Threat Highlights Report

April 2022

WITH secure

Contents

Foreword

The threat landscape for April continues to be dominated by state-backed threats related to the ongoing invasion of Ukraine by Russia and increased tensions between Russia, the United States and the wider NATO alliance. Following months of warnings and advisories regarding the threat that state-backed threat actors present to critical national infrastructure, the security community is now aware of and able to analyze samples of new malware. INCONTROLLER/Pipedream is designed to disrupt industrial control systems used across both public and private sector infrastructure, clearly highlighting the capability and intention of hostile countries to develop malware and tools designed for use in cyber warfare.

While previous months have focused on the demise and retirement of several ransomware groups, it has become clear that the leak of sensitive data relating to the CONTI group has done little to halt their operations, with them continuing to attack targets and leak new data to their ".onion" site. Other groups such as LockBit remain prevalent and new groups such as Blackcat and Blackbyte, show how ransomware remains a widespread issue, despite a shift in media focus to state-backed activities.

This month also highlights a new attack technique called MFA fatigue, as well as providing an insight into LAPSUS$ and CONTI, thanks to leaked chat logs and material pertaining to both group's activities, personnel, and infrastructure.

As always, we hope you enjoy this month's report, and we welcome any feedback you may have.

Ziggy Davies, Threat Intelligence Analyst

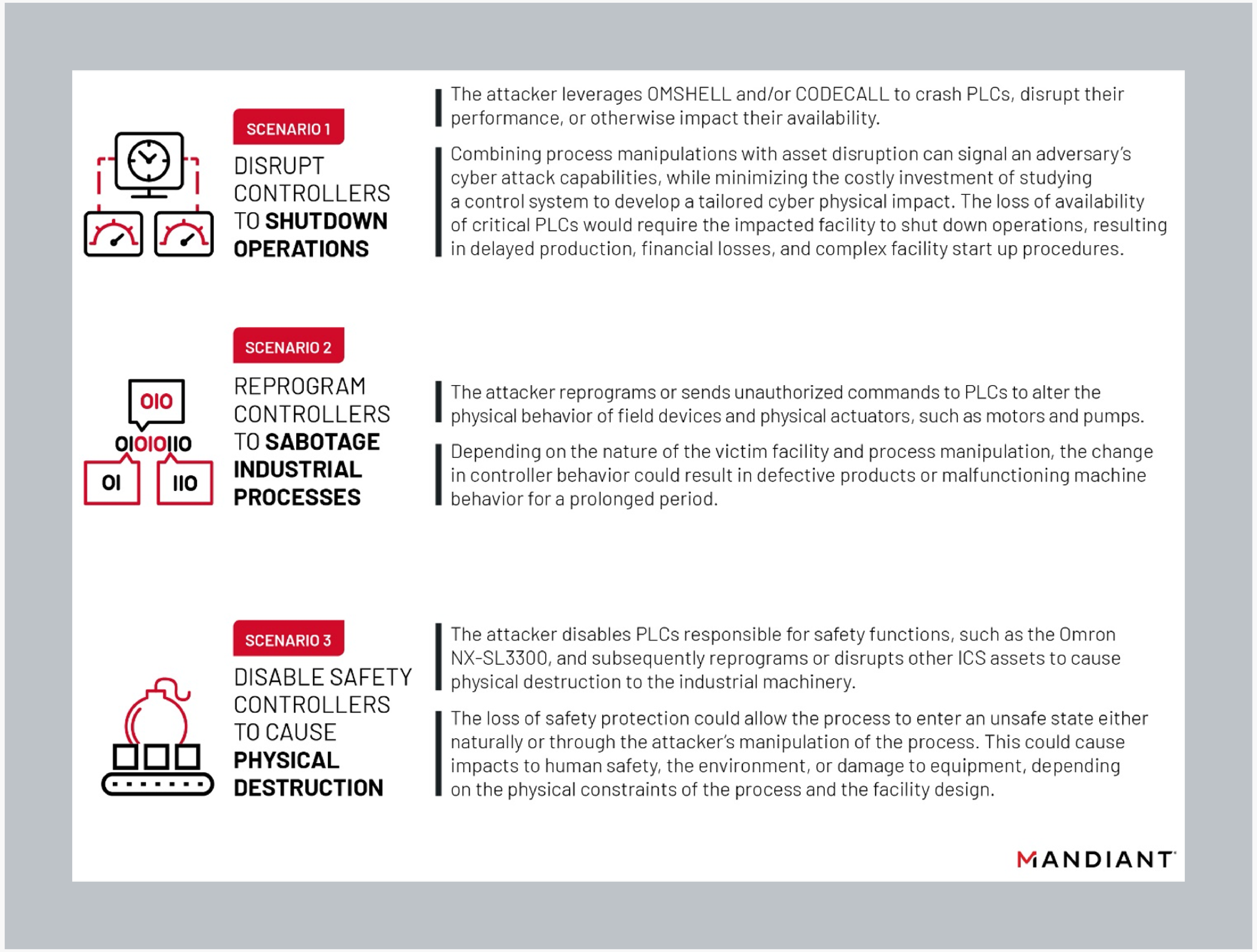
1 Monthly highlights

1.1 CNI targeted with ICS malware

The United States (US) Cyber Security and Infrastructure Security Agency (CISA), FBI, NSA and Department of Energy (DoE) have released a joint alert warning that threat actors are creating bespoke malware designed to target industrial control systems (ICS) used within critical national infrastructure (CNI) such as power stations.

Researchers at Mandiant, working in partnership with Schneider Electric (SE) have been analyzing a set of malicious tools designed to attack ICS systems. They are collectively calling this tooling as “INCONTROLLER”, which is also tracked by Dragos as “Pipedream” and described as being “built to target machine automation devices”.

INCONTROLLER includes three tools called “TAGRUN”, “CODECALL” and “OMSHELL”, which “can interact with specific industrial equipment embedded in different types of machinery leveraged across multiple industries”. Mandiant assesses that INCONTROLLER is “exceptionally rare and dangerous” and has highlighted three possible attack scenarios, which include causing disruption, sabotage, and physical destruction:


010
01010110
01
110
MANDIANT

SCENARIO 1

DISRUPT CONTROLLERS TO **SHUTDOWN OPERATIONS**

The attacker leverages OMSHELL and/or CODECALL to crash PLCs, disrupt their performance, or otherwise impact their availability.

Combining process manipulations with asset disruption can signal an adversary’s cyber attack capabilities, while minimizing the costly investment of studying a control system to develop a tailored cyber physical impact. The loss of availability of critical PLCs would require the impacted facility to shut down operations, resulting in delayed production, financial losses, and complex facility start up procedures.

