Monthly Threat Intelligence Rollup

DEEP seas

03/01/23-04/01/23

Notable Cyberattacks

Summary of noteworthy cyberattacks in the last thirty days.

Incident	Activity Summary
Emotet Returns with New Spam Campaign	After a three-month hiatus, the operators of the Emotet malware (MUMMY SPIDER) have returned with new phishing campaigns delivering their signature Emotet malware.[12] In this new email campaign, the Emotet operators use malicious Microsoft Word documents disguised as invoices. Previous campaigns utilized reply-chain emails. MUMMY SPIDER operators have been observed attaching ZIP archives containing Word documents padded with unused data to inflate the file to over 500 MB in size to evade detection. The malicious Emotet DLL has also been padded to 526MB to hinder detection. As of March 8, the DLL only has a 11/63 score on VirusTotal. Fortunately, Microsoft disabled macros by default in Microsoft Word, degrading Emotet's usual loading vector. Due to this new macro policy, Emotet will likely shift away from utilizing macros in the future to other popular infection vectors like OneNote, .iso images, and JavaScript files. That this campaign utilizes Word documents may hint at a longer development cycle for current Emotet campaigns. Sandbox analysis of Emotet's new .dll indicated that the DeepSeas existing Emotet detection logic will properly identify and classify this threat.
Turkish Government and European Health Care Agency Targeted by YoroTrooper	Cisco is reporting on a new campaign and threat actor, dubbed YoroTrooper, which has been observed targeting Turkish government entities, European government organizations, a Central Asian diplomatic entity, and a European healthcare agency.[3] The attackers behind YoroTrooper have been active since at least 2019 and have been observed using a range of sophisticated tactics and techniques. In the campaign detailed by Cisco, YoroTrooper compromised their victims using spear-phishing emails that contained malicious attachments or links to fake websites. Once compromised, the attackers were able to deploy various remote access trojans (RATs). Information stolen from successful compromises includes credentials from multiple applications, browser histories and cookies, system information, and desktop screenshots. YoroTrooper's main tools include Python-based, custom-built, and open-source information stealers, such as the Stink stealer wrapped into executables via the Nuitka framework and PyInstaller. For remote access, YoroTrooper has also deployed commodity malware, such as AveMaria/Warzone RAT, LodaRAT and Meterpreter.

Emergent Malware and TTPs

Newly emerging malware and tactics, techniques, and procedures identified in the last thirty days.

Malware/Campaign	Activity Summary	TTP Analysis
Emerging Post-Exploitation Framework	CYFIRMA has released their preliminary analysis of a new post-exploitation framework- as-a-service.	The EX-22 developers are observed to possess extensive knowledge of defense evasion and anti-analysis techniques.
Claims 'Fully Undetectable'	(FaaS) called EXFILTRATOR-2 (EX-22).[4] CYFIRMA is "moderately certain" that the operators of EX-22 originate in East Asia and are likely former LockBit affiliates due to identified overlap in both TTPs and C2 infrastructure.	VirusTotal detections of EX-22 samples are currently at a dismal 5/70 rate. According to CYFIRMA, EX-22 is a tool tailor made to spread ransomware throughout corporate networks, as by default it comes with many capabilities making post-exploitation simplistic for users. EX-22 also boasts an elevated reverse-shell, file download and upload, keylogger, and numerous other features well suited to an aspiring cybercrime group seeking an alternative to Cobalt Strike.
UEFI Bootkit Exploits Vulnerability to Achieve Persistence on Secure- Boot-Enabled Systems	ESET has published their analysis of a new UEFI bootkit called BlackLotus which has been available on cybercrime forums for $5,000 since approximately October 2022.[5] Uniquely, BlackLotus can create persistence on up-to-date Windows 11 systems with UEFI Secure Boot enabled by exploiting a vulnerability CVE-2022-21894. This vulnerability was reportedly fixed by Microsoft in January 2022 but remains exploitable as the affected binaries have not been added to the UEFI revocation list.	BlackLotus overcomes the putative patch by introducing its own versions of the legitimate binaries to the system to exploit the vulnerability. Once installed, it installs a kernel driver and a HTTP downloader that communicates with the C&C and can load additional payloads after disabling native Windows security mechanisms, including BitLocker, HVCI, and Windows Defender. UEFI bootkits are of high concern as they permit complete control over the OS boot process. This grants them the ability to function persistently and covertly, with elevated privileges. Until now, only a handful of UEFI bootkits have been detected in the wild and openly reported.
Microsoft Patches Critical Microsoft Word Remote Code Execution Vulnerability	A security researcher released proof-of-concept code exploiting vulnerability CVE-2023-21716 in Microsoft Word, which permits attackers to remotely execute arbitrary code on the affected machine.[6] [7] [8] Microsoft had previously released a patch for CVE-2023-21716 in mid-February; the critical vulnerability is characterized by low attack complexity, no requirement for user interaction, and high impacts on confidentiality, integrity, and availability. Specifically, this vulnerability exploits a vulnerability in the legitimate Microsoft Office wwlib.dll component via a malicious Rich Text Format (RTF) file which may be delivered in a variety of ways.	Microsoft warns that user interaction is not required to open the malicious RTF document. Loading the file in the preview pane is enough to execute the attack. Currently there is no indication that the vulnerability is being exploited in the wild and Microsoft's current assessment is that exploitation is "less likely." Microsoft also released several workarounds, including viewing emails in plain text and enabling Office's File Block Policy if organizations are unable to patch. DeepSeas has deployed a custom Yara rule to aid in identifying exploitations of this vulnerability.

