Monthly Threat Intelligence Rollup

DEEP seas

08/01/23-08/31/23

Notable Cyberattacks

Summary of noteworthy cyberattacks in the last thirty days.

Incident	Activity Summary
New State-Sponsored Activity Identified Targeting Hong Kong Entities Using PlugX	A previously unidentified advanced persistent threat (APT) group named Carderbee employed the legitimate Cobra DocGuard software in a supply chain attack to distribute the Korplug backdoor (also known as PlugX) onto victim computers. This attack involved malware signed with a valid Microsoft certificate. The campaign targeted primarily organizations in Hong Kong, with some in other parts of Asia. Korplug, a backdoor commonly used by various Chinese APT groups, was the focal point of the attack. Notably, the malicious activity utilized a digitally signed downloader with a Microsoft certificate to install the Korplug backdoor. The compromised computers had the Cobra DocGuard software installed, and the malicious software was delivered to a specific location on these systems. The attackers demonstrated sophistication by selectively pushing payloads to about 100 out of around 2,000 compromised computers. This strategy, along with the use of signed malware, suggests a calculated effort to evade detection. This incident underscores the ongoing risk of supply chain attacks and the exploitation of trusted certificates, as highlighted by previous instances of Microsoft-signed malware abuse. Carderbee's motivations and targeted sectors remain uncertain, as do potential connections to other threat actors like Budworm.[i]
Akira Ransomware Exploiting Corporate Cisco VPN Products	The emerging Akira ransomware operation is increasingly focusing on exploiting Cisco virtual private network (VPN) products as an entry point for infiltrating corporate networks, stealing data, and then encrypting it. Akira, established in March 2023, has recently incorporated a Linux encryptor to target VMware ESXi virtual machines. Cisco VPN solutions are commonly used in various industries to ensure secure data transmission for remote employees. Akira has been capitalizing on compromised Cisco VPN accounts to infiltrate corporate networks without setting up additional backdoors or persistence mechanisms. Akira appears to exploit weakly protected Cisco VPN accounts, potentially by brute-forcing credentials or acquiring them from the dark web. There's also speculation that Akira might be exploiting an unidentified vulnerability in Cisco VPN software. Furthermore, Akira stands out for its use of the RustDesk remote access tool, allowing obscured network navigation due to RustDesk's legitimate nature. Akira's recent tactics involve SQL database manipulation, disabling firewalls and enabling Remote Desktop Protocol (RDP), and modifying security settings post-infiltration. Although a decryptor was released for Akira in June 2023, the ransomware's evolving encryptors have rendered the tool ineffective for newer versions. Cisco has affirmed that their VPN products support multi-factor authentication (MFA) and encourage the setup of logging for enhanced incident correlation and auditing.[ii]
Barracuda Email Security Gateway (ESG) Zero Day Remediation Follow-up	An extensive, eight month long global espionage campaign carried out by the Chinese-associated threat group, UNC4841, has been unveiled by Mandiant. Despite remediation efforts of Barracuda ESG appliances, UNC4841 showcased adaptability and sophistication, deploying new, novel malware to maintain a foothold in high priority targets it had compromised before the patch release or post-remediation. The group's targeted backdoor deployment suggests a preparedness to evade remediation actions, aimed at preserving access to critical targets. Specifically, the malware families SKIPJACK, DEPTHCHARGE, and FOXTROT / FOXGLOVE have been observed selectively deployed by UNC4841. These backdoors highlight an increasing level of selectivity in deployment. The timeline of the campaign stretches from October 2022 to June 2023, featuring distinct activity surges around key events such as the Chinese New Year and Barracuda's remediation efforts. The campaign primarily targeted ESG appliances, impacting both public and private sectors globally. While most of the exploitation activity targeted the Americas, sectors like local governments, high tech, and information technology providers were significantly impacted. Mandiant remains confident in attributing UNC4841's activities to support the People's Republic of China. Overlaps with other China-associated

	actors were identified, signaling shared infrastructure and techniques for anonymization. UNC4841's agility and readiness to modify TTPs to counteract defensive actions underline the necessity for ongoing vigilance and continuous hunting for UNC4841 activities within impacted networks. Their persistent drive to maintain access, even under stringent conditions, speaks to the meticulousness of their operations. Consequently, cyber security practitioners must remain on high alert to thwart future UNC4841 incursions.[iii]
Qakbot Dismantled in Joint FBI Operation Duck Hunt	The FBI, in collaboration with various international partners, successfully dismantled the Qakbot botnet, also known as Qbot and Pinkslipbot, through Operation 'Duck Hunt.' This long-standing and extensive botnet has been tied to at least 40 ransomware attacks, targeting global organizations, healthcare providers, and government agencies. The operation resulted in the seizure of nearly $9 million in cryptocurrency belonging to the Qakbot cyber criminal group. Qakbot, acting as an initial infection vector for multiple ransomware gangs like Conti, ProLock, and REvil, was taken down by infiltrating the botnet's infrastructure, including an administrator’s computer. This allowed the FBI to deploy an uninstaller to compromised devices, eradicating the infection and blocking further malicious activities. Collaboration with international agencies, such as Europol and the UK's National Crime Agency, was crucial to the operation's success. This initiative follows the takedown of the Snake botnet in May, indicating coordinated efforts to curb cyber threats.[iv]

