Monthly Threat Intelligence Rollup

DEEP seas

TLP: CLEAR

Notable Cyberattacks

Summary of noteworthy cyberattacks in the last thirty days.

Incident	Activity Summary
Manufacturing Company Targeted, Disrupted by Black Basta Ransomware	On 9 October 2023, a prominent manufacturer of electrical and data transmission equipment in the United Kingdom released a public statement confirming the company had been the target of an unspecified "cyber incident" that disrupted their operations. To date no details regarding the attack have been released, though the choice of target suggests ransomware may have been involved. Fortunately, the company reported no disruptions to their production and shipping operations, suggesting that the attack was limited to the corporate office, or their network was properly segmented and contained the appropriate access controls to prevent a single point of entry from becoming a wider, more serious incident.[i] A later review determined Black Basta ransomware group was responsible for the attack.
Data Leaked in LockBit Ransomware Attack	On 11 October 2023, the DeepSeas dark web team identified leaked data posted to the LockBit ransomware group's extortion website; this is a strong indicator that a leading provider of technology solutions either failed to pay a ransom or refused negotiations. Further research determined that out of the initial LockBit demand for USD 80 million, the company countered with an offer of USD 1.1 million. This likely led to LockBit leaking a 100 MB text file containing the file names of all the leaked data as part of an attempt to further extort the company into raising their ransom payout. Review of the text file is quite illuminating with regards to clientele; these include numerous government agencies, financial institutions, insurance companies, and many others. This speaks to the company's size as well as their ubiquity among businesses and institutions, though it may also bode poorly for the company itself.[ii]
Middle Eastern Governments Crammed with Crambus	An Iranian cyber-espionage group, Crambus, also known as OilRig, MuddyWater, or APT34, orchestrated an extensive cyber intrusion campaign targeting an undisclosed Middle Eastern government from February to September 2023. During this operation, the attackers infiltrated multiple computers, pilfered sensitive files and passwords, and installed a PowerShell backdoor named PowerExchange to monitor and execute commands sent via emails. They also utilized Plink, a network administration tool, for configuring port-forwarding rules and enabling remote access via the Remote Desktop Protocol (RDP). In the past, Crambus has been known for their intelligence gathering and recently incorporated social engineering tactics into its attacks. This group deployed multiple previously undiscovered malware, such as Tokel, Dirps and Clipog, alongside known tools such as Mimikatz. The campaign's timeline details a series of intrusions, backdoor installations, and information exfiltration efforts. Crambus has remained an ongoing and persistent threat to organizations in the Middle East and beyond, displaying a high level of expertise and adaptability in its cyber operations.[iii]
Access Tokens Stolen, Multiple Customers Claim	According to multiple sources, an identity and access management company was reportedly compromised in early October 2023, and HTTP access tokens belonging to its clients were stolen from their support platform. According to one of its clients, which published the most detailed account of their incident, on 2 October an engineer uploaded a HAR file to company's support platform as part of an effort to troubleshoot access issues; within 30 minutes the access tokens within the HAR file had been exploited by attackers in an attempt to create a Super Administrator account in the client's tenant. This suggests two things; the attackers were already well established inside the customer support network, and the attackers were highly skilled with workflows in place to take advantage of these tokens. This points to

	either nation-state activity or, as is more likely the case based on its targeting of hospitality companies, cyber criminals seeking a massive payout. It is also highly likely that the compromise of the company began much earlier than 2 October, though the attack took several weeks from detection to full remediation.[iv]
Russian State, Industrial Organizations Targeted with Golang Backdoor	Beginning in July 2023, Kaspersky Lab detected evidence of a new campaign delivering a backdoor malware coded in Golang to targets; uniquely these targets are Russian state organizations as well as Russian state-owned or state-operated industries. This choice of targeting is unusual as targeting of Russian entities is rare, though perhaps it is simply underreported and thus merely appears to be rare. The last known targeting of Russian industrial targets was conducted by suspected Chinese attackers in 2020 and 2021 and targeted an organization responsible for the design and construction of the Russian Navy's nuclear-powered ballistic missile submarines. The malware itself is relatively simplistic, designed only to conduct basic reconnaissance and file exfiltration and delivered via archive files in ARJ format.[v]

