Monthly Threat Intelligence Rollup

DEEP seas

09/01/23-09/30/23

Notable Cyberattacks

Summary of noteworthy cyberattacks in the last thirty days.

Incident	Activity Summary
Ukrainian Critical Infrastructure Targeted by Russian State Aligned APT28	In a recent advisory, the Ukrainian national CERT provided details of a recent attempt by APT28 to compromise an unspecified critical infrastructure facility in Ukraine. The Russian state aligned APT28 group conducted a spear phishing attack which, if successful, downloaded and executed a number of batch (BAT), VBS, and command (CMD) files. These would end up executing the native Windows 'whoami' command and send the results via HTTP GET request to the attackers, uniquely using Microsoft Edge in headless mode. The attackers also made use of the Tor browser, downloaded from a popular file-sharing service, to further obfuscate their C2 communications. In this instance, the target's IT management personnel successfully blocked this attack by denying Windows Script Host execution, as well as blocking access to the popular Mockbin web service. The use of Mockbin by APT28 is not new. This technique was observed in April 2023 - making it a recent but not new TTP. While it is unsurprising that Russian operatives are targeting Ukrainian critical infrastructure, the steps taken by Ukrainian security personnel to secure their networks against these attacks, particularly ones that heavily utilized native and legitimate Windows tools and services, is noteworthy.[i]
Redfly Group Targeting Critical Infrastructure in the United States	The Chinese state aligned Redfly Group (aka APT17, APT41, Winnti, Shadowpad, etc.) was observed by Symantec to have targeted unspecified critical national infrastructure in the United States for approximately six months. The use of the Shadowpad malware in this incident clearly points to the involvement of a long-running and technically skilled group of operators, dubbed Redfly by Symantec. The purpose of the attackers is unknown. The attackers gained access to the organization in February 2023, resumed activities in May after having remained dormant for three months, and seemingly concerned themselves with conducting lateral movement through the organization's networks until the attack was terminated in August 2023.[ii]
Peach Sandstorm Campaign Targeting DIB, Pharma Industries	In a report released by Microsoft detailing Iranian state aligned activities, APT33 (aka Elfin, Peach Sandstorm) was observed conducting password spraying attacks against numerous companies from January 2023 to June 2023. This activity then evolved into post-compromise exploitation utilizing these valid credentials, in which the attackers loaded legitimate remote administration tools onto compromised systems. This was predominantly AnyDesk, though other techniques were observed, including a Golden SAML attack, as well as using a legitimate VMWare executable to side-load malicious code. The attackers were identified through their use of the EagleRelay tunneling/proxy tool, known to be a bespoke part of APT33's toolset. More worryingly, the attackers made use of the AzureHound tool, permitting them to conduct reconnaissance in Azure Active Directory (now known as Entra ID), followed by the Roadtools tool, to dump data of interest into a single database.[iii]
BlackTech Group Compromising Router Firmware	A recent CISA report, produced in collaboration with international partners, has identified an ongoing campaign by the Chinese state aligned BlackTech group, which targets vulnerable routers belonging to international partners or subsidiaries of Japanese and U.S. corporations. Among their targets of interest are entities in the government, industrial, technology, media, electronics, and telecommunications sectors, particularly those supporting the U.S. and Japanese militaries. In contrast to previous operations, BlackTech has been observed outright replacing the router firmware with a malicious version containing an SSH backdoor which prevents their actions from being logged. This begins with installing an older firmware version, which is then modified in memory to install an unsigned bootloader, and finally modified, unsigned firmware is installed. Cisco IOS routers are a particularly favored target for BlackTech's operations. Detection opportunities include monitoring for unexpected reboots of these devices, outsized SSH traffic originating from a device, and conducting file and memory verification to identify unauthorized changes to device firmware and software.[iv]

