Monthly Threat Intelligence Rollup

DEEP seas

05/02/23-06/01/23

Notable Cyberattacks

Summary of noteworthy cyberattacks in the last thirty days.

Incident	Activity Summary
Akira Ransomware	A recent entry in global ransomware groups, the Akira ransomware has breached corporate networks worldwide, encrypted files, and demanded million-dollar ransoms since its launch in March 2023. The operation claims to have attacked 16 companies in various industries, stealing corporate data for leverage in their extortion attempts. The gang has put a significant amount of effort into their data leak site, offering a jQuery-driven 1980s-style retro look where visitors must navigate by typing in console commands. Akira has leaked the data of four victims on their data leak site, with the size of the leaked data ranging from 5.9 GB to 259 GB. They demand ransoms ranging from $200,000 to millions of dollars and lower the demand for companies that only want to prevent the leaking of stolen data.[i]
Multi-National Operation Claims to Neutralize Snake Malware	The Snake implant is a sophisticated cyber espionage tool developed by Turla, Russia's Federal Security Service (FSB), to collect intelligence on sensitive targets. The FSB created a covert P2P network of infected computers worldwide, with many serving as relay nodes to route disguised operational traffic to and from Snake implants on the FSB's targets. The infrastructure has been identified in over 50 countries, and although it uses infrastructure across all industries, its targeting is purposeful and tactical. The FSB has used Snake to collect sensitive intelligence from high priority targets, such as government networks, research facilities, and journalists. The FSB has also targeted industries in the United States, including education, small businesses, and media organizations, as well as critical infrastructure sectors. The FBI has taken down all infected devices in the U.S. and is working with local authorities outside the U.S. to provide notice of Snake infections and remediation guidance. The FBI has developed the capability to decrypt and decode Snake communications and created a tool called PERSEUS that disables the Snake implant on a specific computer without affecting the host computer or legitimate applications, using information from monitoring the Snake network and analyzing the malware. This isn't the first time the FBI has disrupted Turla's operations and Snake infrastructure. As we've seen even with Botnets like Emotet, just because law enforcement disabled threat actor operations, it doesn't mean the threat actor won't figure out new ways to infiltrate target networks, especially in the case of Russian Intelligence Cyber Actors.[ii]
Avos Locker	Avos Locker compromised Bluefield University located in southwestern Virginia. According to press reports, they commandeered the campus emergency alert system and texted a ransom note to the entire student body. They also posted the school's cyber insurance policy on their victim disclosure site. Both moves are designed to put pressure on the university to pay the ransom.[iii]

MOVEit File Transfer Critical Vulnerability	Over the Memorial Day weekend, threat actors started exploiting a critical vulnerability in MOVEit's File transfer solution.[iv] This vulnerability, known as a SQL injection flaw, allows for "escalated privileges and potential unauthorized access" to targeted systems. DeepSeas CTI's investigation has revealed a potential connection to the infrastructure associated with Fancy Bear (also known as APT28), a Russian state-aligned advanced persistent threat group. However, it is still uncertain whether Fancy Bear is responsible (solely or in part) for these activities, and the extent of their actions is also unknown. Currently, it is unclear whether this represents a complete compromise of MOVEit's supply chain or automated exploitation of an existing vulnerability. DeepSeas CTI suspects the latter scenario. As of May 31, approximately 2,500 instances of MOVEit Transfer were publicly accessible on the internet, with the majority located in the United States. Until a patch is released, it is strongly advised that organizations shut down any MOVEit Transfers and perform a thorough investigation for compromise before applying the patch and bringing the server live again.