Emergent Malware and TTPs

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

Malware/Campaign	Activity Summary	TTP Analysis
Another Critical Vulnerability Identified in Progress FTP Software	Following mass exploitation of the Progress MOVEit FTP software, Progress has issued patches for their WS_FTP software to resolve two severe vulnerabilities, CVE-2023-40044 and CVE-2023-42657.	CVE-2023-40044 boasts a CVSS score of 10/10, the highest possible criticality. This vulnerability is a .NET deserialization vulnerability permitting remote code execution without authorization. Following disclosure of the vulnerability a proof-of-concept exploit was released and quickly weaponized in attacks that were described as 'limited in scale,' though potentially all from the same actor or group based on outside analysis. This is suggesting that widespread exploitation on the scale of MOVEit Transfer may not be long in coming; initial probing of MOVEit Transfer servers began approximately two months prior to the cl0p ransomware group's mass exploitation operation.[vi]
Cobalt Strike 4.9 Circulating Among Cyber Criminals	Beginning in early October 2023, DeepSeas observed purported samples of a leaked or cracked copy of the Cobalt Strike penetration testing framework version 4.9 circulating in the cybercriminal underground.	While Cobalt Strike has long been a favored penetration testing framework for cybercriminals and red teams alike, in recent years it has become something of a mainstay for these groups. The leak of version 4.9 hints that either a penetration testing company has leaked the tool accidentally, or cyber criminals have successfully purchased it via a front company expressly set up for this purpose. Though other 'penetration testing' frameworks are widely available, including Sliver, Metasploit, and Machete, Cobalt Strike is widely considered the gold standard for cyber criminals of all calibers. DeepSeas tested some open-source detection logic intended to catch all versions of Cobalt Strike prior to 4.9 but found the logic lacking. Compounding the issue is the extremely touchy legal team supporting Strategic Cyber LLC, the developers of Cobalt Strike; development of countermeasures to Cobalt Strike invites legal action, and thus developing custom detection logic is problematic.[vii]
Cisco IOS XE Software Web Management User Interface RCE	Recently, Cisco has detected the exploitation of a new vulnerability (CVE-2023-20198) with a CVSS score of 10.0 in the Web User Interface of their Cisco IOS XE software.	When exposed to public-facing networks, the vulnerability impacts both physical and virtual devices and affects servers running Cisco IOS XE with HTTP enabled. When successfully exploited, attackers gain full control over the affected device. To prevent exploitation, Cisco recommends disabling the HTTP server feature on internet-facing systems to mitigate the risk.[viii]
Kinsing Group Observed Exploiting “Looney Tunables” Vulnerability	A cyber crime group responsible for highly technical compromises of cloud environments has begun exploiting a vulnerability in PHPUnit (CVE-2023-9841) dubbed ‘Looney Tunables,’ according to a new report by Aqua Nautilus.	The Kinsing group has previously been observed targeting cloud environments to install crypto mining malware; this is a curious choice of payload given the group’s demonstrated technical competence in exploiting technologies and hardware previously only targeted by nation-state actors and ransomware groups of a high technical caliber. The observed exploitation of CVE-2023-9841 is a shift in tactics to manual exploitation and collection of credentials from cloud service providers, whereas previously the group had largely used automated exploitation for installation of a rootkit and eventually crypto mining malware. The collection of credentials is less unusual; these are usually highly privileged credentials used only by system administrators, rather than rank-