SCENARIO 2

REPROGRAM CONTROLLERS TO **SABOTAGE INDUSTRIAL PROCESSES**

The attacker reprograms or sends unauthorized commands to PLCs to alter the physical behavior of field devices and physical actuators, such as motors and pumps.

Depending on the nature of the victim facility and process manipulation, the change in controller behavior could result in defective products or malfunctioning machine behavior for a prolonged period.

SCENARIO 3

DISABLE SAFETY CONTROLLERS TO CAUSE **PHYSICAL DESTRUCTION**

The attacker disables PLCs responsible for safety functions, such as the Omron NX-SL3300, and subsequently reprograms or disrupts other ICS assets to cause physical destruction to the industrial machinery.

The loss of safety protection could allow the process to enter an unsafe state either naturally or through the attacker’s manipulation of the process. This could cause impacts to human safety, the environment, or damage to equipment, depending on the physical constraints of the process and the facility design.

Mandiant has concluded that INCONTROLLER is very likely linked to a state-backed threat actor “given the complexity of the malware, the expertise and resources that would be required to build it, and its limited utility in financially motivated operations”, and while there is no direct evidence linking the malware with Russia, there have been several other previous ICS and CNI focused malware variants such as Triton, Industroyer and BlackEnergy attributed to them, making it within their playbook and comes at a time when Russia is known to be conducting cyber warfare against Ukrainian CNI.

WithSecure™ Insight

There have been constant warnings and advisories issued by CISA and other security agencies over the past few months relating to the targeting of CNI by state-backed threat actors linked to Russia and INCONTROLLER appears to be yet another sign of the active preparation of cyber warfare by a hostile state.

While INCONTROLLER has been detected and reported on before its deployment, the danger it still presents is real and potentially severe, with the malware being adaptable and the ICS systems it targets being notably difficult to update against attack, leading to possible delays in mitigations being implemented. The specific systems (OPC UA, SE, Omron) that INCONTROLLER targets are widespread and indicate the level of reconnaissance performed by the threat actor, and how they have designed a toolset which specifically targets CNI environments, making their motivation clear.

INCONTROLLER is of course not the only malware that is known to target CNI/ICS with others including Industroyer, Triton, BlackEnergy, Havex and CrashOverride with Ukraine’s computer emergency response team (CERT-UA) recently detecting the use of a new Industroyer2 variant, which was used in conjunction with the recently reported on CaddyWiper malware.

1.2 FA Fatigue: A new attack technique

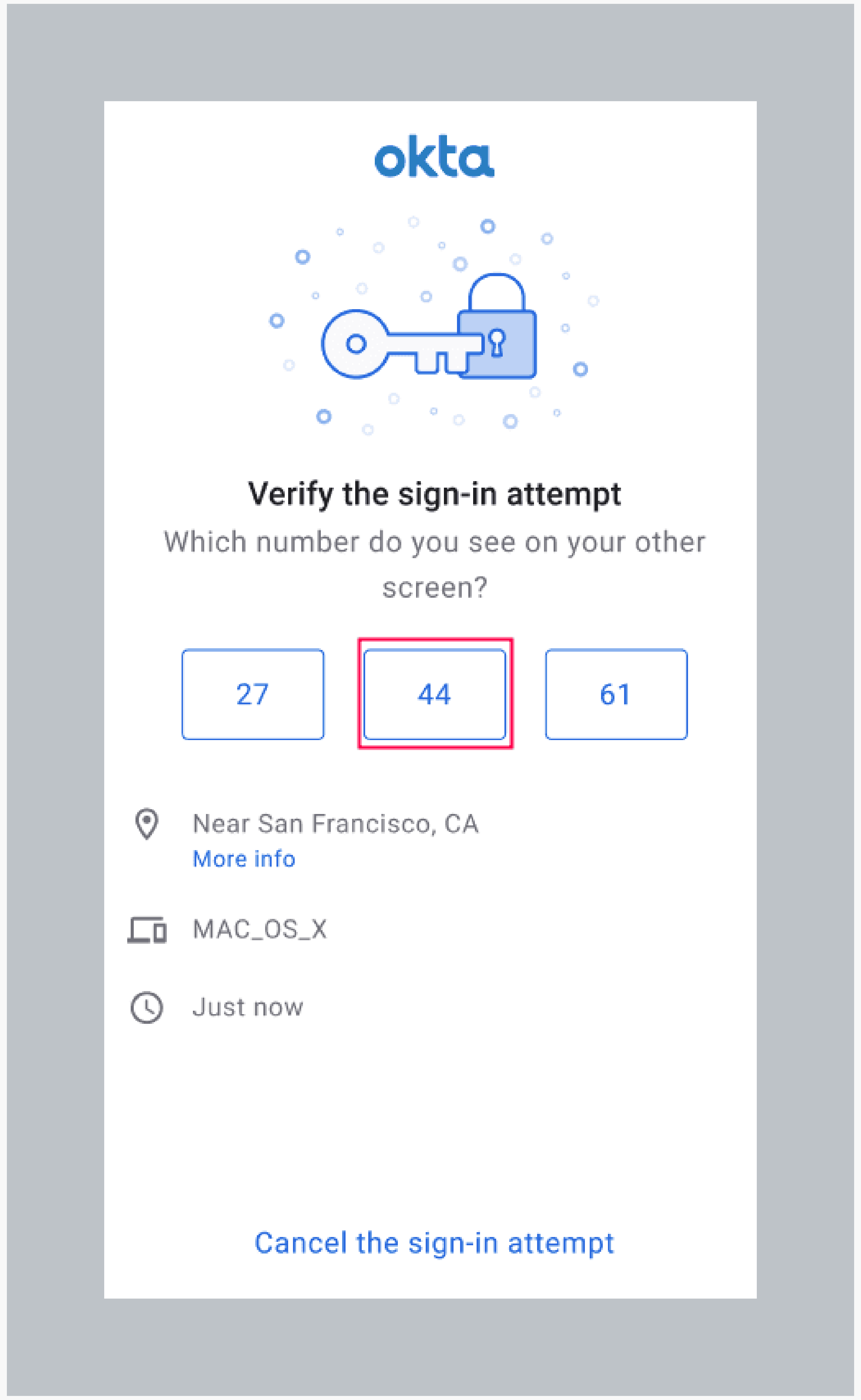
Since December 2021 there have been detections of a new attack technique designed to defeat multi-factor authentication (MFA), and it's simply – be annoying.