Emergent Malware and TTPs

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

Malware/Campaign	Activity Summary	TTP Analysis
Exploitation Methods Identified for New .ZIP Top Level Domain	Google's activation of the .ZIP top level domain (TLD) has caused consternation among and drawn the ire of security researchers worldwide, though exploits utilizing it were not readily apparent. That has changed with the release of at least two exploitation methods.	The first involves inserting an asperand (@) into a URL before the name of a file (e.g., github[.]com/ubunti1804[.]zip becoming github[.]com/@ubuntu1804[.]zip) which, when accessed, will redirect to ubuntu1804[.]zip instead of GitHub. Other tactics may enhance this, such as modifying the asperand's font size or including Unicode forward slash characters that are not properly parsed by the popular Chromium browser (a bug dating to 2016 no less), permitting very long and seemingly legitimate URLs to redirect users to a malicious website or file hosted on that domain. Another potential avenue for exploitation is via the Windows File Explorer; typing in the name of a .ZIP file into the address bar (e.g. ubuntu1804[.]zip) will not open a .ZIP file of the same name, but instead take the user to the domain in a browser. As a prevention method, DeepSeas TDE recommends blocking these TLDs as general policy.[v]
Upward Trend in Linux ESXI Ransomware Variants	This month, DeepSeas observed an increase in reports about ransomware gangs developing variants specifically designed to encrypt Linux ESXi servers. The widespread use of ESXi servers in on-premises and hybrid enterprise environments highlights the importance of creating and deploying detection mechanisms for these devices.	SentinelLabs discovered that 10 different ransomware families were utilizing leaked Babuk Source code to create Linux ESXi variants. This progression was expected since the Babuk Source code was leaked in 2021, but it took until the end of 2022 for threat actors to modify it for their own purposes and test it in various malware zoos and intrusions. Some of these new families and variants appear to be in early stages of development and have not yet affected any victims; while other more established families have already succeeded in carrying out Linux ransomware attacks.[vi]
New OT/ICS Malware Discovered	Mandiant recently uncovered a new type of malware dubbed "COSMICENERGY" that specifically targets Operational Technology (OT) and Industrial Control Systems (ICS). This malware, which was uploaded to a malware repository in December 2021 by an individual in Russia, aims to disrupt the operation of electric power systems by targeting IEC 60870-5-104 (IEC-104) devices, such as remote terminal	COSMICENERGY represents a significant example of specialized OT malware that can cause cyber-physical impacts which are seldom detected or disclosed. Mandiant suspects that this malware was developed by a contractor as a red teaming tool for simulated power disruption exercises conducted by RosTelecom-Solar, a Russian cyber security company. Upon analyzing COSMICENERGY, experts have determined that its capabilities are comparable to those used in previous incidents involving malware, like INDUSTROYER and INDUSTROYER.V2. These earlier variants were employed to disrupt electricity transmission and distribution by exploiting IEC-104. The emergence of COSMICENERGY suggests that the barriers to developing offensive OT capabilities are decreasing as threat actors leverage knowledge gained from previous attacks to create new malware. Given the fact that threat actors often utilize red team tools and publicly available exploitation frameworks for targeted attacks, COSMICENERGY poses a realistic threat to electric grid

	units (RTUs). These devices are commonly used in electricity transmission and distribution operations across Europe, the Middle East, and Asia.	assets. Therefore, owners of OT assets that rely on IEC-104 compliant devices should take proactive measures to prevent the potential deployment of COSMICENERGY in the wild.[vii]
Geacon Project Brings Cobalt Strike Capabilities to macOS Threat Actors	SentinelOne has identified new abilities in Geacon to better target devices using macOS. Geacon is a Go implementation of Cobalt Strike Beacon. Despite being publicly available since 2019, Geacon was not observed being deployed against macOS targets until recently.	SentinelOne discovered multiple payloads of Geacon appearing on VirusTotal in recent months, with the results being a mix of legitimate red team operations and genuine malicious attacks. The two submitted malicious VirusTotal payloads target macOS directly and are compiled for both Apple silicon and Intel architectures. While Geacon can be used legitimately by red teams, possible malicious use of this tool means that Geacon should be closely monitored.[viii]
Man-in-the-middle (MitM) Attacks Increase 35% Since 2022	Man-in-the-middle (MitM) attacks occur when an attacker inserts themselves between a victim and their expected destination to steal information. Recently, threat actors have combined credential phishing with MitM attacks to harvest usernames, passwords, and session cookies.	According to Cofense, there has been a 35% increase in volume of MitM credential phishing attacks reaching inboxes between Q1 2022 and Q1 2023, and 94% of attacks targeted O365 authentication. Users should be reminded of approved online portals, suspicious URLs or attachments should be reported, and alerts on outbound network traffic could be helpful. Most of the observed campaigns feature a harmful website link included in the email's content, rather than being sent as an attachment. Customers should implement multi-factor authentication, a secure VPN, and implement local outbound network traffic alerts on outbound network traffic which match known URL patterns but do not match the legitimate domains.[ix]
BlackCat Ransomware Utilizes Signed Kernel Driver for Evasion	Trend Micro has uncovered a new capability of the BlackCat ransomware, which involves the use of a signed kernel driver along with a separate user client executable. This combination allows the attackers to gain control over various processes on targeted endpoints that are associated with the security agents deployed on those machines. The attackers can manipulate, pause, or terminate these processes.	To avoid detection, malicious actors rely on persistent use of rootkits to hide their malicious code, weaken defenses, and remain undetected for extended periods. The main danger posed by these rootkits lies in their ability to conceal advanced targeted attacks. These attacks are carried out early in the attack chain, enabling the attackers to undermine defenses before launching the actual harmful payloads in victim environments.[x]

