuade the victims to download a program that allows them to access their computer.

They gain access to the system only via this program and can thus manipulate the computer. In most cases, the callers try to sell the victims a software licence or service ("system cleaning") and thereby obtain their credit card information.

In May we saw an increase in the variant where an **error message** is displayed in the browser while surfing, stating that the computer has been locked. Users are asked to call a telephone number to unlock their computers. When they call the number, the fraudsters' approach is exactly the same as a described above. They ask for access to the computer and end up by requesting credit card details.

The pop-ups are mainly displayed in the form of spoof banner advertisements. Another possibility is the misuse of Google ads.

Advertisements that are placed by advertisers and that also match the searched terms are usually displayed above the actual search results. This advertising service is also used by fraudsters. The advertisements imitate well-known companies but redirect visitors to a site run by the fraudster.

Ignore these "screen blockers". Closing the browser usually works; if not, shutting down the computer will help.

In recent weeks, the NCSC has been alerted several times to strange entries in electronic calendars. These are known as calendar spam, the term used to describe unwanted messages that are sent via email and then find their way into the recipient's calendar. Depending on the software, this may happen automatically or after clicking on an attached calendar file.

Spammers and fraudsters use this function to place unwanted messages directly in people's calendars. Victims then either see these entries when browsing the calendar or are reminded of the event by the system when the appointment approaches.

An example of one variant observed is a claim that WhatsApp and or other apps have been hacked. This is a bluff used to entice the recipients to click on a malicious link. Entries with links to dubious investment sites are also

being reported. If users actively refuse such invitations, there is also the risk that the sender will receive a notification confirming that their address is valid. They may then receive even more advertising.

As a countermeasure against calendar spam, many apps only allow automatic entries if the sender is already in the recipient's contact list, i.e. the sender is known to the recipient. However, the spammers have also reacted to this measure.

Over the past week, the NCSC has observed an increase in fraudulent appointment requests that come from a person known to the recipient. In these cases, the fraudsters probably assume that the person is in the contact list and the spam will therefore automatically end up in the calendar.

Ignore dubious calendar entries!

I remember the words of Sun Tzu: *"When able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near."*

Sun Tzu believed that it is not enough to have a plan, we also have to disguise it using deception. I remembered his words when I read Microsoft's tweet about a massive email campaign that's pushing a Java-based STRRAT malware to *steal confidential data* from infected systems while *disguising itself as a ransomware* infection.

Attackers used compromised email accounts to launch the email campaign. The emails contained an *image that posed as a PDF attachment* but, when opened, connected to a malicious domain to download the STRRAT malware.

Email users do not trust Microsoft Word attachments, they trust only pdfs. Predictability leads to vulnerabilities. Weaponized pdfs are used by all cyber attack groups, especially state-spponsored groups.

I remember that through all of 2018, network security company SonicWall had discovered more than 47,000 new attack variants within pdf files.

How can the European National Competent Authorities (NCAs) *complement* the information obtained through the on-site inspections? Well, the answer is called *mystery shopping (MS)*.

According to the European Banking Authority (EBA), *mystery shopping* is understood as an *undercover* research approach used by NCAs, or market research companies that they may have used, to measure quality of customer service and/or gather information about financial products and services and the conduct of Financial Institutions (FIs) towards consumers.

MS may include the use of individuals who may act as potential or actual customers and who are trained and briefed to experience and measure key phases of a product's lifecycle and compliance with particular requirements.

They report back their experiences in a detailed and objective way. They perform specific tasks, for example reviewing how staff perform against pre-determined standards during an interaction with a customer.

That interaction may occur at the pre-contractual, contractual or post-contractual phase and may involve purchasing a product/service, asking questions, or registering complaints.

MS enables supervisors to carry out an assessment, in concrete situations, rather than relying on documents kept by firms, on-site interviews, or surveys.

This is interesting. The EBA was not the place to look for *covert human intelligence experts*, but things change.

Read more at Number 6 below.

DARPA develops a Sarcasm Detector for Online Communications!

SocialSim researchers demonstrate deep learning model capable of accurately classifying sarcasm in textual communications, addressing online sentiment analysis roadblock.

Sentiment analysis – the process of identifying positive, negative, or neutral emotion – across online communications has become a growing focus for both commercial and defense communities.

Understanding the sentiment of online conversations can help businesses process customer feedback and gather insights to improve their marketing efforts.

From a defense perspective, sentiment can be an important signal for online information operations to identify topics of concern or the possible actions of bad actors.

The presence of sarcasm – a linguistic expression often used to communicate the opposite of what is said with an intention to insult or ridicule – in online text is a significant hindrance to the performance of sentiment analysis.

Detecting sarcasm is very difficult owing largely to the inherent ambiguity found in sarcastic expressions.

“Sarcasm has been a major hurdle to increasing the accuracy of sentiment analysis, especially on social media, since sarcasm relies heavily on vocal tones, facial expressions, and gestures that cannot be represented in text,” said Brian Kettler, a program manager in DARPA’s Information Innovation Office (I2O). “Recognizing sarcasm in textual online communication is no easy task as none of these cues are readily available.”

Researchers from the University of Central Florida working on DARPA’s Computational Simulation of Online Social Behavior (SocialSim) program are developing a solution to this challenge in the form of an AI-enabled “sarcasm detector.”

The researchers have demonstrated an interpretable deep learning model that identifies words from input data – such as Tweets or online messages – that exhibit crucial cues for sarcasm, including sarcastic connotations or negative emotions.

Using recurrent neural networks and attention mechanisms, the model tracks dependencies between the cue-words and then generates a classification score, indicating whether or not sarcasm is present.

"Essentially, the researchers' approach is focused on discovering patterns in the text that indicate sarcasm.

It identifies cue-words and their relationship to other words that are representative of sarcastic expressions or statements," noted Kettler.

The researchers' approach is also highly interpretable, making it easier to understand what's happening under the "hood" of the model.

Many deep learning models are regarded as "black boxes," offering few clues to explain their outputs or predictions.

Explainability is key to building trust in AI-enabled systems and enabling their use across an array of applications.

Existing deep learning network architectures often require additional visualization techniques to provide a certain level of interpretability.

To avoid this, the SocialSim researchers employed inherently interpretable self-attention that allows elements in the input data that are crucial for a given task to be easily identified.

The researchers' capability is also language agnostic so it can work with any language model that produces word embeddings.

The team demonstrated the effectiveness of their approach by achieving state-of-the-art results on multiple datasets from social networking platforms and online media.

The model was able to successfully predict sarcasm, achieving a nearly perfect sarcasm detection score on a major Twitter benchmark dataset as well as state-of-the-art results on four other significant datasets.

The team leveraged publicly available datasets for this demonstration, including a Sarcasm Corpus V2 Dialogues dataset that is part of the Internet Argument Corpus as well as a news headline dataset from the Onion and HuffPost.

DARPA's SocialSim program is focused on developing innovative technologies for high-fidelity computational simulation of online social behavior.

A simulation of the spread and evolution of online information could enable a deeper and more quantitative understanding of adversaries' use of the global information environment.

It could also aid in efforts to deliver critical information to local populations during disaster relief operations, or contribute to other critical missions in the online information domain.

Accurately detecting sarcasm in text is only a small part of developing these simulation capabilities due to the extremely complex and varied linguistic techniques used in human communication.

However, knowing when sarcasm is being used is valuable for teaching models what human communication looks like, and subsequently simulating the future course of online content.

Welcome to our monthly newsletter.

Best regards,

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

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

Number 1 (Page 14)

Active Cyber Defence (ACD) - the fourth year

The year four report covers 2020 and aims to highlight the achievements and efforts made by the Active Cyber Defence programme.

Number 2 (Page 17)

From January 2019 to April 2020

Cyber espionage

ENISA Threat Landscape

Number 3 (Page 19)

Further TTPs associated with SVR cyber actors

Number 4 (Page 21)

Safe, Efficient, Reliable: New Science in the Fight Against Killer Drugs

NIST researchers give law enforcement and public health experts new tools to combat fentanyl and other synthetic drugs.

Number 5 (Page 24)

FBI TLP White Flash Alert: Conti Ransomware Attacks Impact Healthcare and First Responder Networks

Number 6 (Page 26)

The European Banking Authority publishes report on mystery shopping activities of national authorities

Number 7 (Page 28)

FluBot "package delivery" scam targeting Android devices

Number 8 (Page 29)

Researchers Demonstrate Potential for Zero-Knowledge Proofs in Vulnerability Disclosure

Research teams led by Galois, Trail of Bits develop capability to mathematically prove exploitability of vulnerable software without revealing critical information

Number 9 (Page 33)

Recommendations for the security of Connected and Automated Mobility (CAM)

Number 10 (Page 36)

Heating up High Performance Computing with Low Temperature Integrated Circuits

Program aims to develop very low temperature device technology to overcome power efficiency limitations in high-performance computing

Number 11 (Page 39)

Russian Foreign Intelligence Service Exploiting Five Publicly Known Vulnerabilities to Compromise U.S. and Allied Networks

Number 12 (Page 41)

From master masons to information architects: how standards can transform reporting (and bring benefits well beyond it)

Gareth Ramsay, Executive Director for Data and Analytics & Chief Data Officer of the Bank of England, webinar hosted by The EDM Council

Number 13 (Page 44)

European Cybersecurity Month (ECSM) 2020 Deployment Report

Number 14 (Page 47)

Masks Under the Microscope

Viewed under a microscope, mask fabrics are complex, varied and beautiful.

