Monthly Threat Intelligence Rollup

DEEP seas

6/01/24-06/30/24

Notable Cyberattacks

Summary of noteworthy cyberattacks in the last thirty days.

Incident	Activity Summary
Coordinated "Operation Endgame" Takes Down Malware Infrastructure	Beginning on 28 May 2024, the FBI released new information about the multinational cybersecurity campaign, Operation Endgame, coordinating law enforcement from the United States, Denmark, France, Germany, the Netherlands, and the United Kingdom, as well as Europol and Eurojust. The campaign aims to dismantle the cyber criminal infrastructure that has caused hundreds of millions of dollars in damages globally. Operation Endgame led to the search, arrest, and takedown of over 100 servers that held numerous malware variants commonly used to steal personal and financial information, which supported the entire cyber criminal ecosystem. The operation so far has claimed success in targeting the services for numerous commodity malware families, such as IcedID, Smokeloader, Pikabot, and Bumblebee, which have infected millions of computers worldwide, targeting industries such as hospital networks and critical infrastructure services. As stated by Robert M. Witt, the FBI Charlotte special agent in charge, "The results of Operation Endgame are astounding and send a strong message to cyber criminals around the world. The FBI has special agents, computer scientists, forensic accountants, and other employees with an expertise in science and technology and the determination to attack cybercriminal networks no matter where they are located."[i]
Hacktivist Group, Sticky Werewolf, Glued to Russian Aviation Industry	This week, Morphisec Labs published an analysis of a new threat group dubbed "Sticky Werewolf." The Sticky Werewolf group has been active since at least April 2023 and is believed by Morphisec to be pro-Ukrainian. This attribution was made due to the group's targeting of AO OKB Kristall, a Moscow-based company involved in producing and maintaining aircraft and spacecraft, along with previous targets, including public organizations in Russia and Belarus, a pharmaceutical company, a Russian research institute dealing with microbiology and vaccine development, and more. Their current infection chain proceeds as follows: a phish is sent to the target containing multiple malicious files, including a decoy PDF and two LNK files masquerading as DOCX files. While the PDF file is benign, the LNK files can establish persistence using the Windows Registry, along with reaching out to the attacker's network share, which then installs a variant of the known CypherIT cryptor. Following deployment of automatic scripts to further establish persistence, the final payload is installed, typically including RATs or stealers, such as Rhadamanthys, Ozone, MetaStealer, DarkTrack, or NetWire, all of which have been used previously for espionage and data exfiltration.[ii]
New Velvet Ant Threat Group Targets BIG-IP	Following an investigation led by incident response company Sygnia, details of a newly identified threat actor were shared with the public. This threat actor, dubbed "Velvet Ant," is a Chinese state-aligned group focused on espionage. In recent news, this group has shown its sophistication through a breach uncovered by Sygnia. In this attack, Velvet Ant achieved persistence in their victim's network for nearly three years by using multiple methods, one of them being a legacy F5 BIG-IP appliance. After discovering the device was exposed to the internet, Velvet Ant discreetly leveraged it for C2 communication. Another reason why they were able to go undetected for so long is that the victim lacked operating system logs and had multiple outdated and vulnerable F5 appliances. After establishing connectivity, Velvet Ant would infect the victim with the venerable PlugX malware, a RAT well-known for its modular plugins, allowing for a large set of additional malicious features. Some recommendations from Sygnia to counter Velvet Ant include limiting outbound internet traffic and enhancing the security hardening of legacy servers.[iii]