Threat Actor Campaigns

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

Threat Actors	Activity Summary
Volt Typhoon Evading Detection in U.S. Critical Infrastructure	Microsoft and several FVEY federal agencies have released information about a new Chinese state-aligned actor dubbed "Volt Typhoon." This group employs so-called "living off the land" techniques to bypass defenses in critical infrastructure within the United States. Volt Typhoon has been active since at least 2021 and has targeted various sectors, including communications, manufacturing, utilities, transportation, construction, maritime, government, information technology, and education. According to Microsoft, the primary objectives of Volt Typhoon are espionage and the ability to disrupt critical communications during times of crisis within the United States. The group's techniques involve leveraging native commands and existing tools to blend in with regular activity, thus evading detection by endpoint and anomaly-based detection systems. To further avoid detection, Volt Typhoon compromises local, small home and office routers for use as command and control (C2) servers located in the same physical vicinity as their victims. By doing so, the malicious connections appear to be legitimate. The operational flow of Volt Typhoon involves executing commands on victim networks to achieve three primary goals: (1) collecting data, including credentials from local and network systems, (2) archiving the collected data for exfiltration, and (3) employing the stolen valid credentials to maintain persistence within the compromised networks. Mitigating the risk posed by adversaries like Volt Typhoon, who rely on valid accounts and employ "living-off-the-land" binaries (LOLBins), presents significant challenges. Detection of activities utilizing normal sign-in channels and system binaries necessitates behavioral monitoring. To address the issue, remediation efforts involve revoking or resetting credentials for compromised accounts.[xi]
New Malicious "Horse Shell" Firmware Implant by Camaro Dragon Targeting Routers	Check Point Research has identified a series of targeted attacks which were aimed at European foreign affairs entities by the Chinese state-sponsored APT group, Camaro Dragon, which in this case also shares TTPs with other state-sponsored Chinese threat actors, such as Mustang Panda. Analysis done by Check Point Research of the attacks uncovered a malicious firmware implant tailored for TP-Link routers; however, due to its firmware-agnostic design, the implant's components can be integrated into various vendors' firmware. This implant features several components, with the focus being a custom backdoor named "Horse Shell," which enables the attackers to maintain persistent access, build an anonymous infrastructure, and enable lateral movement into compromised networks. Some of Horse Shell's specific capabilities include actions like remote shell, file transfer, and network tunneling. Currently, Check Point Research is unsure of the deployment method of the firmware images on the identified infected routers, as well as its usage and involvement in actual intrusions. DeepSeas TDE has deployed custom detection logic in the form of both Yara and network detection rules to identify and defend against this threat.[xii]
APT28 Targeting Ukrainian Civil Society	The APT28 intrusion set, also known as Sofacy, PawnStorm, or Fancy Bear, is a group associated with the Russian GRU. They are notorious for engaging in cyber espionage and sabotage activities. Recently, there has been evidence of APT28 employing various phishing techniques to target Ukrainian civil society. It is worth noting that, historically, APT28 has primarily targeted Western countries. This shift in their victim selection is likely a result of Russia reallocating its resources to address the deteriorating situation in Ukraine. In their recent campaign, APT28 used intriguing techniques, such as leveraging HTTP webhook services like Pipedream and Webhook, as well as compromising Ubiquiti routers to steal victims' credentials. In one instance, APT28 employed the "Browser-in-the-Browser" method, which involved displaying a fake login page to the victim falsely claiming to decrypt a document. Most of the phishing webpages that were discovered were aimed at the UKR.NET webmail service, which is widely used among Ukrainian society. However, it is conceivable that APT28 might