Number 15 (Page 49)

Exploring Research Directions in Cybersecurity

The European Union Agency for Cybersecurity has identified key research directions and innovation topics in cybersecurity to support the efforts of the EU towards a Digital Strategic Autonomy.

Number 16 (Page 51)

Office of the Director of National Intelligence, April 2021

Statistical Transparency Report, Calendar Year 2020

Number 17 (Page 53)

Race Logic: Novel Circuitry Solves a Myriad of Computationally Intensive Problems With a Minimum of Energy

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

Number 1

Active Cyber Defence (ACD) - the fourth year

The year four report covers 2020 and aims to highlight the achievements and efforts made by the Active Cyber Defence programme.

National Cyber Security Centre

"How can we use it to help..." was the theme of our Active Cyber Defence (ACD) efforts in 2020.

As the pandemic took hold, we looked at ways in which we could use the ACD tools, services and projects to support people and organisations moving to a working from home model, and also to protect the health, retail, and other sectors during that critical period.

The year ended with a very different challenge, as we took an important role in responding to the SolarWinds Orion compromise and its impact on the UK.

The aim of the Active Cyber Defence (ACD) programme is to "Protect the majority of people in the UK from the majority of the harm caused by the majority of the cyber attacks the majority of the time."

The report is broken down by individual effort, but these aren't siloed efforts: each service and project influences, supports, and guides the others.

This can be seen in data from the Vulnerability Reporting Service highlighting the scale of the 'Dangling DNS' problem, and the team addressing that problem using data from Protective DNS (PDNS) to improve their detection capability. Similar supportive flows exist across the portfolio, and are growing as the efforts mature.

We've also made this report less "numbers heavy", and instead have tried to focus on key stories and important trends that we have discovered in the course of our work. Despite the uniqueness of the events in 2020, we've included comparisons to 2019 as we have in previous years.

As is mentioned throughout, this is a team effort, including UK public sector, commercial and international partners without whom we wouldn't be able to implement these national scale cyber security defences.

Conclusion

2020 was the fourth year of the NCSC's Active Cyber Defence programme, the aim of which is to make the UK objectively and measurably safer from

cyber attack. Our efforts are focused on commodity attacks that affect the majority of the people in the UK which can be prevented at scale.

We have many approaches, which include but are not limited to:

• direct interaction with members of the public (SERS)

• scanning and notification to system owners (Web Check, Mail Check)

• detection and reporting of attacks to infrastructure providers (Takedown)

• supporting network providers in their own attack detection and response processes (BGP Spotlight)

As we focus on scale and commodity attacks, we do not expect our efforts to prevent every attack; rather, we seek to make life harder for attackers, and to raise their costs to a level that is difficult to sustain.

Additionally, the data we generate (and the experience the teams gain through running these services) gives government a better understanding of the cyber threats currently facing the UK, including the best approaches to combat them.

In the years leading up to 2020, our tools, services, and teams had matured to the extent that we were able to rapidly respond when the pandemic took hold, and to apply our technology and techniques in novel ways.

For example, as cyber criminals attempted fraud through fake online stores purporting to sell PPE, the Takedown service was extended to address this challenge.

As organisations moved their meetings online, analysis from the Observatory fed NCSC research and guidance on remote collaboration tools.

And as cyber criminals and state actors targeted the health and vaccine sectors, the PDNS service was extended to protect them.

This fourth annual report documents many of the valuable contributions the ACD programme made to the cyber security of the UK in 2020.

By providing data and case studies on our efforts, we are demystifying the challenges of large-scale cyber attacks, and shining a light on the ACD services and other solutions that work.
As we continue our efforts to broaden adoption of the approaches and services we've developed, we hope this report provides evidence and

inspiration for others to adopt, adapt, and copy across industry and foreign governments.

To read more: https://www.ncsc.gov.uk/files/Active-Cyber-Defence-ACD-The-Fourth-Year.pdf

Number 2

From January 2019 to April 2020

Cyber espionage

ENISA Threat Landscape

Cyber espionage is considered both a threat and a motive in the cybersecurity playbook. It is defined as 'the use of computer networks to gain illicit access to confidential information, typically that held by a government or other organisation'.

In 2019, many reports revealed that global organisations consider cyber espionage (or nation-state-sponsored espionage) a growing threat affecting industrial sectors, as well as critical and strategic infrastructures across the world, including government ministries, railways, telecommunication providers, energy companies, hospitals and banks.

Cyber espionage focuses on driving geopolitics, and on stealing state and trade secrets, intellectual property rights and proprietary information in strategic fields. It also mobilises actors from the economy, industry and foreign intelligence services, as well as actors who work on their behalf. In a recent report, threat intelligence analysts were not surprised to learn that 71% of organisations are treating cyber espionage and other threats as a 'black box' and are still learning about them.

In 2019, the number of nation-state-sponsored cyberattacks targeting the economy increased and it is likely to continue this way. In detail, nation-state-sponsored and other adversary-driven attacks on the Industrial Internet of Things (IIoT) are increasing in the utilities, oil and natural gas (ONG), and manufacturing sectors.

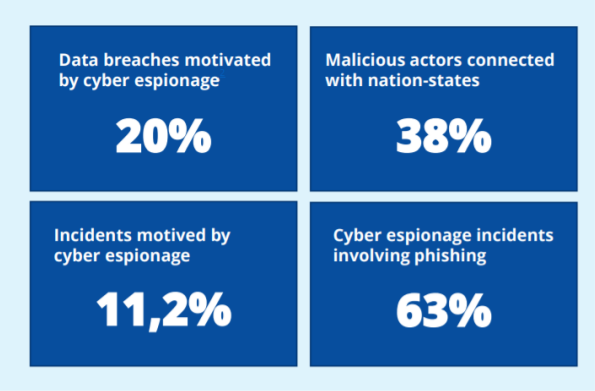
Furthermore, cyberattacks conducted by advanced persistent threat (APT) groups indicate that financial attacks are often motivated by espionage.

Using tactics, techniques and procedures (TTPs) akin to those of their espionage counterparts, groups such as the Cobalt Group, Carbanak and FIN7 have allegedly been targeting large financial institutions and restaurant chains successfully.

- The European Parliament's Committee of Foreign Affairs called upon Member States to establish a cyber-defence unit and to work together on their common defence. It stated that 'the Union's strategic environment has been deteriorating … in order to face the multiple challenges that directly or indirectly affect the security of its Member

States and its citizens; whereas issues that affect the security of EU citizens include: armed conflicts immediately to the east and south of the European continent and fragile states; terrorism – and in particular Jihadism –, cyberattacks and disinformation campaigns; foreign interference in European political and electoral processes'.

- Threat actors motivated by financial, political, or ideological gain will increasingly focus attacks on supplier networks with weak cybersecurity programs. Cyber espionage adversaries have slowly shifted their attack patterns to exploiting third- and fourth-party supply chain partners.



To read more: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cyber-espionage

Number 3

Further TTPs associated with SVR cyber actors

This report provides further details of Tactics, Techniques and Procedures (TTPs) associated with SVR cyber actors. SVR cyber actors are known and tracked in open source as APT29, Cozy Bear, and the Dukes.

UK and US governments recently attributed SVR's responsibility for a series of cyber-attacks, including the compromise of SolarWinds and the targeting of COVID-19 vaccine developers.

Alongside this attribution, the United States' National Security Agency (NSA), Federal Bureau of Investigation (FBI), and Cybersecurity and Infrastructure Security Agency (CISA) released an advisory detailing the exploits most recently used by the group.

The FBI, Department of Homeland Security (DHS) and CISA also issued an alert providing information on the SVR's cyber tools, targets, techniques and capabilities. The SVR is Russia's civilian foreign intelligence service.

The group uses a variety of tools and techniques to predominantly target overseas governmental, diplomatic, think-tank, healthcare and energy targets globally for intelligence gain.

The SVR is a technologically sophisticated and highly capable cyber actor.

It has developed capabilities to target organisations globally, including in the UK, US, Europe, NATO member states and Russia's neighbours.

The NCSC, NSA, CISA and CSE previously issued a joint report regarding the group's targeting of organisations involved in COVID-19 vaccine development throughout 2020 using WellMess and WellMail malware.

SVR cyber operators appear to have reacted to this report by changing their TTPs in an attempt to avoid further detection and remediation efforts by network defenders.

These changes included the deployment of the open-source tool Sliver in an attempt to maintain their accesses.

The group has also been observed making use of numerous vulnerabilities, most recently the widely reported Microsoft Exchange vulnerability.

