Orange
Cyberdefense

Security Intelligence | Research Report

Monthly Report
April 23

4

www.orangecyberdefense.com

Contents

Introduction

Western Digital Discloses Data Breach

Western Digital disclosed a data breach of its network, which disrupted its NAS service, My Cloud. The unnamed attackers gained access to multiple computer systems and claim to have stolen around 10 terabytes of data from the company. It is not yet known what types of data have been stolen, however the attackers are demanding a ransom of a “minimum 8 figures”.

Money Message Cy-X Group Targets Taiwanese PC Parts Maker MSI

Money Message has posted on its data leak website that it has breached the network of Taiwanese PC hardware manufacturer Micro-Star International and stolen source code for software along with other sensitive data. It is demanding payment and threatening to leak all of the allegedly stolen sensitive information within the next five days if the company does not comply. An alleged chat conversation with a representative showed the group as demanding a $4 million ransom in exchange for the 1.5 TB of data it claimed to have stolen.

CISA and Partners Disclose Snake Malware Threat From Russian Cyber Actors

CISA and partners released a joint advisory for a sophisticated cyber espionage tool used by Russian cyber actors. Hunting Russian Intelligence “Snake” Malware provides technical descriptions of the malware’s host architecture and network communications, and mitigations to help detect and defend against this threat.

CISA urges organizations to review the advisory for more information and apply the recommended mitigations and detection guidance.

At a glance

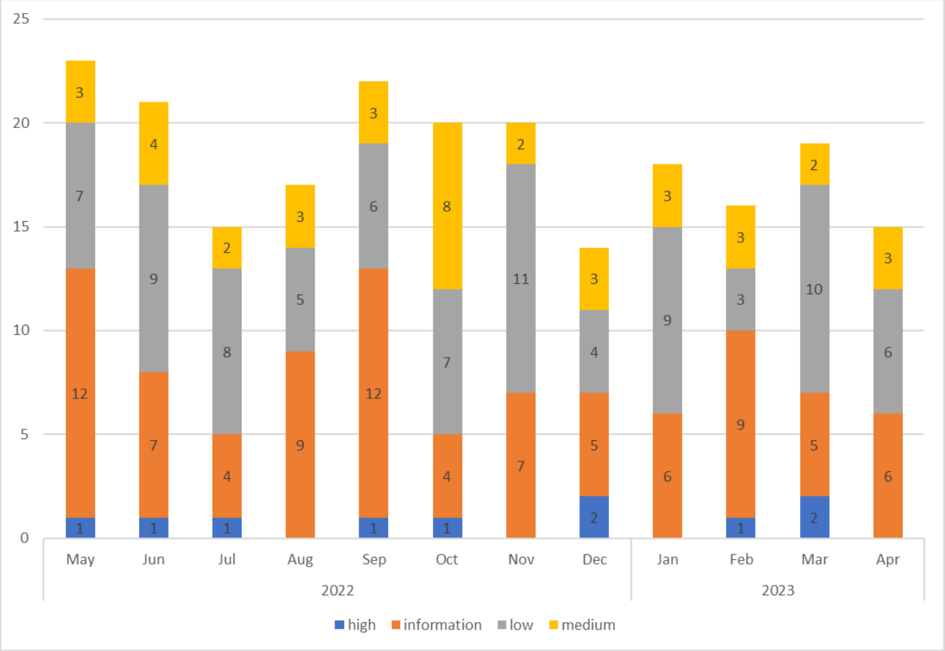
Optional Fix Issued By Microsoft For Secure Boot Zero-Day Used By Malware

Microsoft has issued security updates for a Secure-Boot zero-day vulnerability (CVE-2023-24932) that has been exploited by BlackLotus UEFI malware in the wild. This vulnerability allows attackers to evade Secure Boot protections by executing code at the Unified Extensible Firmware Interface (UEFI) level while Secure Boot is enabled. Successful exploitation relies on the attacker having physical access or local admin privileges on the targeted device. The security patches designed to address CVE-2023-24932 are solely available for supported versions of Windows 10, Windows 11, and Windows Server.

