Monthly Threat Intelligence Rollup

DEEP seas

04/04/23-05/01/23

Notable Cyberattacks

Summary of noteworthy cyberattacks in the last thirty days.

Incident	Activity Summary
FBI Arrests 119 in Genesis Market Takedown Dubbed "Operation Cookie Monster"	Genesis Market, an illegal online marketplace that sold stolen credentials associated with email, bank accounts, and social media platforms, has been dismantled by a coordinated international law enforcement operation which resulted in 119 arrests and 208 property searches in 13 countries.[i] The marketplace had evolved into a major hub for criminal activities, offering access to data stolen from over 1.5 million compromised computers across the world, totaling more than 80 million credentials and serving as one of the largest access brokers for cybercriminals worldwide according to the US DOJ. Genesis Market's takedown is expected to have a "ripple effect throughout the underground economy" as threat actors search for alternatives. Meanwhile, a new dark web marketplace called STYX has emerged offering similar illegal services and is likely to become the next one-stop shop for cybercriminals seeking to purchase access to victim networks.
New CrossLock Ransomware Gang Leading with Golang-Based Ransomware	Cyble has recently identified an up-and-coming ransomware group using the name CrossLock.[ii] The group's signature malware, dubbed CrossLock, is written in the Go programming language, giving the group cross-platform capabilities and enhanced malware analysis obfuscation. The use of the Go programming language for ransomware is a relatively uncommon technique seeing wider adoption by ransomware authors as of 2021. As of 16 April, CrossLock has claimed one organization according to review of their extortion website.
FIN7 Group Exploiting Veeam Vulnerabilities	In a series of recent attacks, the Russian FIN7 cybercriminal group was identified exploiting CVE-2023-27532, a vulnerability with a severity score of 7.5, and permitting an attacker unauthenticated access to a Veeam Backup & Replication instance.[iii] Though this vulnerability was patched in March 2023, proof of concept code emerged two weeks after Veeam released a patch, and probing attacks began shortly thereafter. Some debate remains whether these attacks were the work of FIN7 or a criminal utilizing FIN7's tactics; the use of POWERTRASH and DICELOADER are not conclusive proof of FIN7 claim some researchers. Given FIN7's broad scope of activities and ability to rapidly diversify their capabilities, the attribution of these attacks is likely correct. Fortunately, the attackers were unable to carry out any further malicious activities after being detected and blocked.

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 Rorschach Ransomware Malware Family	Check Point Research discovered a new strain of ransomware this week dubbed "Rorschach."[iv] Rorschach appears to be unique, with no similarities to known ransomware strains, and has no branding or affiliation with known ransomware groups.	The ransomware is partly automated and highly customizable, with unique features such as the use of direct syscalls. It is also one of the fastest encrypting ransomware strains observed due to its implementation methods. Rorschach was observed being deployed using DLL side-loading of a Cortex XDR Dump Service Tool, a loading method not commonly used for ransomware. Check Point claims the Rorschach operators combined the best features from leading ransomware strains and is highly customizable. The identity of the operators and developers of Rorschach is unknown.
New 'Money Message' Ransomware Group	Cyble Research and Intelligence Labs (CRIL) has identified a new ransomware group called Money Message that has been observed targeting both Windows and Linux operating systems and uses admin credentials to access network resources.[v] The group is suspected of leveraging infostealer logs to launch their operations.	Money Message uses a double extortion technique where they exfiltrate data before encrypting and uploading it to their leak site if the ransom is not paid. The group has impacted at least five known victims, mainly from the United States and belonging to different industries, including banking, financial services, and insurance (BFSI), transportation and logistics, and professional services.
Mobile Malware Developer Linked to Android and iOS Spy Agent	Microsoft and Citizen Lab have discovered that an Israel-based company named QuaDream used a zero-click exploit called ENDOFDAYS to compromise iPhones belonging to individuals of interest.[vi]	The attackers exploited a zero-day vulnerability in iPhones running iOS 14.4.2 and earlier versions, using backdated and invisible iCloud calendar invitations. The ENDOFDAYS exploit ran without user interaction and allowed the attacks to be undetectable by the targets. At least five civil society victims of QuaDream's spyware and exploits were identified in North America, Central Asia, Southeast Asia, Europe, and the Middle East, including journalists, political opposition figures, and an NGO worker. The surveillance malware, dubbed KingsPawn, was designed to self-delete and remove evidence of itself from victims' iPhones to evade detection.
New FIN7 'Domino' Backdoor Malware Identified	IBM researchers have discovered new malware being utilized by the Russian FIN7 cybercriminal group which may have been developed by former Conti ransomware developers; alternatively leaked Conti source code may have been used by the developers.[vii]	IBM identified the new FIN7 backdoor dubbed "Domino" in February 2023 while investigating intrusions that included the use of the Conti-affiliated "Dave" backdoor. Domino overlaps closely with Lizar, a malware family previously attributed to FIN7. IBM postulates that former Conti members are also likely involved in these infections due to the use of Dave backdoor, which was attributed to the Conti/Trickbot gang in May of 2022. Further complicating attribution is the overlap between FIN7 and Conti, strongly suggesting a nexus of activity with multiple workflows supporting FIN7 operations. Dave is also known to be used by other former Conti members now working with the Quantum, Royal, BlackBasta, and Zeon ransomware groups. Since Conti's separation in mid-2022, former members and