		and-file users with low privileges. However, there is no evidence that these credentials have been resold or used to support more dangerous operations. Access to these credentials should be considered a severe security risk.[ix]
Long-Running Mozi IoT Botnet Finally Taken Offline	ESET researchers monitoring the Mozi IoT botnet, one of many Internet of Things (IoT) botnets exploiting insecure web-enabled cameras, routers, switches, DVRs, and other common equipment since at least 2019, have reported that the botnet appears to have been seriously and fatally crippled by an update.	The destruction observed by ESET was quite systematic and thorough. A kill switch was activated on or about 27 September, which forced the malware to install an update that killed the parent process and secured the device against further exploitation. Like the Wifatch 'malware,' which secured vulnerable IoT devices against exploitation, the update also disabled commonly exploited ports and system services (e.g., sshd and dropbear). However, unlike Wifatch the update file was signed with the same private keys as the original, all but proving that the original authors were responsible for issuing the kill command. The takedown was most likely done by Chinese government authorities; it was reported that the operators of the Mozi botnet were arrested by Chinese authorities in June 2023. The takedown taking nearly three months may be unsurprising, as it likely required the assistance of the botnet operators to execute. Curiously, the takedown of the botnet commenced in India first with China following suit a week later. Though fatally crippled, this botnet is not the only one in existence nor the most dangerous. IoT botnets are likely to remain a common tool for cybercriminals at all levels for the foreseeable future.[x]
DPRK State-Sponsored Actors Release New Novel Malware	On Oct 31, 2023, Elastic Security Labs reported on a new macOS malware family they discovered, tracing it back to a Python application posing as a cryptocurrency arbitrage bot delivered via a direct message on a public Discord server.	Elastic Security Labs were able to attribute this activity to DPRK based on an analysis of their techniques, network infrastructure, code-signing certificates, and custom detection rules. The main components of this new attack method for DPRK are SUGARLOADER, HLOADER and KANDYKORN. In order, SUGARLOADER is a downloader used by DPRK for initial access on the machine and for initializing the environment for the final stage, installing KANDYKORN. This binary is obfuscated using a binary packer, limiting what can be seen with static analysis. HLOADER is a payload that attempts to masquerade as the legitimate Discord application. As of Oct 2023, it has 0 detections on VirusTotal. HLOADER is a self-signed binary written in Swift. The purpose of this loader is to execute both the legitimate Discord bundle and malicious payload, the latter of which is used to execute Mach-O binary files from memory without writing them to disk. The legitimate binary (/Applications/Discord.app/Contents/MacOS/Discord) is renamed to .lock and replaced by HLOADER. KANDYKORN is the final stage of the execution chain and possesses a full-featured set of capabilities to access and exfiltrate data from the victim's computer. The configuration file is read into memory then decrypted using a RC4 key and parsed for C2 settings. Once communication is established, KANDYKORN awaits commands from the server. This is an interesting characteristic in that the malware waits for commands instead of polling for commands. This would reduce the number of endpoint and network artifacts generated and provide a way to limit potential discovery.[xi]

Threat Actor Campaigns

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

Threat Actors	Activity Summary
Semiconductor Firms Potentially Targeted by APT27	Possibly as part of a nation-state operation, Taiwan, Hong Kong, and Singapore, with a Taiwan Semiconductor Manufacturing (TSMC) lure document, intended to conduct technical espionage in support of the People's Republic of China's economic goal of technological independence from Western nations. Further analysis by EclecticIQ observed numerous overlaps between the observed activity and activity attributed to Carderbee, Budworm, Red Hotel, and other Chinese state-aligned groups. Uniquely, the attackers are utilizing a custom downloader component to deliver Cobalt Strike, itself hosted on a very likely compromised or potentially malicious Cobra DocGuard document storage server. The link to targeting of semiconductor firms is not based on hard evidence, merely inference, though China's various Five-Year Plans are a reliable indicator of where nation state actors will focus their efforts; semiconductor technology and technological independence features prominently in Beijing's most recent economic roadmap.[xii]
QakBot Malware Persists Despite Infrastructure Takedown	A 5 October report by Cisco Talos revealed that operators of the QakBot malware, a commodity criminal malware often used to deliver payloads on behalf of paying customers (so-called Malware-as-a-Service), was not fatally stricken by a coordinated multinational law enforcement takedown effort earlier in 2023. Though this effort succeeded in crippling much of the infrastructure used by QakBot as well as seizing the group's known cryptocurrency wallets, distribution of the malware has continued and even accelerated in recent weeks. The payload of choice for the operators is currently the Remcos RAT as well as Cyclops/Ransom Knight ransomware or a variant thereof. The long-term failure to permanently cripple QakBot's operations highlights the need for unmasking and physically arresting the group's members. The Lurk banking trojan operators who successfully monetized their Angler exploit kit were successfully disabled in one single decapitation strike by Russian authorities after 50 of the group's members were arrested in one day in the late 2010s.[xiii]
JetBrains TeamCity Servers Actively Exploited by Pyongyang	Beginning in early October 2023, Microsoft identified activity by two North Korean state-aligned groups (Diamond Sleet and Onyx Sleet, former ZINC and PLUTONIUM) targeting CVE-2023-42793, a remote code execution (RCE) vulnerability in multiple versions of JetBrains' popular TeamCity software applications. TeamCity is a continuous integration/continuous deployment tool utilized heavily in software development activities and represents a typical supply chain compromise tactic used by North Korean actors. Though the immediate parallel to SolarWinds may seem apparent, unlike SolarWinds, the TeamCity software is not backdoored rather separate installations are under active exploitation. The attack by Diamond Sleet begins by exploiting CVE-2023-42793 before installing bespoke malware families: ForestTiger, RollSling, and FeedLoad, all designed to provide persistent access and dump credentials from LSASS, enabling the actors to carry out a wide variety of malicious actions. Onyx Sleet operates much the same, though using a single malware (HazyLoad) to accomplish the same goals.[xiv]
Winter Vivern Group Exploiting CVE-2023-35730 in Roundcube Webmail Servers	The suspected Russian-aligned Winter Vivern group, which has conducted pro-Belarus and pro-Russian attacks against targets in Europe since at least 2021, has been observed exploiting a cross-site scripting (XSS) vulnerability in Roundcube webmail servers as part of a campaign targeting European governments and think tanks. All observed targeting is consistent with previous Winter Vivern activity. While attribution is difficult, the group is suspected to be Russian aligned due to their targeting, which is consistent with other Russian state-aligned groups such as APT28 and APT29. Indeed, APT28 was observed exploiting this same vulnerability against some of the same targets, strongly hinting that the group is at least aligned with Russian state interests or