To read more:
https://www.ncsc.gov.uk/files/Advisory%20Further%20TTPs%20associated%20with%20SVR%20cyber%20actors.pdf

Tactic	Technique	Procedure
Reconnaissance	T1595.002: Active Scanning	SVR frequently scans for publicly available exploits, most recently including Microsoft Exchange servers vulnerable to CVE-2021-26855.
Initial Access	T1190: Exploit Public-Facing Application	SVR frequently uses publicly available exploits to conduct widespread exploitation of vulnerable systems, including against Citrix, Pulse Secure, FortiGate, Zimbra and VMWare.
	T1195.002: Supply Chain Compromise: Compromise Software Supply Chain	SVR target organisations who supply privileged software to intelligence targets.
	T1199: Trusted Relationship	SVR leveraged access gained from the SolarWinds campaign to compromise a certificate issued by Mimecast, which it then used to authenticate a subset of Mimecast's products with customer systems.
Execution	T1059.005: Command and Scripting Interpreter: Visual Basic	SVR deployed Sibot, a simple custom downloader written in VBS, after compromising victims via SolarWinds.
Persistence	T1505.003: Server Software Component: Web Shell	SVR typically deploy a web shell on Microsoft Exchange servers following successful compromise.
	T1078: Valid Accounts	SVR actors have maintained persistence on high value targets using stolen credentials.

Number 4

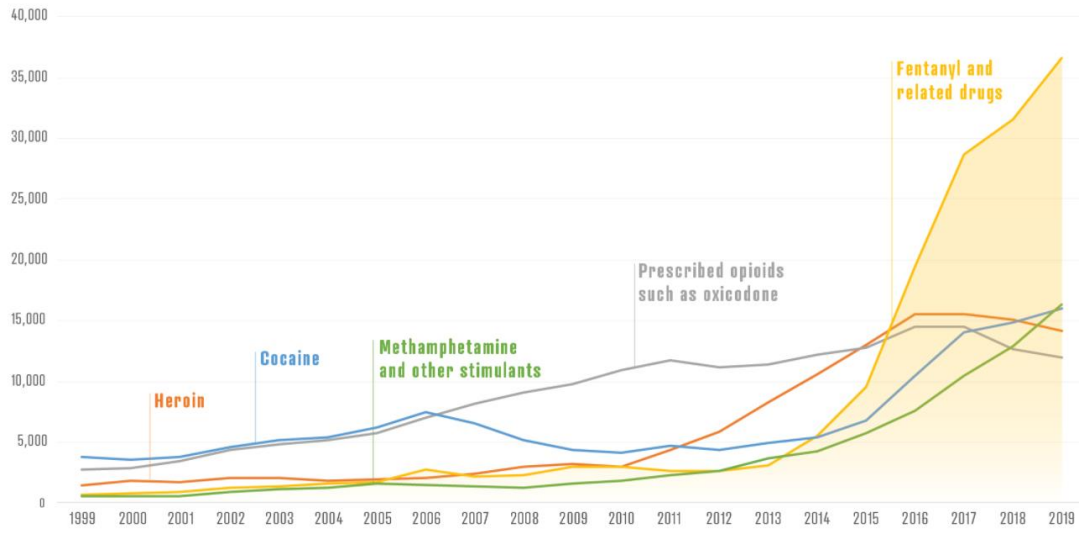
Safe, Efficient, Reliable: New Science in the Fight Against Killer Drugs

NIST researchers give law enforcement and public health experts new tools to combat fentanyl and other synthetic drugs.

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

In the shadow of COVID-19, an older epidemic continues to rage. More than 81,000 people died of drug overdoses in the United States in the 12 months ending last May. That is the highest number ever recorded and a nearly 20% increase from the same period one year before.

This spike in deaths is being driven by fentanyl, a synthetic opioid that mimics the effects of heroin but is up to 50 times more potent. A graph of the overdose statistics from the Centers for Disease Control and Prevention shows the line for fentanyl turning sharply up starting in 2014. It's been rising steeply ever since.



Drug overdose deaths in the United States by drug category. Based on data from the U.S. Centers for Disease Control and Prevention.
Credit: B. Hayes/NIST. Source: U.S. Centers for Disease Control and Prevention

Fentanyl kills so many people in part because it is cheap, potent and easy to manufacture. In addition, clandestine chemists can easily cook up new varieties, or analogues, of fentanyl by tweaking its molecular structure.

Dealers often spike heroin, cocaine and other drugs with fentanyl and its analogues. Users may not know what they're getting, and they can more easily overdose as a result.

The high potency and changeability of fentanyl also present challenges to first responders, police and forensic chemists.

First, it is hazardous. During laboratory or field analysis, for example, particles can become airborne and even a small amount, if accidentally inhaled, can be dangerous.

Second, it hides behind other drugs. Analyzing drug mixtures that contain small but deadly amounts of fentanyl is complicated and requires the ability to detect substances at very low levels.

Third, it can fly under the radar. Traditional laboratory methods are not designed to detect and identify new drug analogues. This can hinder law enforcement and delay the public health response to newly emerging substances.

Photo illustration of 2 milligrams of fentanyl, a lethal dose in most people.
Credit: U.S. Drug Enforcement Administration

Drug abuse has plagued public health for decades, but the unprecedented toll of recent years reflects a new reality. Today's illicit drugs are more dangerous and harder to control than the drugs of decades past.

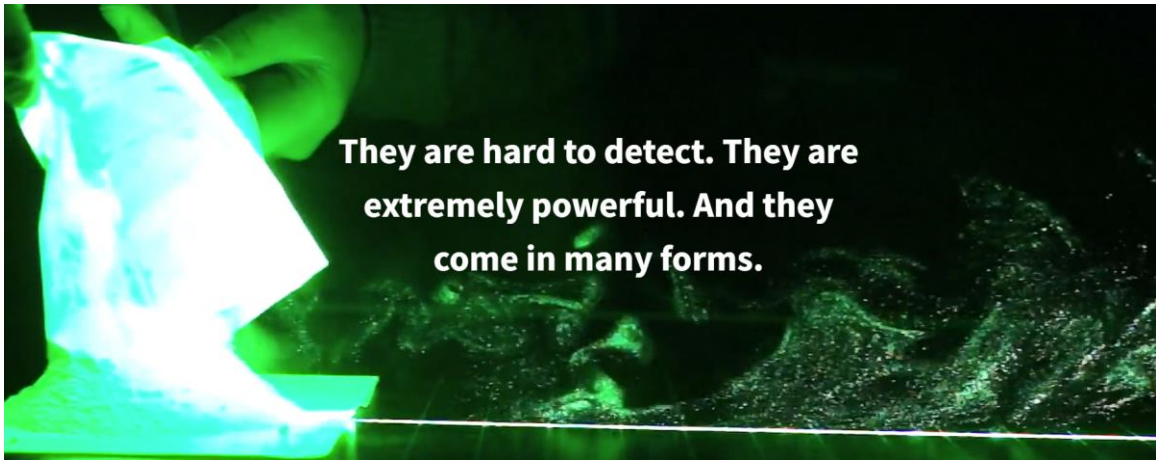
"A new drug might appear, then three or six months later it's gone, replaced by something new," said NIST chemist and program manager Marcela Najarro. "It's a totally different ballgame than 10 or 15 years ago."

Limiting the harm from the opioid epidemic requires expertise from public health, social science, law enforcement and other domains. But one often overlooked need is expertise in the area of analytical chemistry.

As the nation's chemical measurements laboratory, NIST is working on analytical methods to meet these challenges. Researchers with NIST's Forensic Science Program are developing new tools that can speed up the public health response to newly emerging synthetic drugs. They are also improving existing technologies, developing new ones, and collaborating

closely with law enforcement organizations and forensic labs to help them successfully implement solutions. Here is a rundown of what NIST is doing.

To read more: https://www.nist.gov/feature-stories/safe-efficient-reliable-new-science-fight-against-killer-drugs



Number 5

FBI TLP White Flash Alert: Conti Ransomware Attacks Impact Healthcare and First Responder Networks

Summary

The FBI identified at least 16 Conti ransomware attacks targeting US healthcare and first responder networks, including law enforcement agencies, emergency medical services, 9-1-1 dispatch centers, and municipalities within the last year.

These healthcare and first responder networks are among the more than 400 organizations worldwide victimized by Conti, over 290 of which are located in the U.S.

Like most ransomware variants, Conti typically steals victims' files and encrypts the servers and workstations in an effort to force a ransom payment from the victim.

The ransom letter instructs victims to contact the actors through an online portal to complete the transaction.

If the ransom is not paid, the stolen data is sold or published to a public site controlled by the Conti actors.

Ransom amounts vary widely and we assess are tailored to the victim. Recent ransom demands have been as high as $25 million.

Cyber attacks targeting networks used by emergency services personnel can delay access to real-time digital information, increasing safety risks to first responders and could endanger the public who rely on calls for service to not be delayed.

Loss of access to law enforcement networks may impede investigative capabilities and create prosecution challenges.

Targeting healthcare networks can delay access to vital information, potentially affecting care and treatment of patients including cancellation of procedures, rerouting to unaffected facilities, and compromise of Protected Health Information.

Technical Details

Conti actors gain unauthorized access to victim networks through weaponized malicious email links, attachments, or stolen Remote Desktop Protocol (RDP) credentials.

Conti weaponizes Word documents with embedded Powershell scripts, initially staging Cobalt Strike via the Word documents and then dropping Emotet onto the network, giving the actor access to deploy ransomware.

Actors are observed inside the victim network between four days and three weeks on average before deploying Conti ransomware, primarily using dynamic-link libraries (DLLs) for delivery.

The actors first use tools already available on the network, and then add tools as needed, such as Windows Sysinternals and Mimikatz to escalate privileges and move laterally through the network before exfiltrating and encrypting data.