Emergent Malware and TTPs

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

Malware/Campaign	Activity Summary	TTP Analysis
Malware of Many Names Makes Headlines	Recently, both HarfangLab and Cisco Talos have separately discussed a new banking trojan targeting Brazilian users.	Due to both organizations discovering and publishing their findings within a similar timeframe, the malware has two names at the moment: “AllaSenha,” which is used by HarfangLab, and “CarnavalHeist,” which is used by Cisco Talos. Despite the confusion of multiple names, AllaSenha and CarnavalHeist are indeed the same malware. HarfangLab named the malware AllaSenha due to it being a custom variant of “AllaKore,” a well-known open-source RAT. This malware was designed specifically to steal bank account credentials and uses Azure Cloud for the C2 communications and data exfiltration. The cyber criminals currently utilizing this malware gain initial access by sending spam emails with finance-related themes.[iv]
Exposed Critical Authentication Bypass Vulnerability in Veeam Software	IT software company Veeam, which specializes in data protection, backup, and disaster recovery solutions, recently released information about a collection of CVEs that were discovered within various components of their software.	One of the CVEs disclosed, CVE-2024-29849 (CVSS score 9.8), is a flaw in Veeam Backup Enterprise Manager, which allows the management of multiple Veeam backup and replication installations from a single web console. The vulnerability can allow an unauthenticated attacker to log in to the Veeam Backup Manager web interface as any user. After being disappointed in the lace of information provided by Veeam, Sina Kheirkhah, a vulnerability researcher and operator of the Summoning Team website, discovered that the point of initial access for the vulnerability lies in “VeeamRESTSvc,” also known as “Veeam.Backup.Enterprise.RestAPIService.exe.” To see a full breakdown of the vulnerability in question, please reference the report in this entry’s citation.[v]
AgentTesla’s Got a New Coat of Paint	Fortinet security researchers have published the results of recent research carried out on a new variant of the well-known AgentTesla malware, an infostealer malware first discovered around 2014 and written in .NET.	While the malware use case in this situation is nothing novel, being found in a phishing email, the changes made to the malware are worthy of attention. In this variant identified by Fortinet, AgentTesla uses a new way to submit stolen data back to their C2 infrastructure over FTP, instead of using HTTP POST and SMTP as they did previously. The malware uses the “STOR” method in FTP, which is used by FTP to upload a file from a client device to the server. While novel for AgentTesla, other malware families have used FTP communications for data exfiltration. This change may not provide the actors with greater success but is highly likely to confuse existing detection logic expecting AgentTesla to exfiltrate via HTTP and SMTP.[vi]
Patch Tuesday Reveals Critical Windows Server Bug	In this month’s Patch Tuesday from Microsoft, one critical severity vulnerability was addressed which could result in remote code execution (RCE) leading CVE-2024-30080 to be given a CVSS score of 9.8 out of 10.	This exploit targets the Microsoft Message Queuing (MSMQ) protocol of Windows Server operating systems, specifically all versions starting from Windows Server 2008, which is used for communication between applications within different servers or processes. Using MSMQ, attackers can take over an affected server by sending custom-made MSMQ packets. To prevent abuse of this weakness in MSMQ, Microsoft advises updating to the current versions of the Windows Server. To check for current breaches, determine whether the MSMQ service is running and if the TCP port 1801 is open on the server.[vii]

Multiple Critical CVEs Found in Ivanti Endpoint Manager	IT software company Ivanti recently disclosed multiple CVEs in one of their products, all determined to have a CVSS score of 9.6 out of 10 or higher.	The CVEs, which amount to six in total, were brought to the public's attention by Trend Micro's Zero Day Initiative and later classified as CVE-2024-29822 through CVE-2024-29827. These vulnerabilities all relate to the same common issue, that there is an SQL injection vulnerability that is possible in the Core server of their Ivanti Endpoint Manager (EPM) product, specifically in versions 2022 SU5 and before, which allows for arbitrary code execution (RCE). This SQL injection is possible due to a flaw within the "RecordGoodApp" method of EPM, where subpar input validation measures are used to construct SQL queries. After being notified of the issues within EPM, Ivanti has released a hot patch for current versions of EPM, addressing all the divulged problems. DeepSeas has determined that existing coverage is sufficient to detect and block this threat.[viii]
Diamorphine Morphs into New Malware Variant	Avast Threat Labs has pointed out in a recent post that Diamorphine, the well-known Linux kernel rootkit, has been given a new, previously undetected variant.	Diamorphine already had terrifying capabilities, with the malware able to essentially become invisible to a victim and hide all the files and folders that start with a prefix chosen by the attacker. It can also send signals that allow for actions such as hiding and unhiding arbitrary processes, hiding and unhiding the kernel module, and elevating privileges to gain root access. In this new version, however, even more features have been added, including the ability to stop Diamorphine by sending a message to the exposed device by impersonating the X_Tables module of Netfilter, a native Linux framework, and being able to execute arbitrary OS commands using magic packets. DeepSeas has tested samples of this malware and is updating detections accordingly.[ix]
New Flickery Fickle Information Stealer Found	Fortinet's Fortiguard Labs threat research team recently discovered a new infostealer, dubbed "Fickle Stealer" by Fortinet due to the Rust-based stealer's advanced functionality.	Fickle Stealer's functionality comes in the form of flexible targeting, with malware delivery having the option to go through four different means: • A VBA dropper (an .xml file) • A VBA downloader (u.ps1 and forfiles.exe) • A link downloader (bypass.ps1) • An executable downloader The malware also has a range of capabilities, including demonstrating anti-analysis techniques like concealing their malware packer as a legitimate executable by substituting code from the authentic executable with the packer's code and by manipulating the initialize function routine in the packer's function. It should also be noted that due to its frequently changing attack chain, the stealer is likely still in development, and it is currently unknown who developed the stealer.[x]
GrimResource's Forbidding First Appearance	Researchers at Elastic Security uncovered a novel code execution technique using uniquely crafted MSC files, which Elastic Security has dubbed "GrimResource."	This new method allows attackers to execute arbitrary code in Microsoft Management Console (MMC) with low detections, allowing for initial access and detection evasion. It does so by abusing an old cross-site scripting (XSS) bug present in the apds.dll library of the MMC. After attaching a reference to the at-risk Advanced Protocol Detection Service (APDS) resource in the StringTable section of the attacker's crafted MSC file, the adversaries can execute JavaScript impersonating the MMC. After compounding this with DotNetToJScript, which converts .NET assemblies into JavaScript code, the malicious actorscan execute code arbitrarily. This is done through another component of GrimResource, PASTALOADER, which inevitably delivers the final payload of the attack, which is Cobalt Strike.[xi]