Emergent Malware and TTPs

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

Malware/Campaign	Activity Summary	TTP Analysis
BlueCharlie's New TTPs and Infrastructure	Insikt, has been tracking the activities of the threat group BlueCharlie, which is associated with Russia-nexus groups Callisto/Calisto, COLDRIVER, and Star Blizzard/SEABORGIUM. Active since 2017, BlueCharlie traditionally is focused on information gathering for espionage and hack-and-leak operations. The group has demonstrated sophistication in adapting to public disclosures and improving its operational security.	While specific targets are unknown, previous victims have included governments, defense, education, political parties, NGOs, journalists, and think tanks. Recently, Insikt Group observed BlueCharlie creating new infrastructure, comprising 94 domains, likely for use in phishing campaigns or credential harvesting. This indicates a shift in the group's tactics, techniques, and procedures (TTPs) from its previous activities, suggesting that BlueCharlie is evolving in response to industry reporting of its operations. Insikt Group has noticed multiple TTP shifts by BlueCharlie since tracking the group in September 2022, demonstrating the threat actors' awareness of industry reporting and their efforts to obfuscate or modify their activities to thwart security researchers. To defend against BlueCharlie's threat, network defenders should strengthen phishing defenses, implement FIDO2-compliant multi-factor authentication, utilize threat intelligence, and educate third-party vendors.[v]
AWS SSM Agent Serves as Post-Exploitation RAT	Security researchers at Mitiga have uncovered a new post-exploitation technique in Amazon Web Services (AWS) that allows hackers to use the AWS System Manager (SSM) agent as an undetectable Remote Access Trojan (RAT). The attack impacts both Windows and Linux machines and is more difficult to detect compared to traditional malware and backdoors.	The SSM agent, being an Amazon-signed binary used for endpoint management, is pre-installed on many operating system template images, providing attackers with a large pool of hosts for abuse. Mitiga found that the SSM agent can be configured to run in "hybrid" mode even within the limits of an EC2 instance, granting access to assets and servers from attacker-controlled AWS accounts. This allows the agent to run on non-EC2 machines, including on-premises servers and virtual machines in other cloud environments, enabling seamless communication between compromised EC2 instances and attacker-owned AWS accounts. The SSM agent's proxy feature can also be exploited to pass network traffic outside AWS infrastructure, making detection challenging. If hijacking existing SSM agents is not possible, attackers can run parallel SSM agent processes to gain access to the "Run Command" feature, although this leaves more traces and increases the difficulty of establishing persistence. Mitiga recommends restricting the reception of commands in EC2 instances using the VPC endpoint for Systems Manager and setting the original AWS account or organization as the only approved source. Additionally, organizations are advised to remove the SSM agent from the allow-list of antivirus or EDR solutions and integrate the detection techniques provided by Mitiga's report into their SIEM and SOAR platforms. Taking immediate action to mitigate this new technique is crucial given the widespread popularity and initial trust associated with the SSM agent.[vi]
Monti Ransomware Targets VMware ESXi Servers with New	The Monti ransomware, initially discovered in June 2022, has	The Monti ransomware group closely mimics the tactics of the Conti group, even incorporating Conti's leaked source code in previous Monti ransomware variants. While the new Linux

Linux Locker	resurfaced after a two-month hiatus, with a new Linux-based variant and an apparent focus on targets in the legal and government sectors.	variant (Ransom.Linux.MONTI.THGOCBC) maintains some elements of Conti's source code, it features significant alterations, particularly in its encryption algorithm, showing only a 29% similarity to the older variants. This adaptation enhances evasion capabilities, posing challenges for detection and mitigation. To defend against such ransomware attacks, organizations should implement multifactor authentication, follow the 3-2-1 backup guideline, and establish protocols for data protection and recovery. These measures bolster data security and facilitate data restoration in case of encryption or deletion.[vii]
Raccoon Returns After Six Month Break	The developers of Raccoon Stealer, a notorious information-stealing malware, re-emerged after a six-month hiatus to introduce version 2.3.0 to cyber criminals.	Raccoon, operational since 2019 and sold via a Malware-as-a-Service (MaaS) subscription model, extracts data from over 60 applications, encompassing login credentials, credit card info, browsing history, cookies, and cryptocurrency wallets. After facing uncertainty due to the arrest of its main creator and dismantling of its infrastructure in 2022, the malware's new version brings improvements based on feedback and cyber crime trends. Raccoon 2.3.0 includes a quick search tool for easy data retrieval, a system that combats suspicious activities, and a feature that blocks IPs used by security researchers' monitoring bots. Information-stealers pose a significant threat to individuals and businesses, as their wide usage enables various attack vectors. In addition to acquiring a victim's credentials, Raccoon's ability to pilfer cookies could bypass multi-factor authentication, leading to network breaches, data theft, ransomware, and cyber espionage. To counter Raccoon and similar threats, use password managers instead of browser-stored credentials, implement multi-factor authentication, and avoid downloading files from untrusted sources.[viii]