	possibly a subgroup or cell belonging to APT28. The attack is simplistic, utilizing emails with a base64-encoded payload hidden in a SVG image embedded in the body of the email. Due to the lack of a follow-on payload, DeepSeas suspects that the group is simply an access broker for other Russian groups acting at the behest of the Kremlin.[xv]

Dark Web Markets

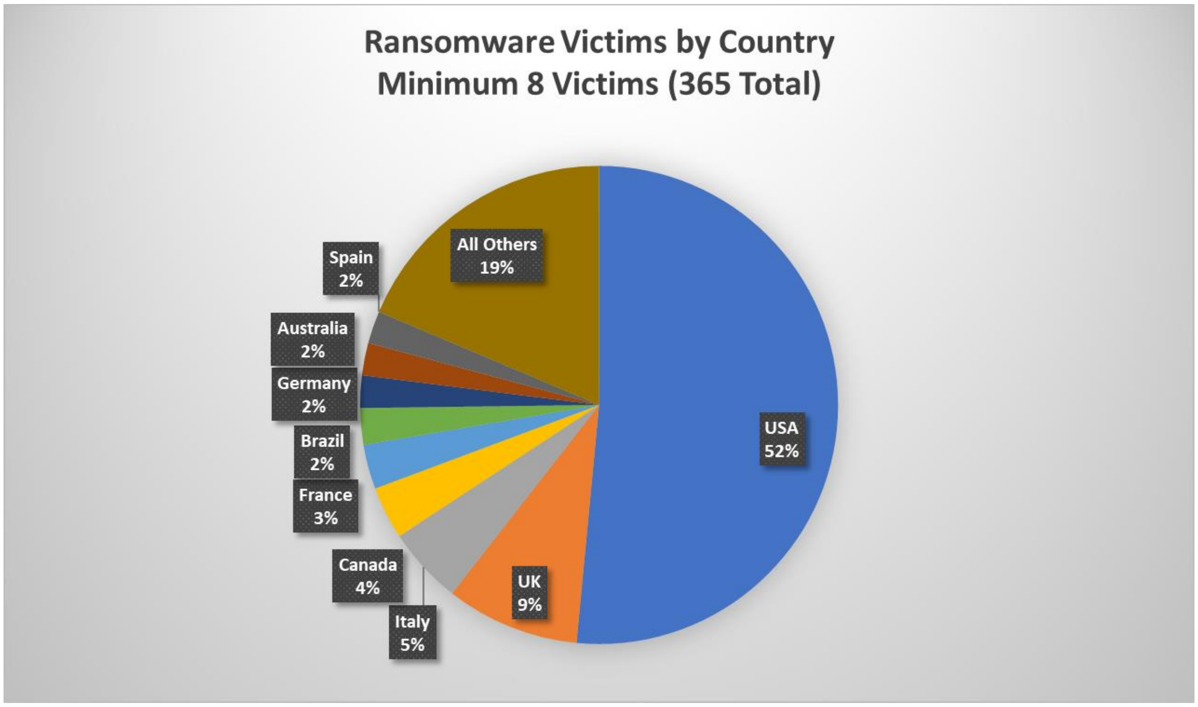
High-profile ransomware data dumps and dark web access sales identified in last thirty days.