	employ similar techniques against other webmail services utilized by Western civil society that supports Ukraine.[xiii]
Attacks on Southern ASEAN Countries	TrendMicro released a new report identifying a purportedly new Chinese state-aligned threat actor group dubbed “Earth Longzhi” (a subgroup of APT41), as well as details regarding the group’s tools and capabilities in a campaign targeting organizations in Taiwan, Thailand, the Philippines, and Fiji. The campaign exploits a vulnerable driver to disable security products, uses a new denial-of-service technique called "stack rumbling," and installs drivers as kernel-level services using Microsoft Remote Procedure Call to evade API monitoring. The group tends to exploit public-facing applications, IIS servers, and Microsoft Exchange servers to install the Behinder web shell. The group's recent targets include government, healthcare, technology, and manufacturing industries, and Vietnam and Indonesia may be their next targets. Although this poses no immediate threat to current DeepSeas clients, Chinese state group toolsets and tactics are often emulated, shared, and adopted by other Chinese groups.[xiv]
APT37 Delivering RokRAT via Overside Short Cut Files	The North Korean state-aligned group ScarCruft, also known as APT37, has been using oversized LNK files to deliver RokRAT malware since July 2022, coinciding with Microsoft's decision to block macros across Office documents. ScarCruft primarily targets South Korean individuals and entities with spear-phishing attacks, and RokRAT is its primary malware of choice for their espionage campaigns. Espionage targeting is regionally focused on South Korea, Japan, Europe, and the United States, especially in the following sectors: government, business services, and manufacturing, along with education, research, and think tanks focused on geopolitical and nuclear policy. The group shifted focus to health-related verticals throughout the majority of 2021, likely in support of pandemic response efforts. The LNK files containing PowerShell commands deploy the RokRAT malware, which is equipped to carry out a range of activities, including credential theft and data exfiltration. ScarCruft continues to pose a considerable threat, launching multiple campaigns and improving its malware delivery methods. Historically, APT43 steals and launders enough cryptocurrency to buy operational infrastructure in a manner aligned with North Korea’s juche state ideology of self-reliance, therefore reducing fiscal strain on the central government.[xv]
Kimsuky Unleashes ReconShark, a Variant of Their BabyShark Malware	SentinelLabs has identified ongoing attacks by Kimsuky, a North Korean state-sponsored APT, using a new malware component called ReconShark, which is being delivered through spear-phishing emails, OneDrive links, and malicious macros. Kimsuky primarily targets organizations across North America, Asia, and Europe and has a long history of intelligence collection and espionage operations in support of the North Korean government. ReconShark functions as a reconnaissance tool to exfiltrate information about the infected platform, indicating that it is part of a Kimsuky-orchestrated reconnaissance operation intended to enable subsequent targeted attacks.[xvi]

Dark Web Markets

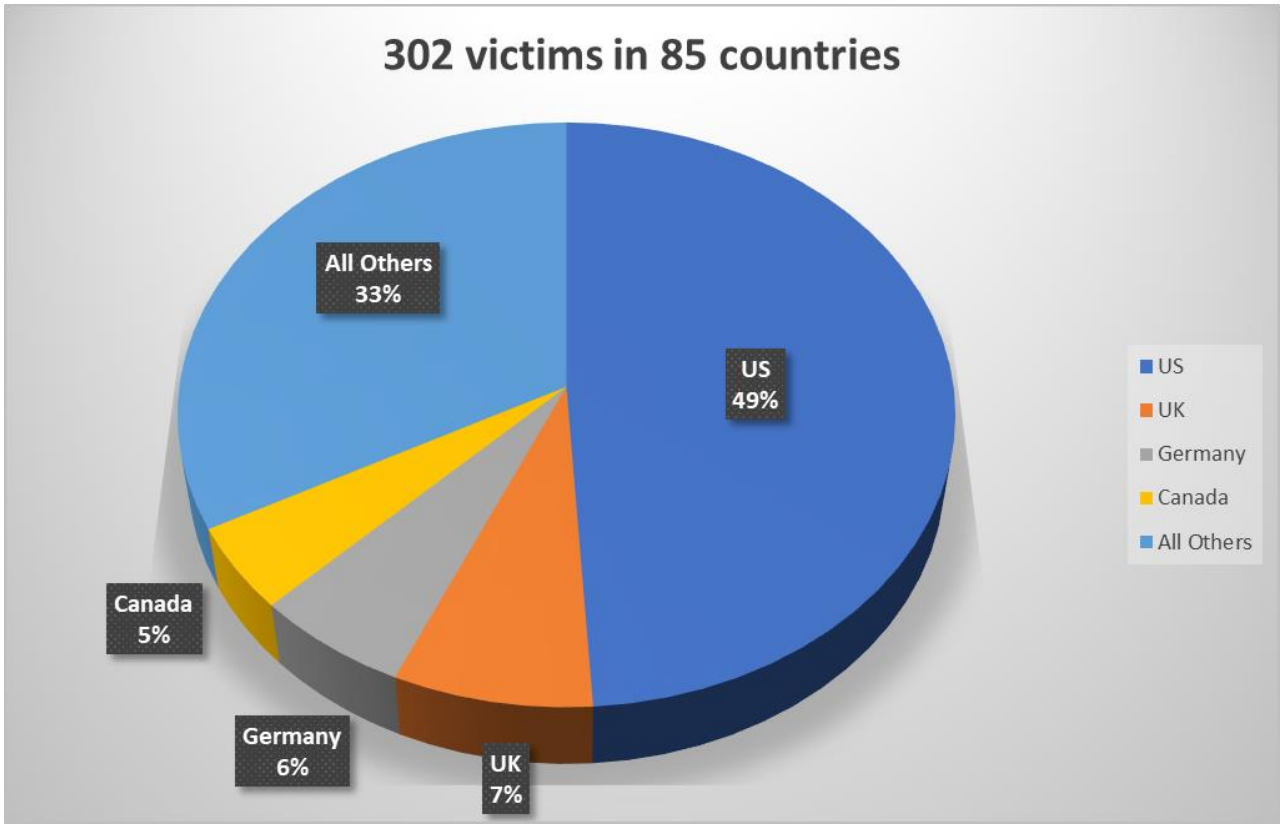
High-profile ransomware data dumps and dark web access sales identified in last thirty days.