Threat Actor Campaigns

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

Threat Actors	Activity Summary
Midnight Blizzard's New MS Teams Phishing Campaign	Microsoft Threat Intelligence identified targeted social engineering attacks by Midnight Blizzard (aka NOBELIUM) using credential theft phishing lures sent via Microsoft Teams chats. The threat actor exploits previously compromised Microsoft 365 tenants to create new domains posing as technical support entities. Through these domains, they send Teams messages attempting to steal credentials and elicit approval for multifactor authentication prompts. The campaign has affected fewer than 40 global organizations, primarily in government, NGOs, IT services, technology, manufacturing, and media sectors. Microsoft has mitigated domain usage and notified affected customers. Midnight Blizzard is attributed to the Russian SVR and primarily focuses on espionage since 2018, using various access methods like token theft and authentication spear-phishing. To counter these attacks, Microsoft recommends phishing-resistant authentication methods, conditional access, trust settings for external domains, and user education on social engineering. Conditional Access App Control is suggested for unmanaged devices.[ix]
SystemBC and Cobalt Strike Used Against African Critical Infrastructure	In late March 2023, Kaspersky Lab identified an attack against an electric utility in southern Africa utilizing the painfully common Cobalt Strike Beacon, as well as a variant of the SystemBC backdoor malware dubbed DroxiDat. Though the initial access point is unknown, the attackers were most likely able to maintain their access via stolen credentials given that numerous Cobalt Strike Beacon implants were delivered over the space of over a week. Whether these initial implants were cleaned up automatically or not is unclear, though it does point towards the attackers lacking the kind of sophistication normally seen with persistent intrusions. Ironically, Kaspersky believes with low confidence that the attack was the responsibility of the FIN12 cyber crime group (aka PISTACHIO TEMPEST), a Russian-speaking ransomware-as-a-service (RaaS) group known to use SystemBC and Cobalt Strike in attacks, particularly against the healthcare sector. A separate series of attacks against a healthcare provider utilized the same DroxiDat/Cobalt Strike combination, with matching license keys, staging directories, and C2 infrastructure. In this latter case, the final payload was Nokoyawa ransomware. DeepSeas reviewed the C2 infrastructure, identifying links to the TA505 threat actor group, which may be incidental, though further work will be required to fully elucidate the links between FIN12, TA505, and Nokoyawa. It may simply be that the network of cyber crime actors is more tightly interwoven than previously thought.[x]
DanaBot Operators Using Fish-Themed C2 Infrastructure	While reviewing customer alerts, DeepSeas analysts identified a failed attempt to load malware on a customer endpoint. Initial analysis of the attack was inconclusive; this is not uncommon but presents unique and often extremely difficult challenges to analysts attempting to reconstruct the attack and determine attribution. Despite these challenges, the final payload was determined to be DanaBot, a malware-as-a-service (MaaS) operated by a probably Russian cyber crime group named SCULLY SPIDER by CrowdStrike. This group is what is known as an initial access broker (IAB), as well as a MaaS. They use their own malware to compromise systems and then sell access to other cyber crime groups, as well as renting their toolkit out to affiliates to use to load their own malware payloads. Ostensibly a banking trojan, the DanaBot malware has evolved since 2017 into a more fully featured toolkit, and while not the most common malware compared to QakBot, IcedID, and Emotet, it is no less fully featured. DeepSeas was also able to identify the group's C2 infrastructure, revealing that the group's current campaign has been in operation since at least March 2023 - potentially longer. The C2 convention is also unique, making use of the names of fish. This convention makes it easy for the attackers to track their infrastructure, but also greatly simplifies tracking by security professionals. DeepSeas once foiled nearly a year of FIN7 operations using this same method.