Mandiant has previously reported on activity attributed to the group they track as UNC2452 (NOBELIUM), which involved the threat actor bypassing account MFA by abusing push notifications. Many organizations allow users to accept MFA requests by confirming push notifications on their connected phone app, and this is being targeted by threat actors with Mandiant writing "the threat actor took advantage of this and issued multiple MFA requests to the end user's legitimate device until the user accepted the authentication, allowing the threat actor to eventually gain access to the account".

Identity and access management company Okta recently addressed the attack technique in an article written by James Brodsky, referring to the technique as an "MFA fatigue attack". The article describes the process as involving:

- Adversary has already stolen primary username/password credentials by some other means;
- Adversary uses them to log in to an account protected by push MFA and does this multiple times in succession;
- Victim gets valid push notifications (normally to a mobile app of some sort) over and over;
- Eventually, the victim tires of this flood of MFA notifications and taps "yes, it's me" instead of "no, it's not me."

The article goes on to describe how to detect such attacks within their platform as well as linking to Azure Sentinel hunting queries hosted on GitHub. As well as suggesting the use of alternative authentication requests, such as number matching notifications as mitigation:



okta

Verify the sign-in attempt

Which number do you see on your other screen?

Near San Francisco, CA

MAC_OS_X

Just now

WithSecure™ Insight

MFA fatigue is not unique to Okta and is known to be leveraged against all MFA authentication platforms, including Microsoft's, and has recently been detected by WithSecure in the wild. The incident investigated by WithSecure involved a threat actor who had obtained legitimate credentials for the targeted user, and when met with MFA simply spammed the request notification function, until the user accepted, granting the attacker access, who then attempted to carry out a business email compromise (BEC) attack.

While push notifications are a convenient type of MFA, this attack technique has highlighted a serious security concern in their use, and companies making use of them should consider alternatives such as number matching or one-time-key requests and disable push notifications where possible.

MFA options such as SMS tokens are of course vulnerable to other attack techniques such as sim-swapping and social engineering, but other options such as hardware keys offer a higher level of security. The training of staff should also be at the forefront of any defences against these techniques, as many attacks can be thwarted through better user awareness.

1.3 The disruption of ZLoader

A collaborative and global operation led by Microsoft's Digital Crimes Unit (DCU) has successfully disrupted the infrastructure of the botnet ZLoader. DCU has posted a blog detailing their legal and technical actions used to take control of the malware's C2 domains, which includes obtaining a court order allowing seizure and sink-holing of the active domains, as well as domains created through the malware's domain generation algorithm (DGA), disrupting the malware's fallback communications.

ZLoader had been active since 2019, and had become active and popular among threat actors, with access being sold on hacker forums and darknet markets, with ESET listing its features as being:

- Ability to steal various data from browsers and Microsoft Outlook, steal cryptocurrency wallets
- Keystroke logging
- HiddenVNC support to allow the operator to remotely control compromised systems
- Support for Zeus-like webinjects, form grabbing and form screenshotting
- Arbitrary command execution (e.g., download and execute other malware)

Microsoft has additionally reported their findings to law enforcement and has linked one person directly to the malware, named Denis Malikov, further stating "Our disruption is intended to disable ZLoader's infrastructure and make it more difficult for this organized criminal gang to continue their activities. We expect the defendants to make efforts to revive ZLoader's operations".

WithSecure™ Insight

ZLoader is just one of many malware variants used to create botnets, but had gained popularity amongst some threat actors, and was being used to commit a broad range of crimes including data theft, fraud and the delivery of other malware types including ransomware. This action by Microsoft is likely futile in terms of stopping the developers of ZLoader and other similar malware from adapting and continuing their criminal endeavours. However, this does demonstrates the continued efforts by security companies and law enforcement to tackle this type of cyber-enabled crime, as well as providing good insight and intelligence into the infrastructure and operations of botnets like ZLoader.

