# Monthly Threat Intelligence Rollup

DEEP seas

01/07/23-31/07/23

# Notable Cyberattacks

**Summary of noteworthy cyberattacks in the last thirty days.**

| Incident | Activity Summary |
|---|---|
| **RomCom Exploiting Windows Zero-Day Vulnerability** | A zero-day vulnerability (CVE-2023-36884) affecting Microsoft Windows and Office products is being actively exploited in targeted attacks against government and defense organizations in Europe and North America. Microsoft disclosed the vulnerability, stating that attackers can leverage a specially crafted Microsoft Office document to achieve remote code execution on the victim's computer. The exploit requires the victim to open the malicious file. No patch has been released yet, but Microsoft is investigating and may issue a patch in its monthly release or an out-of-cycle security update. Mitigation guidance has been provided, and Windows Defender has been updated to defend against this attack vector. The vulnerability has been exploited by an actor known as Storm-0978 (aka RomCom) in attacks against defense and government organizations. The attacks employed Microsoft Word documents posing as information about the Ukrainian World Congress. Storm-0978/RomCom is a Russia-linked threat actor involved in espionage and cybercrime activities associated with the RomCom remote access Trojan (RAT). There are potential ties between Storm-0978/RomCom, Hawker (developer of the Cuba ransomware), and the Industrial Spy ransomware actors, although their exact relationship remains unclear. The severity of the vulnerability necessitates the adoption of all available mitigation strategies until a patch is released. Although the vulnerability has been observed in targeted attacks thus far, its disclosure may inspire other attackers to replicate the exploit.[i] |
| **North Korean Actors Compromise Cloud Service Operator for Crypto Theft** | Beginning on 22 June 2023, the Colorado-based cloud directory service platform JumpCloud was compromised by actors later determined to be North Korean. In the company's disclosure statement, JumpCloud stated that the attackers were intent on affecting a small subset of the company's customer base - just 10 devices across five customers according to JumpCloud and CrowdStrike. Several anonymous sources confirmed to media that the targets of this attack were companies involved in in cryptocurrency, a long-favored target of North Korean hacking teams intent on providing funding to Pyongyang. At least one source named the group most likely responsible for the intrusion at JumpCloud; LABYRINTH CHOLLIMA, more popularly known as Lazarus Group. Though this attack was limited in scale it serves to demonstrate that North Korean state-aligned actors remain talented and motivated to find any way in to compromise their end target. It should also be noted that JumpCloud was remarkably forthright with their incident response activities, something that should be emulated by other companies. Unfortunately, there were few details released regarding the attackers' initial point of access, which has frustrated efforts to harden these access points against unauthorized intrusions.[ii] |
| **U.S. "Critical Infrastructure Agency" Breached via Citrix Vulnerability** | The U.S. government has issued a warning about a critical zero-day remote code execution (RCE) vulnerability, identified as CVE-2023-3519, in Citrix's NetScaler ADC and Gateway products. Hackers exploited this flaw in June to breach a U.S. organization in the critical infrastructure sector. The attackers used the RCE vulnerability to plant a web shell on the target's non-production NetScaler ADC appliance, enabling them to access and exfiltrate Active Directory (AD) data. Fortunately, the targeted NetScaler ADC appliance was in a segregated environment, preventing the hackers from moving laterally to a domain controller. The attackers utilized various techniques to exfiltrate the AD data, including uploading a TGZ archive with a web shell, a discovery script, and a setuid binary to the vulnerable appliance. They performed SMB scanning on the subnet and encrypted the stolen data using the OpenSSL library, disguising it as a PNG image for exfiltration. The Cybersecurity and Infrastructure Security Agency (CISA) has provided detection methods and tactics to help organizations, particularly those in critical infrastructure, determine if their systems have been compromised. Citrix has released updates to address the vulnerability, and NetScaler admins are urged to install them promptly. The |