Sandworm Group Targeting Android, Other Devices	The Russian state-aligned Sandworm Team threat actor group, affiliated with the Russian Foreign Intelligence Service (SVR), has been blamed by Ukrainian authorities for attempts to compromise battlefield devices utilized by Ukrainian soldiers, including the Starlink satellite communications service providing battlefield connectivity. While this kind of intrusion is to be expected, stemming from the capture of communications devices and tablets utilized by Ukrainian soldiers, the sheer number of malware and tools involved (10), as well as targeting of satellite communications, is a unique tactic employed by the Russian operators. It has been many years since Russian state-aligned groups have abused satellite services for malicious purposes, but interception and disruption of satellite communications is a new development for Sandworm. It is highly likely that the experience and knowledge gained from these attacks will be disseminated amongst other Russian state-aligned groups and potentially even shared with other nation-states ideologically aligned with Russia, including China, Iran, and possibly even North Korea. It would be incorrect to assume that these nations were not already working on their own toolset, but live practice is likely to provide Russia and other nation-state operators with enhanced tools, tactics, and procedures for crippling these communications systems that are vital to both military and commercial operations.[xi]
Malicious Distribution of Proxy Server Apps	Security researchers have exposed a large-scale campaign distributing proxy server applications to over 400,000 Windows systems. These devices operate as residential exit nodes without user consent, with the proxy traffic being monetized by the unnamed proxy provider. Such residential proxies are attractive to cyber criminals for orchestrating large-scale credential stuffing attacks from fresh IP addresses. While these proxies have legitimate uses like ad verification, data scraping, and privacy-enhanced routing, malicious distribution is a concern. AT&T Alien Labs uncovered this network proxy nodes established via malicious payloads that secretly install the proxy application. The company behind the botnet claims user consent, but evidence suggests silent installations on infected systems. Notably, the Windows proxy client eludes antivirus detection due to its valid digital signature. The infection begins with hidden loaders in cracked software, installing the proxy application automatically in the background. The proxy client persists through registry keys and scheduled tasks. To protect systems, AT&T suggests searching for the "Digital Pulse" executable and Registry key, deleting them if found. Also, remove the scheduled task "DigitalPulseUpdateTask." Users should avoid pirated software and executables from untrustworthy sources. Indications of proxyware infection encompass degraded performance, unexpected network traffic, frequent communication with unfamiliar IPs/domains, and system alerts.[xii]
U.S. Critical Infrastructure Orgs Targeted in QR Code Credential Phishing Campaign	Security researchers at Cofense identified a phishing campaign, operating since May 2023, that is leveraging malicious QR codes to steal Microsoft credentials across various industries. An unnamed, prominent U.S.-based energy firm was reportedly a major focus of this campaign, with 29% of the observed phishing emails targeting them specifically. Other key industries targeted include manufacturing, insurance, technology, and financial services. The campaign's growth has surged by over 2,400% since May, with monthly increases exceeding 270%. The phishing emails contain malicious QR codes embedded in a PNG or PDF attachment. If scanned, the victim will be redirected, often obfuscated as a Bing redirect URL, to a phishing page impersonating a Microsoft security notification. While QR codes facilitate inbox access, their efficiency in directing users to phishing sites is limited due to the necessity for image capturing devices. Online scanners and mobile devices prompt users to verify the QR code's destination before opening a browser. To counter this threat, educating employees to avoid scanning QR codes in received emails and utilizing automation like QR scanners and image recognition as the initial defense is crucial.[xiii]
HiatusRAT Now Targeting Defense Industrial Base	In March 2023, Lumen Black Lotus Labs unveiled a sophisticated operation called "HiatusRAT," infecting over 100 global edge networking devices. These devices, mainly edge routers, served as a hidden network for command and control (C2) purposes. Despite prior exposure, the group persisted, shifting their focus from Latin America and Europe to Taiwan and U.S. entities. The technique of exploiting these perimeter assets aligns with Chinese threat behavior, as indicated by the 2023 ODNI threat assessment.

	The group's audacity was evident as they continued operations with only minimal adjustments, swapping payload servers. The HiatusRAT malware was found in different versions targeting various architectures, linked by shared communication servers. The new campaign pinpointed Taiwanese targets, with a preference for Ruckus-manufactured edge devices, impacting semiconductor firms, chemical manufacturers, and even a municipal government. Black Lotus Labs acknowledges the challenge of dealing with edge and IoT malware due to the absence of universal cleanup methods. The shift to targeting Taiwan and U.S. entities suggests a strategic change, like other Chinese operations. HiatusRAT poses a threat to the Defense Industrial Base, urging defense contractors to monitor their devices for the presence of this malware.[xiv]
New APT Targeting Tech and Government in Several Countries	In early 2023, a new cyber espionage campaign named Earth Estries was discovered, with activities dating back to 2020. Operating similarly to the unrelated group FamousSparrow, Earth Estries targets government and technological entities across countries like Taiwan, Malaysia, Germany, and the U.S. The campaign employs diverse intrusion tools, including backdoors and hacking tools, utilizing tactics like PowerShell downgrade attacks and leveraging public services like GitHub and Gmail for covert communication. Their primary focus is on government and tech organizations in countries such as Canada, India, and Singapore. Earth Estries employs advanced tactics like DLL sideloading and PowerShell attacks that effectively avoid detection, enabled by compromising internal servers and genuine accounts. Their incorporation of Zingdoor to hinder easy backdoor analysis adds complexity for analysts. This group's methods and code similarities with FamousSparrow suggest a possible link, backed by evidence like shared IP addresses and technical patterns. This connection warrants a thorough investigation into their activities, though the infosec community has tentatively attributed FamousSparrow’s activities to Iranian state-aligned activity. Any investigation should bear this in mind.[xv]