Threat Actor Campaigns

New activity related to threat actor campaigns in the last thirty days.

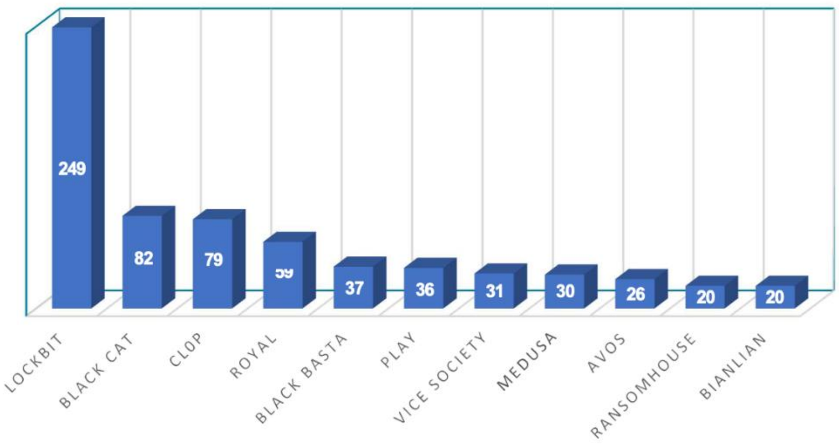
Threat Actors	Activity Summary
MUSTANG PANDA Deploys New Custom Backdoor	ESET research uncovered a new custom backdoor dubbed “MQsTTang” and attributed to the Chinese state-aligned MUSTANG PANDA group.[9][10] ESET first identified MQsTTang while investigating a MUSTANG PANDA espionage campaign targeting political organizations in Europe, Asia, and Taiwan - activities in line with their observed activities since 2020. Since then, MUSTANG PANDA has been refining their lure documents to take advantage of the ongoing unrest in Europe and Asia. ESET describes MQsTTang as a simplistic backdoor that permits attackers to execute arbitrary commands on the victim machine. DeepSeas considers this to be a first-stage tool used to load secondary payloads. MQsTTang unsurprisingly uses the MQTT protocol for C2 communication, which is a protocol typically utilized by IoT devices and benefits the attacker, as MQTT communications are hidden behind a controller which in turn hides the rest of the malicious infrastructure. Currently only two other malware families utilize the MQTT protocol, Chrysaor (Android malware) and MagicRAT, a recently discovered malware attributed to the North Korean Lazarus Group. Although this campaign is unlikely to affect DeepSeas customers Chinese groups often share tools and infrastructure.
Winnti Group Targeting Asian Materials and Composites Industry	Symantec released fresh malware samples from a campaign attributed to the Chinese state aligned Winnti Group which was observed targeting two subsidiaries of an Asian conglomerate, both of which operate in the materials and composites industry.[11] Winnti Group has been active since 2010, and while initially heavily targeting the gaming industry for code-signing certificates, has since expanded their targets to organizations in the semiconductor, telecoms, materials manufacturing, pharmaceutical, media and advertising, hospitality, natural resources, fintech, and food sectors. The group appears focused on targeting intellectual property in a variety of sectors.
UNC2970 Intrusion at U.S. Tech Company Reveals Custom Malware	Mandiant recently released a report detailing a sophisticated cyber espionage campaign carried out by North Korean threat actor group UNC2970, likely associated with the North Korean government.[12] The group is also known as APT37, Group123, and ScarCruft, a group traditionally focused on espionage. UNC2970 has been active since at least 2012 and has been responsible for a variety of cyber espionage campaigns targeting organizations primarily in South Korea, Japan, and the United States. UNC2970 has recently shifted to targeting users directly on LinkedIn, using fake accounts posing as recruiters. In this campaign, UNC2970 boasts several new malware families - the TOUCHMOVE loader, the SIDESHOW backdoor, the LIGHTSHIFT dropper, and the LIGHTSHOW RAT. Interestingly, LIGHTSHOW is another example of tooling that looks to capitalize on the technique of Bring-Your-Own-Vulnerable-Device (BYOVD). BYOVD is a technique that utilizes the abuse of legitimate but vulnerable drivers to bypass kernel level protections. Overall, UNC2970's custom malware tools demonstrate the group's continuing sophistication and expertise in developing advanced cyber espionage capabilities.