P2Pinfect Gets rsagen Ransomware Update	As reported by Cado Security, the authors of the well-known malware family P2Pinfect have recently updated their product to include ransomware capabilities.	Previously, P2Pinfect was a peer-to-peer botnet targeting servers that were hosting publicly accessible instances of Redis, an in-memory data structure store. Now, P2Pinfect can also run “rsagen,” the botnet’s new ransomware payload. The ransomware checks if a ransom note is already present, then begins encryption. Following the execution, rsagen will look through all directories on the target and overwrite all of the contents, changing the file extension into an encrypted “.encrypted” version. Finally, the ransomware creates a database for the encrypted files in a temporary file with a new “.lockedfiles” file extension added. Should the victim pay the attackers for access to their data, rsagen is run again with a decryption token supplied by the assailants.[xii]

Threat Actor Campaigns

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

Threat Actors	Activity Summary
New Threat Group Moonstone Sleet Hails Destruction on its Victims	After careful consideration by Microsoft, the North Korean threat actor previously tracked by Microsoft as Storm-1789 has now been redesignated as “Moonstone Sleet.” This threat group has been attributed to be North Korean state-aligned due to its similarities with its sister organization, Diamond Sleet, more commonly known as Lazarus. This includes reused Comebacker malware code, a known Diamond Sleet tool, along with using similar TTPs such as utilizing social media to deliver weaponized software. Moonstone Sleet differs from Diamond Sleet in various ways, however, setting it apart from the others. Some of these unique avenues include weaponizing PuTTY, an ordinarily benign open-source terminal emulator, developing a pair of loader components named “SplitLoader” and “YouieLoad,” and most startlingly their own ransomware. Microsoft has dubbed the new ransomware strain “FakePenny,” which includes both the loader and encryptor components.[xiii]
New Threat Group LilacSquid Releases Toxic Ink-Themed Malware	Discovered by Cisco Talos, “LilacSquid” is a newly disclosed threat actor that is believed to have affiliations with North Korea, based on TTP overlap with other North Korean backed APT groups such as Andariel and Lazarus. They likely also have espionage-related motivations, as much of the group’s activity is based around establishing persistence to compromised victim organizations for data theft. The current attack chain appears to go as follows: LilacSquid compromises the victim via web application vulnerabilities or compromised RDP credentials; they then will use MeshAgent, an open-source remote management tool for C2 communication, where further malware can be installed. Some of the later malware that comes into play includes PurpleInk, a custom-made RAT adapted heavily from QuasarRAT, along with InkBox and InkLoader, two custom malware loaders. LilacSquid appears to paint a target indiscriminately on anyone who they have the potential to steal from, with past examples including the targeting of U.S. IT organizations building software for the research and industrial sectors, steering toward European energy sector establishments, and pursuing Asian pharmaceutical businesses.[xiv]
UNC5537 Extorts Data Theft Victims	Mandiant, which is now a part of Google Cloud, has shared their findings on a recently identified campaign by the UNC5537 group, a threat actor group new to the security community as of May but known to have clear financial motivations. In this operation, UNC5537 compromised customer data held in Snowflake instances. Snowflake is a multi-cloud data warehousing platform used to store and analyze large amounts of both structured and unstructured data. After exposing the data, the group then advertised the sale of said credentials on cyber crime forums and also extorted victims directly. This was made possible due to the various infostealer malware types the group had used on the company previously. These included stealers such as Vidar, RisePro, Redline, Racoon, Lumma, and MetaStealer. Using this acquired customer data, UNC5537 could easily login to the stolen accounts, perform reconnaissance on Snowflake’s database and external storage collection, and exfiltrate data.[xv]
Pakistan-Based UTA0137 Unleashes New DISGOMOJI Malware	In a post made by Volexity Threat Research, the company’s research team identified a new espionage campaign targeting Indian government entities. This campaign, reportedly operated by the Pakistan-based threat actor UTA0137, employed a new strain of malware dubbed as “DISGOMOJI” by Volexity. The malware is written in Golang and targets Linux systems, a unique choice of tooling for a Pakistani group. Because of this, the Indian government was determined to be their target, as India is known for its use of a custom Linux distribution named BOSS for many of their government workstations. Interestingly, DISGOMOJI uses emojis in the messaging and VoIP platform Discord for C2 communication because it uses a modified version of the venerable discord-c2 protocol. After establishing a connection to the affected machine, UTA0137 has been seen performing post-breach activities such as network