Dark Web Markets

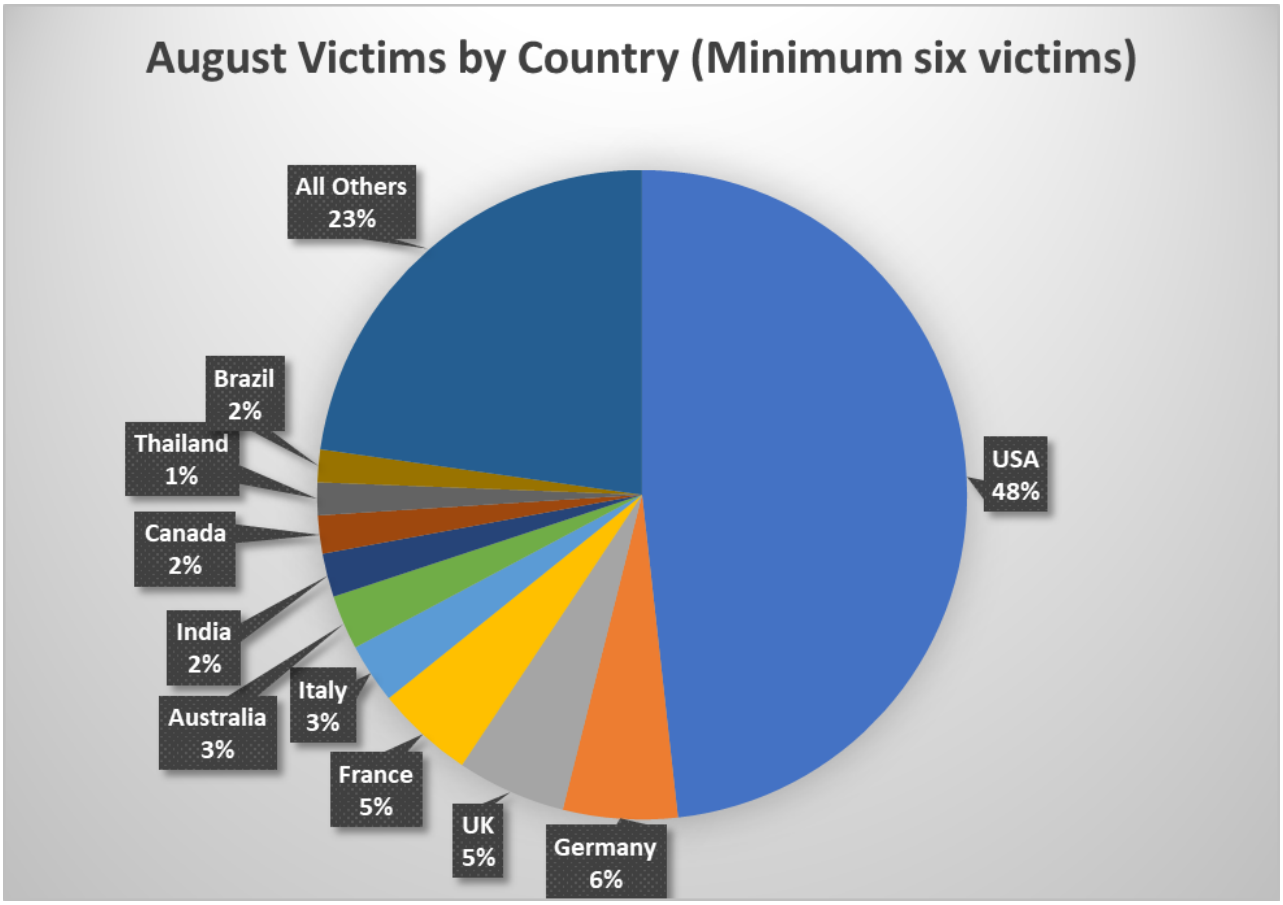
High-profile ransomware data dumps and dark web access sales identified in last thirty days.