| | |
|---|---|
| | vulnerability has been actively exploited by threat actors since it was a zero-day, affecting a significant number of NetScaler ADC and Gateway servers exposed online, with an estimated 15,000 affected appliances. CISA also released commands for organizations to check for signs of compromise related to the CVE-2023-3519 exploitation. In addition to the critical RCE vulnerability, Citrix also patched two less severe vulnerabilities - a reflected cross-site scripting (XSS) bug (CVE-2023-3466) and a privilege escalation to root (CVE-2023-3467). These vulnerabilities have not been observed being exploited in the wild, but threat actors with existing network access may leverage them to increase their control.[iii] |
| **Norwegian Government Breached via Zero-Day Vulnerability** | The Norwegian National Security Authority (NSM) has confirmed that a zero-day vulnerability in Ivanti's Endpoint Manager Mobile (EPMM) solution was exploited by attackers to breach a software platform used by 12 Norwegian ministries. The attackers gained unauthorized access to sensitive data from compromised systems, resulting in a data breach. The CVE-2023-35078 security bug is an authentication bypass vulnerability in Ivanti's EPMM software, allowing remote attackers to access specific API paths without authentication. This vulnerability enables threat actors to steal personally identifiable information (PII) such as names, phone numbers, and other mobile device details. The attackers can also make configuration changes, including creating administrative accounts to further manipulate vulnerable systems. Ivanti has confirmed the active exploitation of the zero-day and urged customers to take immediate action to protect their systems. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) also warned federal agencies to promptly secure their systems against the vulnerability. The deadline for U.S. Federal Civilian Executive Branch Agencies (FCEB) to patch their devices is August 15. It is critical for network administrators to upgrade their Ivanti EPMM (MobileIron) installations to the latest version to safeguard against potential attacks.[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 |
|---|---|---|
| **New Trojan Campaign Targeting LATAM Businesses** | Zscaler ThreatLabz researchers have discovered a sophisticated targeted attack campaign affecting businesses in Latin America. The campaign employs a multi-staged infection chain, utilizing custom modules designed for malicious activities. | The payload of the campaign is a new Latin American Trojan called TOITOIN, which uses XOR decryption to decode its configuration file. The trojan collects system information and data about installed browsers and sends it to the attackers' command and control server in an encoded format. The campaign targets organizations in the LATAM region, evades domain-based detections using Amazon EC2 instances, and employs various evasion techniques and encryption methods. The analysis reveals the presence of downloader modules, injector modules, and additional backdoors, each with a specific role in the infection chain. The campaign demonstrates evolving tactics and the adaptability of threat actors in compromising targeted systems.[v] |
| **New Ransomware Uses Sophos Branding in Attacks** | A new ransomware-as-a-service (RaaS) dubbed SophosEncrypt is actively impersonating the cyber security vendor Sophos. The ransomware encryptor, written in Rust, stands out from contemporary ransomware as it seems to have additional functionalities beyond simply file encryption. | It exhibits capabilities more akin to a general-purpose remote access trojan (RAT), including keystroke logging, system profiling with WMI commands, and the ability to communicate with the attacker via email and Jabber instant messenger. It can also change the Windows desktop wallpaper to display a seemingly legitimate Sophos brand, which is being impersonated by the threat actors. The ransomware avoids encrypting specific directories that could impede system booting or contain unimportant files. Additionally, it checks the language settings on the system and refuses to run if set to use the Russian language. Both samples of this ransomware connect to a command-and-control server address, though they reference a Tor (.onion) dark web address without establishing a Tor connection. One of the samples also contains a hardcoded IP address associated with previously observed Cobalt Strike and cryptominer activity.[vi] |
| **New Turla Backdoor Compromising Ukrainian MS Exchange Servers** | Ukraine's computer emergency response team, CERT-UA, is actively countering cyber threats, particularly targeted cyberattacks against defense forces for espionage purposes. They are monitoring activity related to the CAPIBAR malware, known as "DeliveryCheck" by Microsoft and "GAMEDAY" by Mandiant, using the UAC-0024 identifier since 2022. | CAPIBAR is notable for its server component, which is installed on compromised MS Exchange servers as a MOF file using the Desired State Configuration (DCS) PowerShell tool, effectively converting a legitimate server into a malware control center. The initial compromise involves sending macro documents via email or modifying legitimate documents to trigger PowerShell execution. During this stage, a complex multifunctional KAZUAR backdoor can be loaded onto affected computers. KAZUAR has over 40 functions, including launching JS using ChakraCore, obtaining data from OS logs, collecting artifacts, and stealing authentication data and application databases/configuration files. The activity associated with UAC-0024 and KAZUAR is believed to be the work of the Turla group (also known as UAC-0003, KRYPTON, Secret Blizzard), linked to the Russia's FSB.[vii] |