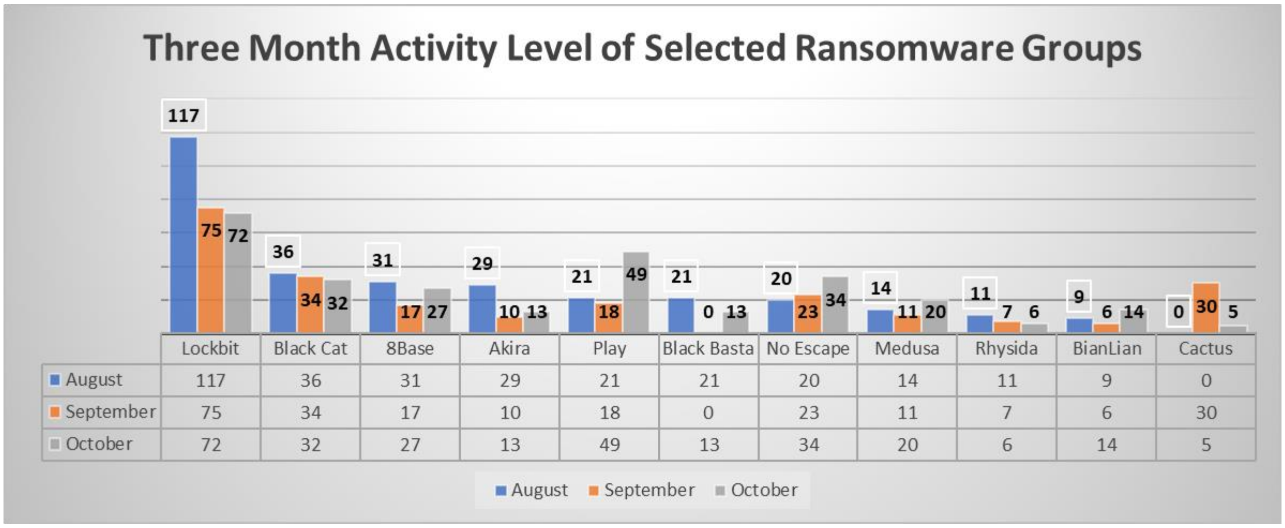
Activity	Note
Access Sale	An actor on a popular Russian crime forum was selling alleged access to a Japanese multinational conglomerate corporation's South American social media account through a third-party portal for USD 1500. This comes on top of recent claims by the ransomware group, Ransomed VC, that it had downloaded multiple terabytes of information belonging to the corporation, putting it up for sale. The same corporation announced that they were the victim of a cyber-attack that exposed corporate information earlier this year.
Access Sale	An actor on a popular Russian crime forum was selling Citrix user access to a large Argentine car dealership with USD 2.2 billion in revenue for USD 3000.
Access Sale	An actor on a popular Russian crime forum was selling access to a U.S. based medical equipment manufacturer with USD 130 million in revenue for USD 5000. The description and poorly redacted screenshot, which the actor provided to prove access, revealed the victim is likely an organization that was also a BlackByte ransomware victim in July.
Access Sale	A new Telegram channel founded last week called FedCreds is selling access to law enforcement email logins and logins for a service other companies use to screen out phony warrantless emergency data requests. The requests allow criminals to impersonate law enforcement, obtain information on victims, and freeze accounts, allowing the criminals easier access to the contents of the victim's account, SIM swapping, and other nefarious activity.
Access Sale	An actor on a popular Russian language crime forum was selling Citrix local admin access to an unspecified European company with more than USD 40 billion in revenue and 21,600 hosts with Cytomic endpoint agents for USD 7,000.
Actor Developments	The SiegedSec hacking team claimed on their new Telegram channel to be attacking industrial control systems in the U.S. as part of what they call Operation Jane. They also claimed to leak data stolen from an Australian software company.
Access Sale	An actor on a major Russian language crime forum was selling access to 7,000 point-of-sale (PoS) terminals with remote access to all of them. Judging from the screenshot provided by the actor the access looks like a point of sale as a service. One victim listed on the screenshot was a privately owned American chain of fast casual restaurants. The buy now price was USD 8,000.
Access Sale	An access seller on a popular Russian crime forum was selling Citrix access to a "giant" U.S. company in the healthcare software vertical with USD 5.8 billion in revenue for USD 4,000.
Access Sale	An access seller on the Exploit crime was selling domain administration access to a U.S. based logistics company with USD 400 million in revenue and 6-700 employees and 1,000 hosts on the network for a buy now price of USD 8,000.
Access Sale	A crime forum access seller offered to sell FTP access to a Shanghai, China-based fabless semiconductor company specializing in chipsets for mobile communications and IoT. The seller wrote, "there is more than one terabyte of data, including documents, presentations, and journals." The price was initially USD 7,000 and was reduced to USD 6,500.
Actor Developments	The infrastructure belonging to one of the longest running ransomware brands, Ragnar locker, was seized in a multinational law enforcement operation on 19 October. The chat site and the victim disclosure site both had front pages announcing the seizure and the participating agencies.