In some cases where additional resources are needed, the actors also use Trickbot.

Once Conti actors deploy the ransomware, they may stay in the network and beacon out using Anchor DNS.

If the victim does not respond to the ransom demands two to eight days after the ransomware deployment, Conti actors often call the victim using single-use Voice Over Internet Protocol (VOIP) numbers.

The actors may also communicate with the victim using ProtonMail, and in some instances victims have negotiated a reduced ransom. View the entire report below.

To read more: https://www.aha.org/system/files/media/file/2021/05/fbi-tlp-white-report-conti-ransomware-attacks-impact-healthcare-and-first-responder-networks-5-20-21.pdf

Number 6

The European Banking Authority publishes report on mystery shopping activities of national authorities

- This publication is the EBA's first step in the fulfilment of its new coordination mandate on mystery shopping activities of National Competent Authorities (NCAs);

- It summarises the most common approaches taken by NCAs on mystery shopping, presents some lessons learned, and identifies good practices;

- Mystery shopping allows NCAs to obtain greater insight into the conduct of financial institutions. The latter are then encouraged to take corrective actions and to better comply with applicable requirements, thus eventually enhancing the protection of consumers.

The European Banking Authority (EBA) published a Report on the mystery shopping activities of NCAs. The EBA collated mystery shopping activities by NCAs with a view to share experiences, learn valuable lessons, and identify good practices for the benefit of the EBA and NCAs that use or intend to use mystery shopping in the future.

The Report covers mystery shopping initiatives of NCAs in respect of products that fall within the scope of action of the EBA's consumer protection mandate, which are consumer credit, mortgage credit, deposits, payment services, electronic money, and payment accounts.

It summarises the most common approaches used by the NCAs, based on the information collated primarily covering the period from 2015 to 2020.

It does so by reviewing three key characteristics of mystery shopping activities: their objective, subject matter and product scope, the methodologies used by NCAs, and the follow-up actions after the mystery shopping was concluded. The Report also identify some lessons learned and sets out good practices.

At this stage, only a limited number of NCAs carried out such mystery shopping activities in their jurisdiction. Moreover, some NCAs reported that discussions are currently taking place at national level on the possibility of adding such powers to relevant competent authorities' mandate, for some of them as part of the implementation of the EU Consumer Protection Cooperation Regulation.

Regarding the lessons learned, the Report explains that mystery shopping allows NCAs to obtain greater insight into the conduct of financial institutions.

This, in turn, encourages them to take corrective actions better to comply with applicable requirements, and eventually enhances the protection of consumers.

Among the good practices identified by the NCAs, most of them concern common procedural aspects such as organising training for NCAs' inspection and supervisory staff, identifying target customer profiles, and defining agreed 'rules' of customer's behaviour.

To read more:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2021/1000492/EBA%20Report%20on%20the%20mystery%20shopping%20activities%20of%20National%20Competent%20Authorities.pdf

Contents

List of abbreviations 3

Executive summary 4

1. Background 6

2. Mystery shopping activities of National Competent Authorities 10

2.1 Objective, subject matter and product scope 10

2.2 Methodologies used 11

2.3 Follow-up actions after the mystery shopping 16

3. Lessons learned 18

3.1 Main benefits 18

3.2 Main challenges 19

3.3 Good practices identified by National Competent Authorities 19

Number 7

FluBot "package delivery" scam targeting Android devices

National Cyber Security Centre

The NCSC is aware that a malicious piece of spyware – known as FluBot – is affecting Android phones and devices across the UK.

The spyware is installed when a victim receives a text message, asking them to install a tracking app due to a 'missed package delivery'.

Scammers and cyber criminals regularly exploit well-known, trusted brands for their own personal gain and the FluBot campaign is a prime example of this.

Android users are urged to familiarise themselves with our guidance and be vigilant to any suspicious-looking text messages, which should be forwarded to 7726. You may visit: https://www.ncsc.gov.uk/guidance/flubot-guidance-for-text-message-scam

If you have already clicked the link to download the application:

You must take the following steps to clean your device, as your passwords and online accounts are now at risk from hackers.

- Do **not** enter your password, or log into any accounts until you have followed the below steps.
- To clean your device, you should:

- Perform a factory reset as soon as possible. The process for doing this will vary based on the device manufacturer and guidance can be found here. Note that if you don't have backups enabled, **you will lose data**.

- When you set up the device after the reset, it may ask you if you want to restore from a backup. You should avoid restoring from any backups created **after** you downloaded the app, **as they will also be infected**.

Number 8

Researchers Demonstrate Potential for Zero-Knowledge Proofs in Vulnerability Disclosure

Research teams led by Galois, Trail of Bits develop capability to mathematically prove exploitability of vulnerable software without revealing critical information

Today, the disclosure process for software vulnerabilities is fraught with challenges.

Cybersecurity researchers and software security analysts are faced with an ethics versus efficacy dilemma when it comes to reporting or sharing discovered bugs.

Revealing a vulnerability publicly may get the attention of the program's developers and motivate a timely response, but it could also result in a lawsuit against the researcher.

Further, public disclosure could enable bad actors to exploit the discovery before a patch or fix can be applied.

Sharing the vulnerability directly with the software maker on the other hand is ethically sound, but may not necessarily prompt action.

As history has shown, software makers are often reluctant or unwilling to engage with outside security teams and the disclosed vulnerabilities are frequently ignored, or corrective action is dangerously delayed.

DARPA's Securing Information for Encrypted Verification and Evaluation (SIEVE) program is exploring potential solutions to this problem through the use of *zero-knowledge proofs (ZKPs)*.

ZKPs are mathematically verifiable problem statements that can be used to reason about software or systems. The proofs can be used publicly without giving away sensitive information.

SIEVE is focused on developing computer science theory and software capable of increasing the expressivity of problem statements for which ZKPs are constructed while also making it easier to use the cryptographic method.

"Prior to SIEVE, one primary focus of applying ZKP research had been on maximizing the speed of communicating and verifying proofs – sometimes

called 'succinct zero-knowledge'," said Josh Baron, the program manager leading SIEVE.

"For applications like cryptocurrency and blockchain transactions, prioritizing communication and verification efficiency is essential. However, for many potential defense applications, including for highly complex proof statements like those that the Department of Defense may wish to employ, achieving total efficiency and optimization across all metrics may be needed."

In the case of vulnerability disclosure, ZKPs could allow a vulnerability researcher (the prover) to convince a software maker (the verifier) that they possess a piece of information – such as a bug or an exploit – without revealing so much information that their potential for a reward is ruined or requiring that they divulge how the information was uncovered.

One year into the SIEVE program, two research teams have demonstrated the first-ever capability to mathematically prove the exploitability of vulnerable software without revealing critical details around the vulnerability itself or the exploit.

One research team led by Galois, Inc., has demonstrated a ZKP for a previously known memory-safety vulnerability in the Game Boy Advance (GBA) Raster Image Transmogrifier, known as grit.

Memory-safety vulnerabilities are a critical class of vulnerabilities that frequently occur in modern software.

In the Galois-led demonstration, a vulnerability researcher was able to interactively convince another party of the existence of the specific vulnerability in around eight minutes.

To achieve this milestone, researchers developed techniques and prototypes that implement a combination of novel program analyses and protocols for proving and evaluating statements in zero knowledge.

Specifically, the team was able to develop a way to compactly mathematically represent memory-safety vulnerabilities, and then create a zero-knowledge proof based on that representation.

Although the current prototype can only produce proofs for programs that use a restricted set of language features, the Galois team aims to extend its capabilities to prove vulnerabilities of any C/C++ program that can be compiled using a standard compiler.

They are also actively researching prototypes that offer ZKPs of more complex claims, such as a program's overall memory safety.

A second team of researchers from Trail of Bits is working to model vulnerabilities at the systems architectural level, which is a lower level of abstraction than Galois is working on.

Their initial work has created a way to represent real-world instruction set architectures as Boolean circuits – or mathematical models of digital logic circuits – compatible with ZKPs so that users can demonstrate their ability to force a public binary into a specific malicious state.

The team's initial work targets the MSP430 microcontroller, a microprocessor commonly used in embedded systems.

From there, they discovered a way to mathematically represent a variety of common vulnerabilities so that ZKPs could be developed to prove the existence of those vulnerabilities.

The ZKP statement sizes ranged from 86MB to 1.1 GB, and took from 23 seconds to 256 seconds to verify on a desktop PC.

As an example, the team was able to prove that a smart lock using the MSP430 microcontroller could be opened via an undisclosed exploit without having to share details about the exploit or vulnerability.

"Essentially, the researchers took a smart lock, locked it, and then threw away the key. They were then able to exploit the underlying MSP430 to unlock it, and developed a zero-knowledge proof of the exploit to show that it could be done without having to share how it was done," explained Baron.

Trail of Bits has so far demonstrated the ability to perform ZKP disclosure for a wide variety of common types of vulnerabilities in MSP430 binaries, including stack and heap overflows, code injection, format string vulnerabilities, and bypassing memory protections, such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR).

The team is now working to expand the list of supported architectures and runtime environments, with the goal of capturing much of the common x86 architecture.

For example, they plan to produce ZKPs of binaries from DARPA's 2016 Cyber Grand Challenge, which run on DECREE – a simple operating system built on x86.