| | | |
|---|---|---|
| **Critical Vulnerability in Citrix NetScaler ADC Permits Remote Code Execution** | Citrix has issued an alert to its customers regarding a critical-severity vulnerability (CVE-2023-3519) in NetScaler ADC and NetScaler Gateway. This vulnerability is already being exploited in the wild, making it a serious threat. | The most severe vulnerability received a score of 9.8 out of 10 and allows attackers to execute code remotely without authentication. To be vulnerable, the affected appliance must be configured as a gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or an authentication virtual server (AAA server). Citrix strongly advises customers to update their NetScaler ADC and Gateway to newer versions that address the issue. Earlier in July, a zero-day vulnerability for Citrix ADC was advertised on a hacker forum, which may be related to the current security issue. Active exploitation of this vulnerability was expected until Citrix released a fix. The updates also include fixes for two other vulnerabilities, CVE-2023-3466 and CVE-2023-3467, which have high severity scores. CVE-2023-3466 is a reflected cross-site scripting (XSS) issue, while CVE-2023-3467 allows an attacker to escalate privileges to those of a root administrator (nsroot). Currently the only way to resolve this issue is to patch NetScaler to current versions and retire any NetScaler ADC instances that are past their end of life (EOL) date.[viii] |
| **New Malware Abusing Ads to Target Users Seeking IT Tools** | A new initial-access malware campaign called Nitrogen has been observed, utilizing malvertising and impersonating legitimate software to compromise business networks. The campaign targets users seeking specific IT tools through Google and Bing ads, aiming to gain access to enterprise environments to deploy second-stage attack tools like Cobalt Strike. | The Nitrogen campaign has been observed targeting organizations in the technology and non-profit sectors in North America. Although the infections were mitigated before further damage, there is a concern that the threat actors may use this infection chain to stage compromised environments for ransomware deployment. The campaign involves a new initial access malware family called Nitrogen, related to the Metasploit Framework (MSF), which is used to generate reverse shell scripts for Nitrogen Stager. Threat actors use various techniques to mask their activity, making comprehensive and robust detection solutions essential. To protect against such campaigns, users are advised to be cautious of served advertisements from search engines and consider using ad-blocking extensions. Restricting virtual file system capabilities via Group Policy Objects (GPO) and being cautious of downloading abnormal file extensions can also enhance security. Users should avoid storing credentials in the Registry and regularly search for credentials in the Registry to mitigate potential risks. Overall, this campaign serves as a reminder for organizations to remain vigilant and employ proactive security measures to defend against sophisticated initial-access attacks.[ix] |