Access Sale	In mid-August, a former known Conti affiliate bought domain admin access to a Central American enterprise network with 2500 hosts and a USD 350 million in revenue for a buy-now price of USD 20,000 from a reliable Exploit crime forum access seller. The company was described as having 500 employees and having dealing with gasoline. A company having 469 employees and USD 357.3 million in revenue also turned up as a No Escape ransomware victim this week. This hints that a prolific, long-time Conti affiliate has become a No Escape ransomware affiliate.
Access Sale	On 13 October, an actor on a popular Russian crime forum was selling multiple accesses to an auto OEM's motors and engineering division, including accounts belonging to administrators, for USD 70,000. Another user chastised the seller for naming the victim in the advertisement, calling the access worthless because of the reveal.
Access Sale	On 14 October, a criminal actor was observed selling what they claimed was a remote code execution (RCE) exploit in F5 Networks' flagship enterprise BIG-IP VPN software for USD 150,000. They did not call it a 0day or further describe the nature of this vulnerability.
Access Sale	On 19 October, an actor on a popular Russian crime forum was selling access to an American restaurant group with USD 182 million in revenue for USD 200.
Access Sale	On 4 August, an access seller on a popular Russian crime forum was observed attempting to sell access to a Chinese based manufacturer of automobile parts for a buy-now price of USD 6,000. A likely victim was also listed as a ransomware victim on the LockBit ransomware site on 23 October.
Access Sale	On 12 October, an access seller on a popular Russian crime forum sold access to a U.S. based company to another Exploit crime forum actor for USD 1000. Based on a screenshot shared by the actor, the victim was probably a Colorado-based snow removal business, as it was listed by LockBit on their site as a victim on 25 October.
Actor Developments	The RansomedVC group opened a new forum for discussing ransomware related topics on or about 20 October. There are already more than 100 members on the forum and several dozen posts. One actor has already launched a new ransomware as a service on the platform called qBit. In one of the first posts, RansomedVC posted a link to what they claim is new data stolen from Colonial Pipeline last spring.
Access Sale	On 20 October, an access seller on a popular Russian crime forum was selling access to a small enterprise in the sports teams and leagues vertical for USD 70.
Access Sale	On 24 October, an access seller on a popular Russian crime forum was selling access to an Australian manufacturer of engines and batteries for unmanned aerial vehicles for USD 900.
Access Sale	On 24 October, an access seller on a popular Russian crime forum was selling access to a U.S.-based manufacturer with USD 12 billion in revenue for USD 10,000. There are several companies fitting the description given by the actor.
Access Sale	On 24 October, an access seller on a popular crime forum was selling access to 19 victims, including what could be major auto manufacturers and an unnamed South Korean computer equipment manufacturer with USD 1.7 billion in revenue.
Access Sale	On 28 October, an actor on a popular Russian crime forum offered to sell access to multiple victims, including a financial services company that is an Indian business intelligence company and a U.S. based advertising and marketing company.
Access Sale	On 30 October, an access seller on a popular Russian crime forum offered to sell access to multiple victims with more than USD 500 million in revenue, including a company in Washington DC, a large Chicago-based real estate firm, and a software and technical consulting company. No buyers have been noted yet.
Access Sale	On 30 October, an access seller on a popular Russian crime forum was noted selling AnyDesk access to an unnamed logistics company with more than USD 140 million in revenue.
Access Sale	On 30 October, an access seller on a popular Russian crime forum was noted selling VPN access to a South Korean based automotive supplier with USD 3 billion in revenue.