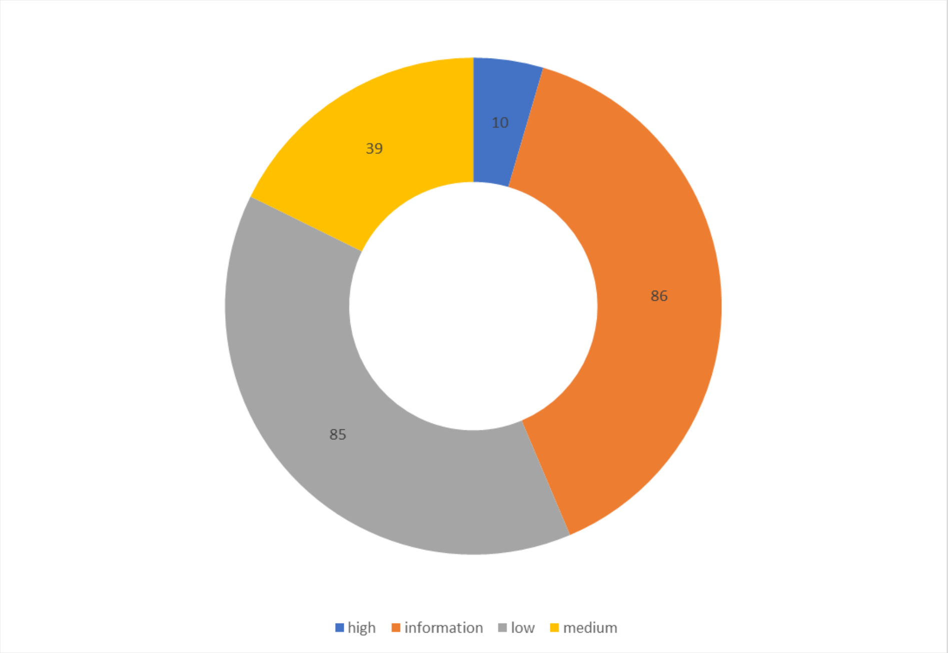
Please bear in mind that Microsoft's security fix for CVE-2023-24932 is disabled by default and will not offer protections. Before enabling this update, customers must carefully follow manual steps to update bootable media and apply revocations.

World Watch Review

The Orange Cyberdefense CERT published a total of 15 new World Watch advisories during April 2023, along with adding updates to a further 24 previously published advisories.



Breakdown of Published Advisories Previous 12 Months



Breakdown of Advisory Criticality for Previous 12 Months

Advisory Summary

As can be seen above there were no advisories rated as high criticality during April with all advisories given criticality ratings of low, medium or information when initially published. These ratings are based on our CERT's assessment of the risk and threat levels associated with the subject of the advisory at the time of publication, so even though an advisory may concern a vulnerability rated as critical by the vendor we may deem it to only initially be medium, if say there is no publicly available exploit. This is under constant monitoring however and subsequent updates will increase our criticality level as required if circumstances should change. Some advisories of note this month are:

718991 - PaperCut vulnerability exploitation leads to Bl00dy and Lockbit ransomware

- A critical vulnerability in a printing management software called PaperCut, used mostly in the Education sector, is being exploited these last 10 days in probable pre-ransomware activity. The authentication bypass vulnerability led to an administrator access with System rights, and from there to unauthenticated RCE on the host. It impacted most versions (above version 8 released in 2008) of the product, and was patched in March in a security advisory sent by the vendor.

- Close to 2,000 exposed instances initially detected by passive scanners were thus most probably vulnerable. Some servers have been compromised by this zero-day vulnerability and hands-on-keyboard activity is suspected using dual-use agents (Remote Monitoring Management tools Atera or Synchro). Furthermore, a public exploit code for the vulnerability was disclosed yersterday by a pentest company, putting at further risk all the remaining unpatched exposed instances.

- Some links to the Silence group (FIN11), thus maybe to TA505/Cl0P ransomware actor, were found when analyzing the infrastructure set up for the attack, with a C2 server also used in the same timeframe for Truebot, a malware part of Silence's arsenal.

719359 - Default secret key configuration in Apache Superset leads to RCE

- Horizon3 researchers discovered over 2,000 Apache Superset servers running with a dangerous default configuration that could lead to remote code execution on the server and on connected databases. The issue stems from a default Flask secret key that administrators are supposed to change, but most never do. Two-thirds of all Superset servers worldwide are expected to be vulnerable to this default configuration.

- The easy-to-exploit vulnerability is tracked as CVE-2023-27524 and received a base CVSS score of 10 from our Vulnerability Intelligence Watch experts. We expect this issue to be widely and very soon exploited in opportunistic attacks now that details have been publicly released.

