Monthly Threat Intelligence Rollup

DEEP seas

06/02/23-07/01/23

Notable Cyberattacks

Summary of noteworthy cyberattacks in the last thirty days.

Incident	Activity Summary
Widespread MOVEit Compromises Linked to Cl0p Ransomware Group	The mass exploitation of CVE-2023-34362 that was reported last week has now been attributed to the activities of the Cl0p ransomware group (aka TA505). This tracks with the group's previous activities in 2023 and 2022, particularly the use of a previously unknown vulnerability in the GoAnywhere MFTS suite which was exploited to great effect in early 2023. Unlike this previous attack, Cl0p has declined to add individual victims to their extortion blog, instead relying on those organizations to contact them directly. This change is unlikely to provide them with great results, as not all victims may have the ability to detect a compromise or determine if the information stolen by the group is worth negotiation. The group's demands to contact them and retrieve a unique chat link for negotiations may be an attempt to hide their negotiations from security researchers; previous negotiations have been publicly (and humorously) disrupted by outside parties. The putative APT28 connection still requires further research to elucidate the full extent of any potential overlap; the IP in question is not a Tor exit node nor a VPN/VPS service, but rather a garden-variety Romanian ISP. DeepSeas TDE CTI will continue to research this unique overlap and will publish and findings separately.[i]
Infotel ISP Reportedly Compromised by Ukrainian Hacktivists	Though hacktivism is often beneath the notice of most security professionals due to a lack of sophistication and persistence, the actions of the Ukrainian Cyber.Anarchy.Squad may represent the single most devastating hacktivist attack to date. The group reportedly attacked the Russian Infotel ISP directly, leading to a complete collapse of network traffic for over 24 hours. Review of Infotel’s connectivity has determined that the ISP remains offline as of this writing. The group claimed to have completely destroyed the ISP's infrastructure, though by what means this was accomplished are unclear. Given that the group published Infotel's full internal client list, cyberattack is highly likely with ransomware or some other data-destruction malware used to cripple the organization. To add further headache, Infotel was responsible for handling interbank communications between the Russian Central Bank and over 100 other Russian financial institutions, including Sberbank, as well as credit lending companies and other financial institutions. DeepSeas TDE CTI expects that such incidents will not be unique. Given the heavy technology sanctions on Russia since February 2022 and a lack of investment in hardware upgrades, end of life equipment and software will continue provide malicious actors entry into Russian networks. Replacement of this equipment and software will be hindered by sanctions and funding shortfalls and provide further opportunity for compromise by determined actors.[ii]
Barracuda Email Security Gateway Appliances Require Replacement	Following the announcement of a critical severity remote command injection (RCI) flaw in the company's Email Security Gateway appliance on 20 May, the company has updated their guidance to recommend complete replacement of the appliances regardless of patching. Beginning in October 2022, CVE-2023-2868 was used by an as-yet unnamed threat actor or group to compromise ESG devices for the purposes of installing a malware suite containing the SALTWATER, SEASPY, and SEASIDE tools for the purposes of stealing proprietary information. Complicating analysis of these malware samples is the use of non-Windows binaries, frustrating easy sandboxing and analysis; though use of ELF/Unix malware is not common it is not rare either and has been used by numerous state-aligned and cybercriminal groups with varying levels of success. DeepSeas TDE will continue to identify samples and ensure that custom logic is developed to defend against this threat. Additionally, Barracuda provided network indicators of compromise, as well as detection logic including both Yara and Suricata detection signatures, which have been deployed by DeepSeas TDE.[iii]
CISA Releases Joint Advisory on LockBit Ransomware	In 2022, LockBit was the most active global ransomware group and RaaS provider based on the number of victims claimed on their data leak site. RaaS groups maintain and sell access to specific ransomware variants to affiliates who deploy the ransomware in

