Monthly Threat Intelligence Rollup

DEEP seas

11/01/23-11/30/23

Notable Cyberattacks

Summary of noteworthy cyberattacks in the last thirty days.

Incident	Activity Summary
ICBC Financial Services Hit by Suspected LockBit Ransomware	On 9 November 2023, the U.S. branch of the Industrial and Commercial Bank of China, the largest lender by assets in China, reported suffering an unspecified cybersecurity incident. Though details remain sparse, media reports that the LockBit ransomware group is responsible for the attack, which has disrupted the trade market for U.S. Treasury bonds. If true, the involvement of a Russia-linked cyber crime group is a curious and unexpected development given the precarious state of Russia's international relations following its misadventures in Ukraine. Western targets are by far considered the prime targets for ransomware actors both large and small, and activities in nations friendly to Russia are heavily discouraged at best, and at worst are cracked down upon by Moscow. Again, if true, this raises questions about whether or not the attack was sanctioned by Moscow. The attack on a U.S. arm of the ICBC rather than the entire ICBC may be an attempt by the ransomware actors to expand into a gray area where operations may or may not be sanctioned, or perhaps part of an effort to pressure the U.S. without directly affecting those systems in China. Given that China is one of the few suppliers of military hardware and other goods left to Russia, this attack is a risky one. If the attack was unsanctioned and invites Moscow's displeasure, the arrest of LockBit members in Russia is likely to follow. If the attack was sanctioned by Moscow, it represents a new development, though not necessarily an unexpected one. There are no friends in international relations, only nations whose interests align with one another, whether temporarily or long-term, and Russia has repeatedly demonstrated that it will conduct operations when and where it pleases, without concern for long-term consequences. DeepSeas will continue to monitor this developing situation for further information regarding the group responsible for the attack.[i]
Long-term Intrusion at Dutch NXP Points at Beijing's Long-term High-tech Ambitions	The scope and scale of a years-long intrusion at Dutch semiconductor manufacturer NXP has been revealed via a Dutch newspaper. The report provides details about a previously unreported incident in which Chinese state-aligned actors intent on industrial espionage compromised NXP's internal networks in late 2017 and persisted on the company's networks until early 2020. The compromise was only revealed after investigation of another compromise of a Dutch airline was identified, and incident response determined that NXP's network was used as a proxy. The attack originated via credential reuse from credentials previously stolen or leaked. While NXP downplayed the incident, claiming the technical designs were too complex to readily copy, China has proven competent at exploiting stolen technical designs. The theft of designs for aircraft engines has led to a generational leap in China's aviation sector, though it is true that semiconductor manufacturing remains vastly more difficult than forging turbine rotors. The group responsible, the Chimera group, has also been implicated in a compromise of an unnamed Taiwanese semiconductor manufacturer, pointing to state-directed activity aimed at bolstering China's own semiconductor manufacturing.[ii]