Tick APT Compromises DLP Software Developer	New intelligence has emerged concerning the Chinese state-aligned Tick APT's latest campaign that targeted a data loss prevention (DLP) software developer in East Asia.[13] Tick has been active since at least 2006 and has previously targeted organizations in Japan, South Korea, and Taiwan. This campaign commenced in mid-2022 when the group compromised an unnamed DLP software developer's build servers and inserted malicious code into the software updates. The malicious software updates were then distributed to the company's customers, including several government agencies and financial institutions in Japan and South Korea. The malware was designed to steal sensitive data from the infected systems and send it back to the attackers' command-and-control (C2) servers. Tick utilized malware in this campaign, which the authors named " ShadowPy." ShadowPy can perform a wide range of malicious activities, including stealing credentials, taking screenshots, recording keystrokes, and exfiltrating data. ShadowPy is also designed to evade detection by using anti-analysis techniques and exploiting vulnerabilities in popular security products. ESET suggests that the Tick group's attack on the DLP software developer is a "slow-ticking time bomb" because the malicious code was inserted into the software updates, which could remain undetected for a long time.
APT41 Attacking Middle Eastern Telecommunications Industry	SentinelLabs recently published a report about a new cyber espionage campaign dubbed "Operation Tainted Love," which is being attributed to the Chinese state-aligned threat actor group APT41 (aka APT17, Winnti, ShadowPad).[14] The campaign targeted telecommunication companies in the Middle East and has been active since 2021. The campaign began with weaponized Microsoft Office documents that delivered malware customized with components of Mimikatz malware used to compromise credentials. This malware then permitted the attackers to carry out reconnaissance, credential theft, lateral movement, and data exfiltration. SentinelLabs' findings emphasizes that Chinese cyber espionage groups are working at a faster pace and are continuously investing in improving their collection of malware in order to avoid being detected, though samples remain elusive and are currently unavailable for testing.
New APT Identified Targeting Ukrainian Government	Kaspersky has identified a new APT group targeting the Ukrainian government's administrative, agriculture, and transportation agencies since late 2022.[15] Kaspersky has dubbed the new group as "Bad Magic." Bad Magic was identified using a new backdoor called PowerMagic and a malicious framework called CommonMagic. Kaspersky noticed that the TTPs observed during this campaign are unique, having no direct mapping or link to any known campaigns thus far. PowerMagic is a PowerShell-based backdoor that executes commands sent by the attackers via C2, and then exfiltrates data to cloud services including Dropbox and Microsoft OneDrive. Each module of the CommonMagic framework is used to perform a certain task, such as communicating with the C2 server, encrypting and decrypting C2 traffic, and executing plugins.
Russian Hackers Increasingly Targeting U.S. and European Healthcare	The pro-Russia hacktivist group KillNet has been launching waves of distributed denial-of-service (DDoS) attacks against healthcare organizations in the United States and Europe.[16] [17] The U.S. Department of Health and Human Services (DHHS) issued an analyst note warning of KillNet's threat to the healthcare sector, stating that the group has compromised a U.S. healthcare organization that supports members of the U.S. military. KillNet primarily uses DDoS attacks as a tool for protest, as they are a relatively simple and low-cost method of disrupting online services and websites. In addition, DDoS attacks can be launched anonymously, which makes it difficult for authorities to track down the perpetrators. Microsoft published analysis of DDoS attacks against healthcare organizations which utilized Microsoft Azure and Defender as part of their defense posture. In November 2022, Microsoft observed 10-20 attacks a day, compared to 40-60 attacks per day in February 2023. DHHS is advising healthcare organizations to take steps to prepare for and defend against DDoS attacks, including developing a response plan, monitoring network traffic, and considering the use of DDoS mitigation services.