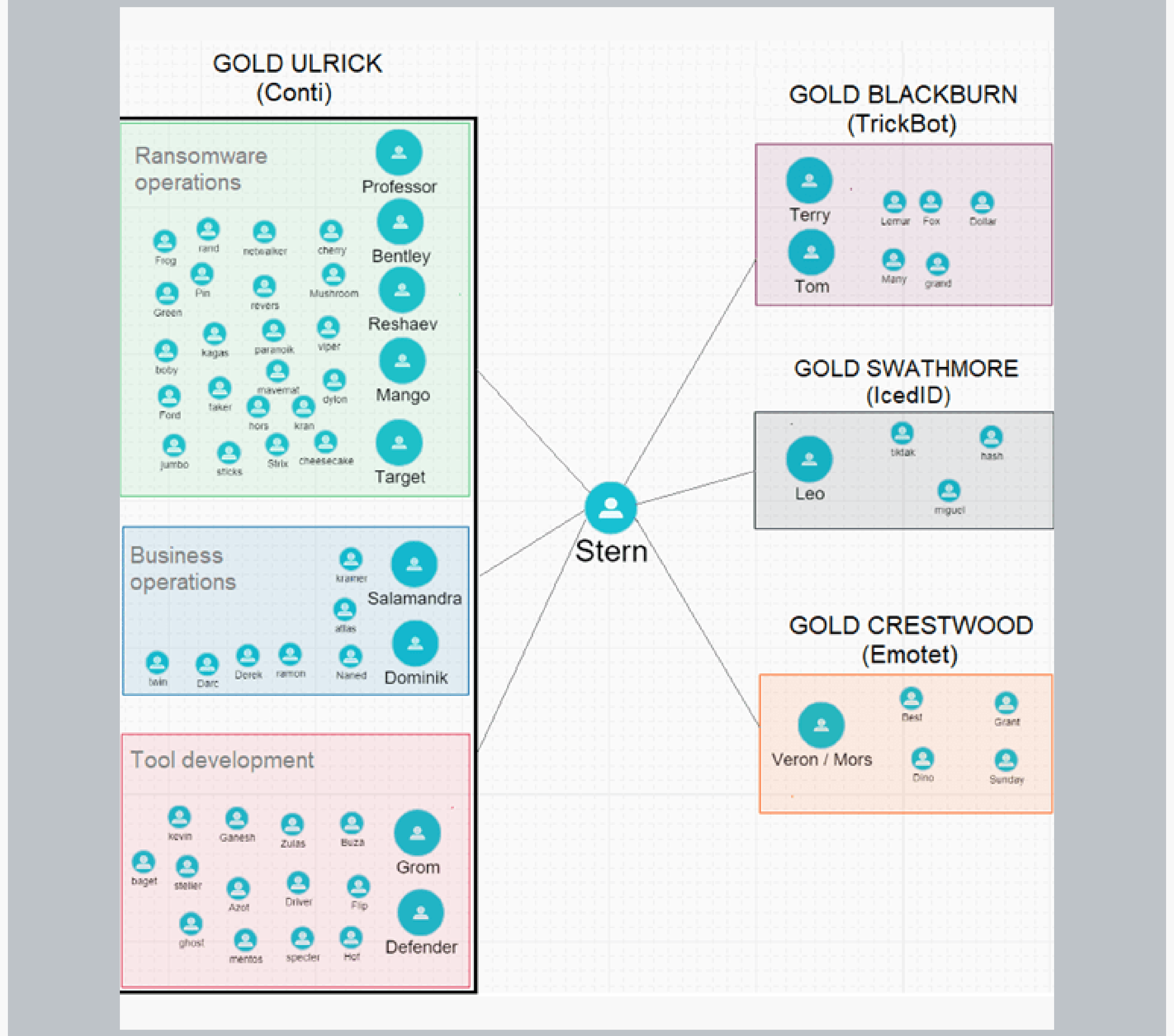
1.4 A breakdown of ContiLeaks

When Russia invaded Ukraine on the 24th of February 2022, the ransomware group CONTI came out in support of Russia. This action seemingly angered one of its members/affiliates who supported Ukraine, leading to the leak of insider information via Twitter of data, chat logs, source code and insights into the inner workings of CONTI. Since this leak, the data has been collated and analyzed by security researchers worldwide, with researcher Will Thomas (BushidoToken) recently releasing a blog post of his findings.

The researcher describes the leaked content as providing "cybercrime researchers an unparalleled look into how Russian-speaking organized hacking groups operate" and starts the blog looking at how CONTI conducts reconnaissance of their targets, with their own "OSINT team" with the blog explaining "this team uses multiple techniques, as well as commercial tools, to find every piece of information about a target that will support the end goal of domain-wide CONTI ransomware deployment. This OSINT Team also may engage with the targets (HUMINT), posing as marketing or salespeople, gathering details and information about managers, executives, and how the company operates for exploitation later".

While the blog explains how CONTI is still using phishing as its major initial access vector, it states "what sets CONTI apart from the rest of their peers in the cybercrime ecosystem is that members of this ransomware group are innovators and quick to leverage newly disclosed techniques", with the group often discussing how to best leverage and exploit new zero-days and add novel techniques to their expansive toolkit.

One thing to become apparent from the leak is the size and complexity of CONTI, with the group seemingly employing around 150 personnel, who are arranged across various departments, with a managerial structure. Researchers at Checkpoint have mapped CONTI's team structure, with the user "Stern" clearly being the de facto CEO of CONTI. Stern engages the other managers and appears to hold the final say on all matters and SecureWorks has done work to map how Stern is connected to other groups including TrickBot, IcedID and Emotet:



Work by Tetra Defense in conjunction with Chainalysis has also identified a clear connection between CONTI and the threat groups Karakurt and Diavol, due to the groups sharing cryptocurrency wallet hosting. Further highlighting the complexity of CONTI's infrastructure, and its place in the cybercriminal underground.

WithSecure™ Insight

The potential intelligence contained within the CONTI leaks data is immense, and so far has provided a wealth of insight into the inner workings of the group, and how they target their victims, gain initial access and develop/deploy tools. This has been incredibly useful to map the group's tactics, techniques and procedures, allowing the tuning of security products and tooling, as well as being a useful resource to provide awareness to frontline staff on threat actor phishing and social engineering tactics.

CONTI is clearly a formidable, well-resourced, and capable threat group, with a wealth of knowledge and skilled personnel and this has been further highlighted by their continued operations following the leak, with them still attacking targets, and leaking data on their website.

A further development caused by the leak is the development of CONTI's source code by third parties for their own use and this has already been demonstrated by hacktivist group NB65, though others are likely to follow suit.

2 Ransomware: Trends and notable reports

2.1 A look at Blackcat/ALPHV

The FBI has released a FLASH alert regarding Blackcat (ALPHV) ransomware variant. The report contains Indicators of Compromise (IOCs) relating to the malware, which allow organizations to better detect and defend against Blackcat attacks and coincided with an investigation on the ransomware by Trend Micro.

Blackcat is a cross-platform ransomware variant, written in the Rust programming language, making it relatively uncommon. Despite this, the group's TTPs closely overlap with BlackMatter and REvil, suggesting a link to or rebranding of the now-defunct groups. Of note, Blackcat is known to gain initial access through the exploitation of vulnerabilities, and their deployment of Cobalt Strike as well as the use of tools including NetScan, Bloodhound and CrackMapExec.

2.2 Russia in the crosshairs

Following the invasion of Ukraine, Russia has found itself in the crosshairs of several threat actors/hacktivist groups who are deploying ransomware/wipers on Russian systems.

Recorded Future is reporting that the group OldGremlin is targeting Russian companies with sanction themed phishing emails, with the end goal of deploying ransomware. The group Network Battalion 65 (NB65) have also deployed ransomware on several Russian targets including the state-owned broadcaster VGTRK, with their malware based on the recently leaked Conti v3 source code.

As the war continues, we are highly likely to see further activity by threat actors/hacktivists motivated by sociopolitical ideology, on both sides of the conflict.