Emergent Malware and TTPs

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

Malware/Campaign	Activity Summary	TTP Analysis
C3RB3R Ransomware Group Exploiting Confluence Vulnerability CVE-2023-22518	On 6 November 2023, Rapid7 released details of a recent intrusion by the Cerber ransomware group which targeted a recently discovered zero-day vulnerability in Atlassian's Confluence software, widespread in corporate, educational, development, and research environments.	In concert with these intrusions, the attackers also utilized CVE-2023-22515, another zero-day vulnerability identified in Confluence in early October 2023 and since patched. Instances on both Linux and Windows systems were affected by the attackers, later identified as the Cerber ransomware group, who were likely using automated exploitation processes to compromise vulnerable internet-facing Confluence servers to deliver their ransomware. Fortunately, in these incidents, the ransomware only affected the single system it was delivered to and did not spread laterally. The attribution to the Cerber ransomware group is a curious one; the group purchased the Magnitude exploit kit several years ago and largely disappeared, restricting its attacks to South Korea and occasionally Japan and other Southeast Asian nations. While it is possible that the group is expanding its operations, given that its ransomware did not spread laterally, it seems more likely that Rapid7's customer environments belong to South Korean companies and that the Cerber ransomware group has not continued to evolve its malware and seek greener pastures abroad. The use of the Magnitude exploit kit was not mentioned by Rapid7 either. It remains unknown whether the group has continued to maintain this tool. DeepSeas considers this unlikely, as with the downfall of Adobe Flash Player, the kit is likely nothing more than a framework for further work at best, and a historical relic at worst. Still, the group has quickly adopted exploitation of a zero-day vulnerability discovered only three days prior, suggesting that its technical competence has not slipped over the years since the days of its worldwide operations.[iii]
Cl0P Ransomware Group Exploiting SysAid IT Vulnerability CVE-2023-47246	On 2 Nov 2023, a zero-day vulnerability classified as CVE-2023-47246 was identified in SysAid Technologies' on-premises software. It was identified under active exploitation by a group dubbed Lace Tempest by Microsoft.	This group overlaps with well-known cyber crime groups TA505, FIN11, and Cl0p and was responsible for widespread exploitation of CVE-2023-34362 in June and July 2023. SysAid, an international IT company, is known to develop and provide IT-related service management software, such as its Help Desk or ITSM services, and is thus a similar target for this group. The vulnerability which affected SysAid IT, a path traversal flaw, was successfully abused by Cl0p via uploading a WAR archive, which is a collection of JAR files, containing malicious payloads into the webroot of SysAid's Tomcat web service. After installation of the malicious payloads, Cl0p began accessing restricted accounts and established control over SysAid's Tomcat web service. Cl0p then uploaded malware to SysAid's systems, specifically its flagship GraceWire Trojan, by injecting it into legitimate processes. Cl0p finally later erased all its actions from the disk of the affected web server and the SysAid on-premises server web logs. Profero, a cybersecurity incident response company, conducted the investigation that identified the zero-day vulnerability, while Microsoft is credited with detecting the CVE under active exploitation in the wild.[iv]

ownCloud MFTS Vulnerability CVE-2023-49103 Exposes Credentials	A critical vulnerability in Kiteworks' ownCloud managed file transfer service (MFTS) software has been assigned a base score of 10, the most severe possible, and scanning for vulnerable instances has been observed to accelerate in the last week.	The vulnerability lies in a third-party library used by the graphapi app in ownCloud; when accessed, the URL provides configuration information which may include admin credentials and license keys. Disabling the app is not sufficient to remediate the issue. Deleting the app entirely is the recommended remediation, specifically from the following location: owncloud/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php. Rotating login credentials is also highly recommended, in case credentials exposed by scanning activity are reused by malicious actors. Given that the Cl0p ransomware group has been notorious for exploiting vulnerable MFTS installations in 2023, and a proof-of-concept exploit is available, it is highly likely that the scanning activity is this group’s handiwork, and that another wave of ransomware attacks via this vector is being planned. Fortunately, unlike MOVEit, ownCloud appears to be less common; only 2,000 instances were identified worldwide.[v]

Threat Actor Campaigns

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

Threat Actors	Activity Summary
Israeli Critical Infrastructure Targeted by WildCard APT Group	A long-running campaign by a threat actor dubbed 'WildCard' by Intezer has been linked to numerous attacks against Israeli institutions over the last three years. It has demonstrated not only a technical competence on the level of nation-state actors but has also repeatedly targeted Israeli educational institutions, IT infrastructure, and power generation targets. The rapid development of different varieties of malware utilized by the WildCard group is notable; not only has the group fielded several different varieties of malware, but the group also switched from coding its malware in C++ to Rust, an interesting choice given that many recent rewrites of malware have sought to use Golang. Intezer's research has shown intriguing links between the activity observed by Intezer and the activity observed by ClearSky, an Israeli cybersecurity company, which suggests the activity is Iranian state-aligned.[vi]