Johnson Controls Suffers Widespread Ransomware Attack	Over the weekend of 23-24 September 2023, industrial control systems manufacturer Johnson Controls International suffered a major ransomware attack by the Dark Angels Team ransomware group which seriously impacted their worldwide operations. According to inside sources, the attack originated from the company's Asia offices where the attackers established persistence. The attack not only impacted the company's VMware ESXi servers but many other devices, as well as follow-on effects which crippled the operations of Johnson Controls International's network of subsidiary companies, including York, Tyco, Simplex, Coleman, and others. Comments from an employee of one subsidiary hint that the attack may have spread from Johnson's networks into the networks of their subsidiaries as well, though no disruption to devices managed by Johnson Controls was noted. The attack appears to have affected only those systems internal to Johnson Controls. Dark Angels Team claimed to have stolen 27 terabytes worth of proprietary data. InfoSec researchers note that the Linux encryptor used by Dark Angels Team is a match for the same tool utilized by the Ragnar Locker ransomware group first observed in 2021. Other tools used by Dark Angels Team are based on leaked Babuk ransomware source code. Altogether, this suggests that Dark Angels Team is a low to medium skill ransomware group.[v]
Spear Phishing Campaign that Ends in Stolen Data Plays Off Azerbaijan and Armenian Conflict	In August 2023, FortiGuard Labs uncovered a spear phishing campaign exploiting the ongoing tensions between Azerbaijan and Armenia. The attack began with a deceptive memo, seemingly from the president of an Azerbaijani company, targeting management teams of associated businesses. The memo plays into the conflict by claiming to have information about a border clash that occurred between Azerbaijan and Armenia. When opened, the memo contained malware that gathered basic information from its targets. It then used HTML smuggling to deliver a password protected archive containing both legitimate images and hidden malware. The malicious installer, written in the uncommon RUST programming language, created a persistent scheduled task and operated stealthily, often outside of office hours. The malware acted as an info stealer, collecting computer information and sending it to a controlled C2 server, revealing an early-stage threat actor attempting to customize attacks for each infected target. Who this threat actor may be is not currently known; though, given the region and historical tensions, either Russia or Iran may be responsible for this activity.[vi]

Emergent Malware and TTPs

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

Malware/Campaign	Activity Summary	TTP Analysis
Limited Social Engineering Campaign Targeting Okta Customer Administrators	In the past 30 days, numerous U.S. based customers of Okta have reported social engineering attacks against their internal service desk personnel. Attacks consist of attempting to convince the help desk staff to reset all multifactor authentication for highly privileged users.	In cases where this social engineering was successful, the attackers would then impersonate those highly privileged users within the organization's networks for purposes that remain unspecified. These attacks make use of existing access or compromised credentials in the initial stages. Though once MFA was compromised in the attackers' favor, the attackers were observed demonstrating a thorough understanding of the intricacies of multifactor authentication - adding new identity provider applications, setting up so-called 'secondary' single sign-on capabilities, elevating privileges, removing 2FA and MFA requirements from accounts, and other actions on objective. While Okta declined to point the finger at any group that may have been responsible, the scope and scale of the attack points toward either a highly resourced cyber criminal group or to a still unnamed nation state actor. The latter is the most likely option, as configuring MFA and altering accounts points toward a longer-term intent, likely for espionage purposes. There was also some confusion about the warning from Okta with some commentators believing that Okta itself was socially engineered. This was not the case, as Okta provisioning is managed at the client level and not by Okta itself.[vii]
Backdoored Linux Download Manager Campaign Ran for Three Years	A popular Linux file download manager was the target of a long-running attack, serving up a backdoored version of the download manager software to the Linux community.	Identified as a variant of the Bew malware and first identified in 2013, the malware profiled the system, captured credentials and cryptocurrency wallet files, and targeted cloud services, passwords in particular. Unlike many other ostensibly legitimate but weaponized programs, this incident is unique in that the malware was apparently delivered via a redirection when users attempted to download the legitimate program from the official website. Researchers have been unable to attribute the attack to any group or actor, nor were they able to determine whether the official website had been compromised to deliver the malware, though this could be the case. There exists evidence that the website may have delivered the backdoored version of the program only to users matching a specific profile. Ironically, numerous users between 2020 and 2022 identified unusual behavior associated with the software but did not sufficiently pull the thread to identify malicious behavior. This attack highlights that, while Linux malware is not particularly common, it remains a threat that should be monitored.[viii]
Earth Lusca Group Targeting Central Asia, Latin America with Linux Backdoor	A recent report by Trend Micro detailed a new campaign carried out by a Chinese state aligned group, dubbed Earth Lusca, that has been targeting government agencies, technology	The attackers utilized a revamped version of the Trochilus backdoor, a malware associated only with APT31, as well as Cobalt Strike for lateral movement post-compromise. The code, which overlaps between Trochilus and the new backdoor dubbed SprySOCKS, is a strong indication that APT31 has resumed operations after a presumed hiatus to refresh their toolsets. The attackers have also integrated components of the Sakula malware, a known Chinese nation state tool, as part of