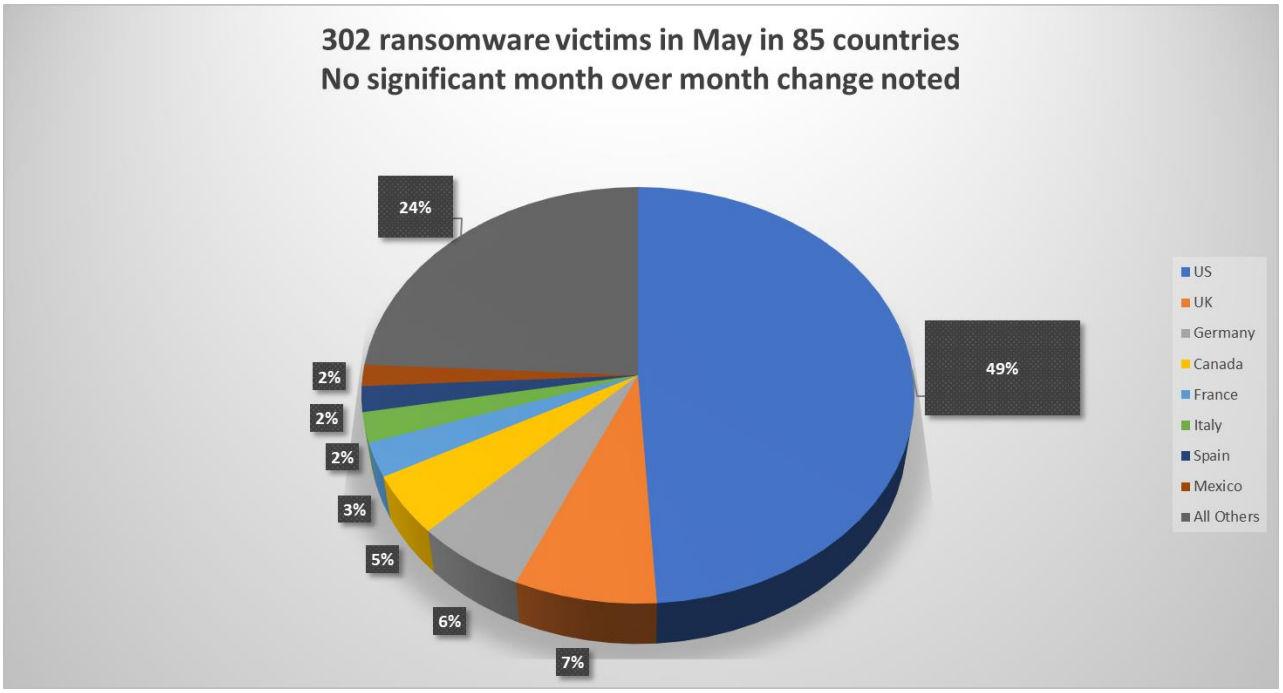
Activity	Note
Access Solicitation	A Russian speaking actor on the XSS crime forum is looking for help compromising the email accounts of employees of LucasFilm Animation so he can log into their Slack channels and collect information about the third season of the animated Star Wars series, Bad Batch. He did not disclose why he wants this information.
Access Sale	An access seller on the Russian language XSS crime forum sold VPN access to what he claimed was the Dubai office of U.S. based Affiliated Managers Group (NYSE: AMG), a USD 2.3 billion investment management company for USD 700.
Access Sale	An access seller on the Russian language XSS crime forum is selling what he claimed was Citrix access to Ricoh USA and Bayer and could evade 2FA on the accounts. He did not name a price.
Access Sale	An access seller on the Russian language Exploit cybercrime forum is selling access to a U.S. based manufacturing company with USD 5.7 billion in revenue. Companies fitting that profile include ThermoSafe Brands, Ricoh America, and Avon Cosmetics.
Access Sale	A new RAMP forum access seller is selling a login for the system administrator allowing RDP access to “a well-known company” with 3,500 employees and between USD 1.6 billion and 2.6 billion in revenue. It includes access to KeePass and saved passwords to internal systems in the browser. They are also selling Citrix workspace access to a U.S. based healthcare company with USD 1 billion in revenue and more than 10,000 employees for USD 3,000.
Access Sale	A user at the Russian language XSS crime forum is selling access to a U.S. based law firm with USD 400 million in revenue. A public business directory lists the Dallas based Haynes and Boone law firm as having that revenue figure. He was also selling admin access to a U.S. based construction company with USD 5 billion in revenue for BTC 0.15 but appeared to cancel the sale for an unknown reason. Balfour Betty and TopBuild are listed as having USD 5 billion in revenue on ZoomInfo
Access Sale	An Exploit crime forum access seller is selling VPN-RDP local admin access to an unidentified U.K. based food and beverage enterprise with USD 1 billion in revenue for a buy now price of USD 4,000.
Data Sale	An Exploit crime forum user is selling what they claim is data belonging to three giant companies. They claim to have 14.6 GB of data belonging to BAE Systems, 4.4 GB of data belonging to Leidos, and 1.31 GB belonging to ADT. They also included a link to what they claim are the BAE System files. The buy now price is USD 10,000. It is unclear if that is for all three or for each one.
Tool Sale	A new Exploit crime forum actor, with no track record against which to judge his credibility, is selling what he claims are two zero-day exploits - an Adobe Reader remote code execution (RCE) with sandbox escape (SBX) for USD 140,000 and a Microsoft Outlook remote code execution zero-click exploit leading to remote code execution when receiving/downloading emails in Outlook without requiring any user interaction such as reading a malicious email or opening an attachment for USD 200,000. There is no indication that he has completed a sale of either of these supposed zero-days.
Tool Sale	RAMP forum user **spyboy** is selling what he claims is an EDR terminator effective against a long list of EDRs, including Carbon Black, SentinelOne, and Check Point. The first five buyers will pay USD 1,500, and then the price goes to USD 3,000. Notably, he will not work with groups using ransomware.