	exchange for payment. LockBit has attracted affiliates through various methods, including allowing them to receive ransom payments directly, publicly disparaging other RaaS groups, engaging in publicity stunts, and offering a user-friendly interface for their ransomware. The group's success is driven by continuous innovation in their administrative panel and supporting functions. Additionally, LockBit and other notable variants constantly update their tactics, techniques, and procedures (TTPs) for deploying and executing ransomware. LockBit affiliates employ legitimate freeware and open-source tools for malicious purposes during their intrusions. These tools are repurposed by LockBit to perform activities like network reconnaissance, remote access, tunneling, credential dumping, and file exfiltration. PowerShell and batch scripts are commonly used for system discovery, reconnaissance, password/credential retrieval, and privilege escalation. Additionally, artifacts from professional penetration-testing tools like Metasploit and Cobalt Strike have been detected in their operations. DeepSeas TDE currently has custom detections to defend against LockBit attacks.[iv]
8Base Ransomware Group Activity More Than Doubles in June	First observed in March 2022, the 8Base ransomware group maintained a low profile and cadence of activity, with approximately two victims observed per month. In the month of July 2023, however, the group's activities have at least doubled. Since the beginning of July, the group has more than doubled their list of victims, having added 25 new compromises to their extortion site. Much like many other ransomware groups, the group utilizes other malware-as-a-service platforms to deliver their ransomware. In this case utilizing the Smokeloader malware to drop their ransomware, though it has also been observed in conjunction with the Redline infostealer. The group's ransomware itself shares some similarities with RansomHouse ransomware group, principally in the wording and layout of the ransom notes, as well as their use of a customized version of the Phobos ransomware that appends the *.8base or * eight extension to encrypted files. At present, it is unknown why the group's activities (and presumed successes) have surged in the month of June 2023. It may be speculated that the group is capitalizing on available proof of concept exploits for MOVEit and other third-party software often utilized by businesses of all sizes, though no evidence has been uncovered to support this speculation. Given that the group's ransomware is built on the Phobos ransomware, and the group utilizes commercial malware to initiate their attack, existing detections are sufficient to block this attack successfully.[v]

Emergent Malware and TTPs

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

Malware/Campaign	Activity Summary	TTP Analysis
New Endpoint Defense Disablement Tool	On May 21, 2023, an individual known as spyboy started promoting a Windows endpoint defense evasion tool on the Russian-language forum Ramp. The tool, demonstrated in a video under the name "Terminator," allegedly has the capability to bypass twenty-three (23) EDR and AV controls.	Currently, spyboy is selling the software for prices ranging from $300 USD (for a single bypass) to $3,000 USD (for an all-in-one bypass). As of now, the Terminator software requires administrative privileges and User Account Controls (UAC) acceptance to function properly. Once executed with the appropriate level of privilege, the binary will write a legitimate and signed driver file called Zemana Anti-Malware to the C:\Windows\System32\drivers\ folder. This technique resembles other Bring Your Own Driver (BYOD) campaigns observed in use by threat actors over the past few years. After being written to the disk, the software loads the driver and has been observed terminating user-mode processes of AV and EDR software. DeepSeas is currently developing and deploying custom detection logic to identify and defend against this threat.[vi]
SeroXen RAT Increasing in Popularity	SeroXen is a recently emerged Remote Access Trojan (RAT) that gained popularity in 2023. Marketed as a legitimate tool, it provides undetected access to computers and is available for purchase at affordable prices, including a monthly license for $30 or a lifetime bundle for $60.	SeroXen is a fileless RAT known for effectively evading static and dynamic analysis. It incorporates various open-source projects, such as Quasar RAT, r77-rootkit, and NirCmd command line, to enhance its capabilities. Although initially prevalent among the gaming community, it is expected that SeroXen will eventually target companies instead of individual users. The RAT is based on Quasar RAT, an open-source remote administration tool that has a history of being associated with malicious activities carried out by threat actors, APT groups, and government attacks. SeroXen is a modified branch of Quasar RAT, featuring additional functionalities. DeepSeas TDE is currently working to deploy custom detection logic to defend against this threat.[vii]
Pre-Authentication Remote Code Execution on Fortigate VPN (CVE-2023-27997)	A critical vulnerability in FortiOS SSL VPN has been exploited in attacks against government, manufacturing, and critical infrastructure organizations. The flaw allows unauthenticated attackers to achieve remote code execution by exploiting a heap-based buffer overflow weakness in FortiOS and FortiProxy SSL-VPN.	Fortinet discovered the vulnerability during a code audit following recent attacks exploiting another SSL-VPN zero-day (CVE-2022-42475). Fortinet has released security updates to address the vulnerability and is working closely with customers to monitor the situation. Customers with SSL-VPN enabled are advised to upgrade to the latest firmware release promptly to mitigate the risk. Fortinet's proactive approach of releasing patches before disclosing vulnerabilities aims to give customers time to secure their devices before threat actors can create exploits by reverse engineering them.[viii]