	companies, and telecommunications firms primarily in Central Asia, but also Latin America, for espionage purposes.	SprySOCKS, thus further strengthening the Chinese nation state connection. True to form, the group has been observed exploiting zero-days in public facing Fortinet, Zimbra, Microsoft Exchange, GitLab, and Progress Telerik servers to gain access - a hallmark of previous APT31 operations. The SprySOCKS malware not only handles basic malicious functions, including fingerprinting a compromised system, but also permits the attackers access via an interactive shell to carry out further malicious activities once a beachhead has been established. Interestingly, aside from stealing credentials and documents of interest, the attackers were also observed, in at least one instance, deploying Shadowpad, a backdoor normally associated with the Winnti Group (aka APT17/APT31), suggesting that digital overlap is stronger than previously assessed.[ix]
Indonesian AMBERSQUID Group Targeting Obscure AWS Services in Cryptojacking Attacks	A recent SysDig report outlined the activities of a new group of presumed Indonesian cyber criminals who infected victims with Docker images containing crypto mining malware which targeted several obscure Amazon Web Services products. These include Amplify, CodeBuild, CloudFormation, SageMaker, EC2 Auto Scaling, and ECS itself.	Crypto mining malware by itself is more of an annoyance than a serious threat, as it is often noisy and quickly detected by security solutions. The malware is also particularly resource-intensive, leading to rapid detection by even novice security personnel. More worrying are the implications that these services are not only exploitable, but, at least when excluding EC2, they are often overlooked by security vendors due to their obscurity, placement, and, as in this case, the fact that the attackers contain their code entirely in AWS rather than on an endpoint or server controlled by a victim. This effectively punts the security ball into Amazon's court, which is yet another point to bear in mind when considering migration to cloud-based services. In this case, the AMBERSQUID attackers were intent on mining cryptocurrency, though the potential for data theft and other malicious activities was made fairly evident by SysDig's analysis. In some cases, the cost to a single victim was over $10,000 in AWS bills. Even more worrying is that while AWS has robust logging tools that would permit analysts to identify such a compromise, other cloud service providers at a lower price point may not or may not prioritize this level of security.[x]
Bumblebee Loader Returns with New Obfuscation, C2 Features	Intel 471 recently identified a new Bumblebee Loader campaign that began on 01 September which has demonstrated a series of changes from previous campaigns. The operators added a new domain generation algorithm (DGA) using the life top level domain (TLD), as well as dropping the familiar WebSocket protocol for an entirely TCP-based protocol.	Updates and changes to the malware's command and control (C2) structure form the most interesting technical changes to the group's toolset, though by no means are these the only changes. The use of Web-based Distributed Authoring and Versioning (WebDAV) services, in this case the publicly available 4shared service, is not particularly novel considering the operators of the IcedID malware were observed utilizing it in early 2023. It is unique to see Bumblebee utilizing it, however, as these services are often treated as legitimate. This is especially true in small to medium business environments where the higher cost of on-premises or off-premises services come with similar capabilities. This would be particularly attractive to financially motivated groups (FIN7, FIN8, FIN9, etc.) that have demonstrated a penchant for targeting suppliers, vendors, and third parties to their intended targets to harvest credentials, insert themselves into email threads and deliver malware.[xi]
Dependabot Impersonations Result in Stolen Secrets and Password Stealing Malware	In July 2023, a noteworthy cyber security incident unfolded as malicious actors made abnormal commits to	The malicious actors, who are unknown at this time, utilized stolen GitHub personal access tokens to execute the fraudulent commits which aimed to exfiltrate the affected GitHub project's defined secrets and compromise end users by implanting password stealing malware in JavaScript files. The attackers