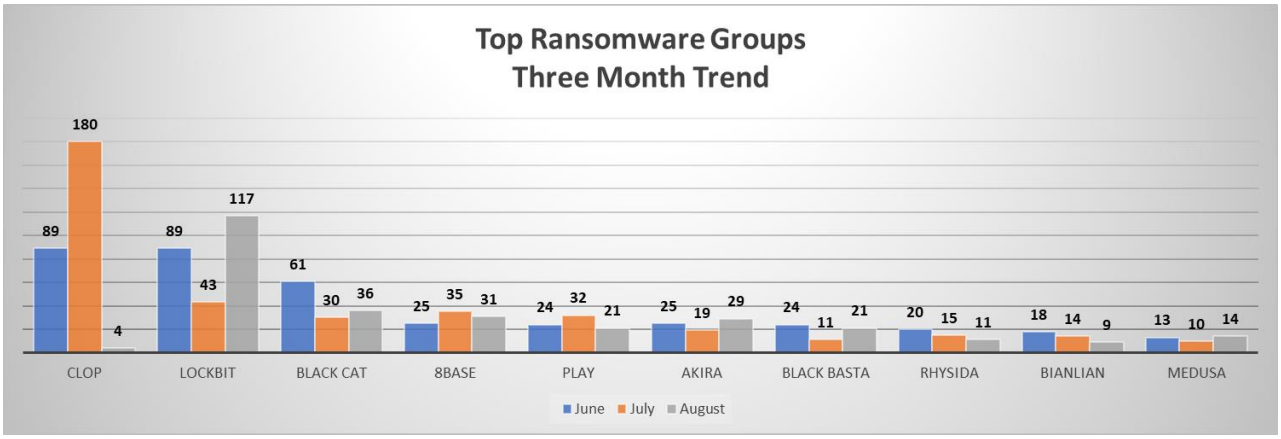
Activity	Note
Access Sale	On 28 July, an access seller on a private Russian crime forum offered access to an unnamed healthcare organization in the United Kingdom with USD 17.6 billion in revenue.
Access Sale	On 2 August, an access seller on a private Russian crime forum offered to sell access to a U.S. based possible critical infrastructure entity in the energy, utilities, and waste vertical with USD 483 million in revenue.
Access Sale	On 2 August, an access seller on a private Russian crime forum offered to sell access to a U.K. based pharmacological company with USD 4 billion in revenue. They likely sold this access on 3 August.
Access Sale	On 3 August, an access seller on a private Russian crime forum offered to sell local admin access to a U.S. based manufacturing enterprise with USD 1.2 billion in revenue for USD 4,000.
Access Sale	On 3 August, an access seller on a private Russian crime forum offered to sell Citrix and Outlook access to a "big corp in world wide (sic), everyone has heard the name of this company" with USD 6.4 billion in revenue and more than 40,000 employees for USD 5,000.
Access Sale	On 4 August, a member of a private Russian crime forum advertised the sale of RDP access to an Indonesian company with USD 15 billion in revenue for USD 2,000.
Access Sale	On 4 August, a member of a private Russian crime forum advertised RDweb access to an unidentified educational enterprise with USD 2.3 billion in revenue for USD 4,000.
Access Sale	On 6 August, a member of a private Russian crime forum advertised Citrix user access to an unidentified hospitality company with USD 2.6 billion in revenue and 7,000 employees for USD 1,500.
Access Sale	On 7 August, a member of a private Russian crime forum advertised selling admin rights to an instant messenger service with more than one billion users for a buy now price of USD 100,000.
Access Sale	On 10 August, a member of a popular public crime forum advertised selling domain admin access to a Brazilian digital certificate authority with USD 96 million in revenue for USD 5,000. They claimed there are more than 10 million digital certificates available to steal.
Access Sale	On 10 August, a member of a private Russian crime forum advertised selling domain user access to a U.S. based company with USD 1.6 billion in revenue for a buy now price of USD 3,000.
Access Sale	On 14 August, an access seller on a popular public crime forum was selling Citrix access to an unnamed U.S. based construction company with USD 461.4 million in revenue.
Access Sale	On 14 August, an access seller on a private Russian crime forum was selling Citrix RDP domain user access to an unnamed manufacturer of appliances and consumer goods with USD 2.6 billion in revenue for USD 5,000. The actor shared a poorly redacted screenshot purporting to prove their access, which revealed the likely victim.
Access Sale	On 15 August, an access seller on a private Russian crime forum was selling domain admin access to an unidentified enterprise in Central America with USD 350 million in revenue for USD 20,000. The enterprise has something to do with refining, selling, or transporting gasoline. The access was likely sold to a long-time, notorious ransomware affiliate.
Access Sale	On 15 August, an access seller on a popular public crime forum was observed offering Global Protect access to an American religious organization with USD 4.8 billion in revenue for USD 4,000. The seller canceled the sale after 2FA foiled their access attempt.