By The Numbers

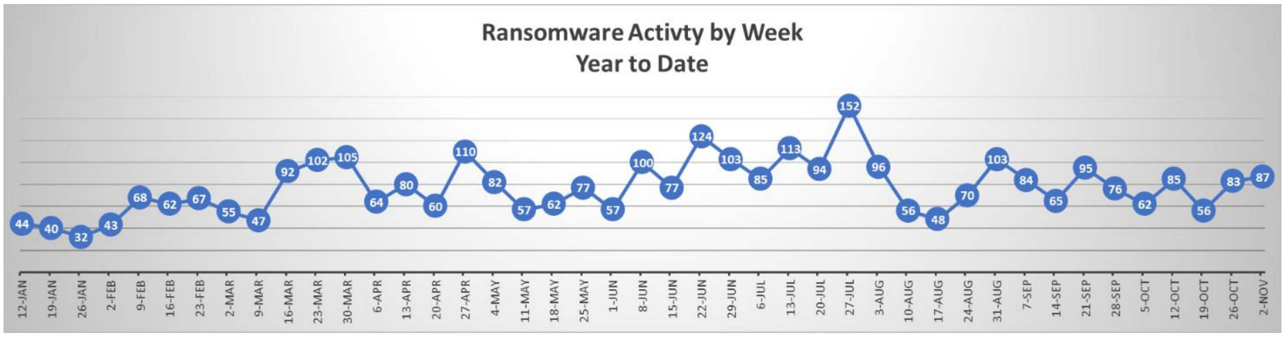
Summarizing incidents in graphical format