# Threat Actor Campaigns

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

| Threat Actors | Activity Summary |
|---|---|
| **Mustang Panda Deploying Modified PlugX Dubbed 'SmugX'** | Check Point Research recently provided details of a campaign conducted by the Chinese state-aligned MUSTANG PANDA group, which has been targeting governments in Eastern Europe since at least December 2022. The group has switched tactics, using a modified version of the venerable PlugX remote access trojan delivered via a so-called HTML smuggling attack, resulting in low detections. HTML smuggling in and of itself is hardly a new technique, though MUSTANG PANDA has not been observed utilizing it before. Analysis of the intended targets not only points to Europe as the primary target but also reveals the group's intent. Ukraine, Hungary, Slovakia, Czechia, and the United Kingdom are all prominently targeted, strongly suggesting that MUSTANG PANDA is conducting espionage for political purposes regarding the Russo-Ukrainian War. That this campaign started and has continued for the past seven months is no surprise either, as the war has accelerated in intensity over the winter of 2022-2023. Analysis of the lures found that the group has included pixel tracking in their lures, permitting them to monitor basic interactions with their lure documents. The technique is simple but effective. The attackers are likely using this to determine the efficacy of their spear phishing. The attackers were also observed removing their malware from at least one infected system, not only suggesting active monitoring of a compromised system but a desire to remain hidden.[x] |
| **Charming Kitten Conducting Espionage with New PowerShell, Mac Malware** | A recent espionage campaign conducted by the Iranian state-aligned Charming Kitten group (aka APT42, TA453) was observed by Proofpoint in May 2023 targeting nuclear security and foreign policy experts, as well as think tanks with a new PowerShell-based backdoor dubbed GorjolEcho. The initial stages of this attack were observed to be a change in tactics for Charming Kitten, switching from VBA macros and remote template injection to archive files hosted on cloud storage sites containing malicious LNK files. While not novel, it is certainly an effective strategy, as blocking cloud storage sites such as Dropbox has proven to be untenable in corporate environments. The malware itself is a unique PowerShell-based backdoor, though, in at least one instance, Charming Kitten was unable to compromise a target's machine due to their target utilizing MacOS. Within a week, the attackers had ported their malware to MacOS (dubbed NokNok) to solve this problem and attempted exploitation again utilizing the same infection chain.[xi] |
| **New Storm-0558 Group Exploiting Cloud Services for Espionage** | Beginning in May 2023, a Chinese state-linked group, dubbed Storm-0558 by Microsoft, initiated a complicated series of exploits to gain access to Microsoft-hosted Outlook Web Access in Exchange Online email accounts via forged authentication tokens. The tokens were forged using a stolen MSA key, which permitted Storm-0558 attackers the ability to exploit a token validation issue and impersonate Azure AD users, thus permitting access to enterprise mail. Precisely how the MSA key was acquired by Storm-0558 is currently unknown, as is the full scope and scale of the compromise. The only reliable way to detect this attack would be to monitor for any anomalies in login activity, e.g., logins at unusual times, from unusual devices, at unusual locations. This is predicated on having such logs available to begin with, which is often a low priority for many organizations and, in the case of Outlook Web Access and ancillary services such as Outlook.com, is only visible to Microsoft.[xii] |
| **APT29 Shifting to Personally Targeted Attacks on Ukrainian Diplomats** | APT29, a group of hackers associated with Russia's Foreign Intelligence Service (SVR), has been observed targeting diplomatic missions globally in a new campaign. Their primary method of attack has been through phishing lures related to diplomatic operations, such as government communications, embassy updates, diplomat schedules, and event invitations. However, recent observations indicate a shift in their tactics, with a focus on targeting diplomats themselves rather than the embassies or other government entities. APT29 has also been observed targeting diplomatic missions in Ukraine by exploiting the need for vehicles among recently placed diplomats; 22 out |

| | |
|---|---|
| | of over 80 foreign missions in Kyiv were targeted, indicating a significant and highly targeted operation. The evidence pointing to APT29's responsibility includes similarities to their previous campaigns, the use of their known tactics, and code similarities with previous malware used in APT29-linked operations. The new approach of targeting individuals increases the likelihood of successful compromises within organizations. These lures have broader applicability and are more likely to be forwarded within diplomatic communities and organizations, expanding the range of potential targets. Given the Russian invasion of Ukraine and the importance of intelligence on Ukraine and its allies, diplomatic missions remain high-value targets for espionage.[xiii] |
| **FIN8 Utilizing BlackCat Ransomware** | The financially motivated cybercrime gang known as FIN8 (also called Syssphinx) has been observed using a revamped version of the Sardonic malware to deploy BlackCat ransomware payloads on backdoored networks. FIN8 has been active since at least January 2016, targeting industries such as retail, restaurants, hospitality, healthcare, and entertainment. They are known for large-scale, sporadic campaigns and have impacted numerous organizations. Recently, FIN8 switched from using BADHATCH to a C++-based backdoor called Sardonic. However, a newer version of this backdoor was observed in December 2022 attacks, showing significant code rewriting to avoid detection and similarities with previously disclosed details. Despite the changes in the backdoor, FIN8's known techniques were still employed. While FIN8's main goal has been stealing payment card data from Point-of-Sale (POS) systems, they have expanded their attacks to include ransomware deployment to increase profits. In June 2021, they were seen deploying Ragnar Locker ransomware on a financial services company's compromised systems in the United States. Later, in January 2022, White Rabbit ransomware was also linked to FIN8, further solidifying their involvement. More recently, Symantec spotted FIN8 using BlackCat (also known as ALPHV) ransomware in December 2022 attacks alongside the new Sardonic malware variant. Symantec emphasizes that FIN8 continues to develop and refine its capabilities and malware delivery infrastructure to evade detection, demonstrating the threat actors' determination to maximize profits from their victims.[xiv] |