Threat Actor Campaigns

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

Threat Actors	Activity Summary
Asylum Ambuscade Group Branches Out into Espionage	Building off a Proofpoint report about the 404 Traffic Direction System, ESET has released a report about a former entirely cybercriminal group focusing on Central Asia and parts of the former Soviet Union, which has now shifted into cyberespionage activities in Eastern Europe. While overlap between criminal groups is common, a shift to the targeting of governments, along with small and medium businesses, is decidedly uncommon. Further review suggests that the group has been in operation since at least mid to late 2020, conducting cryptocurrency theft and other activities. The shift to adding cyberespionage to their activities, unsurprisingly, was first observed in March 2022, shortly after the outbreak of the Russo-Ukrainian War that February. This points to a Russian nexus of activity, as Moscow likely pulled in talent from cybercrime groups to backfill a talent shortage, as observed Asylum Ambuscade targets were government officials in and around Ukraine. DeepSeas TDE CTI has deployed the available network indicators from ESET, gathered samples of their malware for analysis, and is currently sandboxing malware samples to determine whether existing coverage is sufficient to counter this threat.[ix]
UNC3886 Continuing to Target ESXi Vulnerabilities	Back in late 2022, Mandiant revealed Chinese threat actor UNC3886 utilizing new malware that impacted VMware ESXi hosts, vCenter servers, and Windows virtual machines (VM). UNC3886 has primarily targeted defense, technology, and telecommunication organizations located in the U.S. and APJ regions. Through ongoing research, Mandiant has discovered additional techniques used by UNC3886 to evade EDR solutions and target systems that do not support EDR solutions, such as network appliances, SAN arrays, and VMware ESXi hosts. These techniques include harvesting credentials from a vCenter Server, exploiting a zero-day vulnerability for privileged commands, deploying backdoors on ESXi hosts, and tampering with logging services to hinder investigation. UNC3886 must have admin access to the hypervisor to exploit the vulnerability gained via stolen credentials. To counter UNC3556's unique attacks, organizations need to maintain vigilance by monitoring both the operating system layer and the underlying infrastructure appliances. Regular patching, maintenance, and monitoring of these appliances are crucial. DeepSeas TDE has developed and deployed custom Yara and Suricata rules to identify and defend against this threat.[x]
MSTIC Links DEV0586 To Russian GRU	Microsoft Threat Intelligence Center (MSTIC) has provided updated details about a Russian state-sponsored threat actor formerly known as DEV-0586, which has now been named Cadet Blizzard. Cadet Blizzard is associated with the Russian General Staff Main Intelligence Directorate (GRU) but operates separately from other known GRU-affiliated groups. The group has conducted destructive cyber operations, including attacks on Ukrainian government organizations, defacements of Ukrainian websites, and hack-and-leak operations. Cadet Blizzard has been active since at least 2020 and continues to target government organizations and IT providers in Ukraine, Europe, and occasionally Latin America. The group utilizes a variety of tools and techniques, including living-off-the-land tactics to gain initial access, moving laterally, collecting information, and deploying persistence mechanisms. Microsoft advises organizations to implement multifactor authentication, review remote access infrastructure, enable controlled folder access, and block certain process creations to mitigate the risk posed by Cadet Blizzard. DeepSeas TDE is currently analyzing the artifacts from this report and will deploy custom detection signatures if necessary.[xi]
APT15 Leveraging New Backdoor Against Foreign Ministries in the Americas	The Chinese state-aligned Flea group (aka APT15, NICKEL) has been observed targeting foreign ministries primarily in the Americas. The campaign lasted from late 2022 to early 2023 and involved the use of a new malware dubbed Graphican. While the campaign focused on foreign affairs ministries, the group also targeted a government finance department, a corporation selling products in Central and South