	hundreds of GitHub repositories that were impersonating Dependabot, a free GitHub feature that automatically updates GitHub dependencies.	did this by employing a GitHub action called "hook.yml" to transmit the secrets to an external URL. The attacks impacted both public and private repositories, with most victims being Indonesian users. This incident underscores the importance of vigilance when obtaining code, even from trusted sources like GitHub, and the need for fine grained personal access tokens to reduce the risk of compromise. The incident illustrates the increasing sophistication of supply chain attacks, with attackers using fake commits, credential theft, and Dependabot impersonation to evade detection.[xii]
Vulnerability in Common Software Library Assigned 10/10 Severity by Google	A vulnerability in the libwebp library exploited by the NSO Group's Pegasus mobile malware framework has been assigned a 10/10 severity and CVE ID (CVE-2023-5129). This vulnerability was originally disclosed as a Chrome weakness (CVE-2023-4863, sometimes conflated with the BLASTPASS vulnerability) but later reclassified.	The reclassification of CVE-2023-5129 as a libwebp flaw is significant as it affects various projects using libwebp, including 1Password, Signal, Safari, Mozilla Firefox, Microsoft Edge, Opera, and native Android web browsers. While the vulnerability has been exploited by NSO Group's Pegasus malware, it is very likely capable of working just as well on Windows devices using the aforementioned internet browsers. A relatively simple solution is to use Microsoft Windows' Group Policy Object (GPO) feature to force internet browsers to update to the latest versions. This is also likely to resolve many other issues encountered due to vulnerabilities in these products. Other products will require updating as well.[xiii]

Threat Actor Campaigns

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

Threat Actors	Activity Summary
Dalbit Group Continues Hacking Campaign Against South Korean Industries	A Chinese hacking team, potentially a state sponsored group given their tactics, techniques, and procedures (TTPs), has intensified attacks against South Korean industries. The Dalbit Group, known for their use of fast reverse proxy tools and reliance on open-source tooling to conduct their attacks, has compromised over 50 South Korean companies in the past year, an impressive rate of success by any metric. The group predominantly targets high tech, industrial, chemical, construction, automotive, and the semiconductor industries, all of which are high priority targets outlined in China's most recent Five-Year Plan. These official government economic plans provide a roadmap by which China's state aligned groups conduct operations. Dalbit initially targets outdated and/or vulnerable web servers and SQL servers to install a variety of common webshells. The attackers then import their toolsets, conduct internal reconnaissance, and lateral movement, often with the use of Mimikatz, before exfiltrating data of intelligence or economic value. Perhaps most annoyingly, when finished, the group utilizes BitLocker to lock the system before demanding a ransom.[xiv]
North Korean State Operations Evolve, Remain Multifaceted	The North Korean state aligned APT37 group (aka Reaper, ScarCruft, etc.) has made minor modifications to an existing spear phishing campaign which previously utilized Compiled HTML Help (CHM) files to deliver a RokRAT malware variant. The campaign is now delivering the same malware but via the more popular LNK file tactic. Concurrently, North Korean attempts to spear phish security researchers worldwide has continued to accelerate since first being detected in 2021, this time making use of months' worth of effort to lure researchers onto private platforms (WhatsApp, Signal, etc.) to provide them with weaponized software packages containing zero-day exploits. The group has also created a weaponized debugging tool called GetSymbol, ostensibly used to retrieve debugging symbols from so-called symbol servers for reverse engineering. Unfortunately, this tool also permits North Korean operators to download and execute arbitrary code on the system. These operations highlight the fact that while North Korean operations aimed at cryptocurrency exchanges may garner the limelight for their scope and scale, other offices within Pyongyang's Reconnaissance General Bureau remain active and highly skilled at developing new and novel ways to compromise targets of interest.[xv]