In this way, SIEVE is building on over a decade of DARPA research in how to formalize cybersecurity.

Number 9

Recommendations for the security of Connected and Automated Mobility (CAM)

The Connected and Automated Mobility (CAM) sector is an entire ecosystem of services, operations and infrastructures comprised of a variety of actors and stakeholders.

Under a new regulation set by the United Nations, car manufacturers are required to secure vehicles against cyberattacks.

In the European Union, the new regulation on cybersecurity will be mandatory for all new vehicle types from July 2022 and will become mandatory for all new vehicles produced from July 2024.

Moreover, the UNECE Regulation and related ISO standards apply to all CAM stakeholders who must ensure that their products and services conform to cybersecurity goals.

Increased connectivity and technological development in the ecosystem through various services, components and technologies are continuously expanding.

Therefore, within the CAM sector, where innovation and market growth are expanding, global players in the CAM sector face a risk of cyberattacks.

Connected services may be attacked by cyber-attackers and create cyber fraud, data breach and privacy incidents, as well as software overrides resulting in dangerous situations and accidents when part of the vehicle to everything (V2X) network is attacked, thereby threatening the drivers, road users and companies.

Efforts across the whole industry should be made to ensure that even if one system is compromised and/or tampered, the rest of the systems remain unaffected.

The interlinking of systems and services (both inside and outside the vehicle) and thus intelligent and connected mobility are already revolutionising users' lives.

The whole ecosystem involved in the CAM lifecycle has to cope with key challenges that add complexity to responding and managing CAM cybersecurity risks.

Today, connected vehicles, connected environment and connected infrastructure should be designed with new capabilities and features that have the potential to provide increased safety, better vehicle performance, competitive digital products and services, more comfort, environmental friendliness, as well as convenience for its end-users.

Governments, manufacturers, private companies (incl. SMEs and start-ups) as well as IT enterprises are all involved in the future development of intelligent and connected and automated mobility.

Fixed and mobile telecommunication infrastructure is necessary for cars to communicate with the smart road infrastructure (I2V and V2I), with devices (V2D), between vehicles (V2V), with other networks such as access to cloud infrastructure (V2N) as well as within the vehicle.
The aim of this report is to provide a high-level overview of the cybersecurity challenges in the CAM sector and to highlight both the concerned CAM actors and associated recommendations.

Cybersecurity in the CAM ecosystem is partially standardised and the role of standards is widely recognised.

All stakeholders' contributions to the CAM ecosystem are intertwined. Standards and regulations are often not adopted uniformly worldwide, and therefore some countries may advance faster than others in building a safe and secure cybersecurity system around CAM infrastructure.

In the context of growing cybersecurity threats and concerns about cybersecurity and data protection, this report aims to identify the main challenges in the current situation and to propose actionable recommendations for the different stakeholders involved in the CAM ecosystem to enhance the level of security and resilience of CAM infrastructures and systems in Europe.

Challenges in the CAM ecosystem arise from the whole lifecycle, therefore this report points to detailed challenges that the stakeholders are facing across Europe.

The recommendations proposed by ENISA aim to guide all CAM ecosystem stakeholders and to contribute to the improvement and harmonisation of cybersecurity in the CAM ecosystem in the European Union.

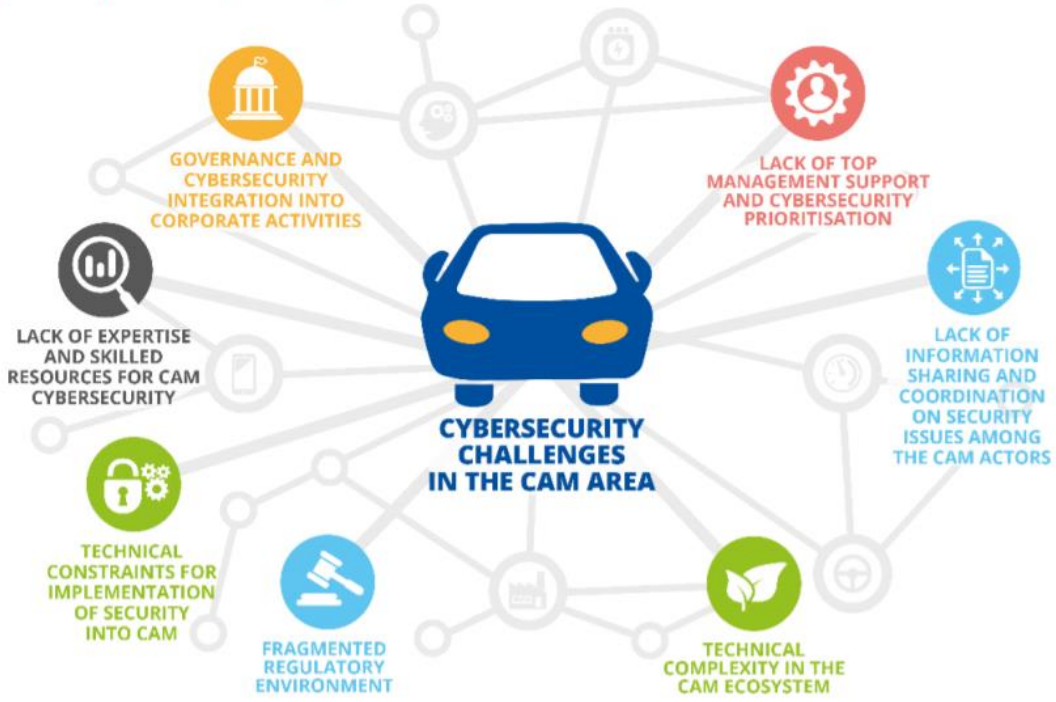
Using a layered approach of primary and secondary research, this report summarises insights across a complex CAM ecosystem.

Primary research methods included a survey and a series of interviews and validation discussions with key stakeholders from the CAM ecosystem.

Secondary research methods included desktop research of works of ENISA, official statistics, academic research, external studies and official documents, white papers, legislation, policies, strategies and initiatives to identify challenges and lessons learnt on cyber incidents against the CAM ecosystem.

To read more:
https://www.enisa.europa.eu/publications/recommendations-for-the-security-of-cam

Figure 1: Cybersecurity Challenges in the CAM area



Number 10

Heating up High Performance Computing with Low Temperature Integrated Circuits

Program aims to develop very low temperature device technology to overcome power efficiency limitations in high-performance computing

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

High performance computing (HPC) is a critical enabler of defense applications – from processing data at the tactical edge to powering weather prediction systems.

Historically, the advancement of HPC has been driven by new generations of integrated circuit (IC) technologies and continuous improvements in transistor density, performance, and energy efficiency.

However, Moore's Law – the guiding principle behind conventional transistor scaling – is slowing due to a host of technical challenges, including operating voltage reduction, making it difficult to continue with this paradigm.

The limitations of conventional computing technologies make it exceedingly difficult to keep pace with the demands for faster and more dense computational power in an energy efficient way.

"Today, we're aggressively reaching the end of Moore's Law scaling and are faced with the inability to scale power density much further in order to improve computing performance," said Jason Woo, a program manager in DARPA's Microsystems Technology Office (MTO).

"A viable solution is cold computing. While microelectronics is typically designed to operate at room temperature, we know that device characteristics improve significantly at reduced temperatures. Very low temperature devices – those operating at 77K or below – have the potential to overcome the power scaling limit, but challenges exist when you apply them to very large scale integration."

To overcome the barriers to thermal and power density scaling in HPC systems, DARPA developed the Low Temperature Logic Technology (LTLT) program. LTLT seeks to enable a dramatic improvement in performance over power when operating electronics at temperatures close to that of liquid nitrogen (~77K or -321F).

The goal of LTLT is to develop high-performance, low-temperature 14nm node or below complementary metal-oxide-semiconductor (CMOS)

FinFETs by making modifications to advanced very large scaled integration (VLSI) processes.

The resulting device/circuit technology should be capable of achieving a 25X improvement in performance/power compared to state-of-the-art (SOA) central processing units (CPUs) operating at room temperature. LTLT also seeks to develop and demonstrate a compact static random-access memory (SRAM) cell that can operate at 77K to complete the basic circuit elements needed for HPC engines.

To achieve the program's objectives, LTLT aims to exploit the unique device/material characteristics and performance of today's advanced nodes FinFETs operating at very low temperatures to develop transistors and memory cells with superior performance/power than is realizable by simply cooling current SOA VLSI technologies.

The program is broken out into two separate research areas.

The first will focus on researching, developing, and delivering a fabrication technology for highly integrated, advanced node CMOS operating at 77K, with low supply voltage and high performance.

The target technology will be able to integrate low temperature transistors, SRAM cells with 25X lower switching energy at 77K, and a supporting circuit/system design.

The second area in the program will explore advanced research concepts focused on high-risk/high payoff FinFET VLSI-compatible solutions for individual technical challenges at 77K.

Three specific challenges will be explored, which include ultra-low power, high-speed scaled transistors with new switching or transport mechanisms; compact, high speed, low energy SRAM cells; and new circuit techniques that utilize novel LTLT transistors and memory cells to achieve a 45X performance/power improvement.

The LTLT program will also utilize the benefits of DARPA's recently unveiled Toolbox Initiative.