	America, and at least one victim in an unnamed European country. Flea has a history of targeting government entities, diplomatic missions, and embassies, indicating an interest in espionage rather than cybercrime. In this campaign, they utilized various tools, including the Graphican backdoor, as well as other tools attributed to Flea in the past. Graphican is an evolution of the Ketrican backdoor, previously used by Flea and based on the venerable BS2005 malware. Graphican distinguishes itself by employing the Microsoft Graph API and OneDrive for its command-and-control infrastructure. This technique of utilizing the Microsoft Graph API and OneDrive as a command-and-control server was previously observed in a campaign by the Russian state-sponsored APT group Fancy Bear in 2022. Flea has been active since at least 2004, adapting its tactics, techniques, and procedures (TTPs) over time. In recent years, their focus has shifted, with North and South America becoming more prominent targets. Foreign ministries remain a key target for Flea, indicating consistency with regards to their activities. Flea is considered a large and well-resourced group, resilient to exposure and takedowns. The development of a new backdoor and the use of notable techniques demonstrate Flea's continued activity and adaptation in the cybersecurity landscape. DeepSeas TDE is currently assessing the Graphican malware for custom detection logic.[xii]
New "Muddled Libra" Targeting Service Providers' Customers	The Muddled Libra threat group poses a significant risk to organizations in the software automation, BPO, telecommunications, and technology industries. The group is noted for its adeptness at social engineering and adapting to new technologies, presenting a formidable challenge even for organizations with robust cyber security defenses. Palo Alto has found Muddled Libra responsible for a series of interconnected incidents between mid-2022 and early 2023, primarily targeting large outsourcing firms serving high-value cryptocurrency institutions and individuals. They employ a phishing kit called 0ktapus, which simplifies the setup of a complex infrastructure for attacks like fake authentication portals and targeted smishing. This enables even less skilled attackers to achieve a high success rate. Muddled Libra exhibits a wide range of attack techniques, including social engineering, smishing, and utilizing open-source penetration testing tools. They are highly adaptable, swiftly shifting to alternative attack vectors when one avenue is blocked. Once established, Muddled Libra proves difficult to eradicate, demonstrating a profound understanding of modern incident response frameworks. They specifically target downstream customers of their victims, using stolen data and frequently returning to refresh their dataset. Their breaches have clear objectives, focusing on stealing information from high-value clients to facilitate subsequent attacks. To protect against Muddled Libra, it is recommended to implement multi-factor authentication (MFA) and single sign-on (SSO), while emphasizing comprehensive user awareness training to identify social engineering attempts. Organizations should assume that Muddled Libra is well-versed in incident response strategies and establish out-of-band response mechanisms in case of a breach. Maintaining up-to-date credential hygiene, monitoring critical defenses, and enforcing access restrictions are also crucial. Additionally, restricting anonymization services at the firewall level is advisable.[xiii]
Fancy Bear Exploiting Ukrainian WebMail Vulnerability to Support Espionage Activities	Recorded Future's Insikt Group, in collaboration with Ukraine CERT-UA, has uncovered a campaign targeting high-profile entities in Ukraine. The campaign, correlated with a spear-phishing campaign discovered by Recorded Future's Network Traffic Intelligence, exploited the vulnerability CVE-2020-35730 in Roundcube, an open-source webmail software. By leveraging news about Russia's war against Ukraine, the campaign enticed recipients to open emails, leading to the immediate compromise of vulnerable Roundcube servers. Key targets include the targeting of a regional Ukrainian prosecutor's office, a central Ukrainian executive authority, and reconnaissance activities involving other Ukrainian government entities and an organization involved in Ukrainian military aircraft infrastructure upgrade and refurbishment. The campaign is linked to historic BlueDelta activity, which exploited the Microsoft Outlook zero-day vulnerability CVE-2023-2397 in 2022. CERT-UA attributes the activity to APT28, also known as Forest Blizzard and Fancy Bear, a group associated with the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). The BlueDelta phishing campaign exploits vulnerabilities in Roundcube to run

	reconnaissance and exfiltration scripts. The malicious scripts redirect future incoming emails to an actor-controlled email address, perform reconnaissance on the target Roundcube server, and exfiltrate session cookies, address books, and user information from Roundcube's database. The BlueDelta campaign appears to enable military intelligence gathering to support Russia's invasion of Ukraine, given its targeting and geopolitical backdrop. To mitigate the risk of exploitation, it is crucial for potential targets to ensure that their Roundcube software is fully patched and up to date.[xiv][xv]
Volt Typhoon Deploys New Tradecraft	Chinese nation-state actor Volt Typhoon, also known as Vanguard Panda, has been active since mid-2020, employing advanced techniques to maintain remote access to targeted organizations. Security company CrowdStrike has been tracking the group and discovered their use of never-before-seen tradecraft. Volt Typhoon relies on ManageEngine Self-service Plus exploits for initial access, followed by custom web shells for persistent access and living-off-the-land (LotL) techniques for lateral movement. Volt Typhoon has targeted U.S. government entities, defense organizations, and critical infrastructure, prioritizing operational security and utilizing a broad range of open-source tools against a limited number of victims to conduct long-term malicious activities. One incident involved an unsuccessful attack where Volt Typhoon leveraged a web shell disguised as a legitimate identity security solution, allowing them to avoid detection. Analysis revealed that the web shell had been deployed six months prior, indicating extensive prior reconnaissance of the target network. Another notable discovery was a trojanized version of tomcat-websocket.jar containing three new Java classes, one of which functioned as a web shell capable of executing encoded and encrypted commands. This indicates the use of a backdoored Apache Tomcat library as a persistence technique, enabling ongoing access to high-value targets. CrowdStrike noted that Volt Typhoon's advanced understanding of the victim's environment and their ability to remain undetected during reconnaissance efforts demonstrate their persistence and evasive tactics. They actively covered their tracks as they delved deeper into the targeted infrastructure. DeepSeas TDE has added custom Yara rules provided by CrowdStrike to enhance existing Volt Typhoon detections.[xvi]
MuddyWater Group Deploys New C2 Framework	The Iranian state-sponsored group MuddyWater has been using a newly discovered command-and-control (C2) framework called PhonyC2 since 2021, according to cybersecurity firm Deep Instinct. The framework was observed in an attack on the Israeli research institute, Technion, in February 2023. PhonyC2 is structurally and functionally similar to MuddyWater's previous Python 2-based C2 framework called MuddyC3. The group continuously updates the PhonyC2 framework and changes tactics to evade detection. MuddyWater, also known as Mango Sandstorm or MERCURY, is a cyber espionage group affiliated with Iran's Ministry of Intelligence and Security (MOIS) since 2017. MuddyWater's attack chains typically involve exploiting vulnerable public-facing servers and employing social engineering techniques to gain initial access. The group utilizes tactics such as creating sock puppets, posing as job recruiters, journalists, or think tank experts to deceive targets. The use of social engineering is a consistent feature in Iranian advanced persistent threat (APT) groups engaged in cyber espionage and information operations. Deep Instinct discovered the PhonyC2 framework in April 2023 on a server associated with MuddyWater's infrastructure used in the Technion attack. Ligolo, a reverse tunneling utility commonly used by the threat actor, was also found on the same server. PhonyC2 is a post-exploitation framework that generates payloads connecting back to the C2 server to receive instructions from the operator. It is considered a successor to MuddyC3 and POWERSTATS. The framework supports various commands, including payload generation, dropper creation, enumeration of connected machines, execution of commands across hosts, PowerShell shell access to remote computers and persistence mechanisms.[xvii]
Andariel Group Returns with New Remote Access Trojan	The North Korea-linked threat actor, Andariel, used a previously undisclosed malware called EarlyRat to exploit the Log4j Log4Shell vulnerability in attacks last year, according to a report by Kaspersky. Andariel, also known as Silent Chollima and Stonefly, is associated with North Korea's Lab 110, which houses other hacking units like APT38 (BlueNoroff) and is collectively known as the Lazarus Group. Andariel conducts espionage attacks against foreign governments and military entities, while