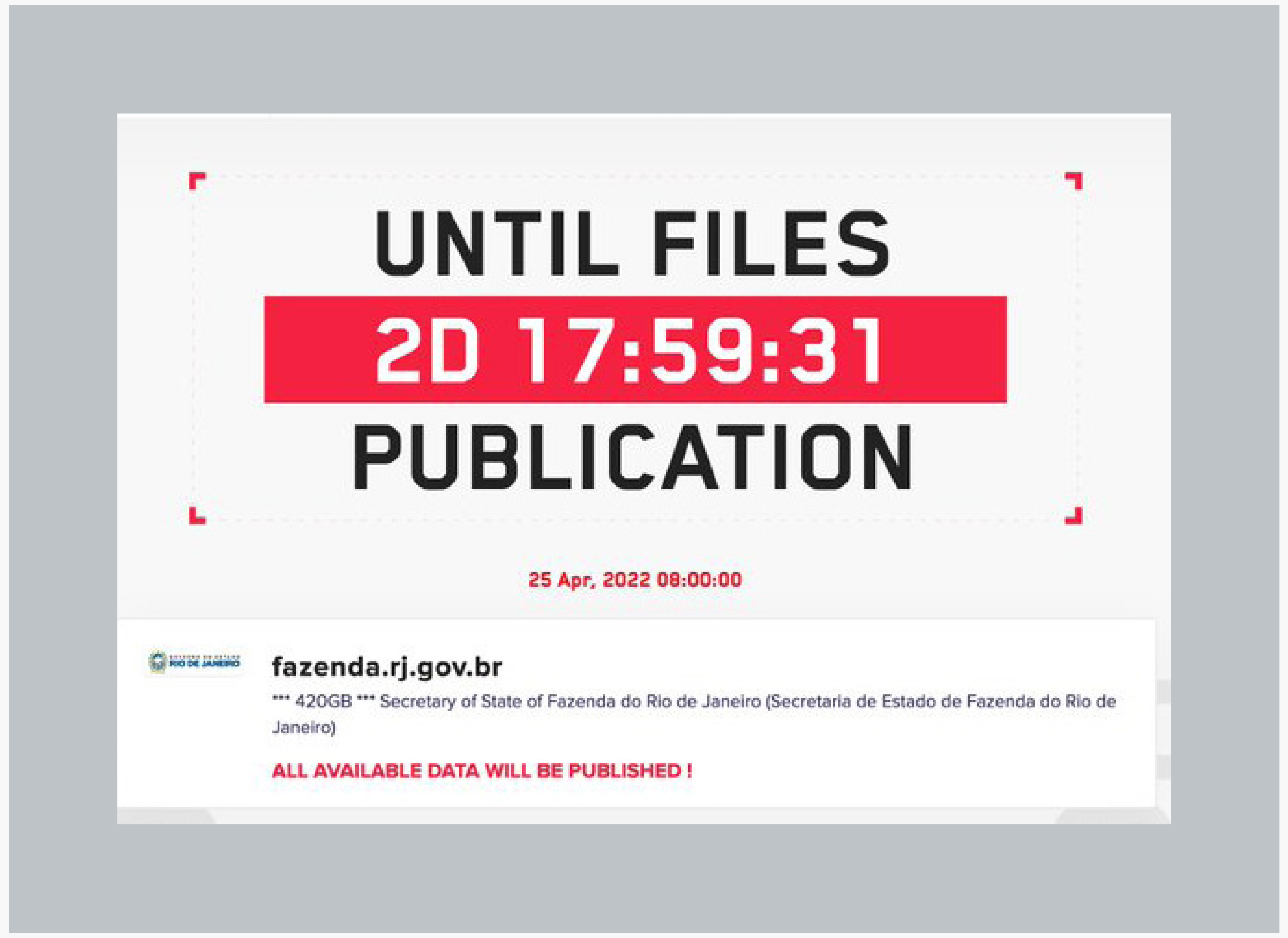
2.3 Quantum: a 4-hour attack

An incident involving a ransomware variant called "Quantum" has been investigated by The DFIR Report, with the time between initial access to ransomware execution being an extremely short 3 hours and 44 minutes.

The threat actors behind the attack gained initial access using the trojan IcedID which was hidden within an ISO file that was likely delivered by a phishing email. The actor then quickly began hands-on-keyboard activity, lateral movement and finally encryption. This is unusual as threat actors will often spend days, if not weeks within their target environment before launching the final stages of their attack. This makes Quantum particularly dangerous as it reduces the time defenders have to take action from initial detection before damage is done.

2.4 LockBit strike Rio de Janeiro finance department

One of the most prolific ransomware groups LockBit has struck the secretary of state for finance of Rio de Janeiro. The group claim to have exfiltrated about 420GB of data, which has since been published on the group's ".onion" leak site:



UNTIL FILES
2D 17:59:31
PUBLICATION

25 Apr, 2022 08:00:00

fazenda.rj.gov.br

*** 420GB *** Secretary of State of Fazenda do Rio de Janeiro (Secretaria de Estado de Fazenda do Rio de Janeiro)

ALL AVAILABLE DATA WILL BE PUBLISHED !

Recorded Future note that "since the demise or retirement of rivals like Darkside, Avaddon and REvil, LockBit has become one of the most commonly seen RaaS platforms".

2.5 BlackByte breakdown

Researchers from Unit 42 have published an excellent threat assessment of the ransomware variant BlackByte. This RaaS group and variant emerged in July 2021 and initially focused on the exploitation of the ProxyShell vulnerability to gain initial access to their victims. The report notes that "due to the high-profile nature and steady stream of BlackByte attacks identified globally in early 2022, the operators and/or affiliates behind the service likely will continue to attack and extort organizations" with the FBI also recently advising that BlackByte was being used to target CNI.

2.6 Nokoyawa, a Nempty strain

SentinelLabs have recently released an analysis on a new ransomware variant named "Nokoyawa". This malware is reportedly a new variant of the historic strain Nemty and an update to a variant called "Karma".

The research notes several findings including errors in the malware's coding stating the "custom hashing algorithm appears to have flaws as it doesn't seem logical nor does it appear to work as expected", which results in multiple unintended folders being potentially skipped during encryption. Additionally, the findings note that despite the ransom note claiming files were "compromised", no ".onion" leak site has been detected for the group.

3 Other notable highlights in brief

3.1 Spring4Shell

A vulnerability in the Spring Framework has been published and assigned CVE-2022-22965, with a critical CVSS rating of 9.8. The Spring Framework is an application framework and inversion of control container for the Java platform and is widely used by Java web applications such as web servers, this vulnerability can allow remote code execution (RCE) on vulnerable systems.

While an exploit has been made publicly available, a blog post by Spring notes that several parameters need to be in place for vulnerability to occur, and in default applications, this will not be the case, but caveats “however, the nature of the vulnerability is more general, and there may be other ways to exploit it that have not been reported yet”. Comparisons to Log4j are also unfounded, as while both are vulnerabilities in commonly used java frameworks, Spring4Shell is likely only present in very few instances in comparison to Log4j.

3.2 Viasat shutdown was AcidRain attack

The previously reported attack on Viasat’s infrastructure in Ukraine, which concurred with the initial invasion of Ukraine by Russia has been confirmed as a cyber-attack involving a wiper called “AcidRain”. Researchers at Sentinel One were able to analyze a sample of the malware and confirm that it functions as an ELF MIPS wiper targeting modems and routers, and while there are some similarities between AcidRain and other malware such as VPNFilter and Cyclops Blink, which are both attributed to the Russian-state that they “cannot definitively tie AcidRain to VPNFilter (or the larger Sandworm threat cluster)”.

3.3 Spying at 10 Downing Street

Researchers at Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy at the University of Toronto have released a statement regarding their detection of Pegasus spyware on UK government networks including 10 Downing Street.

Pegasus spyware is developed by the Israeli company NSO Group and is known to have been sold to hostile states and used to conduct espionage, with the mobile phone spyware’s functionality including reading text messages, tracking calls, collecting passwords, location tracking, accessing the target device's microphone and camera, and harvesting information from apps.