719017 - Service Location Protocol (SLP) vulnerability facilitates DoS attacks

- Researchers from Bitsight and Curesec jointly discovered a vulnerability affecting the Service Location Protocol (SLP). SLP is a legacy network protocol that allows devices to discover and advertise services on a local network. The vulnerability, tracked as CVE-2023-29552, could be exploited by a remote attacker by sending a specific network packet (UDP Service Type Request) with a spoofed source IP address in order to perform UDP-based denial-of-service attacks with an amplification factor of up to 2200x. The vulnerability received a CVSS score of 8.6 from our Vulnerability Intelligence Watch experts.

- It is important to note that the vulnerability stems from a protocol weakness, which allows new service registration by default without adequate limitation, so a proper patch would involve changing the standard which defines the SLP v2 protocol (RFC 2608). Therefore, no patch is expected at the time.

712413 - April Patch Tuesday recap: LPE vulnerability exploited in Nokoyawa ransomware attacks

- As part of its April Patch Tuesday release, Microsoft fixed a zero-day vulnerability of high severity which was exploited in Nokoyawa ransomware attacks for local privileges escalation. As a reminder, Nokoyawa is a Windows ransomware that surfaced in February 2022 and whose strain has several similarities with the JSWorm, Karma and Nemty ransomware. We track the operation in a dedicated World Watch advisory available here.

- Identified as CVE-2023-28252 and located in Microsoft Common Log File System Driver, the vulnerability can only be exploited by a local attacker which needs to have the ability to execute code and corrupt another specially crafted base log file object so that a fake base log file item is treated as a real one and thus increases his privileges. The flaw thus received a maximum overall CVSS Score of 7.5 out of 10.

- The Microsoft Patch Tuesday release also patched several critical vulnerabilities, but not yet exploited by threat actors. Among these vulnerabilities, the flaw tracked as CVE-2023-21554 is a critical remote code execution vulnerability in the Microsoft Message Queuing service (an optional Windows component available on all Windows operating systems) and has been dubbed QueueJumper. Finally, another vulnerability identified as CVE-2023-28250 and affecting the Pragmatic General Multicast protocol installed with the MSMQ service may require your attention. An attacker can exploit this vulnerability to send a specially crafted file to the victim's network in order to carry out remote code execution.

Editor's Notes

Here the team will provide commentary on a news item, expansion on something specific such as a single incident, or could be as expansive as coverage on trends observed in the threat landscape.

Ric

Benchmarking OT Standards and Guidelines

Managing IT security through standards, guidelines, and control sets has become a mature process over the decades that it has been practiced. They typically have years of reiterations and refinements that have resulted in comprehensive security controls, clear guidance, consistency, continuous improvement processes, and built-in regulatory compliance, leading to these robust frameworks being viewed as credible solutions to safeguarding information systems from a variety of threats. Documents such as ISO/IEC 27001 and NIST SP 800-53 are so widely adopted that they are practically household names and each are accompanied by a broader set of supporting documentation, too.

However, despite operational technology (OT) having comparatively mature standards for concepts such as safety (e.g., IEC 61025, IEC 61511, IEC 61508, IEC 61882), it seemingly has nascent cyber security standards, guidelines, and control sets (contracted to just 'standards' from here for brevity). Moreover, in 2022 a study by SANS[1] noted that the implementation of cyber security controls within an OT environment is the responsibility of the "Owner or operator of the control system" at 37.7% and "Engineering manager" at 36.2%, clearly delineating the OT security boundary. In fact, the same study also highlighted the misconception that IT security practices and controls can simply be reappropriated for an OT environment, which is frequently not the case.

As opposed to the few de-facto IT security standards, OT has a number of relatively recent and competing standards. To understand these better, I was recently a part of a team that conducted a study to better understand and benchmark these OT document sets against one another, as well as their IT security counterparts. While the research paper is not yet released (although will be soon), the following presents some very brief commentary of seven prominent OT document sets based on the analysis conducted.

The *NIST CSF*, while not entirely OT focused, positions itself as a framework for critical national infrastructure (CNI), of which OT is a commonly utilized technology. It provides a comprehensive overview of requirements, categories, and controls required to effectively implement security measures for CNI. Among other aspects, it covers technical and social controls and links back to organizational security policies. Although comprehensive in its overview, it does not provide implementation guidance for security controls; however, it does refer to external resources for that advice.

[1] D. Parsons, "The state of ICS/OT cybersecurity in 2022 and beyond" 2022.