	also engaging in cybercrime to generate income for the country, which is under sanctions. Its cyber arsenal includes the Maui ransomware and various remote access trojans and backdoors like Dtrack, NukeSped, MagicRAT, and YamaBot. In the Log4Shell attack chain, Andariel targeted unpatched VMware Horizon servers. The latest discovery by Kaspersky reveals that EarlyRat is distributed through phishing emails with Microsoft Word documents. When the recipients enable macros, VBA code is executed, leading to the download and execution of the trojan. EarlyRat is a simple backdoor designed to gather system information, exfiltrate data to a remote server, and execute arbitrary commands. It shares similarities with MagicRAT and is written using the PureBasic framework. Andariel also utilizes off-the-shelf tools like 3Proxy, ForkDump, NTDSDumpEx, Powerline, and PuTTY for further exploitation of the target. The group constantly updates its custom tools and develops new malware, making it a complex and evolving threat. DeepSeas TDE will be deploying custom detection signatures to identify and defend against EarlyRat.[xviii]

Dark Web Markets

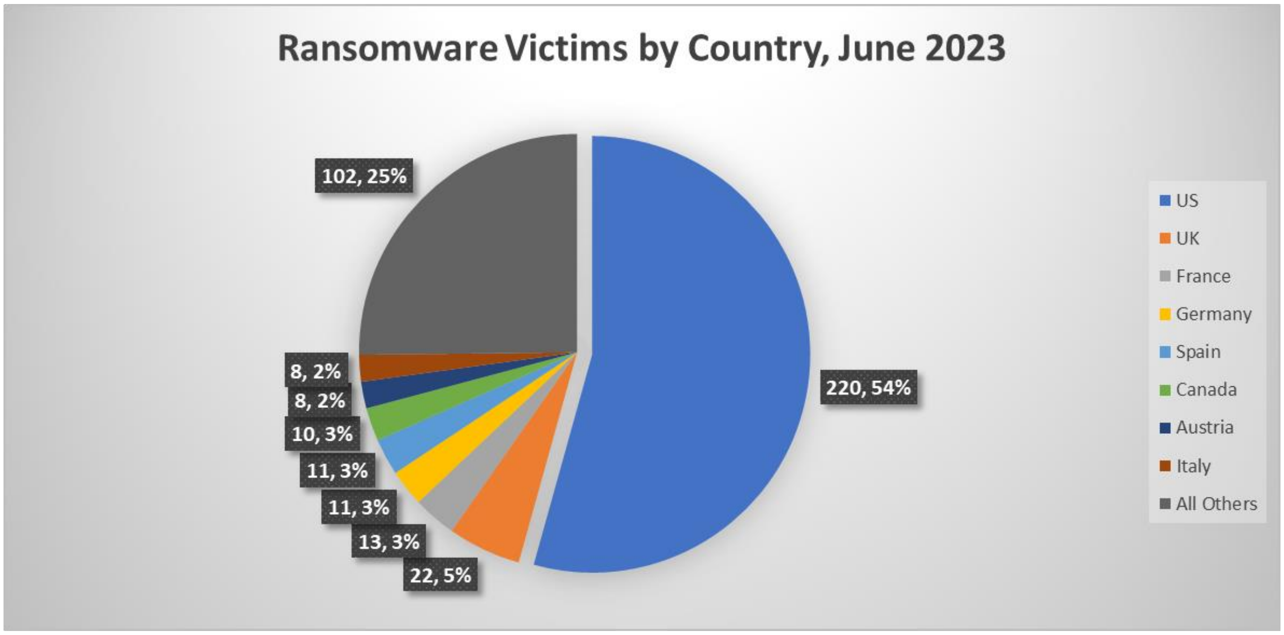
High-profile ransomware data dumps and dark web access sales identified in last thirty days.