Dark Web Markets

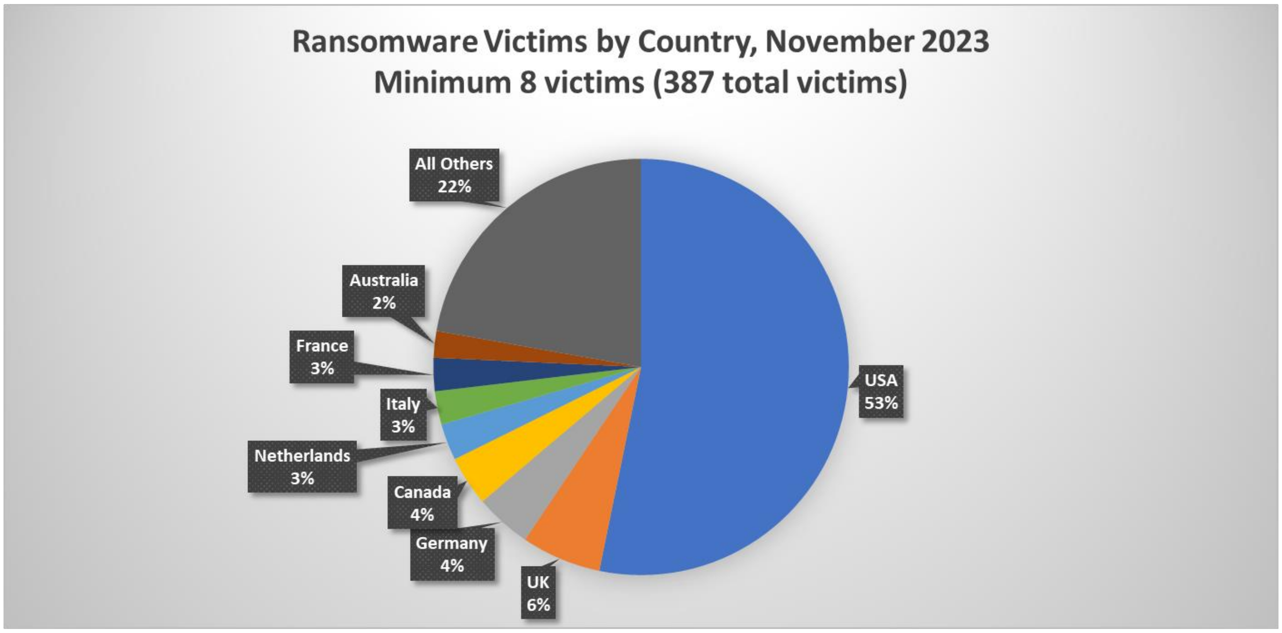
High-profile ransomware data dumps and dark web access sales identified in last thirty days.