Dark Web Markets

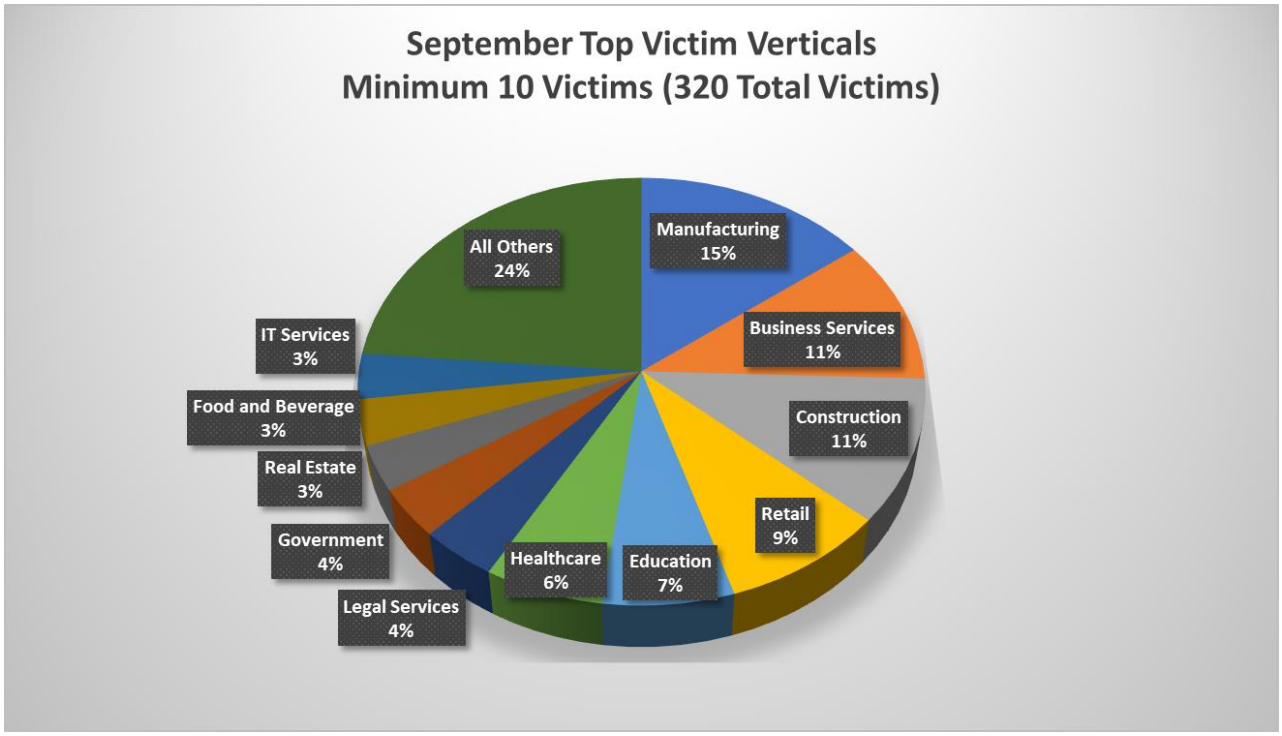
High-profile ransomware data dumps and dark web access sales identified in last thirty days.