	reconnaissance, tunneling, vulnerability abuse, credential theft, and data exfiltration.[xvi]
RedJuliett Added to China's Cyber Arsenal	Between November 2023 and April 2024, Insikt Group identified and monitored activity by a new Chinese nation state group which Insikt Group has dubbed "RedJuliett." The group's operations, believed to be based in Fuzhou, China, are aimed at espionage in support of Beijing's policymaking in Taiwan, particularly focusing on its critical technology companies. RedJuliett has also been seen targeting government, education, technology, and diplomatic organizations in other countries and territories, including Hong Kong, Malaysia, Laos, the Philippines, South Korea, Kenya, Rwanda, Djibouti, and the United States. They have been seen performing network reconnaissance, privilege escalation, and post-exploitation using web shells. The group did so by exploiting vulnerabilities in their victim's internet-facing devices, such as their firewalls, load balancers, and VPNs, to gain initial access and also used techniques like SQL injection and directory traversal. For example, RedJuliett used SoftEther, a VPN client, to manage their infrastructure, such as compromised servers from Taiwanese universities. To mitigate such threats, Insikt Group recommends organizations should enhance vulnerability patching, employ defense-in-depth strategies, and regularly audit and secure internet-facing devices.[xvii]
A Secret Spice from a Sneaky Chef	Cisco Talos exposed a new RAT which the company named "SpiceRAT." This RAT has been attributed to the group "SneakyChef" due to it being used in an ongoing phishing campaign by the group, targeting government agencies in Europe, the Middle East, Africa, and Asia. Initial access was made using LNK or HTA files within the phishing emails to download the malware to the target. SpiceRAT is made of four main components: • A legitimate executable file (RunHelp.exe) • A malicious DLL loader (ssMUIDLL.dll) • An encrypted payload (CGMIMP32.HLP) • Downloaded plugins (Moudle.dll) These parts together provide SpiceRAT various methods of attempting to avoid detection, performing reconnaissance, establishing persistence, and communicating with its C2 server.[xviii]