IEC 62443 is specifically focused on OT, or Industrial Automation and Control Systems (IACS) as it is called by its creators, the International Society of Automation (ISA). It consists of an exhaustive series of standards that provide a range of requirements and controls to asset owners, integrators, maintainers, and vendors. It covers multiple security levels, complete with guidance for how to implement each control. However, although it refers to external resources, it does not do this at an individual control level.

ISO/IEC 27019 is the ISO/EC 27000 series' answer to 'information security controls in the energy utility industry'. It consists of a thorough set of objectives and controls for OT that are mapped to security policies within other documents of the ISO/IEC 27000 series, in which it resides. It presents OT-specific supplementary guidance for controls provided in ISO/IEC 27002, the controls list for the series, but it does not provide controls where it deems that no OT-specific commentary is required. The individual controls do not contain references to external sources, but there are some in the bibliography.

The *UK National Cyber Security Centre's (NCSC) Cyber Assessment Framework (CAF)* is their guidance, as a competent authority, for relevant organizations to implement controls compliant with the Network and Information Security Regulations. CAF uses an outcome-based approach consisting of four high-level objectives, each containing control categories and sub-categories. It implies the requirement for information security policies but does not explicitly state which are required. There is high-level guidance for implementing controls, bolstered by examples. The framework utilizes references heavily for implementation and other guidance, particularly ISO/IEC 27001 and IEC 62443.

The UK's *Office for Nuclear Regulation*'s *(ONR) Security Assessment Principles (SyAPs)* focus on the nuclear sector and thus provides guidance towards its regulation. There are no immediately obvious security objectives in the documents; however, they can be derived from the provided security control categories. No in-depth control implementation guidance is provided, but the requirements are extensive such that they can be used as high-level guidance. There are no external resources referenced by SyAPs throughout its documents.

Finally, the *North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP)* plan is a set of standards consisting of a comprehensive set of documents covering many controls. Multiple documents contain different control categories, which have multiple sub-categories. Although no in-depth implementation guidance is provided, example evidence can be used as high-level guidance. Additional use of Violation Security Levels is incorporated to determine the level of non-compliance to the standard. NERC CIP does not provide any references to external resources.

So, what does this all mean? Unexpectedly, the security controls present within these OT standards are generally mature and even comparable to their IT counterparts. However, there are a few notable areas where improvements can be made. For example, many of the OT standards do not provide explicit implementation guidance. Instead, they often refer back to primarily IT-focused parent standards or provide only implicit guidance through example evidence or requirements for having correctly implemented each control. This, as you may imagine, could make it challenging for organizations to effectively apply these controls to their OT environments, as the guidance may not be suitable for them. There are also discrepancies between the documents where one may focus more heavily on a given area, which may lead to varying levels of implementation quality and effectiveness for organizations depending on the standards they adopt.

Ultimately, however, despite the expected nascent nature of these standards, they seem to be mature in their high-level comprehensiveness of controls and suggested areas of focus for OT-security. This is a positive outcome, as there is less work for the providers of these standards to reach a level of excellence in their advice and guidance. Therefore, hopefully OT cyber security will progress at a rate that is adequate to stave off the much-vaunted OT cyber apocalypse we've been warned about.