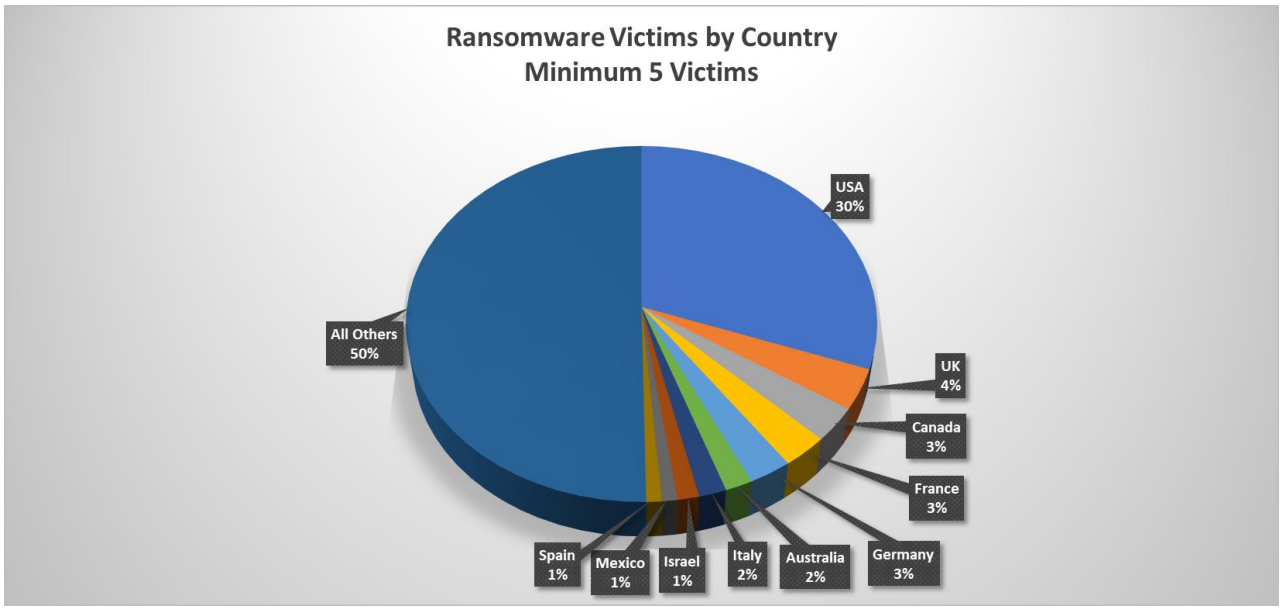
Activity	Note
Actor Developments	On 22 August, a known ransomware affiliate bought Citrix domain user access to a Singaporean company with USD 880 million in revenue in the enterprise resource planning and software development & design vertical for USD 2,000. On 5 September, Global Logistics Properties showed up on the LockBit site as a victim. The actor who bought the access was originally identified as a Conti ransomware affiliate. After Conti's shutdown, he continued to buy access, but his affiliation was undetermined until now.
Access Sale	On 5 September, an actor on a popular Russian language criminal forum sold domain user access to an enterprise in the oil and gas vertical with USD 200 million in revenue for USD 2,000. A probable ransomware affiliate bought the access. The actor who sold this access also sold access to Global Logistics Properties, which became a LockBit victim.
Access Sale	On 5 September, an actor on a popular Russian language crime forum advertised RDP workgroup user access to a company with USD 3.5 billion in revenue for USD 1,500. The actor provided screenshots purporting to demonstrate access to the victim's desktop. There were four different medical practice management apps on the desktop, including one specific to podiatry, suggesting the victim may be a hospital, a hospital system, or a medical billing company.
Access Sale	On 5 September, an actor on a second-tier Russian language crime forum advertised VPN access to a British Petroleum owned system in Malaysia. He claimed there is unspecified access to communications with Gas Malaysia Energy Services and the East Malaysia Planters Association.
Actor Developments	According to a security research collective known as VX Underground, a member of the Black Cat/AlphV ransomware gang claimed to find an employee of MGM Resorts on LinkedIn, impersonated that employee, and got the MGM help desk to reset their password, which led to a major network outage that shut down casinos, took down the reservation system, and locked guests out of their rooms. The incident caused Moody's Analytics to warn that the attack could impact MGM's credit rating, saying the attack highlighted "key risks to their operations."
Access Sale	On 11 September, an access seller on a Russian language crime forum was selling access to an unnamed American entity in the energy, utilities & waste vertical for USD 1,500. A LockBit affiliate bought the access with the condition that he'd be able to get his money back if the access didn't work out. Based on the description, the putative victim was Mississippi-based electricity cooperative 4-County Electric Power Association. However, after buying, the LockBit affiliate complained that the access was a honeypot and demanded his money back, which the seller refused.
Access Sale	On 11 September, an access seller on a Russian language crime forum was selling access to an unnamed Italian company with USD 6.9 billion in revenue for USD 4,000. The victim is likely a building services and facility management company.
Access Sale	On 13 September, an access seller on a Russian language crime forum was selling RDP access to a German manufacturer in the chemical and petrochemicals vertical with USD 4 billion in revenue for USD 5,000.
Actor Developments	Black Cat ransomware posted a long explanation of their attack on MGM Resorts on the Black Cat victim disclosure site, claiming they "have super administrator privileges to their Okta [server], along with Global Administrator privileges to their Azure tenant. They made an attempt to evict us after discovering that we had access to their Okta environment…" and that they "successfully launched ransomware attacks against more than 100 ESXi hypervisors in their environment on September 11th after trying to get in touch but failing." They claimed they continued to have access to MGM's environment and would launch additional attacks if MGM continued to refuse to negotiate.