The DARPA Toolbox provides open licensing opportunities with commercial technology vendors to the researchers behind the Agency's programs.

Through this initiative, DARPA researchers – or performers – are provided easy, low-cost, scalable access to state-of-the-art tools and intellectual

property (IP) under predictable legal terms and streamlined acquisition procedures.

Additional information about the Toolbox and the commercial suppliers participating in this initiative can be found here, https://www.darpa.mil/work-with-us/darpa-toolbox-initiative

Interested proposers have until May 18, 2021 to submit their proposals. Additional information on LTLT's goals and objectives can be found in the Broad Agency Announcement, https://beta.sam.gov/opp/110fc53cc3274eb4a7af78299ad2186c/view?keywords=LTLT&sort=-relevance&index=&is_active=true&page=1

Number II

Russian Foreign Intelligence Service Exploiting Five Publicly Known Vulnerabilities to Compromise U.S. and Allied Networks

The National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) jointly released a Cybersecurity Advisory, "Russian SVR Targets U.S. and Allied Networks," to expose ongoing Russian Foreign Intelligence Service (SVR) exploitation of five publicly known vulnerabilities.

This advisory is being released alongside the U.S. Government's formal attribution of the SolarWinds supply chain compromise and related cyber espionage campaign.

We are publishing this product to highlight additional tactics, techniques, and procedures being used by SVR so that network defenders can take action to mitigate against them.

Mitigation against these vulnerabilities is critically important as U.S. and allied networks are constantly scanned, targeted, and exploited by Russian state-sponsored cyber actors.

In addition to compromising the SolarWinds Orion software supply chain, recent SVR activities include targeting COVID-19 research facilities via WellMess malware and targeting networks through the VMware vulnerability disclosed by NSA.

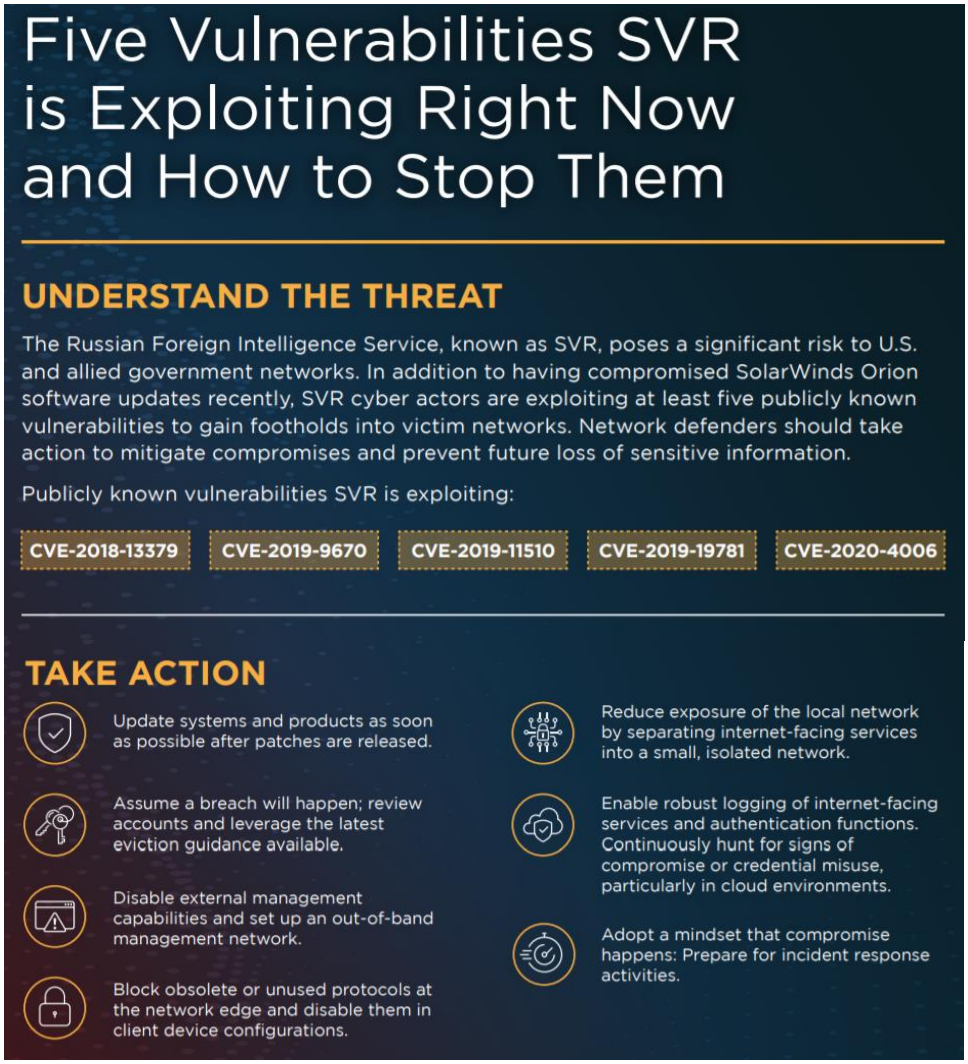
This was highlighted in NSA's Cybersecurity Advisory, "Russian State-Sponsored Actors Exploiting Vulnerability in Workspace ONE Access Using Compromised Credentials."

NSA, CISA, and FBI strongly encourage all cybersecurity stakeholders to check their networks for indicators of compromise related to all five vulnerabilities and the techniques detailed in the advisory and to urgently implement associated mitigations. NSA, CISA, and FBI also recognize all partners in the private and public sectors for comprehensive and collaborative efforts to respond to recent Russian activity in cyberspace.

NSA encourages its customers to mitigate against the following publicly known vulnerabilities:

- CVE-2018-13379 Fortinet FortiGate VPN

- CVE-2019-9670 Synacor Zimbra Collaboration Suite
- CVE-2019-11510 Pulse Secure Pulse Connect Secure VPN
- CVE-2019-19781 Citrix Application Delivery Controller and Gateway
- CVE-2020-4006 VMware Workspace ONE Access



For more information, review the advisory at: https://media.defense.gov/2021/Apr/15/2002621240/-1/-1/0/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF

or visit: https://www.nsa.gov/What-We-Do/Cybersecurity/Advisories-Technical-Guidance/

Number 12

From master masons to information architects: how standards can transform reporting (and bring benefits well beyond it)

Gareth Ramsay, Executive Director for Data and Analytics & Chief Data Officer of the Bank of England, webinar hosted by The EDM Council

Hello all – it's a great pleasure to be speaking to you. I'd like to thank John Bottega and the EDM Council for virtually hosting us today.

I want to begin by talking about cathedrals.

The great cathedrals of Europe were built in the Middle Ages by teams of skilled stone masons.

To get the dimensions of the building right, it is said that each team would use measures based around the body of the master mason: his foot, his stride, his arm, and so on. And so a local standard was born.

Those standards were designed with one specific use in mind – the construction of that cathedral. And very useful they were, too. But they were closed systems – the foot and the yard used to build one cathedral were different from those used to build another.

And this was not just an English peculiarity: across the channel, a foot length in Strasbourg was 295 mm, a foot in Paris was 325 mm, but a foot in Bordeaux was a relative whopper at 344 mm.

Of course people came to understand the great benefits of enforcing universal, common standards.

In part for maintaining the cathedrals themselves, so that new, replacement stones could be sourced that would fit snugly between their neighbours.

But the benefits of universal measurement standards could be applied a long way beyond the niche discipline of cathedral building.

Now some of you may think that today's financial system is not perfectly comparable to the glorious gothic cathedrals of the Middle Ages.

But like those cathedrals, many of the data systems underpinning today's financial firms and markets were built with narrow reference to their own needs, by their own master masons – their CIOs and systems architects.

They too were closed systems. Each needed to be able to record, track and manipulate its data.

Its data points needed to fit snugly alongside each other. But the design of each system often paid little attention – understandably – to any broader public good.

In this speech, I want to talk about whether there are wider public benefits that might flow from standardising these data labels, and set out a way forward to reap those benefits collectively.

So let me turn from mediaeval architecture to data.

At a central bank like the Bank of England, data is our life blood. We depend on our ability to access it, analyse it, and draw conclusions from it to set policies.

Effective management and use of data is how we meet our goals.

Of course, we are far from alone here – many organisations rely heavily on their use of data. But we are, perhaps, different to many in that the vast majority of the data we want is generated by others rather than ourselves.

The data we care about is the sum of millions of financial and economic interactions, taking place every second. And much of that data is captured and stored by financial institutions, as they go about serving their customers.

We need to get our hands on that data. We need data on the financial system in aggregate and also on specific markets within it, to help us understand where risks are emerging and to help us calibrate policies to maintain stability. And we need data about individual regulated firms, for our work as supervisor and as resolution authority.

So we have built data collection processes to give us that data. We publish reporting instructions. Firms then go through various steps: they interpret our instructions, identify the right data within their systems, put in place processes to integrate, cleanse and check the data, and then sign it off and deliver it to us.

But the amount of data we collect through these processes has been growing. It's hard to capture all of our data collections in a single measure.

But the accompanying chart shows the number of data points we collect through our regular rule-based banking collections.

Since 2014, this has grown around seven-fold. This growth has partly been a response to the financial crisis of 2008, when regulators and authorities around the world discovered huge gaps in what they knew, and what they could see, of risks emerging in the financial sector.