Diana

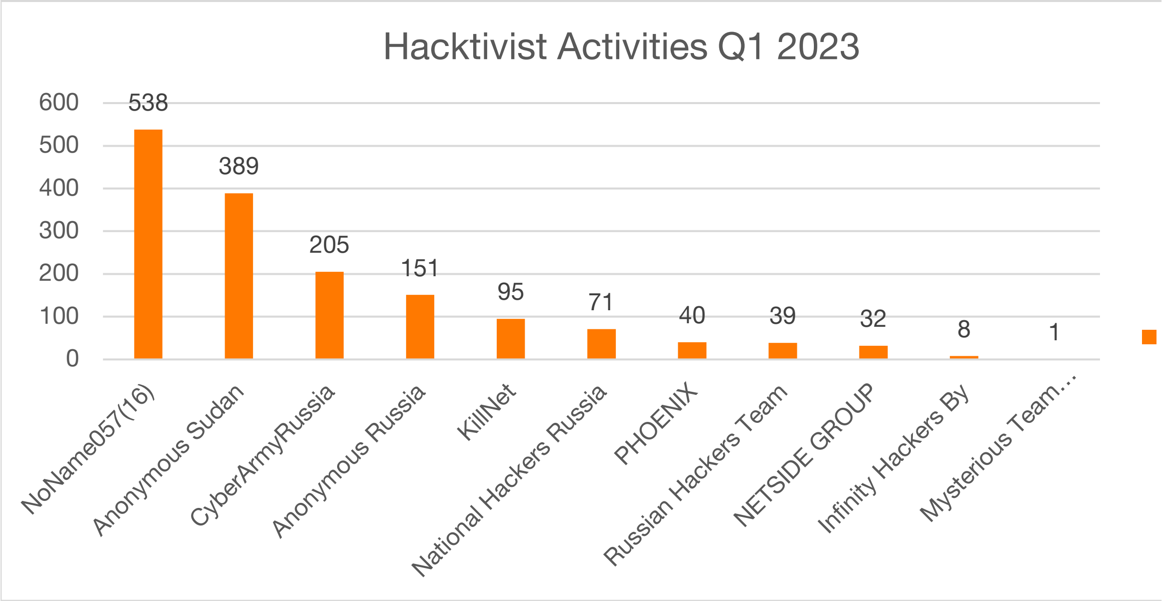
Current Hacktivism in the Nordics

Since January, when a hacktivist group named *Anonymous Sudan* began, we started monitoring some of the hacktivist groups that have been targeting the Nordics, namely Sweden, Denmark, Norway and Finland.

A recent study[2] conducted by Radware looked at hacktivist activities between February 2023 and April 2023 and has shown that NoName057(16) was one of the most active groups, politically driven and pro-Russian. This group has caught our attention only in the beginning of May where they targeted Sweden and Denmark heavily. Anonymous Sudan has been classified by Radware as religiously driven, which makes sense since they have publicly stated their mission to attack anyone opposing Islam. While Anonymous Sudan targeted Sweden and Denmark during February and March, they have lately focused heavily on Israel.

Intel471, who we have a collaboration with for research purposes, has been sharing their hacktivism data with us. During Q1, they also saw NoName057(16) to be by far the most active group, followed by Anonymous Sudan, CyberArmyRussia and Killnet.

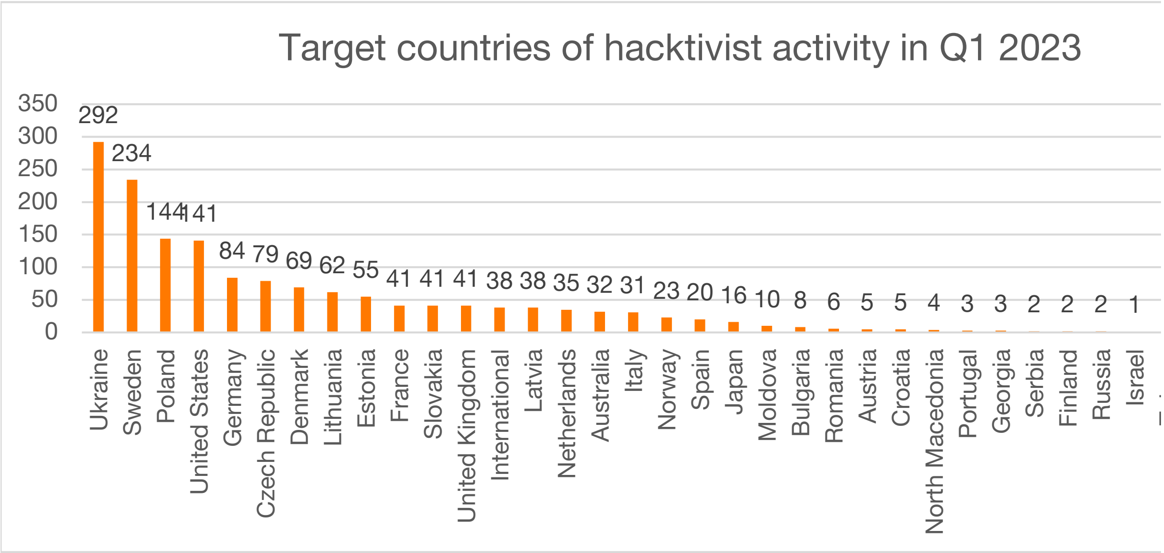
[2] https://www.radware.com/security/threat-advisories-and-attack-reports/hacktivism-unveiled-april-2023/



Many hacktivist groups use Telegram as their main communication channels. The data that is presented here shows the announcement of a specific target in the respective Telegram channel.