Dark Web Markets

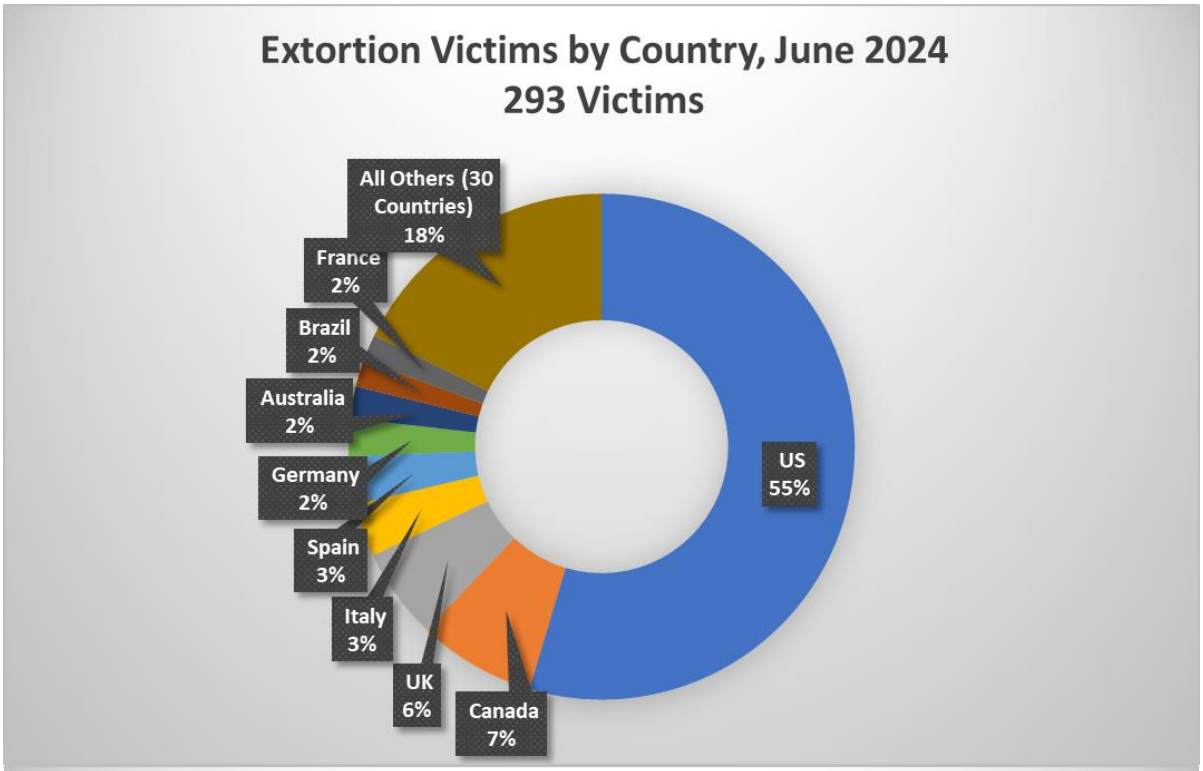
High-profile ransomware data dumps and dark web access sales identified in last thirty days.