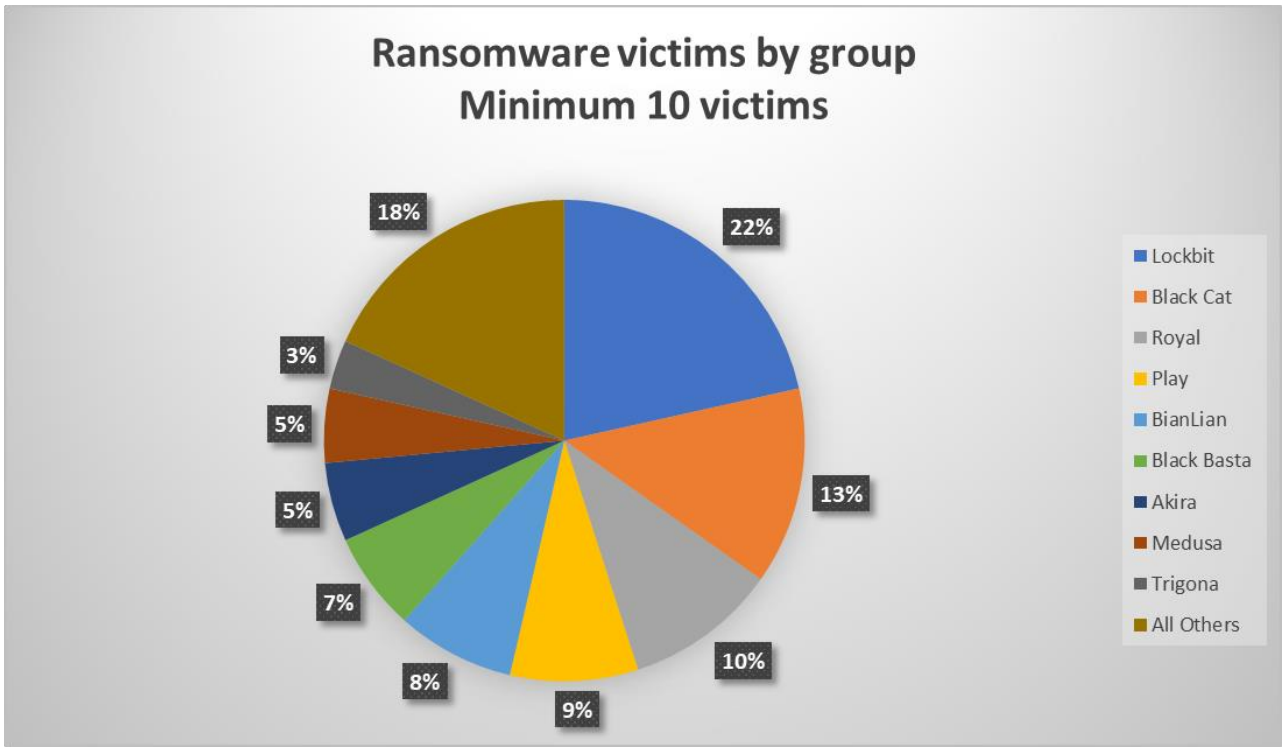
Tool Sale	A well-known Exploit crime forum tool seller is selling a private implementation of CVE-2023-21839 Oracle WebLogic RCE and an implementation of CVE-2023-32673 (HP Hardware Diagnostics EtdSupp LPE), both with a GUI for ease of use and the ability to pass sessions to and from Cobalt Strike.
Data Sale	A new user on the Exploit crime forum claimed to have sold 137 GB of data stolen from cybersecurity firm Dragos. Dragos confirmed that a new employee had been compromised but denied that any of the data stolen was valuable. Of note, the user's screenname was previously used by Saud al-Qahtani, a former advisor to the king of Saudi Arabia, on the Hack Forums, a notorious hangout for many young inexperienced hackers. Qahtani was responsible for procuring malware for the Kingdom and was also thought responsible for leading the operation that murdered Washington Post journalist Jamal Khashoggi. It is highly likely that the actor is an imposter and not the actual al-Qahtani.