Activity	Note
Access Sale	A user on a popular Russian-language crime forum is selling access to an Outlook mail user at a U.S.-based retail company with USD 2 billion in revenue for USD 100. They claimed that 2FA is not enabled.
Access Sale	A user on a prominent Russian-language crime forum is selling VPN/RDP/Jira access to a U.S.-based government contractor who provides software services to the U.S. military and the USG with USD 1.5 billion in revenue for a buy now price of USD 1,500.
Actor Developments	A new crime forum called Exposed (exposed[.]vc) is positioning itself as a successor forum to the now defunct RaidForums and Breached Forums. Unlike the previous two forums, Exposed has set up a separate section especially for ransomware discussions and is attempting to attract ransomware operators to use the forum for advertising and recruitment. So far, actors purporting to represent LockBit, Trigona, Rhysida, No Escape, and Medusa ransomware teams have made posts on the forum.
Access Sale	An actor on a prominent Russian-language crime forum is selling domain admin access to a Vietnamese telecom provider with USD 730 million in revenue for a buy now price of USD 4,800.
Data Sale	An actor on a Russia-language crime forum is selling what they claim to be 10 TB of data stolen from food service giant Sysco. In March 2023, Sysco announced that they were compromised, and customer data was leaked, but the data hadn’t surfaced yet.
Access Sale	An actor on a popular criminal forum offered to sell what they claimed was an SSH shell in a server owned by French consulting giant Cap Gemini for USD 2,000. They later withdrew the offer. It is unknown whether they sold or lost the access.
Access Sale	A known ransomware-associated actor on a popular Russian-language criminal forum is selling access to a purported Bangladeshi bank for USD 30,000. They claimed that there are no hidden issues with the access, it’s just that the bank is “not my kind of target.”
Actor Developments	The patriotic pro-Russia hacking group KillNet announced that, along with REvil and the hacking group Anonymous Sudan, they would be attacking the European banking system and the SWIFT messaging system on or about 16-17 June. This time, they promised that it would be a different kind of attack instead of the mostly ineffectual distributed denial of service attacks they have made against western targets in the last year. It is unknown if they have legitimately enlisted former members of REvil for the attack. It seems more likely that they have assumed the REvil brand as it is notorious in the West as a dangerous group, and their intent is to cause concern and fear. They did not specify what form the attack would take.
Access Sale	An actor on a popular crime forum is selling what they claim is access to a Maxar Technologies commercial imaging satellite for USD 15,000. He has not offered any proof of access, and it doesn’t appear that he has sold it yet.
Tool Sale	An actor on a prominent crime forum is selling a purported zero-day in a popular customer relationship management (CRM) software suite for USD 6,000. They did not disclose which CRM it is, only noting that there are more than 10,000 hits for this CRM on Shodan search engine competitor FOFA.
Access Sale	A reputable actor on a prominent Russian-language crime forum claimed that they have obtained “unique access to a panel with which I can input any American number, and for the rest of time, one time per hour I can get the coordinates (longitude/latitude) of this person on the map" and is willing to sell data from this access for USD 2,000/day, USD 10,000/week, or USD 30,000/month for up to five phone numbers.
Access Sale	An actor on another crime forum is selling what they claim is domain admin access to an unnamed U.S.-based medical insurance company with USD 40 million in revenue for USD 1,500.