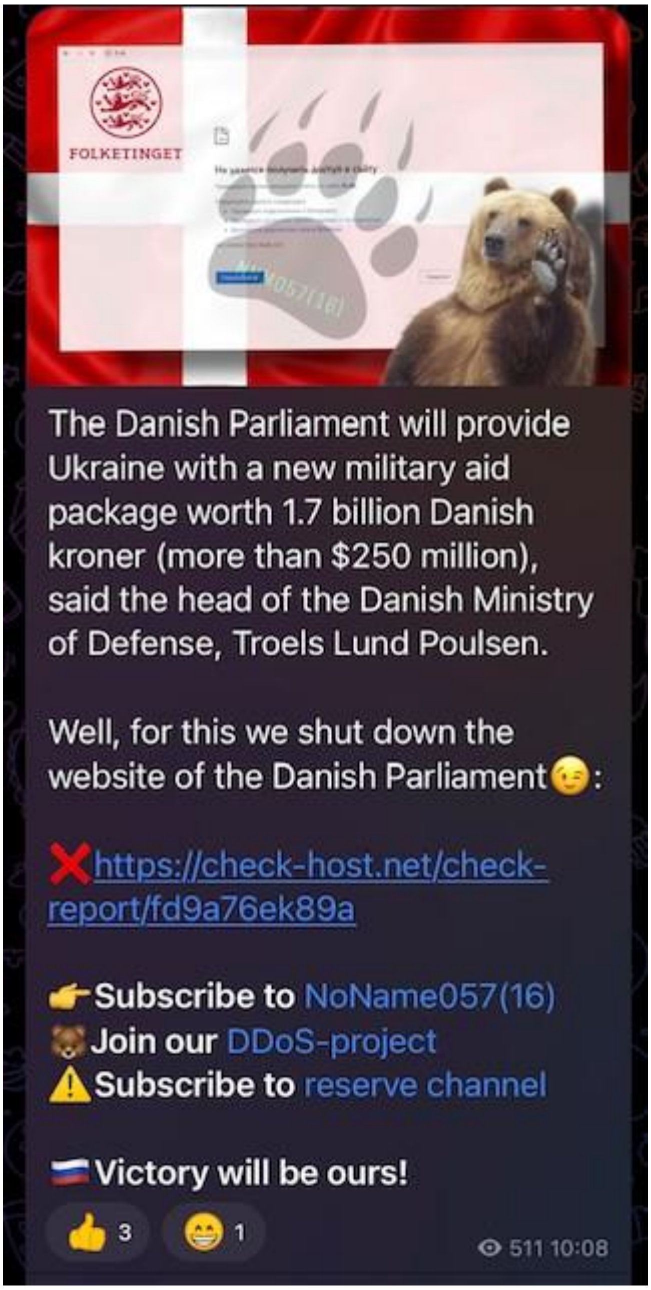
Our CERT has recently reported on another hacktivist group called Killnet that began its activity just before the Ukraine war began and has since then conducted many politically motivated DDoS attacks and is now rebranding into a private military hacking company called Black Skills. Besides a very similar country target profile as NoName has; Sweden, Denmark, Norway and Finland all have been impacted by Killnet's attacks. Despite going "private", Killnet promised to continue its destructive activities supporting Russia's interests. Regardless of its latest re-organization, Killnet has continued to target several organizations worldwide, the most important of these attacks involved a leak of data belonging to 4,639 individuals presumably linked to NATO.

When looking at what countries have been mostly impacted in Q1 2023, we see Sweden in second place. We expect that April and May will most likely put Sweden and Denmark again in the top 10 impacted countries.



On the 9th of May, NoName targeted at least 9 different countries using the Russian holiday called "Victory Day" that commemorates the Soviet victory over Nazi Germany in 1945. The countries they targeted were blamed for either having demolished monuments of former Soviet figures or executed NATO exercises that NoName would then use to call their attacks "Victory Exercise". Countries impacted during the 9th of May were Ukraine, Czech Republic, Latvia, Canada, Poland, Germany, Great Britain and Lithuania.

NoName focused heavily on Denmark between the 10-11th of May, justifying their DDoS attacks with the reason that the "Danish Parliament will provide Ukraine with a new military aid package" (see screenshot). As can be seen, this hacktivist group has a very high pace in moving between countries, using pro-Russian narratives to justify their attacks. Sweden was heavily targeted in the first week of May, in between Sweden and Denmark, countries such as Poland, Great Britain, Ukraine and Latvia were also attacked by NoName for politically motivated reasons.