# Dark Web Markets

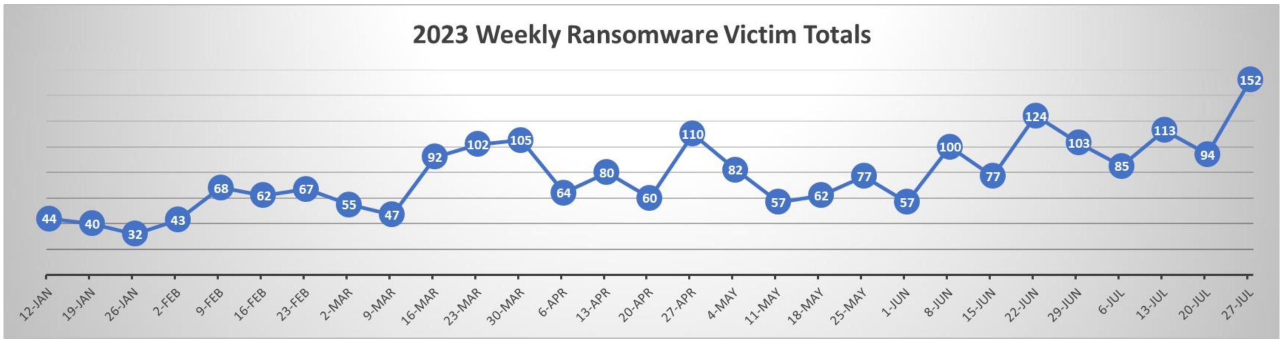
**High-profile ransomware data dumps and dark web access sales identified in last thirty days.**