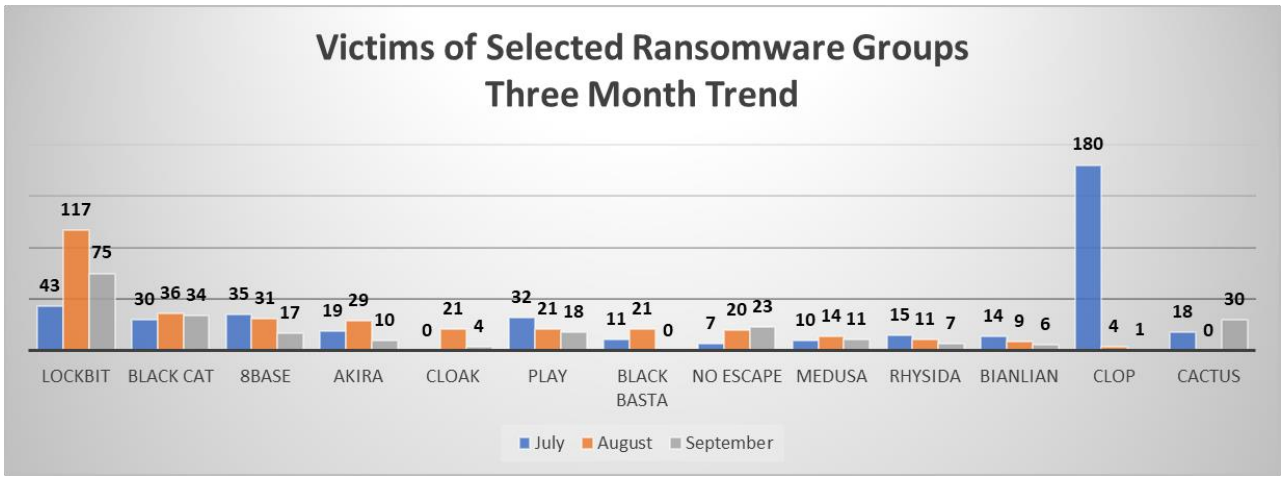
Access Sale	On 18 September, an actor on a Russian language forum offered to sell a shell in the environment of an Indonesian enterprise in the oil and gas vertical with USD 2.3 billion for USD 2,000.
Actor Developments	A new ransomware as a service called Kuiper was advertising for affiliates in a popular Russian language crime forum. As of yet, there are no further details, such as if there is a victim disclosure site or if it is based on an existing ransomware binary or a new family, etc.
Data Sale	Ransomed VC - which contrary to its name is an extortion group and doesn't yet employ ransomware - claimed to release more than 3 GB of data belonging to Sony. Sony is still investigating the leak.
Actor Developments	No Escape ransomware claimed Texas-based construction company Powerhouse Retail Services as a victim. Powerhouse was noted for sale in a popular Russian language crime forum in the middle of August.
Tool Sale	A reliable seller of EV certificates on a popular Russian language crime forum is raising his price to USD 6,500 per certificate due to "the increasing complexity of obtaining an EV certificate from GlobalSign." GlobalSign is a certificate authority specializing in EV certificates for IoT systems.
Data Sale	An actor on a popular English language crime forum posted a link to a database containing sales data, customer support call summaries, employee credentials, and partial SSN data for employees of T-Mobile. There have been multiple T-Mobile breaches in the last five years.
Tool Sale	An actor on a popular Russian language forum, with a very positive reputation among his fellow criminals, is selling a Windows local privilege escalation 0Day, to one buyer, written in Delphi, and affecting Windows Server 2008-Windows Server 2022 and Windows 7-11. The exploit was supposedly tested with a variety of tools, including Cobalt Strike and custom tools. The price is USD 250,000 and payable through the forum escrow only.
Access Sale	An actor on a popular Russian language crime forum was selling Fortinet VPN/RDP access to an American software and technical consulting company with USD 350 million in revenue for a buy now price of USD 3,000. The sales offer was eventually withdrawn after he reported losing access.
Access Sale	An actor on a popular Russian crime forum is selling local user access to a tax preparer, likely in North Carolina. There is access to the latest version of Drake tax preparation software. Price is USD 2,000. This access will most likely be used for tax filing fraud rather than ransomware, as tax filing season is approaching, and tax fraud remains a popular line of business among cyber criminals.
Tool Sale	Multiple actors on popular Russian language crime forums are selling pirated versions of the latest version of Cobalt Strike and artifact kits for between USD 2,500 – USD 7,500. This suggests that there will soon be an uptick in malicious use of Cobalt Strike 4.9 in the very near future.