The Danish Parliament will provide Ukraine with a new military aid package worth 1.7 billion Danish kroner (more than $250 million), said the head of the Danish Ministry of Defense, Troels Lund Poulsen.

Well, for this we shut down the website of the Danish Parliament😉:

❌https://check-host.net/check-report/fd9a76ek89a

👉Subscribe to NoName057(16)
🐻Join our DDoS-project
⚠️Subscribe to reserve channel

🇷🇺Victory will be ours!

👍 3 😁 1 👁 511 10:08

While hacktivism is nothing new, the Ukraine war has brought this ecosystem to another level, for Sweden we observe that hacktivist groups targeting Sweden are both motivated by ideology and the current political situation of the ongoing Ukraine war and Sweden's efforts to join NATO. Pro-Russian hacktivist groups have shaped the recent attacks against Sweden and Denmark, these are closely connected to NATO activities; and thus, we do expect that this trend we are currently observing will continue.

Good News Cyber

- Faster detection of compromised networks: According to three different cyber security companies, the "dwell time", or the amount of time an attacker remains within a compromised network before being discovered, has dropped to only a few weeks. Sophos reported that the median dwell time had dropped to 10 days, whereas Mandiant previously reported 16 days and Secureworks 11. The Sophos report caveats that how you interpret the data will determine whether this is good news or not. The proliferation of Cy-X attacks where the intention is to get in, usually quickly exfiltrate data and then let the victim know either by encrypting with ransomware or by posting on their leak sites, could be reducing dwell time. That said they did note that non-ransomware dwell times dropped from 34 days to 11 also so we are optimistically deciding to consider this good news.

- The operation of the CryptBot malware has been disrupted by Google. Google announced that it had begun legal action against distributors of the CryptBot infostealer, and a New York judge has given a temporary restraining order that permits Google to shut down current and future domains that are connected to the distribution of CryptBot.

- Europol coordinated an operation targeting the "Monopoly Market" on the dark web, arresting 288 suspects and seizing 50.8 million euros in cash and virtual currencies, 850 kilograms of drugs, and 117 firearms. The operation sends a strong message to criminals on the dark web that international law enforcement has the means and ability to identify and hold them accountable. The largest number of arrests were made in the United States, followed by the United Kingdom and Germany. Investigations to identify additional individuals behind dark web accounts are still ongoing.

- Microsoft's Digital Crimes Unit, cybersecurity firm Fortra and the Health Information Sharing & Analysis Center announced legal action to seize domains related to criminal activity involving cracked copies of the security testing application Cobalt Strike, which has become a favorite tool for cybercriminals to carry out attacks. The court order targets 16 anonymous "John Doe" actors engaged in a range of criminal behavior, from ransomware activity to malware distribution and development. Microsoft has pioneered the use of domain seizure as a way to disrupt the technical infrastructure malicious hackers rely on. The action against illicit Cobalt Strike applications is the culmination of a year-long investigation.

- The Threat Response Unit (TRU) of eSentire has begun a multi-pronged onslaught against the Gootloader Initial Access-as-a-Service Operation. Gootloader is a large cybercrime organisation that has been operating since 2018 and has been targeting law firms and corporate legal departments in the US, Canada, the UK, and Australia. It was named as one of the top malware strains of 2021 by the Cybersecurity and Infrastructure Security Agency (CISA). Gootloader tailors its victim pool to a subset of organisations most likely to pay a hefty ransom by employing SEO poisoning to lure victims to malicious WordPress blogs. Joe Stewart and Keegan Keplinger's research revealed that Gootloader infects legal professionals by attracting them to blogs filled with "legal agreements" and "contracts".

Stewart and Keplinger used Gootloader page data to confirm a connection between the Gootloader Operator and the REvil Gang. They also narrowed down the timeframes of all REvil-sponsored Gootloader ads to the day. The researchers discovered that the Gootloader virus operator has built a feature to prevent security researchers from discovering his payloads, they revealed that they and other security defenders may use a similar method to conceal end-users from the Gootloader Operator, proactively safeguarding organisations from infection. Stewart has also constructed a crawler to find live Gootloader webpages and is sharing technical details with search engine providers so steps can be put in place to block them.