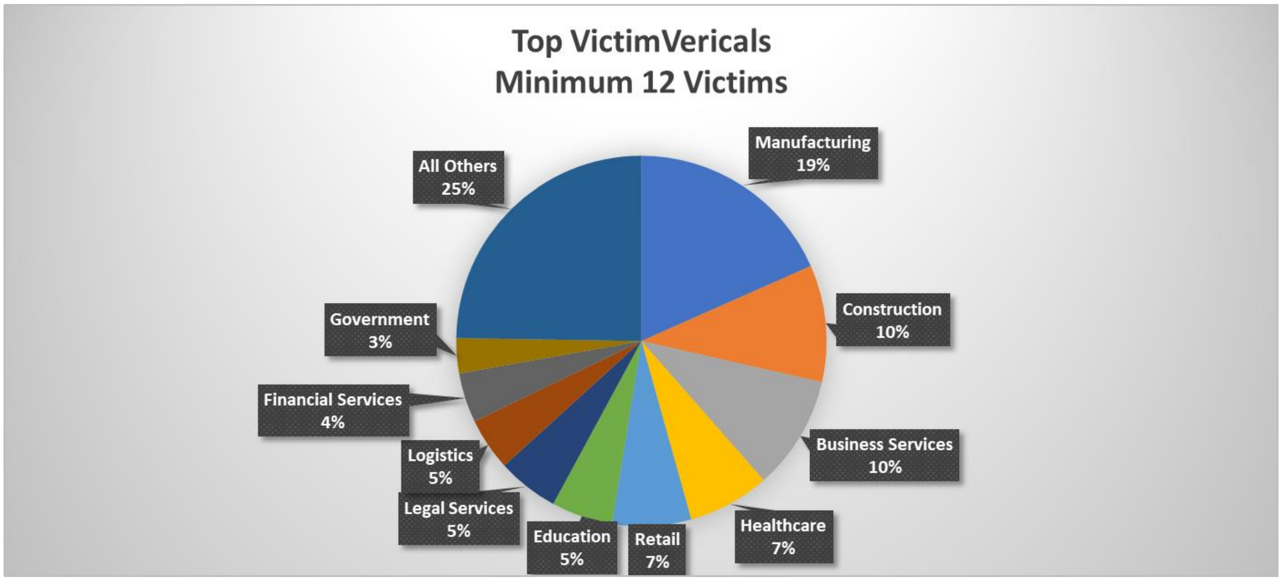
Activity	Note
Actor Developments	Black Cat successfully blackmailed pharmaceutical trials company Advarra into negotiating after it posted intimate photos of what it claimed was an officer at the company and vowed to never under any circumstances remove them. They were removed the next day, probably signaling that the blackmail worked.
Actor Developments	LockBit posted all the data it claimed to have about Boeing on its site.
Access Sale	An actor on a popular clearnet Russian-language crime forum was selling what he claims to be a zero-day exploit in the Joomla content management system. He did not offer any further description or name an asking price.
Access Sale	An actor on the Russian-language Exploit crime forum attempted to sell Citrix VPN access to multiple victims, including a hospital system and a software and technical consulting company.
Access Sale	An actor on a popular private Russian-language crime forum sold AnyDesk domain admin access to what he described as the “bank of one of the world’s most well-known car brands” with USD 800 million in revenue for USD 40,000.
Access Sale	An actor on a popular private Russian-language crime forum was selling root access to a Japanese power company.
Access Sale	An actor on a popular private Russian-language crime forum was selling Citrix local admin access to a U.S.-based grocery distributor.
Access Sale	An actor on a popular private Russian-language crime forum was selling Citrix admin access to an unnamed German company with USD 11.4 billion in revenue for USD 3,000. There are two German auto parts manufacturing companies listed with that revenue figure on the business intelligence site ZoomInfo.
Access Sale	An actor on a popular private Russian-language crime forum was selling Citrix user and domain access to several companies with more than USD 50 million in revenue.
Access Sale	An English-speaking actor on a popular clearnet Russian-language crime forum sold what he claimed was a zero-day RCE in F5 Big IP products for USD 100,000 payable in Monero to former Conti ransomware affiliate Danger1488. He did not further describe the exploit. His credibility is unknown, but he has had four successful transactions using the forum’s automated escrow system.
Access Sale	An actor on a popular clearnet Russian-language crime forum was selling what he claimed was a remote code exploit zero-day vulnerability in Digi EX12 network routers for USD 25,000.
Access Sale	An actor on a popular clearnet Russian-language crime forum was selling domain user access to a U.S.-based civil engineering/construction company with USD 426.5 million in revenue for USD 1,000.
Access Sale	An actor on a popular clearnet Russian-language crime forum was selling domain user access to a U.S.-based outsourcing company with USD 722.4 million in revenue for USD 1,800.
Access Sale	An actor on the Russian-language Exploit crime forum was selling RDP local admin access to an unnamed U.S.-based automotive manufacturer with USD 682 million in revenue for USD 1,900.

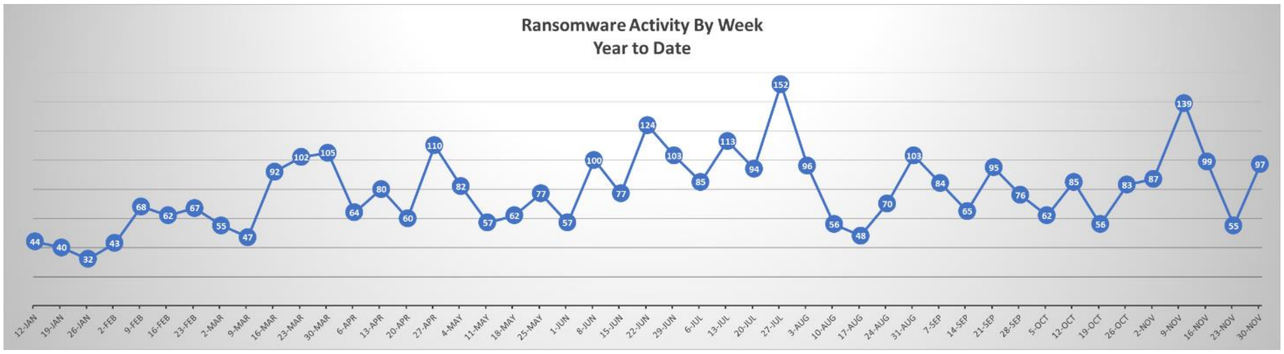
Access Sale	An actor on a popular private Russian-language crime forum was selling RDP user domain access to a U.K.-based apparel and accessories retailer with USD 1.7 billion in revenue for a buy now price of USD 1,500.
Access Sale	A popular crime forum access seller was selling Citrix domain user access to a U.S.-based architecture and construction company with USD 292.3 million in revenue for USD 2,000.
Access Sale	An actor on a popular clearnet Russian-language crime forum was selling SSH private keys, Docker logins, and other material belonging to CreditOne Bank. A few days later, he reported losing access because a “rat” posted the identity of the victim on X, formerly called Twitter.
Access Sale	A new crime forum access seller with no track record against which to judge his credibility was selling what he claims was VPN RDP access to a U.S.-based manufacturing/building materials company with more than USD 32.5 billion in revenue for BTC 0.5.