Citizen Lab state the infections at 10 Downing Street are “associated with a Pegasus operator we link to the United Arab Emirates”, a known user of Pegasus.

3.4 LAPSUS$ compromised T-Mobile

KrebsOnSecurity recently reviewed leaked Telegram chat logs between the group members of LAPSUS$, which reveals the group was able to access T-Mobile systems on multiple occasions, including access to their customer management system Atlas, and were able to steal source code for a range of the company’s projects. The chat logs also provide good insight into the group’s personnel and TTPs, which include the purchasing of credentials on dark web markets and the use of social engineering.

3.5 Apple 0-days

CISA has raised awareness surrounding security updates which are available for both macOS and iOS devices, due to two vulnerabilities tracked as CVE-2022-22674 and CVE-2022-22675. The urgency of this publication relates to the detection of these vulnerabilities being exploited in the wild, with CISA stating "apply the necessary updates as soon as possible".

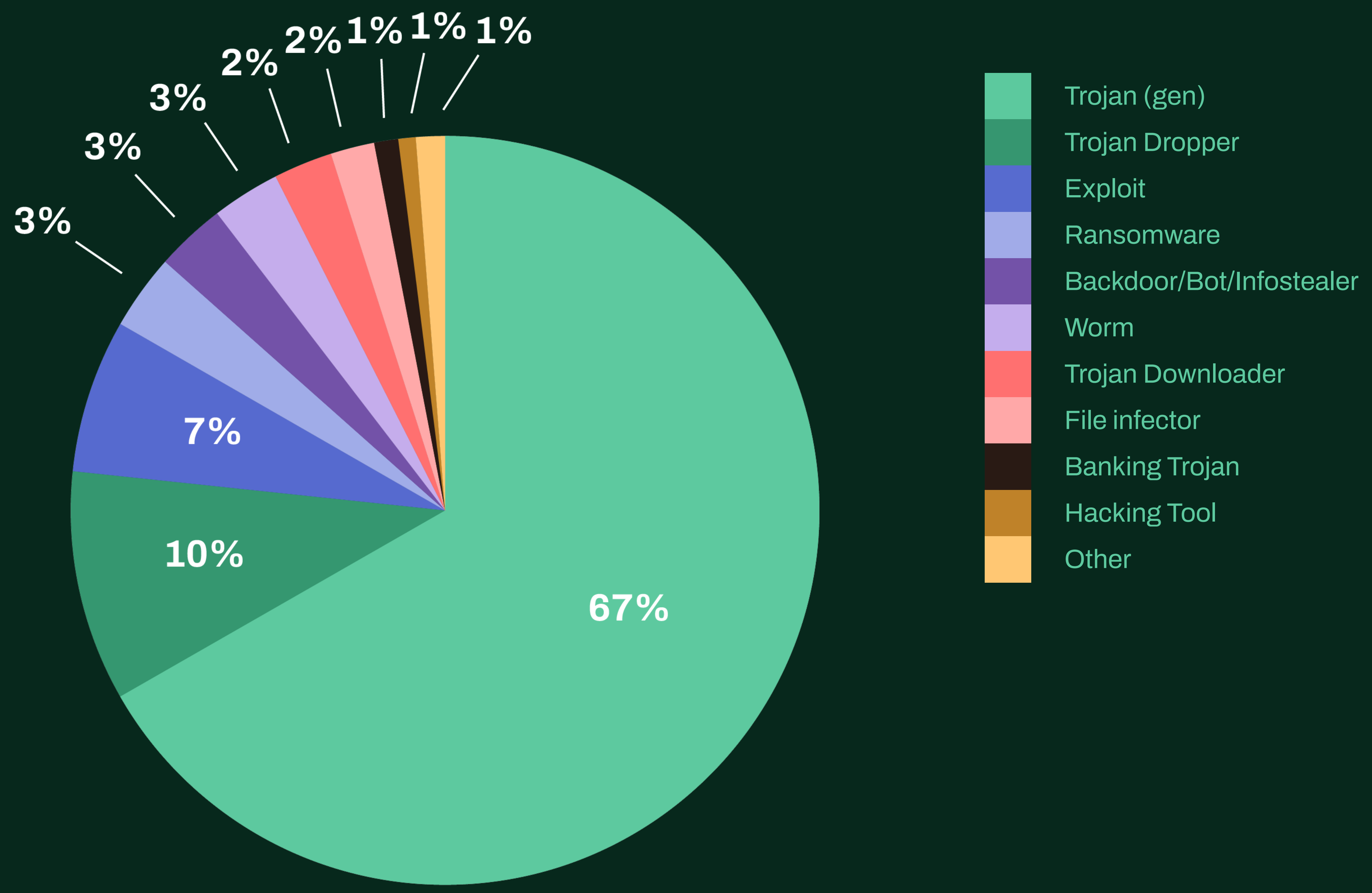
3.6 RPC vulnerability creates risk

A critical vulnerability in Microsoft systems running SMB protocol has "raised alarms" and is expected to be the target of threat actors seeking to exploit the vulnerability. While the setup of most modern networks will likely prevent this attack from occurring remotely, the real risk is highlighted as being from threat actors who have already gained local access, as the vulnerability would allow them "to spread very quickly to any Windows machine in the network". Microsoft has released a patch for the issue, but research by Censys suggests there are 824,011 running the vulnerable SMB protocol exposed to the internet.

4 Threat data highlights

4.1 Malware types

On the malware front, most detected threats have been various droppers and exploits. These threat types continue to remain prevalent in the first quarter of 2022.