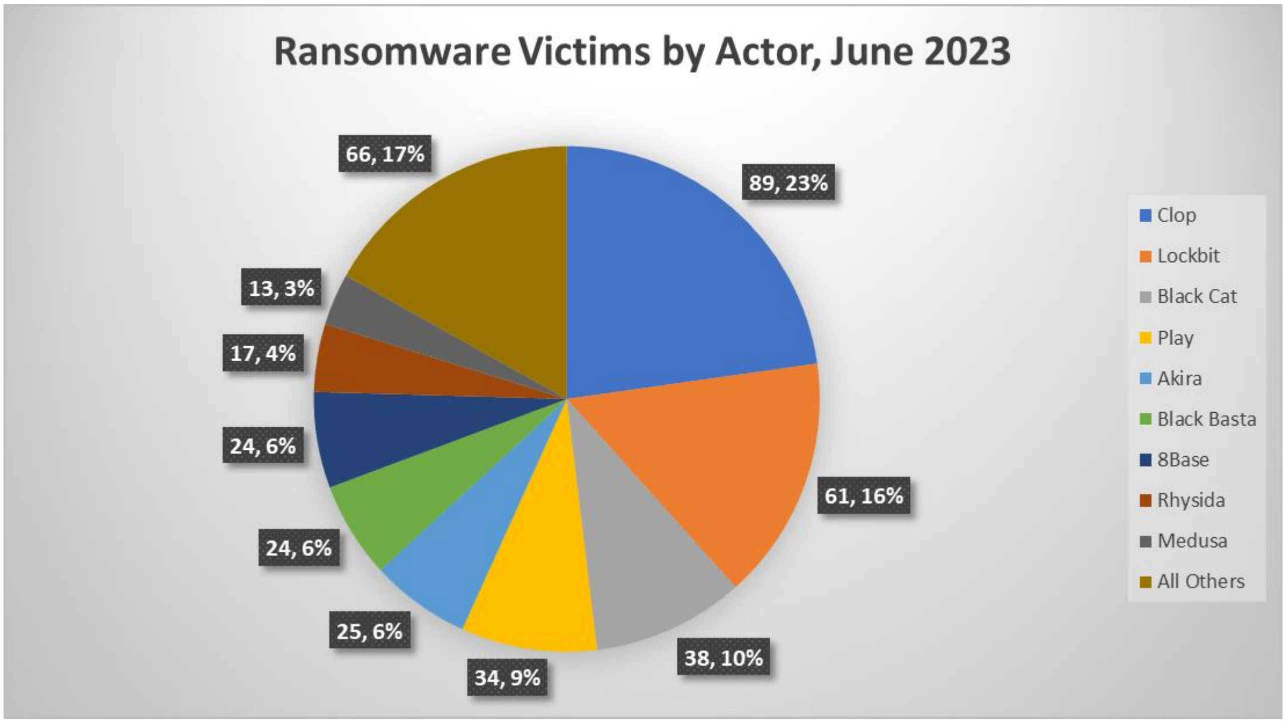
Access Sale	A known access seller is offering Citrix access to a Germany-based IT company with USD 5.6 billion in revenue for a buy now price of USD 9,000. There was a bidding war for the access, and a known ransomware operator made an initial bid of USD 1,200. German IT integration and consulting company Bechtle has USD 5.6 billion in revenue according to ZoomInfo.
Access Sale	Another crime forum access seller is selling local admin access to an Israel-based aerospace and defense company with USD 143 million in revenue for USD 5,000. Israeli jet engine part manufacturer Bet Shemesh Engine Holdings has USD 143 million in revenue according to ZoomInfo.
Access Sale	Finally, another known access seller is selling RDP domain admin access to a host belonging to the Department of Health and Human Services (HHS) for USD 6,000. They did not offer proof of access.

By The Numbers

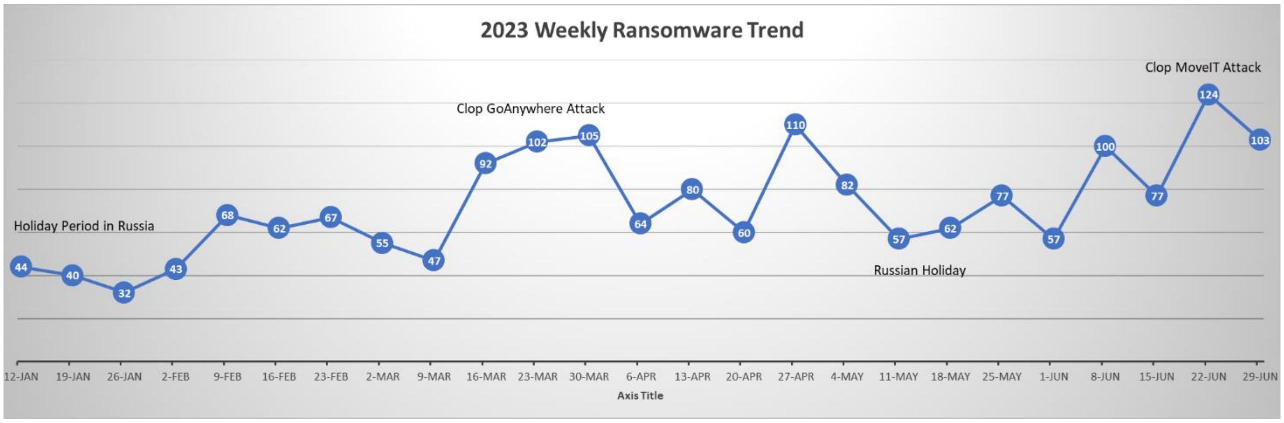
Summarizing incidents in graphical format

