Cybersecurity Awareness Calendar

RANSOMWARE

May 2021
This calendar will feature a different topic each month to spread awareness of key aspects of cybersecurity and showcase ECSO members’ and partners’ solutions and services in the relevant areas to potential users.

The monthly themes for 2021 are planned as follows:

- **January** – Phishing
- **February** – Internet of Things
- **March** – Cloud Security
- **April** – Malware
- **May** – Ransomware
- **June** – Cybersecurity Skills
- **July** – Cyber Exercises
- **August** – Cybersecurity Summer School
- **September** – Mobile Devices & Bring Your Own Device (BYOD)
- **October** – Gender Diversity in Cyber
- **November** – Safe User Authentication & Password Hygiene
- **December** – Cybersecurity Trends 2022
In April 2020, Interpol issued a Purple Notice alerting police in all its 194 member countries to the heightened ransomware threat. This came after the organisation detected a significant increase in the number of attempted ransomware attacks against organisations and infrastructure engaged in the virus response. Ransomware is being used to hold hospitals and medical services digitally hostage; preventing them from accessing vital files and systems until a ransom is paid - source

According to Acronis, 2021 will be the “Year of Extortion” as ransomware continues to be the most prominent cyberthreat. One strain in particular, Maze ransomware, was widely used during the past year and accounted for nearly 50% of all ransomware cases - source

A report from Sophos shows that the average cost to rectify the impacts of recent ransomware attacks (considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc.) has more than doubled in the past year - source
RESOURCES FROM ECSO MEMBERS
RANSOMWARE: PLANNING FOR RESILIENCE

Ransomware is no longer just an emerging trend—it is a common widely-used tactic that threatens private and public sector as well as individuals and the amount of threat actors using ransomware as a form of attack are growing in numbers and in conniving techniques. The general rules advise not to pay ransom, implement security measures to prevent attacks, create backups and consider cloud, have solid incident response plans. Today’s top three challenges:

- ransomware extortionists ramping up attacks
- ransomware operators improving disruption ability
- lack of resilience in business growth and service strategies

There are ways to improve protection against ransomware without adding tons of new tools or trying to recruit specialised talent. One strategy is a Security-as-a-Service approach. Accenture Security is a leading provider of such cybersecurity services. They offer advanced robust incident response services to address Ransomware amongst other. Robust crisis management, continuity of operations plans, endpoint detection and response (EDR), encryption, patching infrastructure are only some mitigation recommendations they based their approach on. Accenture’s service of a rapid assessment of capabilities to respond to threats like ransomware includes:

- review of current endpoint and network technology in-place for detection/prevention
- review of security operations and incident response processes
- review of current threat intelligence

Presentation video here, more content from Accenture here and here.
THE DANGERS OF RANSOMWARE

How to keep your business safe?

The Cybersecurity Agency of Catalonia has created #Negocibersegur, a campaign addressed to companies to learn how to keep them safe against cyber attacks and to identify the main vectors of attack and entry of ransomware.

In the section of #Negocibersegur which deals with malware protection, it is highlighted that one should avoid compromising business assets. This objective should be achieved through awareness and effective protection software. You need to be prepared to avoid having an impact in the event of a ransomware attack.

By @ciberseguracat #Negocibersegur #ECSO #CyberAwareness
"Backup and Recover" is the specific toolbox of the Global Cyber Alliance (GCA) Cybersecurity Toolkits where you will find free tools and resources to mitigate the impact of a ransomware attack.

But do not be too confident. Protecting your business or your work against ransomware attacks will require paying attention to other aspects of your cybersecurity such as keeping your systems up to date, to securing your email, among other things. The best advice would be simply to explore the toolkits in depth and find the best resources and solutions for your situation.

Ransomware is a growing global concern, and it requires a globally coordinated response. This is why GCA is a proud member of international efforts such as the Ransomware Task Force (RTF) and the No More Ransom! Project (coordinated by Europol). We encourage you to explore these links together with GCA's own blog posts and news on the matter and some interesting materials from some of their partners, such as Mastercard (Trust Center) or the Cyber Readiness Institute.

PREVENT PHISHING AND MALWARE WITH GCA’S FREE CYBERSECURITY TOOLKITS

- Cybersecurity Toolkit for Small Business (multilingual)
- Cybersecurity Toolkit for Journalists
Ransomware is an attack in which the attacker restricts access to the victim’s service (or device), asking for a ransom to return access. The attack can be successful by hooking authentication systems, simply changing the password or encrypting data (like CryptoLocker does). The “ransom” to pay to the cybercriminals, usually is through a hard-to-trace electronic payment method, such as cryptocurrency.

Ransomware is almost always distributed through spam attacks. The spam email contains an attachment disguised as a legitimate file or includes a URL link in the message text.

To activate the payload, most ransomware requires user action. Educating employees to recognise and defend against cyber-attacks is essential.