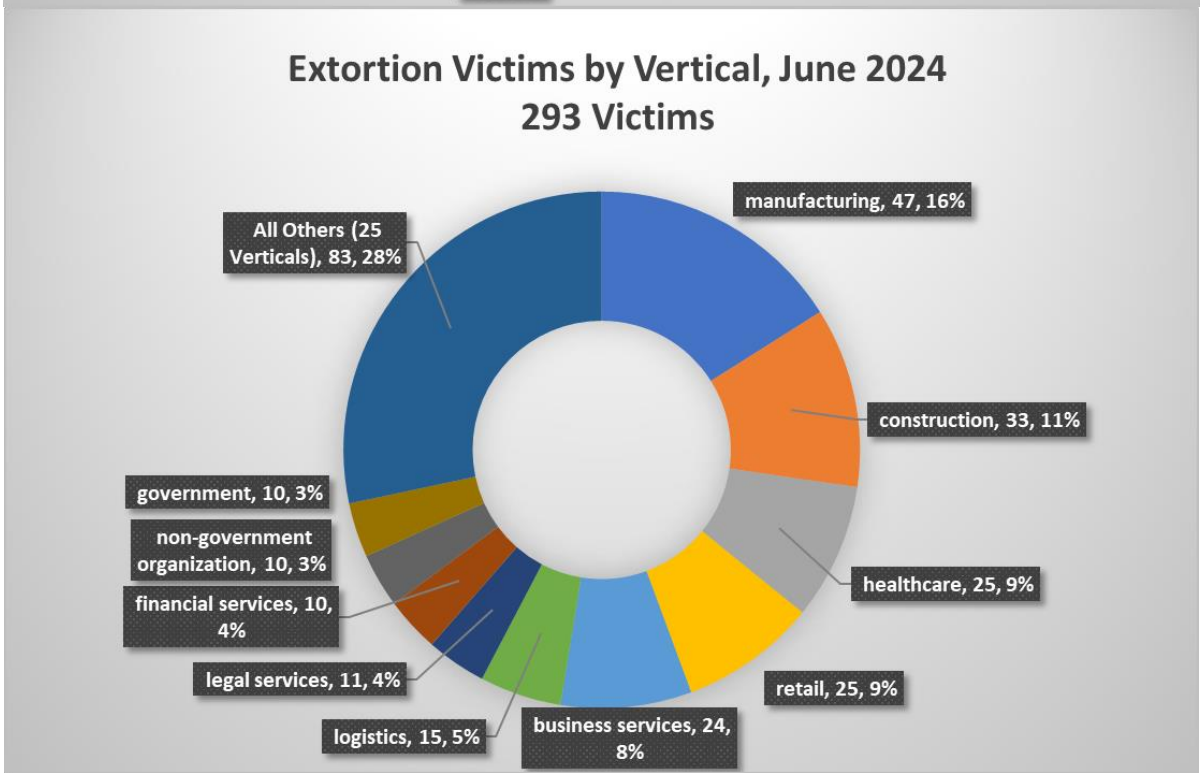
Activity	Note
Access Sale	An actor on several popular Russian-language crime forums was selling what he claims is a Windows local privilege escalation (LPE) 0day that escalates privileges from Medium to System in two seconds with a 99.4% success rate for USD 120,000.
Data Sale	An actor on an English language crime forum posted databases they claimed to have stolen from petrochemical, food and beverage, or another third-party company that exposed the PII of employees and customers of those companies.
Access Sale	An actor on a popular Russian-language crime forum was selling access to a cloud belonging to a U.S-based business services firm with more than USD 100 million in revenue for USD 10,000. They claimed there are files going back to 2014 on the cloud server and that the company has worked with the "biggest countries in the world [sic]."
Data Sale	An actor on a recently seized forum was selling what they claimed to be a database of student and staff PII from a U.S.-based school district for USD 1,000.
Data Sale	An actor on a popular Russian-language crime forum was selling a 103 GB database of customer data belonging to a computer part manufacturer. They did not name a price.
Access Sale	An actor on a popular Russian-language crime forum was selling Rdweb access to a German business services company with USD 2.3 billion in revenue for a buy-now price of USD 16,000.
Access Sale	An actor on a popular Russian-language crime forum put multiple victims up for sale in both forums this week, including an automotive retailer, a cybersecurity company, and a major U.S. financial institution. It's suspected they gained these accesses using compromised Snowflake credentials.
Access Sale	An access seller on a popular Russian-language crime forum was selling domain admin access to a Canadian media company with USD 344 million in revenue and a U.S.-based biotech company with USD 453 million in revenue.
Access Sale	An access seller on a popular Russian-language crime forum was selling admin access to a SolarWinds instance at an unnamed Latin American company, supposedly allowing access to around 200 customers, including banks.
Access Sale	An access seller on a popular Russian-language crime forum was selling domain admin access with AnyDesk and ScreenConnect accesses to a U.S.-based enterprise in the restaurants and hospitality vertical with USD 3.7 billion in revenue. The actor later reported that they had lost access.
Data Sale	An actor on a popular English-language crime forum uploaded a database breached this month by notorious criminal IntelBroker from an internation real estate giant. It was obtained by "exploiting a recently found Atlassian Jira 0-day and was leaking it's AWS config settings in the Jira." They posted a sample of the data as proof.
Data Sale	A well-known cyber criminal on a formerly popular forum was observed selling data stolen from an international chip manufacturer, including intellectual property, customer data, and employee data. They posted samples of the data but did not name a price.