At the same time, technological change has been increasing the volume of data being produced, and the demands we can put upon the data. Like many of the financial firms we regulate, we want to make more extensive use of this bountiful data, using bigger datasets and newer, more complex analytical techniques.

These developments – the availability of, and need for, more data, and the desire to do more with it – have put growing strains on the processes and systems we use to collect it in the first place. That poses a growing challenge for us and for firms who are sending us the data, each firm doing so independently and in a different way.

And if it's hard for firms to supply us the right data, well, that matters for us. It may take industry longer to meet our requests. And if different firms interpret our requests in different ways, that makes it harder for us to draw conclusions from the data we receive.

To read more:
https://www.bankofengland.co.uk/speech/2021/april/gareth-ramsay-webinar-hosted-by-the-edm-council

Number 13

European Cybersecurity Month (ECSM) 2020 Deployment Report

The EU Cybersecurity Act (CSA) came into force on 27 June 2019 with an emphasis on making cybersecurity a priority in awareness campaigns.

In accordance with Articles 4 and 10 of the CSA, the European Union Agency for Cybersecurity (ENISA) must promote a high level of cybersecurity awareness, including cyber hygiene and cyber literacy among citizens, organisations and businesses.

Since 2012, the Agency has been raising public awareness of cybersecurity risks through an annual EU-wide awareness-raising campaign aimed at citizens, organisations and businesses – the European Cybersecurity Month (ECSM).

The month-long campaign every October across Europe, and beyond, promotes cybersecurity awareness and education, and provides guidance on good practices for individuals and organisations in order to create a more cyber secure culture across the EU and increase resilience.

The COVID-19 pandemic changed the scope of the ECSM, but not the level of outreach or success.

Every year, the ECSM has been an interactive month with in-person events spread across countries. It has been a platform for sharing ideas and campaign materials between countries.

The campaign includes new collaboration, workshops, conferences, training sessions and much more.

This year, the pandemic posed a great challenge, namely to transfer this platform to a digital one –for both organisers and participants.

ENISA was up for the challenge. The Agency set forth an ambitious online campaign, entitled 'Think Before U Click', with the social media hashtag #ThinkB4UClick.

The action plan called for an ambassador's programme, a partnership programme and a social media programme.

The online ECSM 2020 campaign was a success, garnering three times more engagement than the previous year.

Each year, the ECSM addresses the disparity between cybersecurity practices across EU Member States.

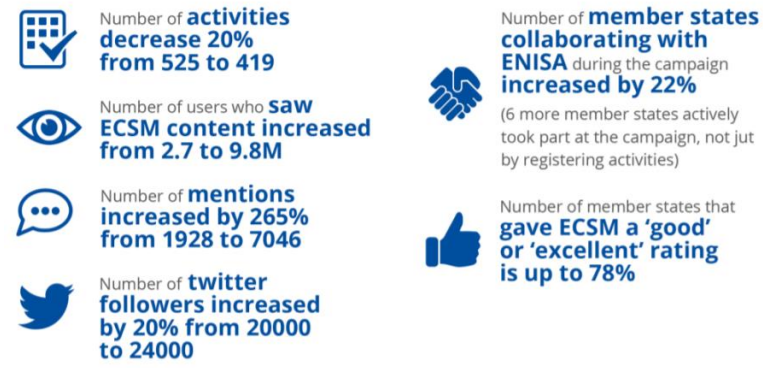


Figure 2: Planning of social media activities

Table 3: Number of #CyberSecMonth campaign mentions per country on a worldwide scale

Most active countries

	COUNTRY	MENTIONS	REACH
1	Italy	281	246 475
2	United Kingdom	215	99 882
3	Norway	137	158 972
4	Spain	91	123 722
5	Romania	85	29 930
6	Greece	60	28 994
7	France	58	63 186
8	Germany	46	129 298
9	Belgium	39	110 723
10	Ireland	38	32 089
11	Iceland	37	32 380
12	Poland	35	2879
13	United States	30	114 174
14	Croatia	29	2724
15	India	28	279 826
16	Slovenia	27	13 397
17	Czech Republic	25	1071
18	Lithuania	21	5534
19	Mexico	20	18 839
20	Bosnia and Herzegovina	19	4032

The report: https://www.enisa.europa.eu/publications/ecsm-deployment-report-2020

Number 14

Masks Under the Microscope

Viewed under a microscope, mask fabrics are complex, varied and beautiful.

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

To understand how something works, it helps to see it up close.

A team of researchers took this approach when studying the fabric masks that people wear to slow the spread of COVID-19.

Those masks work by blocking some of the virus-filled droplets and smaller particles, called aerosols, that an infected person exhales, and they also offer some protection to the wearer by filtering incoming air.

The researchers wanted to know how well different fabrics filter out those particles and what makes some fabrics better filters than others.

Their research indicates that that cotton fabrics tend to perform better than synthetics, with cotton flannels being particularly effective.

After being exposed to the moisture in a person's breath, cotton fabrics perform better still.

As part of this research, one team member, Edward Vicenzi, used a scanning electron microscope to examine the fabrics up close.

Vicenzi works at the Smithsonian's Museum Conservation Institute, where he studies the history and origin of objects in the museums' collection.

He is also a visiting researcher at NIST. His images gave the scientists important insights into the particle-filtering properties of different fabrics. And they can give us all a sense of the beautiful, textured, woven world right in front of our faces.

Polyester is a synthetic material that, like many fabrics, is made up of individual fibers bundled into yarns then woven together. The image shows the cross-sectional shapes of the individual fibers. The researchers used images such as this one to measure the width of the individual fibers — a key variable that affects particle filtration.

The entire scale bar in this image is 125 micrometers, or millionths of a meter, wide — a bit wider than an average human hair.

Aerosols that might contain the coronavirus vary in size, but smaller ones might be one-hundredth the width of the fibers in this image, and some are even smaller. Fabric masks do not capture all of these small aerosols, but they capture many of them, which slows the spread of the disease.

To read more: https://www.nist.gov/feature-stories/masks-under-microscope

Number 15

Exploring Research Directions in Cybersecurity

The European Union Agency for Cybersecurity has identified key research directions and innovation topics in cybersecurity to support the efforts of the EU towards a Digital Strategic Autonomy.

Resilience, technological sovereignty and leadership are essential for the EU and as such, they are addressed by the new EU Cybersecurity Strategy.

In an effort to support this cybersecurity strategy, the European Union Agency for Cybersecurity releases today a report intended to look into digital strategic autonomy in the EU and suggests future research directions.

What is Digital Strategic Autonomy?

Digital strategic autonomy can be defined as the ability of Europe to source products and services designed to meet the EU's specific needs and values, while avoiding being subject to the influence of the outside world.

In the digital world, such needs may encompass hardware, software or algorithms, manufactured as products and/or services, which should comply with the EU values, and thus preserve a fair digital ecosystem while respecting privacy and digital rights.

To ensure the sourcing of such products and/or services complies with the EU's needs and values, the EU has the option to self-produce them autonomously, or in the case where products and services are acquired from third countries, to certify them and validate their compliance.

However, in cases where there is a high dependence on sourcing, the EU should still be capable of operating its digital infrastructures without giving rise to any possible detrimental influence.

Hence, Europe needs to maintain the capability to produce its critical products and services independently.

In short, digital strategic autonomy means the capacity for the EU to remain autonomous in specific areas of society where digital technologies are used.

Why such a move?

The new challenges brought about by the digitalisation of our environment raise questions on our capacity to retain ownership and control of our personal data, of our technological assets and of our political stand. Such are the main dimensions to be considered under the idea of digital strategic autonomy.

Furthermore, the COVID-19 pandemic highlighted the importance of cybersecurity and the need for the EU to continue to invest in research & development in the digital sector. Within this context, ENISA's report sets and prioritises the key research and innovation directions in cybersecurity.

Key Research Directions: which are they?

The report identifies the following seven key research areas:

1. Data security;
2. Trustworthy software platforms;
3. Cyber threat management and response;
4. Trustworthy hardware platforms;
5. Cryptography;
6. User-centric security practices and tools;
7. Digital communication security.

For each of these areas, the report introduces the current state-of-play in the EU, includes an assessment of current and expected issues. The analyses included serve the purpose of issuing recommendations on cybersecurity related research topics. Such recommendations intend to highlight the bases needed to bolster the EU's digital autonomy.

Who is the report intended for?

Policymakers: the report provides objective-driven strategic guidance on future projects and investments in cybersecurity and can be used for the development of industrial and research policies;

Researchers: the analysis of the areas presented could serve as a guide to address the current research and technological challenges and help to re-assess priorities accordingly.