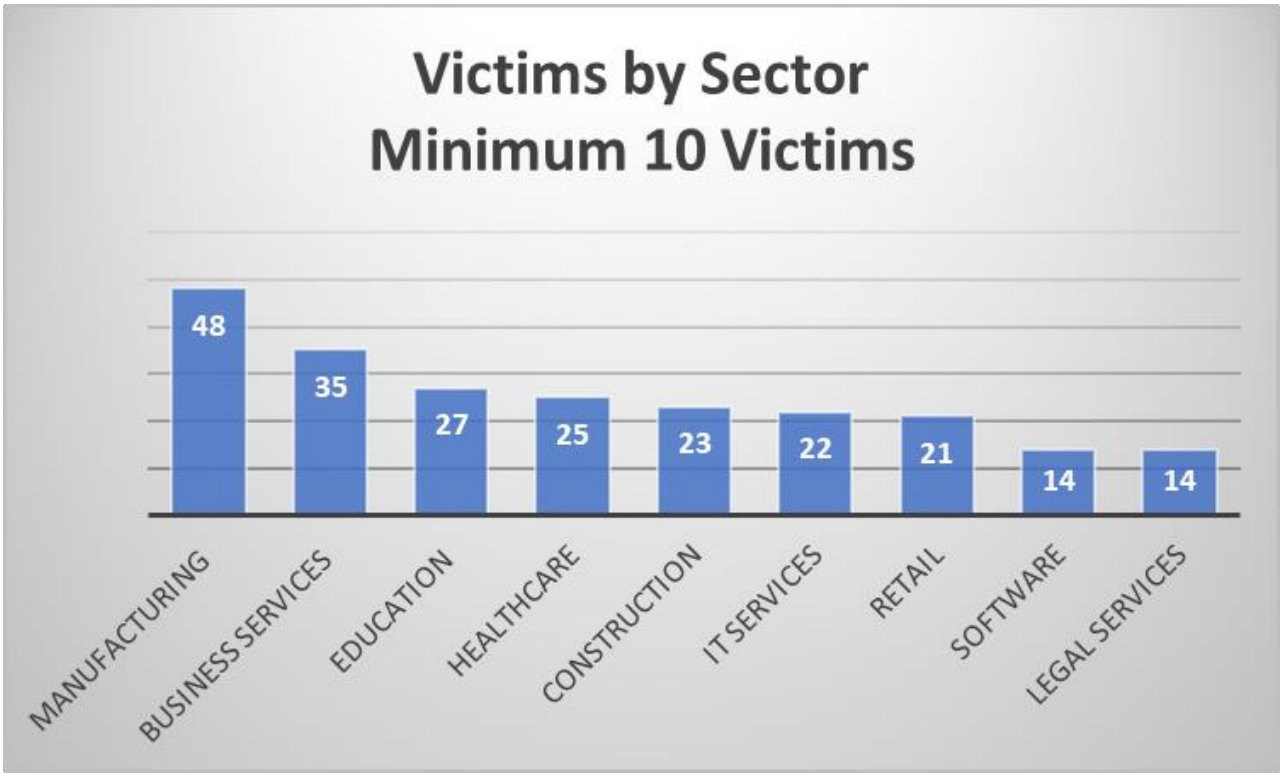
By The Numbers

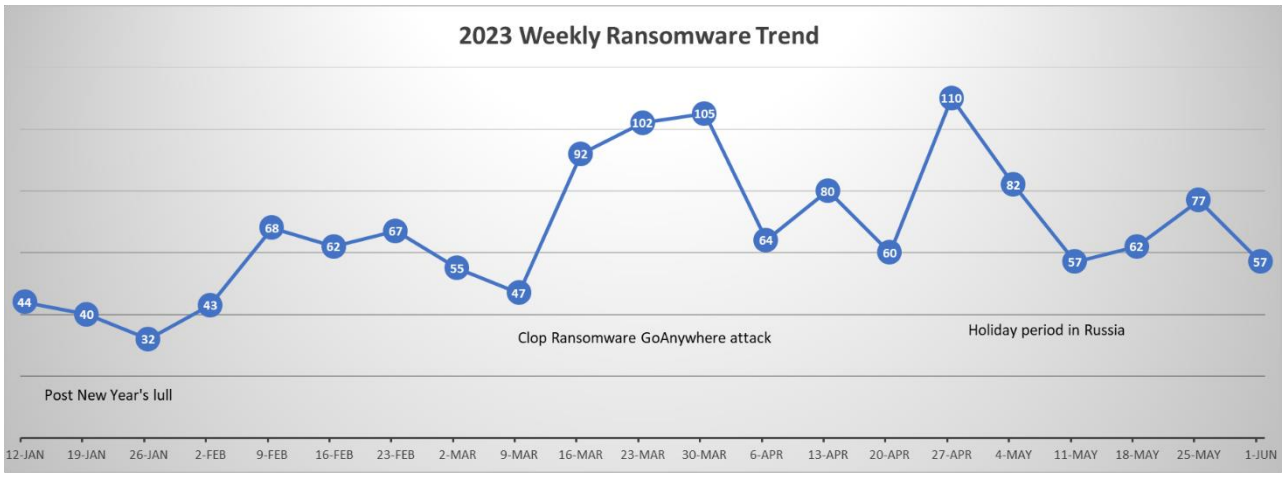
Summarizing incidents in graphical format






Ransomware victims by group
Minimum 10 victims
22%
13%
10%
9%
8%
7%
5%
5%
3%
18%
Lockbit
Black Cat
Royal
Play
BianLian
Black Basta
Akira
Medusa
Trigona
All Others


Victims by Sector
Minimum 10 Victims
48
35
27
25
23
22
21
14
14
MANUFACTURING
BUSINESS SERVICES
EDUCATION
HEALTHCARE
CONSTRUCTION
IT SERVICES
RETAIL
SOFTWARE
LEGAL SERVICES


2023 Weekly Ransomware Trend
44
40
32
43
68
62
67
55
47
92
102
105
64
80
60
110
82
57
62
77
57
Post New Year's lull
Clop Ransomware GoAnywhere attack
Holiday period in Russia
12-JAN
19-JAN
26-JAN
2-FEB
9-FEB
16-FEB
23-FEB
2-MAR
9-MAR
16-MAR
23-MAR
30-MAR
6-APR
13-APR
20-APR
27-APR
4-MAY
11-MAY
18-MAY
25-MAY
1-JUN

[i] https://news.sophos.com/en-us/2023/05/09/akira-ransomware-is-bringin-88-back/
[ii] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a
[iii] https://www.databreaches.net/avos-locker-starts-leaking-student-data-from-bluefield-college-claims-to-still-have-access/
[iv] https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023, https://www.rapid7.com/blog/post/2023/06/01/rapid7-observed-exploitation-of-critical-moveit-transfer-vulnerability/
[v] https://medium.com/@bobbyrsec/the-dangers-of-googles-zip-tld-5e1e675e59a5