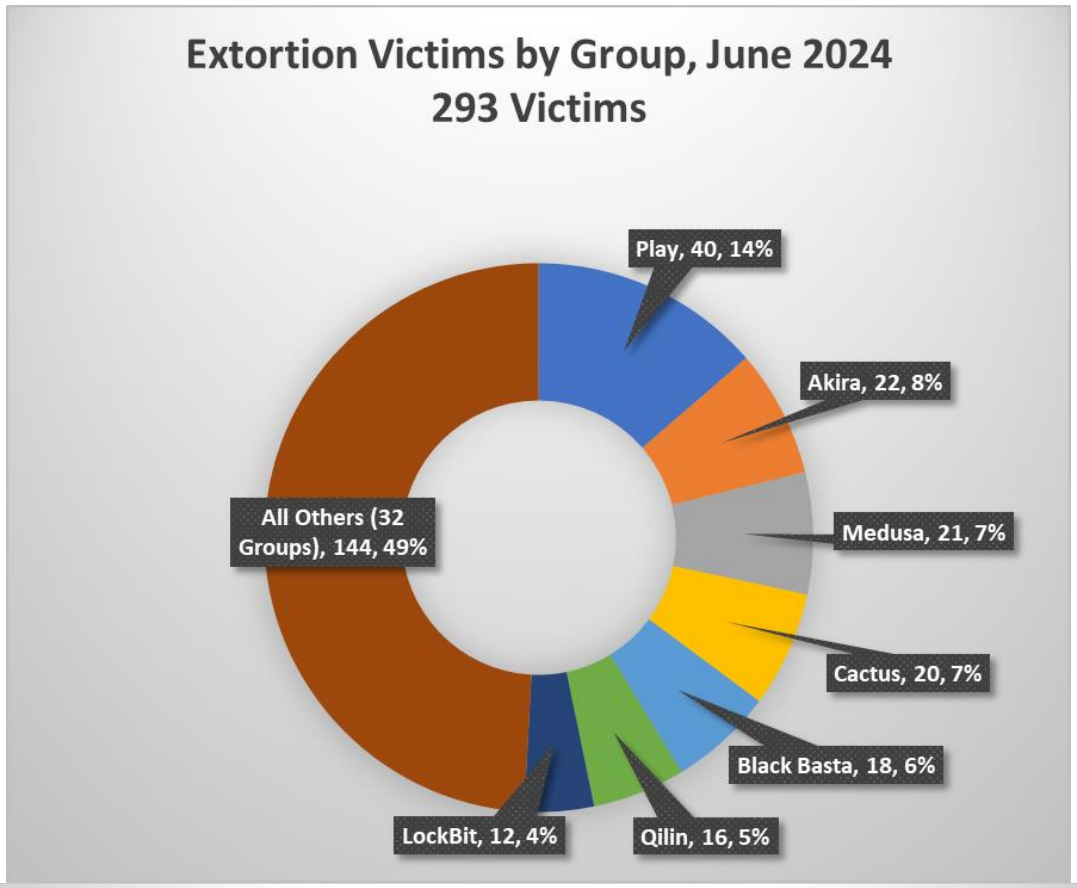
Access Sale	An access seller on a popular Russian-language crime forum was selling local admin access to a Swiss-based organization with USD 71.7 million in revenue.
Access Sale	An access seller on a popular Russian-language crime forum was selling VPN and ManageEngine ServiceDesk credentials to a multibillion-dollar fast food corporation with over USD 10 billion in revenue in an unnamed European country. Numerous companies fit this profile.
Access Sale	An access seller on a popular Russian-language crime forum was selling RDweb access to an Australian furniture retailer with USD 1.7 billion in revenue for USD 10,000.
Data Sale	An actor notorious for their exploitation of Snowflake claimed to be selling a database stolen from U.S. luxury retailer Nieman Marcus for USD 50,000. Nieman Marcus confirmed the breach.

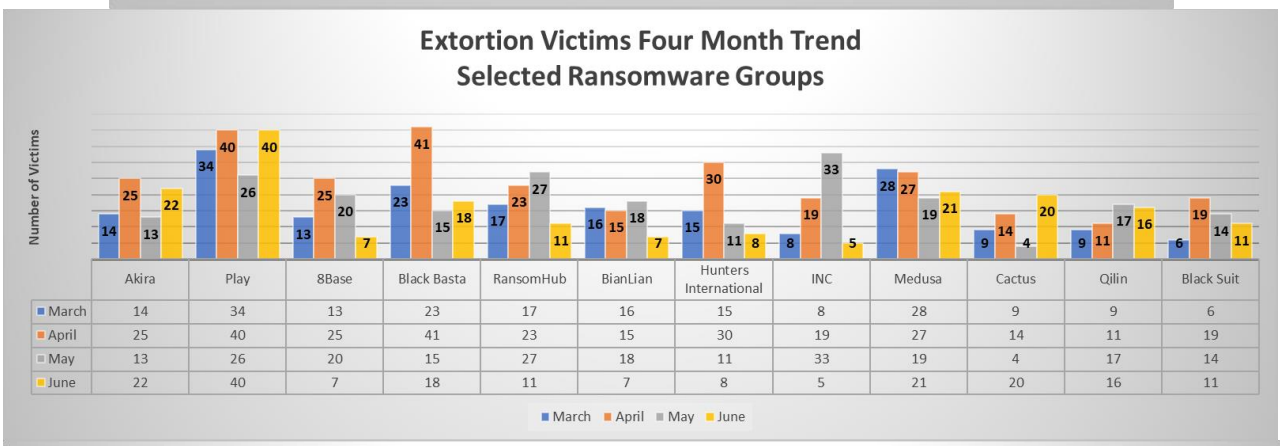
By The Numbers

Summarizing incidents in graphical format









	Akira	Play	8Base	Black Basta	RansomHub	BianLian	Hunters International	INC	Medusa	Cactus	Qilin	Black Suit
March	14	34	13	23	17	16	15	8	28	9	9	6
April	25	40	25	41	23	15	30	19	27	14	11	19
May	13	26	20	15	27	18	11	33	19	4	17	14
June	22	40	7	18	11	7	8	5	21	20	16	11

New Detection Content

Noteworthy new detection logic added in the last 30 days, excluding rule tuning.