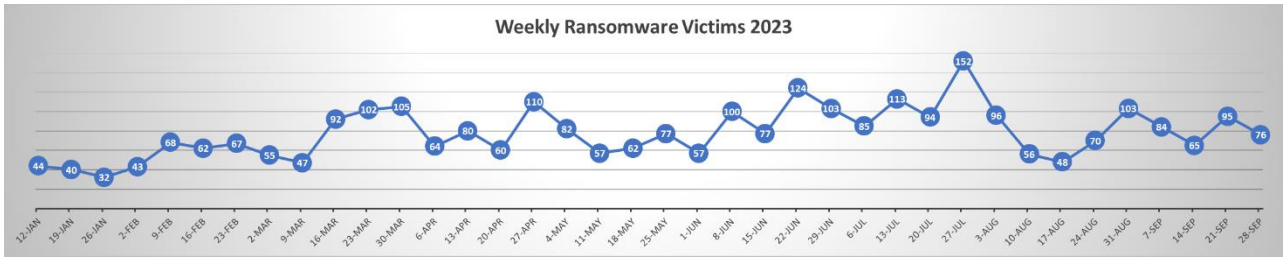
By The Numbers

Summarizing incidents in graphical format






Victims of Selected Ransomware Groups
Three Month Trend
43 117 75
30 36 34
35 31 17
19 29 10
0 21 4
32 21 18
11 21 0
7 20 23
10 14 11
15 11 7
14 9 6
180 4 1
18 0 30
LOCKBIT
BLACK CAT
8BASE
AKIRA
CLOAK
PLAY
BLACK BASTA
NO ESCAPE
MEDUSA
RHYSIDA
BIANLIAN
CLOP
CACTUS
July
August
September


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 84 65 95 76
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
7-SEP
14-SEP
21-SEP
28-SEP

[i] https://cert.gov.ua/article/5702579
[ii] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/critical-infrastructure-attacks
[iii] https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-value-targets/
[iv] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-270a
[v] https://www.bleepingcomputer.com/news/security/building-automation-giant-johnson-controls-hit-by-ransomware-attack
[vi] https://www.fortinet.com/blog/threat-research/threat-Actors-exploit-the-tensions-between-azerbaijan-and-armenia
[vii] https://sec.okta.com/articles/2023/08/cross-tenant-impersonation-prevention-and-detection
[viii] https://securelist.com/backdoored-free-download-manager-linux-malware/110465/
[ix] https://www.trendmicro.com/en_us/research/23/i/earth-lusca-employs-new-linux-backdoor.html
[x] https://sysdig.com/blog/ambersquid/
[xi] https://intel471.com/blog/bumblebee-loader-resurfaces-in-new-campaign
[xii] https://checkmarx.com/blog/surprise-when-dependabot-contributes-malicious-code/
[xiii] https://www.bleepingcomputer.com/news/security/google-assigns-new-maximum-rated-cve-to-libwebp-bug-exploited-in-attacks/
[xiv] https://asec.ahnlab.com/en/47455/
[xv] https://asec.ahnlab.com/en/56756/, https://blog.google/threat-analysis-group/active-north-korean-campaign-targeting-security-researchers/