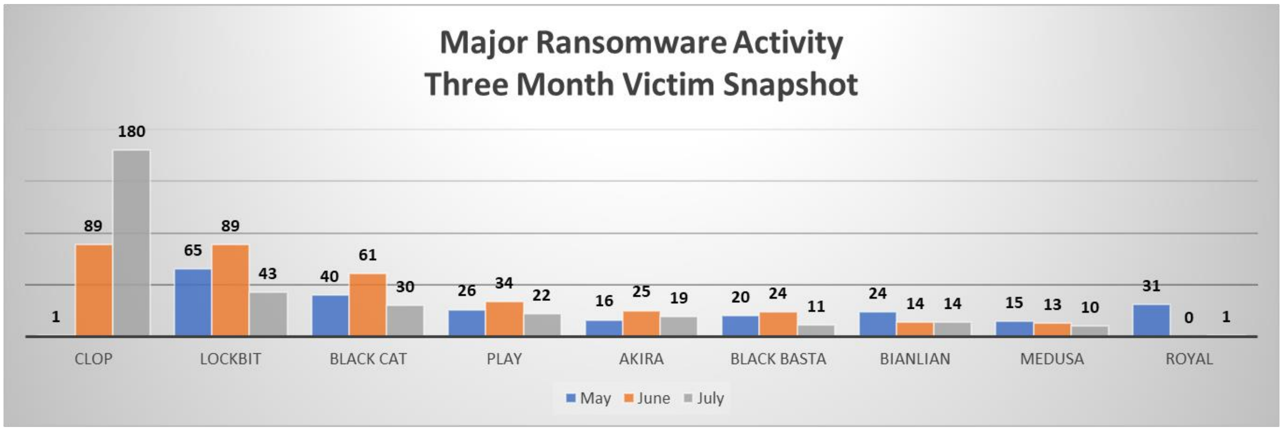
| Activity | Note |
|---|---|
| **Actor Developments** | An access seller on multiple top-tier Russian language criminal forums set up their own Onion website to sell compromised companies on Tor hidden services. The site had 48 accesses for sale to start and has sold 12 of them so far. They claim that all accesses are domain admin accesses. The standard starting price per access is BTC 0.5 (~USD 15,000) and is negotiable. Information given for each victim includes country, revenue, industry vertical, and number of hosts and users on the network. Only two victims – the China-based airline Air Macau and the Danbury, Connecticut, school district – could be identified with any degree of certainty |
| **Access Sale** | An actor on a prominent Russian-language crime forum is selling FTP access to what they claim are 25 million health records belonging to a U.S. company with USD 55 billion in revenue for USD 9,000. They did not share proof of access, and there is no evidence they have made the sale. |
| **Access Sale** | An actor on two prominent Russian language crime forums is selling Citrix/file transfer access to a German internet service provider with USD 519 million in revenue for USD 500. Additionally, a different access seller is selling access to an entity in the department store/shopping center/superstore/retail vertical with USD 17.4 billion in revenue for USD 1,000. |
| **Access Sale** | On 12 June, a likely ransomware affiliate on a popular Russian-language criminal forum was selling access to what they claimed was a Bangladeshi bank for USD 30,000, stating they were not interested in exploiting the access. At the same time, the BlackCat ransomware group claimed the Bangladeshi Krishi Bank as a victim. Assuming Krishi Bank was the same access being sold, there are three possibilities: they successfully sold the access to another ransomware team; they failed to sell the access and exploited it themselves confirming that they are a member of the BlackCat ransomware team; or it is pure coincidence and Krishi Bank has been attacked by multiple actors. |
| **Data Sale** | An actor on a Russian-language crime forum offered for sale 193 Cisco AnyConnect credentials belonging to employees of an unidentified U.S. based software company with USD 1.9 billion in revenue, 6,500 employees and a stock listing for USD 3,000. |
| **Access Sale** | An actor on a crime forum offered to sell access to a U.K.-based company with around USD 4 billion in revenue and 18,000 employees for USD 4,000-9,000, depending on whether he had domain admin access or not (they were unsure). They then subsequently lost access. |
| **Access Sale** | An actor on a Russian-language crime forum was selling access to the network attached storage and email systems belonging to an unidentified enterprise located “somewhere in southern Asia” with USD 10 billion in revenue for USD 5,000. The seller has nine successful access sales on the forum and is likely credible. |
| **Tool Sale** | An actor on a popular Russian-language crime forum was selling what they claimed was a SharePoint pre-auth remote code execution (CVE-2023-29357 and CVE-2023-24954) vulnerability for USD 20,000. They were also selling a local privilege escalation (LPE) for CVE-2023-29360 elevating user privileges to system for USD 8,000. They noted that these vulnerabilities were patched on 13 June. |
| **Access Sale** | An actor on a crime forum was selling RDP local admin access to a Canada-based enterprise with approximately USD 3.1 billion in revenue for USD 6,500. Based on the description there were numerous credible candidates for the victim in the financial, petrochemical, healthcare, and public utilities sectors. |
| **Access Sale** | An actor on multiple crime forums was advertising access to a real estate company with USD 1.2 billion in revenue, and successfully sold access to a different real estate company with USD 3 billion in revenue. Both companies remain unidentified. |