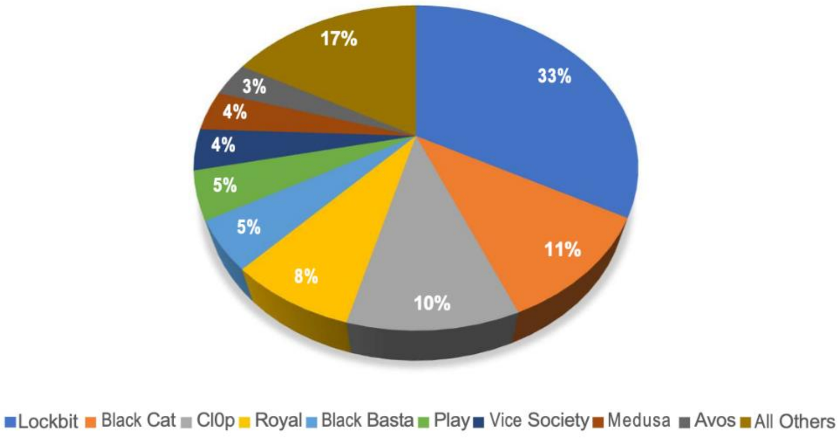
By The Numbers

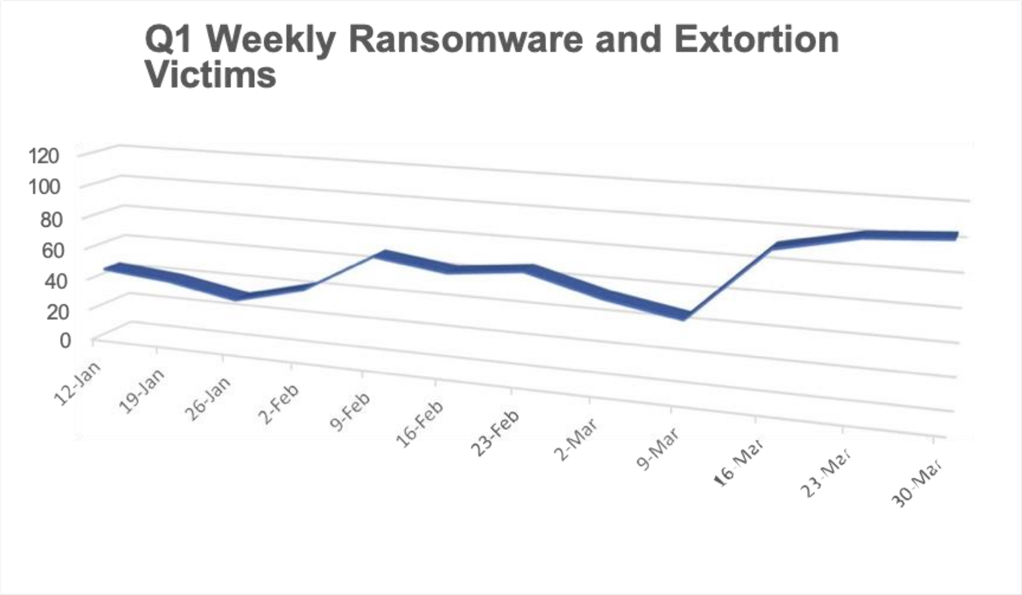
Summarizing incidents in graphical format