[vi] https://www.sentinelone.com/labs/hypervisor-ransomware-multiple-threat-actor-groups-hop-on-leaked-babuk-code-to-build-esxi-lockers/, https://blog.talosintelligence.com/ra-group-ransomware/, https://blog.cyble.com/2023/05/12/blacksuit-ransomware-strikes-windows-and-linux-users/
[vii] https://www.mandiant.com/resources/blog/cosmicenergy-ot-malware-russian-response
[viii] https://www.sentinelone.com/blog/geacon-brings-cobalt-strike-capabilities-to-macos-threat-actors/
[ix] https://cofense.com/blog/cofense-intelligence-strategic-analysis-2/
[x] https://www.trendmicro.com/en_us/research/23/e/blackcat-ransomware-deploys-new-signed-kernel-driver.html
[xi] https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/, https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_Living_off_the_Land.PDF
[xii] https://research.checkpoint.com/2023/the-dragon-who-sold-his-camaro-analyzing-custom-router-implant
[xiii] https://blog.sekoia.io/apt28-leverages-multiple-phishing-techniques-to-target-ukrainian-civil-society/
[xiv] https://www.trendmicro.com/en_us/research/23/e/attack-on-security-titans-earth-longzhi-returns-with-new-tricks.html
[xv] https://thehackernews.com/2023/05/north-koreas-scarcruft-deploys-rokrat.html, https://asec.ahnlab.com/en/51751/
[xvi] https://www.sentinelone.com/labs/kimsuky-evolves-reconnaissance-capabilities-in-new-global-campaign/