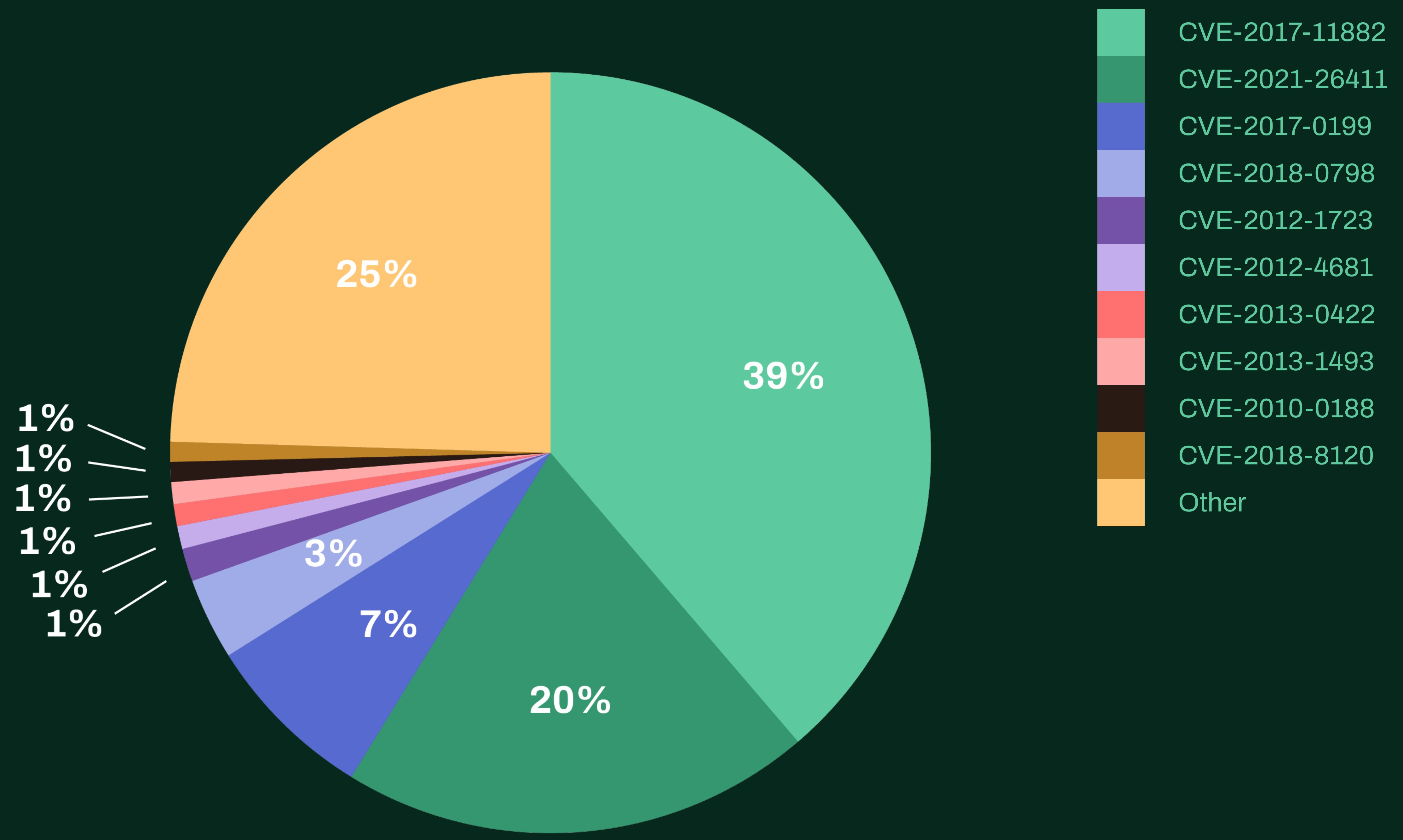
4.2 Exploits

CVE-2017-11882 is a vulnerability in MS office products and provides remote code execution for the attacker.

CVE-2021-26411 an internet explorer memory corruption vulnerability which follows at the second place. This vulnerability is exploited by malicious websites.

CVE-2017-0199 is a remote code execution vulnerability in MS Office and Wordpad exploited by a specially crafted file.

In April, CISA added 45 CVEs to the list of vulnerabilities exploited in the wild. These vulnerabilities affect multiple applications on various operating systems, ranging from internet explorer on windows to network routers and spring framework.



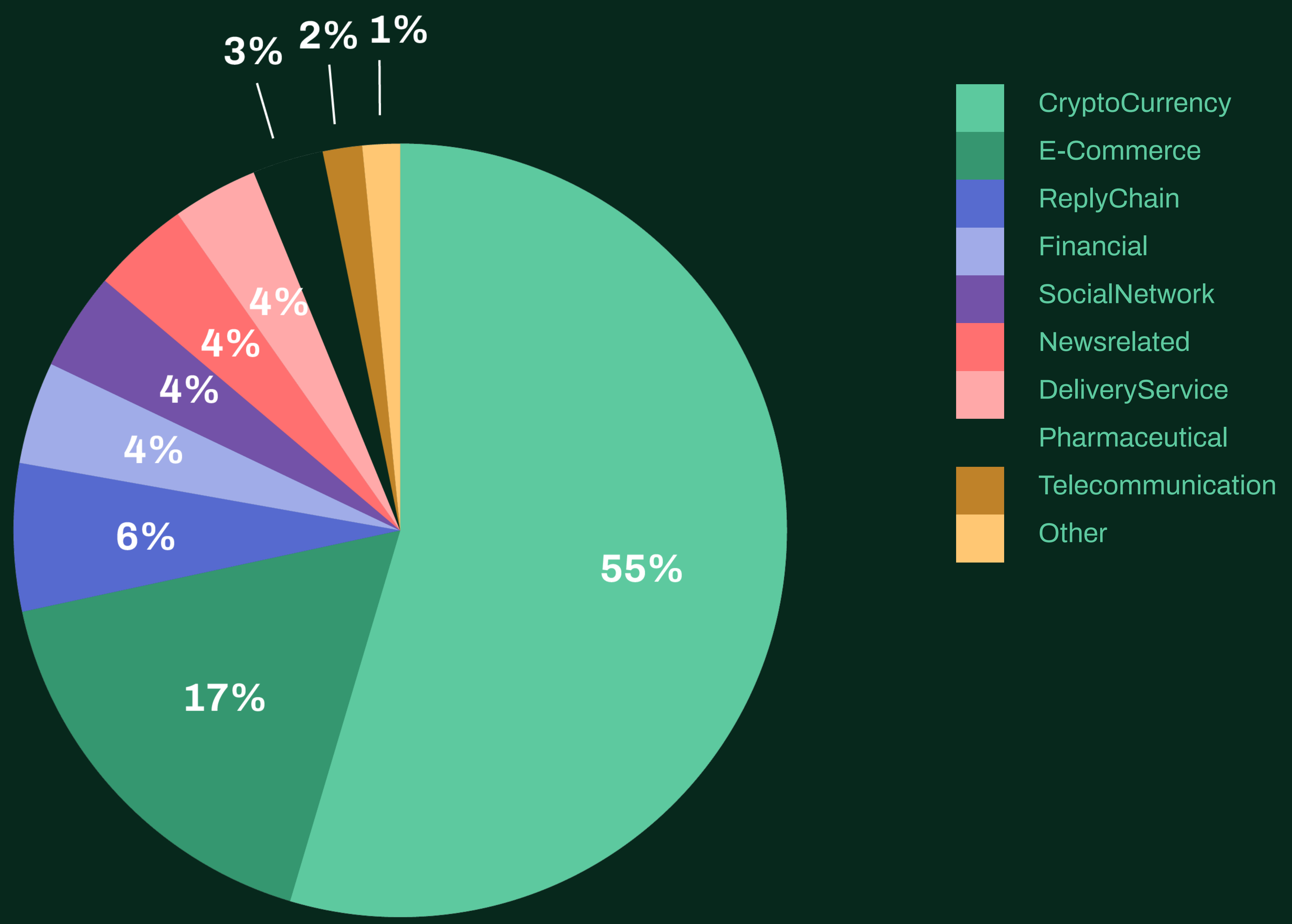
4.3 Email threats

Cryptocurrency and e-commerce themes dominate the spam landscape. Cryptocurrency saw big volumes in April with a bigger scam campaign at the beginning of the month targeting Italians.