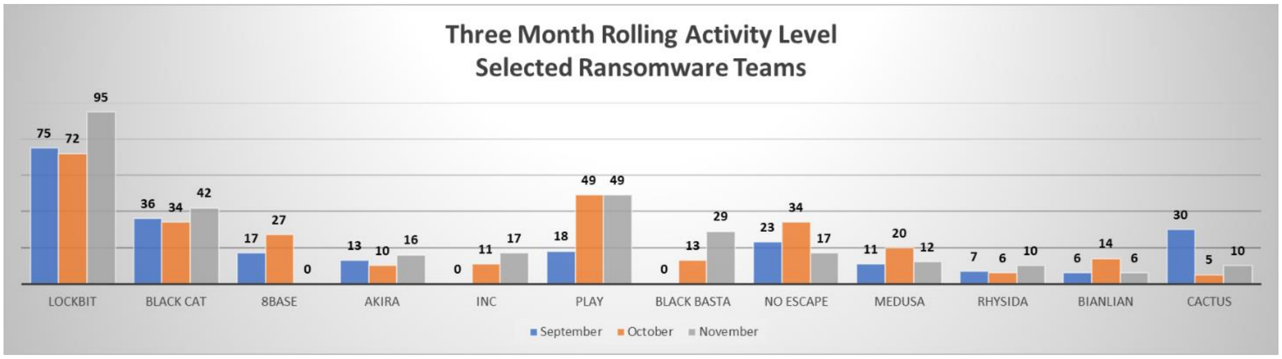
By The Numbers

Summarizing incidents in graphical format






Ransomware Activity 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
139
99
55
97
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
9-NOV
16-NOV
23-NOV
30-NOV


Three Month Rolling Activity Level
Selected Ransomware Teams
LOCKBIT 75 72 95
BLACK CAT 36 34 42
8BASE 17 27 0
AKIRA 13 10 16
INC 0 11 17
PLAY 18 49 49
BLACK BASTA 0 13 29
NO ESCAPE 23 34 17
MEDUSA 11 20 12
RHYSIDA 7 6 10
BIANLIAN 6 14 6
CACTUS 30 5 10
September
October
November

New Detection Content

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

EDR Evasion – WMIC Uninstall Carbon Black Command

- Looking for commands used by a threat actor to attempt to uninstall Carbon Black EDR:
    - https://superuser.com/questions/234104/uninstalling-programs-silently-via-cmd
    - https://attack.mitre.org/techniques/T1562/001/

ADFind – Active Directory Discovery Tool

- ADFind is a tool to enumerate users, groups, and computers of the Windows domain:
    - https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/

[i] https://www.theguardian.com/technology/2023/nov/10/ransomware-attack-on-china-biggest-bank-disrupts-us-treasury-market

[ii] https://www.techradar.com/pro/security/chinese-hackers-sneakily-stole-secrets-from-dutch-chip-company

[iii] https://www.rapid7.com/blog/post/2023/11/06/etr-rapid7-observed-exploitation-of-atlassian-confluence-cve-2023-22518/

[iv] https://www.sysaid.com/blog/service-desk/on-premise-software-security-vulnerability-notification, https://profero.io/posts/sysaidonpremvulnerability/, https://www.rapid7.com/blog/post/2023/11/09/etr-cve-2023-47246-sysaid-zero-day-vulnerability-exploited-by-lace-tempest/, https://twitter.com/msftsecintel/status/1722444141081076219

[v] https://owncloud.com/security-advisories/disclosure-of-sensitive-credentials-and-configuration-in-containerized-deployments/

[vi] https://intezer.com/blog/research/wildcard-evolution-of-sysjoker-cyber-threat/