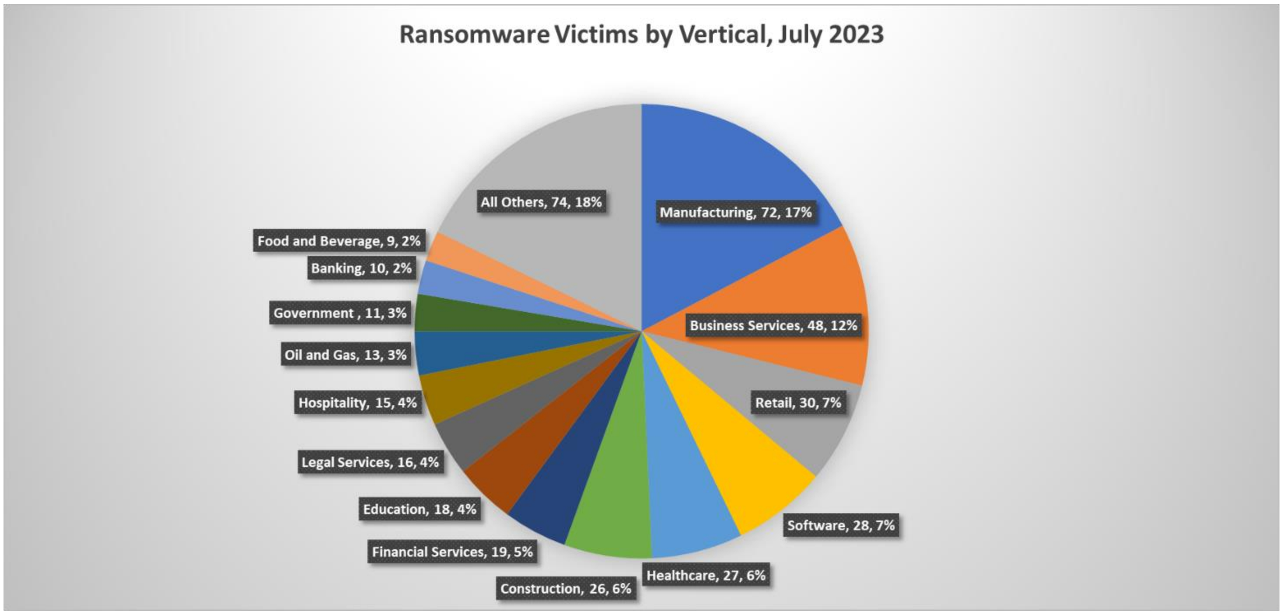
| | |
|---|---|
| **Access Sale** | An actor on a prominent crime forum advertised web shell access to a Linux server belonging to a construction company with more than USD 5 billion in revenue in the United Arab Emirates. There are more than six companies matching that description in the emirate of Dubai alone. |
| **Access Sale** | An actor on a prominent Russian-language crime forum was selling RDP local admin access to a Dominican Republic-based retailer in the gas station and convenience store vertical with 1,300 employees and USD 190 million in revenue. |
| **Access Sale** | An actor on a Russian-language crime forum offered for sale access to the private GitHub projects page for restaurant management and meal delivery app ChowNow. They claimed to identify multiple vulnerabilities in ChowNow thanks to their access. |
| **Tool Sale** | An actor on multiple crime forums advertised what they called WormGPT – a ChatGPT alternative for black hat actors. As an example of the capability, they posted a screenshot of a malicious Python script written by WormGPT. A license costs EUR 100 for one month, or EUR 550 for a year, or EUR 5,000 for a private build of the model. |
| **Tool Sale** | A respected actor on a premier Russian crime forum released a new attack framework in June that has received favorable reviews from the forum administration and appears to be gaining popularity. The framework dubbed **DarkGate Loader** is designed to target cryptocurrency wallets but looks like it could delivery just about any payload. The licensing rate is USD 1,000/day, USD 15,000/month, or USD 100,000/year. |
| **Tool Sale** | An actor on a popular public crime forum is selling a 0/1-Day in an unnamed VPN/firewall/router device that they claim is already known and circulating, but does not yet have a CVE assigned and is without fixes. They claim there are 20,000 devices vulnerable to this RCE on Shodan. |
| **Access Sale** | An actor on a popular Russian-language crime forum is selling access to a prominent France-based software company for a buy now price of USD 20,000, access to the S3 instance and 410 TB of data belonging to a major medical device manufacturing giant for a buy now price of USD 20,000, and admin access with full rights to 22,100 hosts belonging to a Switzerland-based energy company for a buy now price of USD 20,000. Two long time ransomware actors are engaged in a bidding war for the latter. |
| **Access Sale** | An actor on a Russian-language crime forum likely sold access to an unidentified U.S. based company with around 5,000 hosts and USD 2.3 billion in revenue to a likely ransomware actor for USD 16,000. The same actor also had a U.K. based auction house in operation since the 1700s and with USD 6 billion in revenue on sale for around USD 120,000. |
| **Access Sale** | An actor on a Russian-language crime forum is selling access to what they claim is an industrial automation company that provides services to the automobile industry. Access to the company, based in western Europe, is up for sale for USD 5,000. |
| **Access Sale** | An actor on a Russian-language crime forum was selling domain admin access to a U.K. National Health System hospital with 4,000 hosts on the network for USD 10,000. |
| **Access Sale** | An actor on a Russian-language crime forum was selling local network access and root shell on the mail server for an unnamed African fintech mobile payments app with 10 million Android downloads, 35 million users, and USD 50 million in revenue for USD 10,000. |