An update on the Ukraine situation from the email landscape.

In April, the volumes of spam emails have been lower than in March. March saw few different campaigns with higher volumes in addition to the constant flood but in April there has not been significant campaigns exploiting the situation. There are still Ukraine themed scams but less in volume.

In addition to the scams, information warfare is visible in the Ukraine theme. In these emails, information is being shared “for the benefit” of the recipients while the resources and links are strongly Russia sided information and news outlets.



5 WithSecure™ Research Highlights

5.1 5.1 Insight from a large-scale phishing study

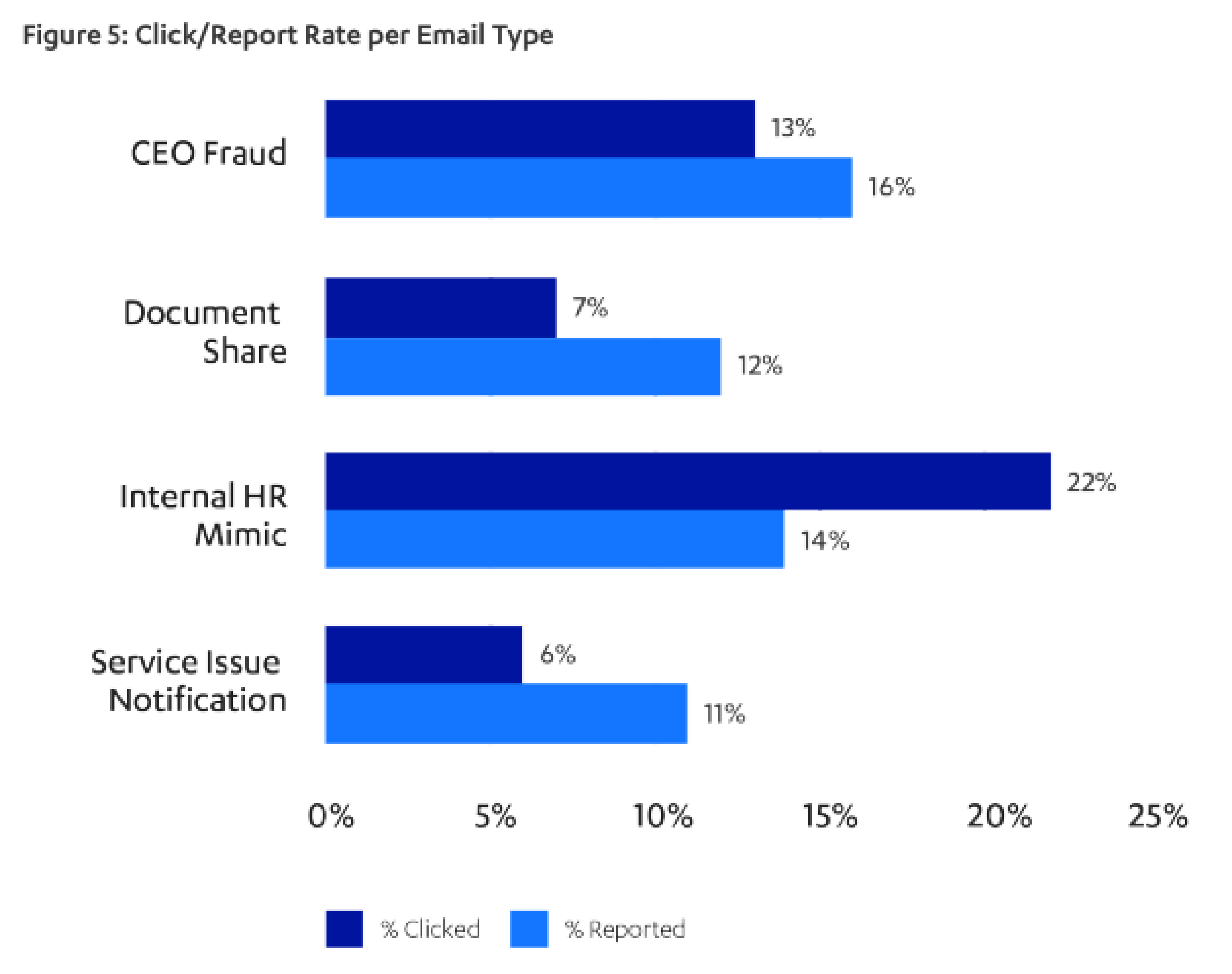


Figure 5: Click/Report Rate per Email Type

WithSecure conducted a large-scale email phishing study, seeking to explore why phishing continues to be paramount access method of malicious cyber actors. 82,402 individuals participated in the study, made up of staff from our organizations. We believe this study to be the largest so far to explore which tactics are most effective in driving clicks on phishing emails.

In the study WithSecure found that staff generally regarded as less prone such as people in the IT related roles were no less susceptible to phishing than those in other areas of the business.

For an example in participating organization A had a 26% DevOps and 24% IT susceptibility while the organization overall was 25%.

Secondly, it was found that the number of suspicious emails that are reported are directly influenced by the process of reporting an email. This means that when there is no direct button in the email client to report emails as suspicious there is far fewer reported emails. When a direct button is present in everyone's email clients, there are over three times as many reports for phishing emails.

Thirdly speed is of the essence. When a phishing email arrives, within the first minute three times as many people have clicked on it than reported it. This number evens out on the 30minute mark where slightly more people have reported the email than clicked on it.

https://www.f-secure.com/content/dam/press/en/media-library/reports/to-click-or-not-to-click.pdf

Who We Are

WithSecure™ is cyber security's reliable partner. IT service providers, MSSPs and businesses along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection & response is powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ is part of F-Secure Corporation, founded in 1988, and listed on the NASDAQ OMX Helsinki Ltd.

W/TH®
secure