According to Exprivia’s CyberSecurity Observatory, 4Q2020 recorded an increase in ransomware attacks in the Italian perimeter. In particular, there was an increase of 50% compared to 3Q2020 and of 650% compared to the value recorded in 1Q2020. If you want to better understand this trend you can download the Exprivia Threat Intelligence Report here.

Exprivia considers training on awareness and skills in general as a fundamental security control. Consult our awareness program here.
F-SECURE ON RANSOMWARE THREATS

Threat actors always look for new ways to maximise the effectiveness of their operations and fight against the rising maturity of defenders. In this article, F-Secure discusses two approaches that have become popular in ransomware attacks: (i) targeting the confidentiality of sensitive data within victim organisations through exfiltration and subsequent ransom demands not to release the data into the public sphere, and (ii) rapid ransomware deployment. While the latter brings new serious risks, F-Secure also observes that the use of the new techniques makes threat actors ‘noisier’ with their ransomware attacks, providing defenders with opportunities to detect and respond.

For organisations, choosing whether to pay a ransom is often a difficult choice. Even if payment is necessary to save the business, it presents a series of both moral and legal challenges that can be insurmountable. For example, can you adequately mitigate the risk of indirectly funding a terrorist group and thus committing a criminal act? In this publication, F-Secure experts share their views on the issue. In particular, they argue that it is better to remove the taboos associated with being compromised and help organisations improve their responses to ransomware attacks, so we could move to a point where extortion is no longer a viable business model for the criminals.
Ransomware is one of the incidents with the worst consequences faced by companies, blocking the information on computers and networks, in order to demand a ransom from the victims in exchange for unblocking it or even for its non-dissemination.

To help SMEs to avoid this threat, INCIBE, the Spanish National Cybersecurity Institute, has recently published the guide "Ransomware: an approach guide for the business owner", which explains what it is and how it works, how to protect your business, how to recover from a ransomware attack and how to strengthen the most important link in the chain, the employee.

In addition, this May, the new section "TemáTICas Ransomware" is published (in Spanish) with additional and updated resources to train staff to prevent this threat, and to react in time and recover as soon as possible in the event of a ransomware attack.
RANSOMWARE – WHAT IS IT ABOUT? AND WHAT CAN WE DO ABOUT IT?

WHAT IS IT ABOUT?
It might appear as random attacks that self-propagate or in a worm-like manner continuously deliver malware. Or you’ll find ransomware as targeted attacks being manually executed by very good organised criminal groups. Ransomware can also be ideologically motivated with the aim of causing simply destruction.

WHAT CAN WE DO ABOUT IT?
1. Choose a comprehensive protection with a secure browser solution including a shielded virtualised browser for accessing external websites
2. Web application firewalls prevent your websites from becoming a gateway for ransomware
3. Avoid uploading infected files by analysing all uploaded files through an enterprise anti-virus engine (WAF’s ICAP protocol based)
Ransomware is a type of malware (malicious software) that encrypts the files on a victim's device or a network's storage devices. Yet, this malware can infect not only desktop computers but also mobile devices, smartphones, and tablets as well. Also, ransomware does not make any distinction among victims: a private person can become a victim just like a huge corporation.

Ransomware often threatens the victim with permanent data destruction unless a ransom is paid to the cybercriminal. The payment usually should be done through a tough-to-trace electronic payment method such as Bitcoin.

In this blog post, CIRCL (Computer Incident Response Center, Part of Securitymadein.lu) shows an example of the most prominent type of ransomware (called ‘CTB-Locker’), and how an infected device looks like.
The last two years were marked by a series of even more elaborate targeted ransomware attacks on organisations (companies and institutions). These attacks are characterised by a greater than normal degree of sophistication and preparation.

Although Big Game Hunting mainly affects organisations able to pay a high ransom, it must be understood that these organisations are not chosen simply on that basis. Attackers scan the networks of an array of large companies and government bodies in search of a vulnerability that they can easily exploit. The huge advantage of these attacks was how simple they were to implement.

These large companies have to take adequate measures to protect themselves against it.

Check out Thales' website [here](#).

The following response actions are advised if an attack actually occurs:

- Adopt the right reflexes
- Ensured a managed response to the crisis
- Seek technical support
- Communicate at the right level
- Do not pay ransoms
- File a complaint
- Restore systems from healthy sources
HACK-IT-IN is the most famous cybersecurity conference of the FrenchTech Bordeaux, organised by TEHTRIS and the ENSEIRB MATMECA Engineering School.

The themes of cyber defense and cyberattack are at the heart of concerns, to stick to the technical reality and current threats. Come and find out the current issues of cybersecurity, as well as the offensive and defensive techniques of the moment! REGISTER HERE.