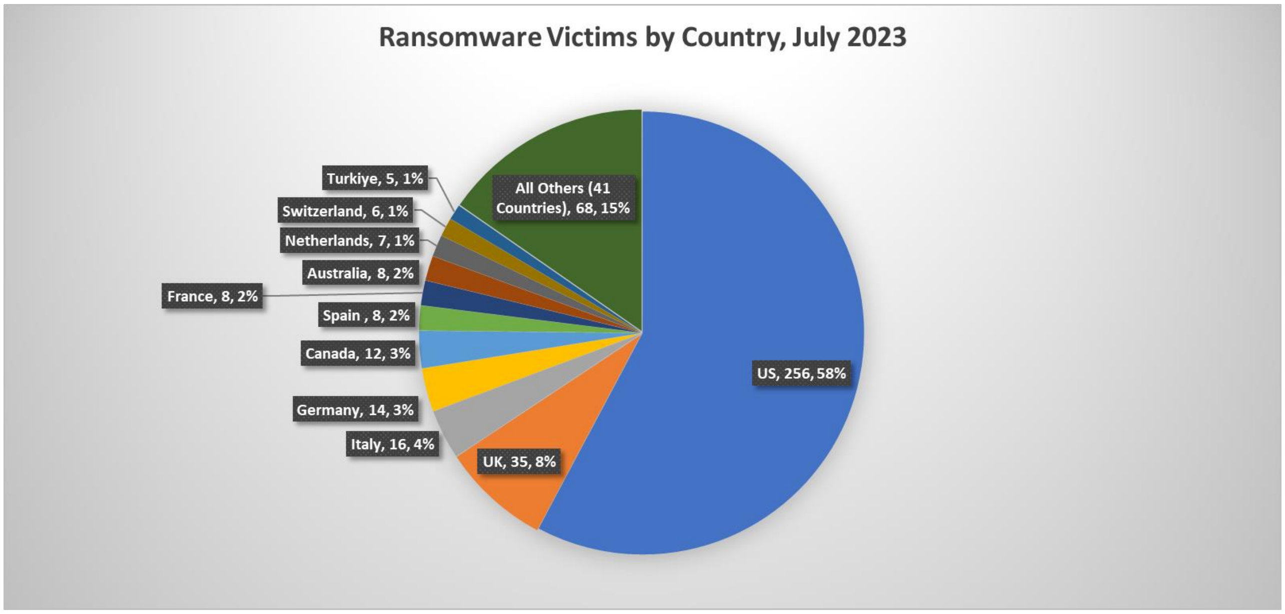
# By The Numbers

Summarizing incidents in graphical format


2023 Weekly Ransomware Victim Totals


Major Ransomware Activity
Three Month Victim Snapshot


Ransomware Victims by Vertical, July 2023



Ransomware Victims by Country, July 2023

[i] https://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/microsoft-zeroday-exploit

[ii] https://jumpcloud.com/blog/security-update-incident-details

[iii] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-201a

[iv] https://www.bleepingcomputer.com/news/security/ivanti-patches-mobileiron-zero-day-bug-exploited-in-attacks/, https://www.bleepingcomputer.com/news/security/norway-says-ivanti-zero-day-was-used-to-hack-govt-it-systems/, https://www.bleepingcomputer.com/news/security/cisa-warns-govt-agencies-to-patch-ivanti-bug-exploited-in-attacks/

[v] https://www.zscaler.com/blogs/security-research/toitoin-trojan-analyzing-new-multi-stage-attack-targeting-latam-region

[vi] https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/

[vii] https://twitter.com/msftsecintel/status/1681695399084539908, https://cert.gov.ua/article/5213167, https://malpedia.caad.fkie.fraunhofer.de/details/win.delivery_check

[viii] https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467

[ix] https://news.sophos.com/en-us/2023/07/26/into-the-tank-with-nitrogen/

[x] https://research.checkpoint.com/2023/chinese-threat-actors-targeting-europe-in-smugx-campaign/

[xi] https://www.proofpoint.com/us/blog/threat-insight/welcome-new-york-exploring-ta453s-foray-lnks-and-mac-malware

[xii] https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/

[xiii] https://unit42.paloaltonetworks.com/cloaked-ursa-phishing/

[xiv] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/Syssphinx-FIN8-backdoor