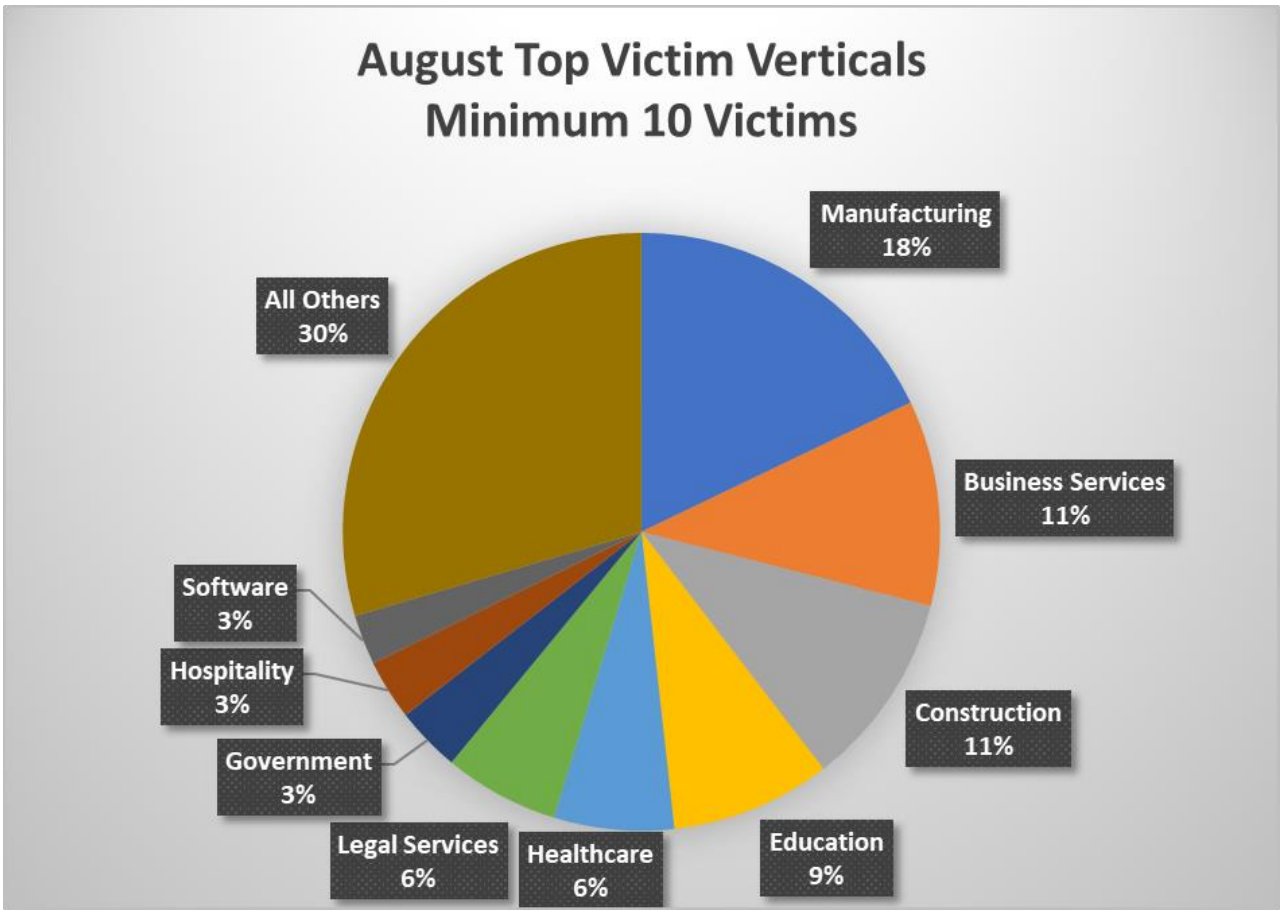
Access Sale	On 17 August, an access seller on a public crime forum was observed selling a SQLi vulnerability and RCE vulnerability to a server on a subdomain belonging to a Japanese maker of computer equipment and peripherals with USD 13 billion in revenue.
Access Sale	On 21 August, an actor in a prominent Russian-language crime forum was observed selling Citrix user access to a U.S. based aviation company, described as a “large carrier, current operator” with more than 1,000 hosts on the network and USD 3.6 billion in revenue. The actor posted a screenshot demonstrating that they had executed a nltest command to enumerate domain controllers.
Access Sale	On 21 August, an actor in a prominent Russian-language crime forum was selling RDP local admin access to a Norwegian technology consulting company with USD 2.7 billion in revenue for USD 5,000.
Access Sale	On 22 August, an actor on a prominent Russian-language crime forum probably sold RDP local admin access to a U.S. based software and technical consulting company with USD 4.5 billion in revenue for USD 4,000. The victim was likely also a Black Basta victim in September 2022.
Other Developments	DeepSeas analysts noted 25 access sales of companies with more than USD 5 million in revenue by 10 different actors in cyber crime forums in the past week. At least four of those accesses were sold to known or suspected ransomware affiliates. Eleven of those accesses were for U.S. based companies. The point of entry for 10 of those accesses were Citrix or other Cisco products.
Access Sale	An access seller on a popular Russian-language public crime forum was selling local admin access to a U.S. based retailer with USD 15 billion in revenue for USD 500.
Access Sale	An access seller on a popular Russian-language public crime forum is selling Pulse Secure access to a U.S. based retailer in the vitamins, supplements, and health stores vertical with USD 20-22 billion in revenue.
Access Sale	An access seller on a prominent Russian-language crime forum is selling local admin access to a U.S. based provider of customer relationship management software with USD 12.8 million in revenue.
Tool Sale	A malicious actor on a popular Russian-language public crime forum was selling two VirusTotal individual enterprise accounts and VirusTotal Enterprise API access. The user accounts were priced at USD 1,600 and USD 1,300 depending on the number of queries they were allowed, while the API access was priced at USD 600.