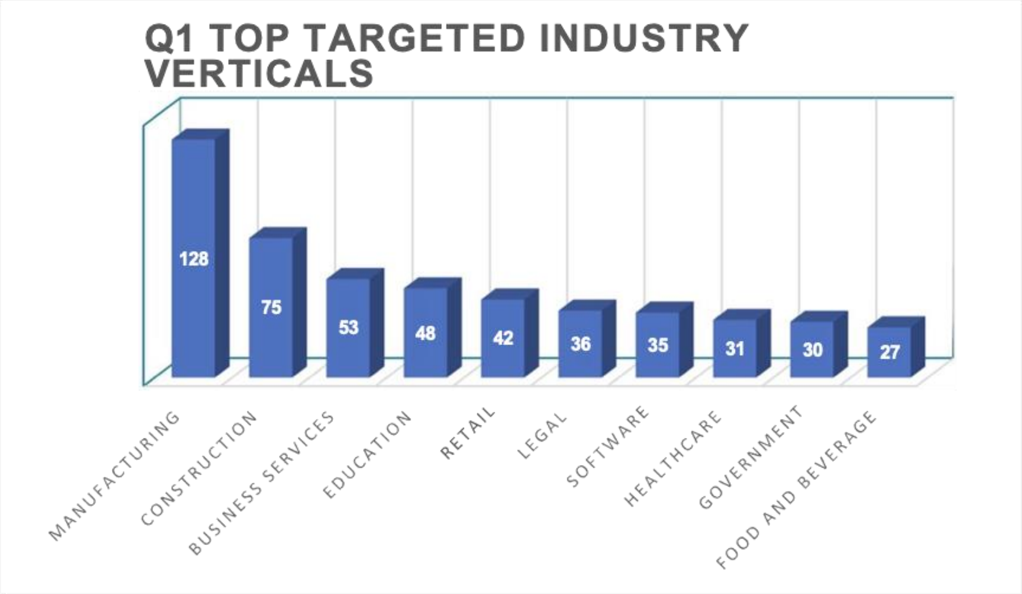
Q1 RANSOMWARE VICTIMS BY GROUP



Q1 Share of Claimed Victims by Group




Q1 Weekly Ransomware and Extortion Victims


Q1 TOP TARGETED INDUSTRY VERTICALS

[1] https://twitter.com/Cryptolaemus1/status/1633099154623803394
[2] https://www.bleepingcomputer.com/news/security/emotet-malware-attacks-return-after-three-month-break/
[3] https://blog.talosintelligence.com/yorotrooper-espionage-campaign-cis-turkey-europe/
[4] https://www.cyfirma.com/outofband/exfiltrator-22-an-emerging-post-exploitation-framework/
[5] https://www.welivesecurity.com/2023/03/01/blacklotus-uefi-bootkit-myth-confirmed/
[6] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21716
[7] https://www.bleepingcomputer.com/news/security/proof-of-concept-released-for-critical-microsoft-word-rce-bug/
[8] https://twitter.com/jduck/status/1632471544935923712
[9] https://www.welivesecurity.com/2023/03/01/blacklotus-uefi-bootkit-myth-confirmed/
[10] https://www.welivesecurity.com/2023/03/02/mqsttang-mustang-panda-latest-backdoor-treads-new-ground-qt- mqtt/

[11] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/blackfly-espionage-materials
[12] https://www.mandiant.com/resources/blog/lightshow-north-korea-unc2970
[13] https://www.welivesecurity.com/2023/03/14/slow-ticking-time-bomb-tick-apt-group-dlp-software-developer- east-asia/
[14] https://www.sentinelone.com/labs/operation-tainted-love-chinese-apts-target-telcos-in-new-attacks/
[15] https://securelist.com/bad-magic-apt/109087/
[16] https://therecord.media/killnet-ddos-hospitals-healthcare-russia
[17] https://www.microsoft.com/en-us/security/blog/2023/03/17/killnet-and-affiliate-hacktivist-groups-targeting-healthcare-with-ddos-attack