- **DS_SNOWFLAKE Malicious IP Match**
  - Multiple rules have been implemented to detect activity from IP addresses identified by SNOWFLAKE as part of their incident response. These rules search for evidence of connections in logs for Office 365, Linux, Windows, AWS and AWS Cognito logs, and multiple firewall solutions.
- **AWS GuardDuty: UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS**
  - This finding informs you when your EC2 instance credentials are used to invoke APIs from an IP address that is owned by a different AWS account than the one that the associated EC2 instance is running in. To rule out a potential attack and verify the legitimacy of the activity, contact the IAM user to whom these credentials are assigned.
- **AWS GuardDuty: Policy:S3/BucketPublicAccessGranted**
  - This analytic informs you that the listed S3 bucket has been publicly exposed to all authenticated AWS users or has been made publicly accessible on the internet because an IAM entity has changed a bucket policy or ACL on that S3 bucket. If a bucket's ACLs or bucket policies are configured to explicitly deny or to deny all, this finding may not reflect the current state of the bucket. This finding will not reflect any S3 Block Public Access settings that may have been enabled for your S3 bucket. In such cases, the effective Permission value in the finding will be marked as UNKNOWN. If this activity is unexpected for the associated principal, it may indicate that the credentials have been exposed or your S3 permissions are not restrictive enough.
- **Endpoint Time Change Flood**
  - This detection detects a simple script that constantly changes the date to prevent the EDR from reporting events.
- **AWS GuardDuty: Trojan:EC2**
  - This analytic looks for various findings related to trojan activity observed in an EC2 instance. These findings include BlackholeTraffic, DGADomainRequest, DNSDataExfiltration, DriveBySourceTraffic, DropPoints, and PhishingDomainRequest. These types of findings could indicate that one or more EC2 instances have been compromised or are running malware.
- **NetSupport RAT**
  - Looking for indicators of the NetSupport remote access tool that has been seen utilized by malicious actors. If this is not approved software in an environment, it may indicate an intrusion.

---

[i] https://fbi.gov/news/press-releases/operation-endgame-coordinated-worldwide-law-enforcement-action-against-network-of-cybercriminals

[ii] https://blog.morphisec.com/sticky-werewolfs-aviation-attacks

[iii] https://sygnia.co/blog/china-nexus-threat-group-velvet-ant/

[iv] https://harfanglab.io/en/insidethelab/allasenha-allakore-variant-azure-c2-steal-banking-latin-america/, https://blog.talosintelligence.com/new-banking-trojan-carnavalheist-targets-brazil/

[v] https://summoning.team/blog/veeam-enterprise-manager-cve-2024-29849-auth-bypass/

[vi] https://www.fortinet.com/blog/threat-research/new-agent-tesla-campaign-targeting-spanish-speaking-people

[vii] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-30080

[viii] https://zerodayinitiative.com/advisories/ZDI-24-507/, https://forums.ivanti.com/s/article/Security-Advisory-May-2024

[ix] https://decoded.avast.io/davidalvarez/new-diamorphine-rootkit-variant-seen-undetected-in-the-wild/

[x] https://fortinet.com/blog/threat-research/fickle-stealer-distributed-via-multiple-attack-chain

[xi] https://elastic.co/security-labs/grimresource

[xii] https://cadosecurity.com/blog/from-dormant-to-dangerous-p2pinfect-evolves-to-deploy-new-ransomware-and-cryptominer

[xiii] https://microsoft.com/en-us/security/blog/2024/05/28/moonstone-sleet-emerges-as-new-north-korean-threat-actor-with-new-bag-of-tricks/

[xiv] https://blog.talosintelligence.com/lilacsquid/
[xv] https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion
[xvi] volexity.com/blog/2024/06/13/disgomoji-malware-used-to-target-indian-government/
[xvii] https://go.recordedfuture.com/hubfs/reports/cta-cn-2024-0624.pdf
[xviii] https://blog.talosintelligence.com/new-spicerat-sneakychef/