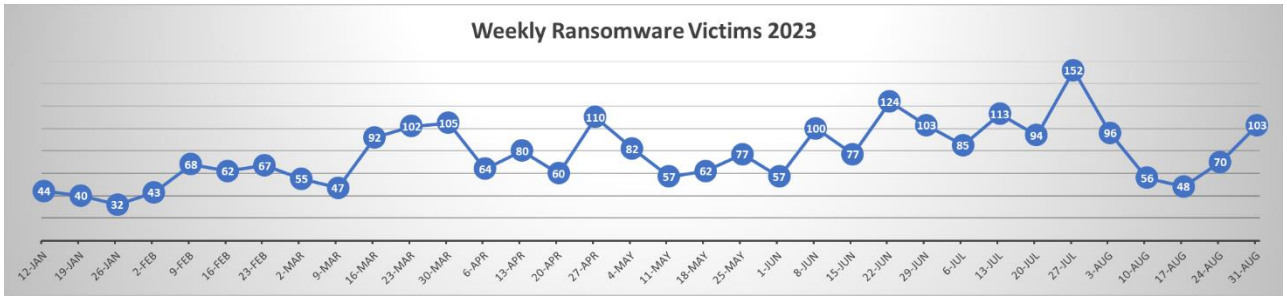
By The Numbers

Summarizing incidents in graphical format






August Top Victim Verticals
Minimum 10 Victims
Manufacturing 18%
Business Services 11%
Construction 11%
Education 9%
Healthcare 6%
Legal Services 6%
Government 3%
Hospitality 3%
Software 3%
All Others 30%


Weekly Ransomware Victims 2023
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 85 113 94 152 96 56 48 70 103
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 6-JUL 13-JUL 20-JUL 27-JUL 3-AUG 10-AUG 17-AUG 24-AUG 31-AUG

[i] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/carderbee-software-supply-chain-certificate-abuse
[ii] https://www.bleepingcomputer.com/news/security/akira-ransomware-targets-cisco-vpns-to-breach-organizations/
[iii] https://www.mandiant.com/resources/blog/unc4841-post-barracuda-zero-day-remediation
[iv] https://www.fbi.gov/news/stories/fbi-partners-dismantle-qakbot-infrastructure-in-multinational-cyber-takedown
[v] https://go.recordedfuture.com/hubfs/reports/cta-2023-0802.pdf
[vi] https://www.mitiga.io/blog/mitiga-security-advisory-abusing-the-ssm-agent-as-a-remote-access-trojan
[vii] https://www.trendmicro.com/en_us/research/23/h/monti-ransomware-unleashes-a-new-encryptor-for-linux.html
[viii] https://cyberint.com/blog/financial-services/raccoon-stealer/
[ix] https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/
[x] https://securelist.com/focus-on-droxidat-systembc/110302/
[xi] https://ssu.gov.ua/en/novyny/sbu-exposes-russian-intelligence-attempts-to-penetrate-armed-forces-planning-operations-system
[xii] https://cybersecurity.att.com/blogs/labs-research/proxynation-the-dark-nexus-between-proxy-apps-and-malware
[xiii] https://cofense.com/blog/major-energy-company-targeted-in-large-qr-code-campaign/
[xiv] https://blog.lumen.com/hiatusrat-takes-little-time-off-in-a-return-to-action/
[xv] https://www.trendmicro.com/en_us/research/23/h/earth-estries-targets-government-tech-for-cyberespionage.html