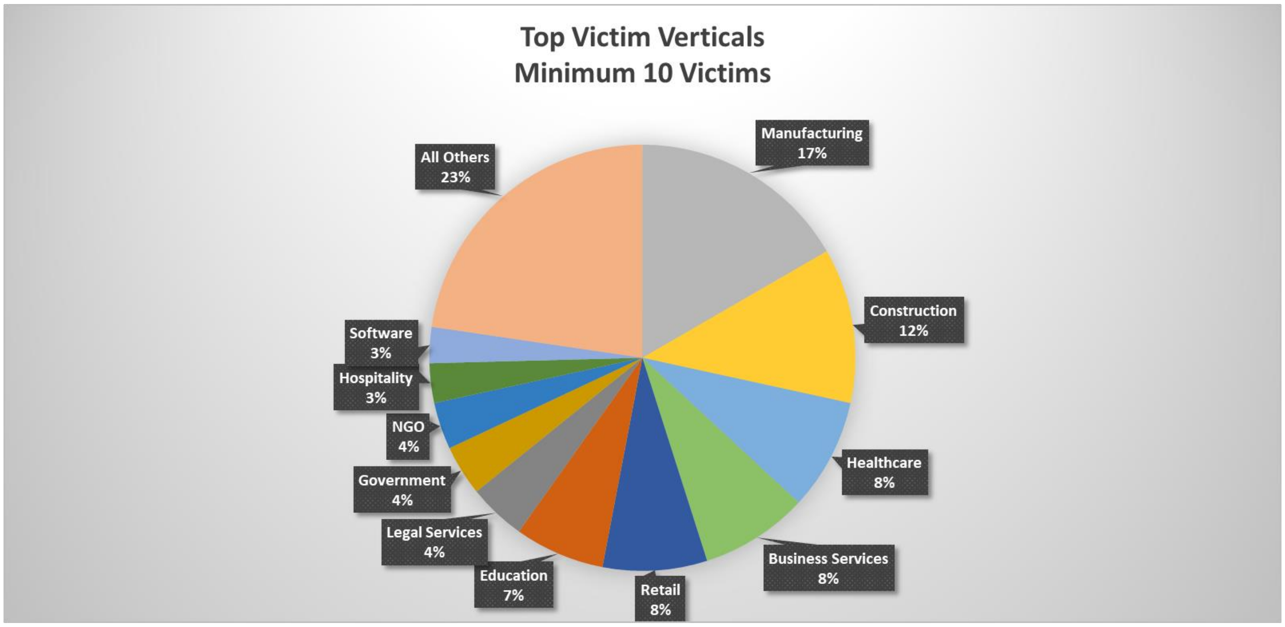




	Lockbit	Black Cat	8Base	Akira	Play	Black Basta	No Escape	Medusa	Rhysida	BianLian	Cactus
■ August	117	36	31	29	21	21	20	14	11	9	0
■ September	75	34	17	10	18	0	23	11	7	6	30
■ October	72	32	27	13	49	13	34	20	6	14	5

TLP: CLEAR


Ransomware Activty by Week
Year to Date
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
62
85
56
83
87
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
5-OCT
12-OCT
19-OCT
26-OCT
2-NOV


Top Victim Verticals
Minimum 10 Victims
Manufacturing 17%
Construction 12%
Healthcare 8%
Business Services 8%
Retail 8%
Education 7%
Legal Services 4%
Government 4%
NGO 4%
Hospitality 3%
Software 3%
All Others 23%

New Detection Content

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

Possible WS_FTP Server Exploit

- Looking for suspicious commands and child processes which may indicate an exploit of a vulnerable WS_FTP server. See the references for examples:
    - https://www.rapid7.com/blog/post/2023/09/29/etr-critical-vulnerabilities-in-ws_ftp-server/
    - https://www.sentinelone.com/blog/threat-actors-actively-exploiting-progress-ws_ftp-via-multiple-attack-chains/

GlassFish Web Shell Remote Command

- Looking for suspicious child process of GlassFish with a network connection which could indicate remote commands to a web shell on the server. The child process commands should be investigated for maliciousness.

VSDiagnostics.exe Indirect Command Execution

- Legitimate executable found in Visual Studio that can be used to execute malicious commands or other binaries.
    - https://github.com/tsale/Sigma_rules/blob/main/LOL_BINs/VSDiagnostics_LoLBin.yml

[i] https://therecord.media/manufacturing-giant-hit-with-cyberattack
[ii] DeepSeas proprietary sources
[iii] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/crambus-middle-east-government
[iv] https://www.beyondtrust.com/blog/entry/okta-support-unit-breach
[v] https://securelist.ru/ataki-na-industrialnyj-i-gosudarstvennyj-sektory-rf/108229/
[vi] https://www.huntress.com/blog/critical-vulnerabilities-ws_ftp-exploitation
[vii] DeepSeas proprietary sources
[viii] https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/
[ix] https://blog.aquasec.com/loony-tunables-vulnerability-exploited-by-kinsing
[x] https://www.welivesecurity.com/en/eset-research/who-killed-mozi-finally-putting-the-iot-zombie-botnet-in-its-grave/
[xi] https://www.elastic.co/security-labs/elastic-catches-dprk-passing-out-kandykorn
[xii] https://blog.eclecticiq.com/chinese-state-sponsored-cyber-espionage-activity-targeting-semiconductor-industry-in-east-asia
[xiii] https://blog.talosintelligence.com/qakbot-affiliated-actors-distribute-ransom/
[xiv] https://www.microsoft.com/en-us/security/blog/2023/10/18/multiple-north-korean-threat-actors-exploiting-the-teamcity-cve-2023-42793-vulnerability/
[xv] https://www.welivesecurity.com/en/eset-research/winter-vivern-exploits-zero-day-vulnerability-roundcube-webmail-servers/