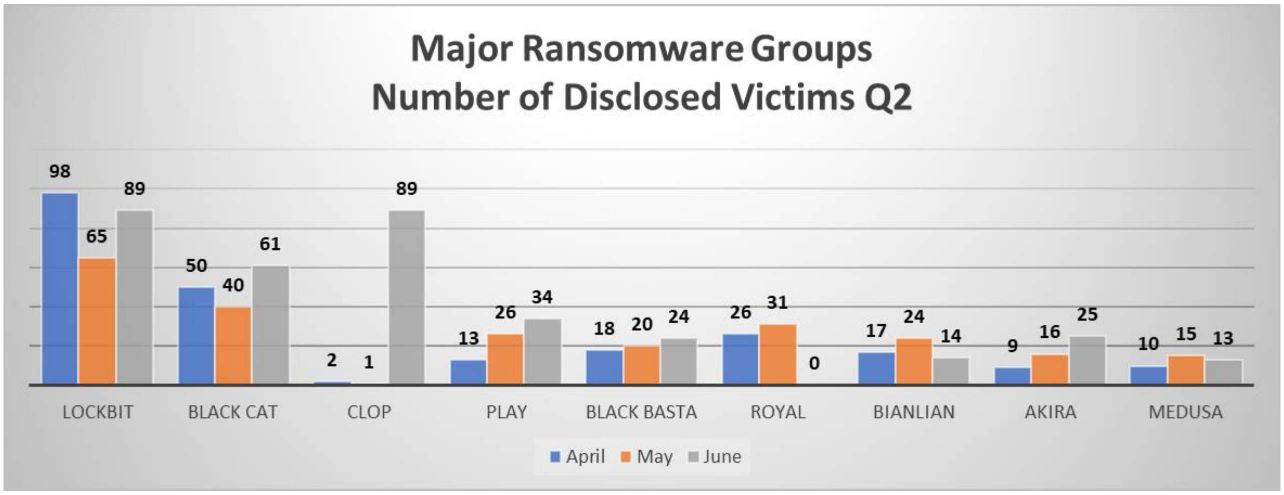


Ransomware Victims by Country, June 2023



Ransomware Victims by Actor, June 2023


2023 Weekly Ransomware Trend
Holiday Period in Russia
Clop GoAnywhere Attack
Russian Holiday
Clop MoveIT Attack
44
40
32
43
68
62
67
55
47
92
102
105
64
80
60
110
82
57
62
77
57
100
77
124
103
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
8-JUN
15-JUN
22-JUN
29-JUN
Axis Title


Major Ransomware Groups
Number of Disclosed Victims Q2
98
65
89
50
40
61
2
1
89
13
26
34
18
20
24
26
31
0
17
24
14
9
16
25
10
15
13
LOCKBIT
BLACK CAT
CLOP
PLAY
BLACK BASTA
ROYAL
BIANLIAN
AKIRA
MEDUSA
April
May
June

[i] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

[ii] https://twitter.com/igorsushko/status/1667058373274275840

[iii] https://www.barracuda.com/company/legal/esg-vulnerability

[iv] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

[v] https://www.bleepingcomputer.com/news/security/8base-ransomware-gang-escalates-double-extortion-attacks-in-june/

[vi] https://www.reddit.com/r/crowdstrike/comments/13wjrgn/20230531_situational_awareness_spyboy_defense/

[vii] https://cybersecurity.att.com/blogs/labs-research/seroxen-rat-for-sale

[viii] https://www.fortinet.com/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign

[ix] https://www.welivesecurity.com/2023/06/08/asylum-ambuscade-crimeware-or-cyberespionage/

[x] https://www.mandiant.com/resources/blog/vmware-esxi-zero-day-bypass

[xi] https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/

[xii] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/flea-backdoor-microsoft-graph-apt15

[xiii] https://unit42.paloaltonetworks.com/muddled-libra/

[xiv] https://go.recordedfuture.com/hubfs/reports/cta-2023-0620.pdf

[xv] https://cert.gov.ua/article/4905829

[xvi] https://www.crowdstrike.com/blog/falcon-complete-thwarts-vanguard-panda-tradecraft/

[xvii] https://www.deepinstinct.com/blog/phonyc2-revealing-a-new-malicious-command-control-framework-by-muddywater

[xviii] https://securelist.com/lazarus-andariel-mistakes-and-easyrat/110119/