**Hack-IT-N 2021 Cybersecurity Conference**

**Cyber incident response with an XDR & Malware / Ransomware Patrol**

- Cyber incident response with an XDR (FR) by Jerome ATHIAS (TEHTRIS).
  This talk is about performing cyber incident response with an XDR. Pros and cons of using this technology while responding to a ransomware attack against a hospital (true story). The various steps will be presented. It goes further traditional methods of forensics and incident response.
  Jerome Athias is a cybersecurity expert with 20 years of experience. He worked for large companies around the world as a pentester, consultant and in SOCs. He is now Senior CERT Consultant for TEHTRIS. He was speaker for conferences like BlackHat or RSA.

- Malware / Ransomware Patrol
  POC Use Case by INP researchers about charges hunting with "Gorilla" in addition to polymorphic searches / unassembled charges.
Cryptographic ransomware is one of the greatest cyberthreats in today’s digital world. Ransomware attacks encrypt data files and make them unreadable; the damage is irreversible unless a huge ransom is paid. It has already attacked private companies, public institutions, and critical infrastructures, creating disruption often leaving victims out of business.

At the Interdisciplinary Center for Security Reliability and Trust of the University of Luxembourg, they have developed a prototype of an anti-ransomware solution, UshallNotPass, that prevents ransomware from encrypting files before damage is done. UshallNotPass is effective against a very large class of ransomware, including NotPetya, WannaCry and other notorious ransomware families, while using absolutely minimal system resources.

We encourage you to reach out to SnT to learn more about UshallNotPass and their research available [here](#) and [here](#).

Contacts:
Dr. Ziya Alper Genç (ziya.genc@uni.lu)
Prof. Gabriele Lenzini (gabriele.lenzini@uni.lu)
Prof. Peter Y. A. Ryan (peter.ryan@uni.lu)
RESOURCES FROM THE COMMUNITY
The CyberPeace Institute is working on shifting attention from the dominant focus on the financial impact of ransomware to the human harms and societal consequences of these attacks. They take a victim-centred perspective and explore long-term effects of ransomware targeting critical infrastructure and essential services. Please get in touch if you would like to contribute! More HERE

"eBanking – but secure!" is an independent platform of the Lucerne School of Information Technologies meant to assist you in retaining your personal information security (also against Ransomware), with a focus on e-banking. More HERE
Ransomware has become one of the most dangerous threats to organisations, using exploits, wrong configurations, credential theft and spear phishing to spread. We need technical solutions for the first ones, but awareness is our best ally to prevent the success of spear phishing, creating human firewalls.

Learn more

DEALING WITH EVOLVING RANSOMWARE DURING THE PANDEMIC

Basic hygiene and training to quickly and properly react are the best tools we have to fight ransomware. In the end, everything is about the tradeoff between effort and revenue, staying above the average means we are not profitable enough for attackers.

Learn more

ACTIVATING HUMAN FIREWALLS TO FIGHT RANSOMWARE

Ransomware has become one of the most dangerous threats to organisations, using exploits, wrong configurations, credential theft and spear phishing to spread. We need technical solutions for the first ones, but awareness is our best ally to prevent the success of spear phishing, creating human firewalls.

More HERE
Ransomware does not encrypt all corporate devices overnight. Once the network is breached, it takes a few weeks for the attack to incubate and the criminals to gain control over the corporate network.

Ransomware Takes Time to Incubate

Check out this article which provides an attack example and explains its mechanisms.

Do You Need Help Unlocking Your Digital Life?

The No More Ransom (NMR) project showcases the value of public-private cooperation in tackling cybercrime. NMR offers over 100 free of charge decryption tools to help ransomware victims retrieve their files. The project was launched in 2016, is available in 37 languages and supported by more than 160 partners worldwide.

Check out the No More Ransom website!
Including the human factor in cyber security to minimise the pain of ransomware attacks by building emotional firewalls. When we help people overcome the impulse of fear, decisions based on reason can prevail. More here
SUPPLEMENT YOUR EXISTING IT SECURITY INFRASTRUCTURE TO PROTECT YOURSELF AGAINST MALWARE!

VMRay focuses on a single mission: to help organisations protect themselves against the growing global threat potential: their automated malware, ransomware & phishing analysis and detection solutions help enterprises around the world minimise business risk, protect their valuable data and safeguard their brands. More HERE

ONLY 52 % OF RANSOMWARE ATTACKS USE E-MAIL ATTACHMENTS TO SUCCEED!

Some ransomwares exploit such applications vulnerabilities as 'command injections' to succeed. The YAGAAN source code scanner detects those vulnerabilities in your source code, and many others. More HERE
THANK YOU!

for your time

Cybersecurity Awareness Calendar is an initiative launched by:
European Cyber Security Organisation (ECSO)
29, rue Ducale
1000 - Brussels

www.ecs-org.eu
secretariat@ecs-org.eu

@ecso_eu

/company/ecso-cyber-security/