Further Information:
https://www.enisa.europa.eu/publications/cybersecurity-research-directions-for-the-eu2019s-digital-strategic-autonomy/

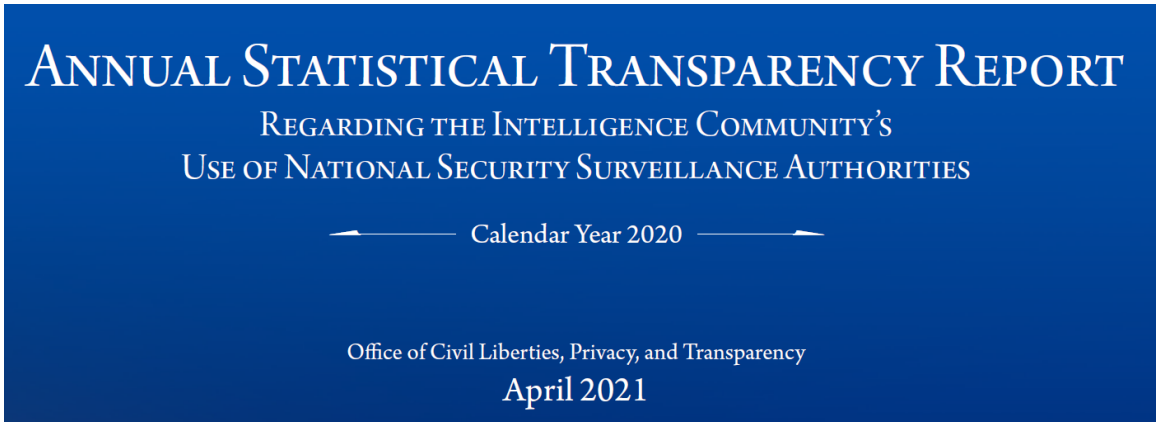
Number 16

Office of the Director of National Intelligence, April 2021

Statistical Transparency Report, Calendar Year 2020

Office of the Director of National Intelligence

Consistent with the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended (codified in 50 U.S.C. § 1873(b)), and the Intelligence Community's (IC) Principles of Intelligence Transparency, the Office of the Director of National Intelligence released the eighth annual Statistical Transparency Report Regarding Use of National Security Surveillance Authorities.



This report provides the public with statistics and contextual information on the scope of the government's use of FISA authorities, National Security Letters, and other national security authorities.

In conjunction with other publicly released material, this report adds insight into the rigorous and multi-layered oversight framework governing the IC that safeguards the privacy and civil liberties of United States (U.S.) person and non-U.S. person information acquired pursuant to these national security authorities.

"We are pleased to publish ODNI's eighth annual statistical transparency report," said Ben Huebner, Chief, ODNI Office of Civil Liberties, Privacy, and Transparency.

"The Intelligence Community remains committed to providing the public with information about how we apply important national security authorities. The information in today's report will help foster continued public dialogue regarding how the Intelligence Community protects national security, our privacy, and our liberty."

Additional public information on national security authorities is available at the Office of the Director of National Intelligence's (ODNI) website, www.dni.gov; the Intelligence Community's website, www.intel.gov; and ODNI's Tumblr site, IC on the Record, at IContheRecord.tumblr.com.

FISA Title I, Title III, and Title VII Sections 703 and 704

- All of these authorities require individual court orders based on probable cause.
- Titles I and III apply to FISA collection targeting persons within the United States.
- Sections 703 and 704 apply to FISA collection targeting U.S. persons outside the United States.
- Because individual courts orders are required, bulk collection is not permitted.

FISA Title VII Section 702

- Commonly referred to as "Section 702."
- Requires individual targeting determinations that the target (1) is a non-U.S. person (2) who is reasonably believed to be located outside the United States and (3) who has or is expected to communicate or receive foreign intelligence information.
- Because individual targeting decisions are required, bulk collection is not permitted.

Number 17

Race Logic: Novel Circuitry Solves a Myriad of Computationally Intensive Problems With a Minimum of Energy

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

From the branching pattern of leaf veins to the variety of interconnected pathways that spread the coronavirus, nature thrives on networks — grids that link the different components of complex systems.

Networks underlie such real-life problems as determining the most efficient route for a trucking company to deliver life-saving drugs and calculating the smallest number of mutations required to transform one string of DNA into another.

Instead of relying on software to tackle these computationally intensive puzzles, researchers at the National Institute of Standards and Technology (NIST) took an unconventional approach.

They created a design for an electronic hardware system that directly replicates the architecture of many types of networks.

The researchers demonstrated that their proposed hardware system, using a computational technique known as race logic, can solve a variety of complex puzzles both rapidly and with a minimum expenditure of energy.

Race logic requires less power and solves network problems more rapidly than competing general- purposed computers.

The scientists, who include Advait Madhavan of NIST and the University of Maryland in College Park and Matthew Daniels and Mark Stiles of NIST, describe their work in Volume 17, Issue 3, May 2021 of the ACM Journal on Emerging Technologies in Computing Systems.

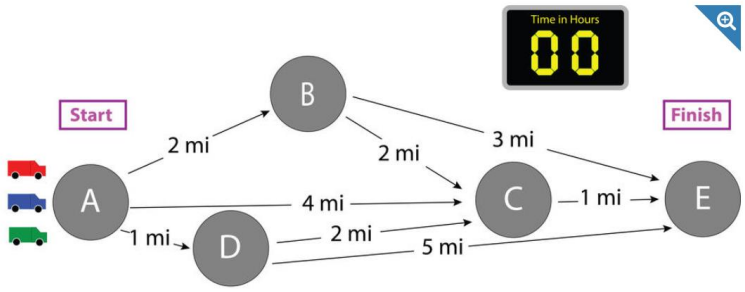
A key feature of race logic is that it encodes information differently from a standard computer. Digital information is typically encoded and processed using values of computer bits — a “1” if a logic statement is true and a “0” if it’s false. When a bit flips its value, say from 0 to 1, it means that a particular logic operation has been performed in order to solve a mathematical problem.

In contrast, race logic encodes and processes information by representing it as time signals — the time at which a particular group of computer bits transitions, or flips, from 0 to 1.

Large numbers of bit flips are the primary cause of the large power consumption in standard computers. In this respect, race logic offers an advantage because signals encoded in time involve only a few carefully orchestrated bit flips to process information, requiring much less power than signals encoded as 0s or 1s.

Computation is then performed by delaying some time signals relative to others, determined by the physics of the system under study. For example, consider a group of truck drivers who starts at point A and must deliver medicine to point E as fast as possible. Different possible routes go through three intersections — call them B, C and D.

To determine the most efficient route, the race logic circuit evaluates each possible segment of the trip, such as A-B and A-D. If A-B takes more time to travel than A-D, whether it's because the path is longer or has more traffic, A-B will be assigned a longer delay time. In the team's design, the longer time delay is implemented by adding additional resistance to the slower segment.

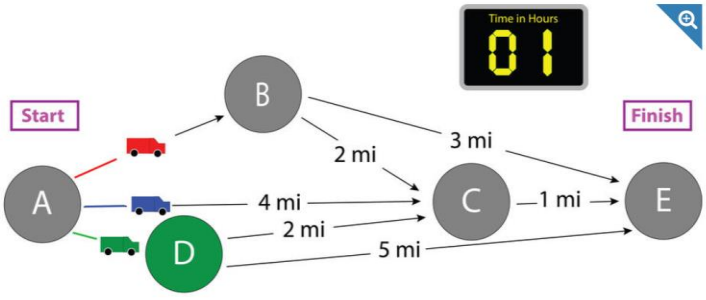


Numbers next to lines show distance in miles between Cities A, B, C, D, and E.

Each truck travels at the same speed --1 mile per hour -- and each travels in a different initial direction.

The object is to get from the start at City A to the finish at City E in the shortest amount of time.

Credit: NIST

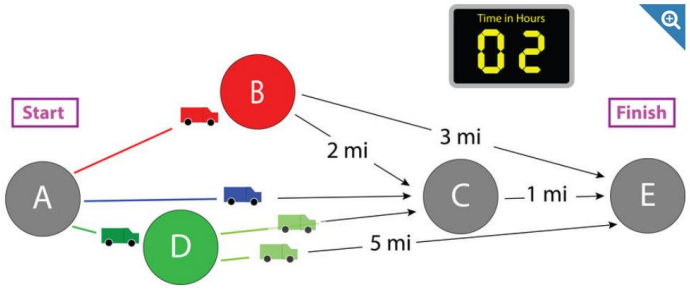


After 1 hour:

The **red** truck is halfway to City B. The **blue** truck is one-fourth of the way to City C.

The **green** truck has reached City D and claimed it for green.

Credit: NIST

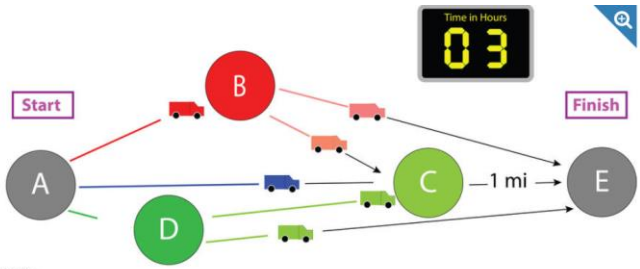


After 2 hours:

The **red** truck reaches City B and claims it for red. The **blue** truck is half of the way to City C.

The **green** truck stops and sends off two related (**light green**) trucks from City D, which it already claimed.

Credit: NIST



After 3 hours:

The **red** truck, having claimed City B, sends out two light red trucks -- one toward City C and one toward City E. The **blue** truck is still only 3/4ths of the way to City C.

One **light green** truck reaches City C first and claims it. The other **light green** truck has moved 2 miles toward City E.

Credit: NIST

To read more: https://www.nist.gov/news-events/news/2021/05/race-logic-novel-circuitry-solves-myriad-computationally-intensive-problems

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.