		developers have been identified in new gangs but are likely still collaborating on old and new tools.
Play Ransomware Group Deploys New Grixba Malware, VSS Copying Tool	Symantec has identified two custom tools developed by the Play Ransomware group (also known as PlayCrypt or Balloonfly).[viii]	The first, named Grixba, is an infostealer and network-scanning tool which is used to enumerate software and services via Windows Management Instrumentation (WMI), Windows Remote Management (WinRM), Remote Registry, and Remote Services. The tool then checks for the existence of various antivirus and endpoint security software solutions, backup software, remote administration tools, and various other software before exfiltrating stolen data back to Play Ransomware. The second tool, named "VSS Copying Tool," enumerates files and folders in a VSS snapshot, then copies the files on the VSS volumes from compromised devices prior to encryption, thus defeating Windows protections against this activity. Play Ransomware is typical of modern ransomware groups, where attackers exfiltrate data from victim networks before encrypting them, thus these tools are typical for their profile. While Play Ransomware has previously focused on organizations in Latin America, it has begun widening its scope to new areas.

Threat Actor Campaigns

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

Threat Actors	Activity Summary
New RedGolf Infrastructure Identified	Recorded Future's Insikt Group has identified new operational infrastructure associated with custom Windows and Linux backdoor KEYPLUG, attributed to the threat activity group RedGolf.[ix] It is highly likely that RedGolf is a Chinese state-sponsored group that has carried out state-sponsored espionage activity in parallel with financially motivated operations for personal gain since at least 2014. RedGolf has been observed targeting and spying on a wide range of industry verticals, targeting aviation, automotive, education, government, media, information technology, and religious organizations. Organizations whose products or activities may be of strategic interest to the Chinese government and security services are at increased risk of targeting. RedGolf overlaps with threat activity reported under the aliases APT41/BARIUM, and a 2020 DOJ indictment states that a RedGolf-associated threat actor boasted of connections to the Chinese Ministry of State Security (MSS).
MERCURY and DEV-1084 Attack and Destroy On-Premises and Hybrid Environments	Microsoft Threat Intelligence has identified destructive operations carried out by MERCURY, a nation-state actor linked to the Iranian government, which attacked both on-premises and cloud environments.[x] Despite the threat actors attempting to pass the activity off as a standard ransomware extortion campaign, the attackers' end goal remains data destruction and disruption. The impact of the attack included the destruction of cloud resources, which is a new development in MERCURY's previous tactics of conducting attacks against target assets on-premises. Microsoft believes that MERCURY worked in partnership with another actor, DEV-1084, to carry out the destructive actions. The attack investigated by Microsoft likely exploited known vulnerabilities in unpatched applications for initial access before moving laterally throughout the network.

New MuddyWater Infrastructure and TTPs	Group-IB has identified new MuddyWater infrastructure, as well as the malicious use of legitimate remote tools including ScreenConnect, Remote Utilities, and Synco during intrusions on Israeli and Egyptian insurance, manufacturing, and telecommunications companies.[xi] MuddyWater has been attributed to Iran's Intelligence Ministry by the US Congressional Research Service. Historically, MuddyWater has targeted military, telecommunications, manufacturing, education, and oil and gas companies in Turkey, Pakistan, UAE, Iraq, Israel, Saudi Arabia, Jordan, USA, Azerbaijan, and Afghanistan. According to Group-IB, MuddyWater has used the legitimate SimpleHelp software suite on at least eight of their newly discovered servers to evade detection and maintain persistence on compromised systems. Group-IB remains unsure what other follow-on payloads are being used in these campaigns. Initial access is likely gained via phishing campaigns linked to cloud storage that hosts SimpleHelp installers.
GALLIUM Group Deploying PingPull Malware Variant Against South Africa, Nepal	In early March 2023, Unit 42 researchers identified new activity by the Chinese state-aligned GALLIUM group, which Unit 42 calls Alloy Taurus, targeting the South African military.[xii] The targeting is in line with previously observed GALLIUM activity, as well as Chinese government priorities; the Nepalese connection involves organizations conducting long-term urban development projects in Nepal. Both are geopolitical concerns for Beijing. The PingPull malware is a known malware family utilized by GALLIUM, though the Linux variant identified in this attack is an interesting new development.
RustBucket Malware Expands Pyongyang's Malware Arsenal	A recently identified sample of malware dubbed 'RustBucket' has been loosely attributed to the North Korean state-aligned Bluenoroff group, a subgroup under the larger Lazarus Group that is thought to comprise Pyongyang's Reconnaissance General Bureau (RGB) spy agency.[xiii] Though the malware itself is rather pedestrian, permitting attackers to load additional payloads and carrying out C2 communications, it is intended for use on MacOS systems. MacOS malware is not rare, especially among state-aligned groups. The Vietnamese-aligned APT32 was notorious for developing highly capable and evasive malware for MacOS. RustBucket is part of a growing trend of MacOS malware among both state and cybercriminal actors. In this case however, the attackers were identified through a rookie mistake common to North Korean groups; reuse of previously identified command and control servers.

Dark Web Markets

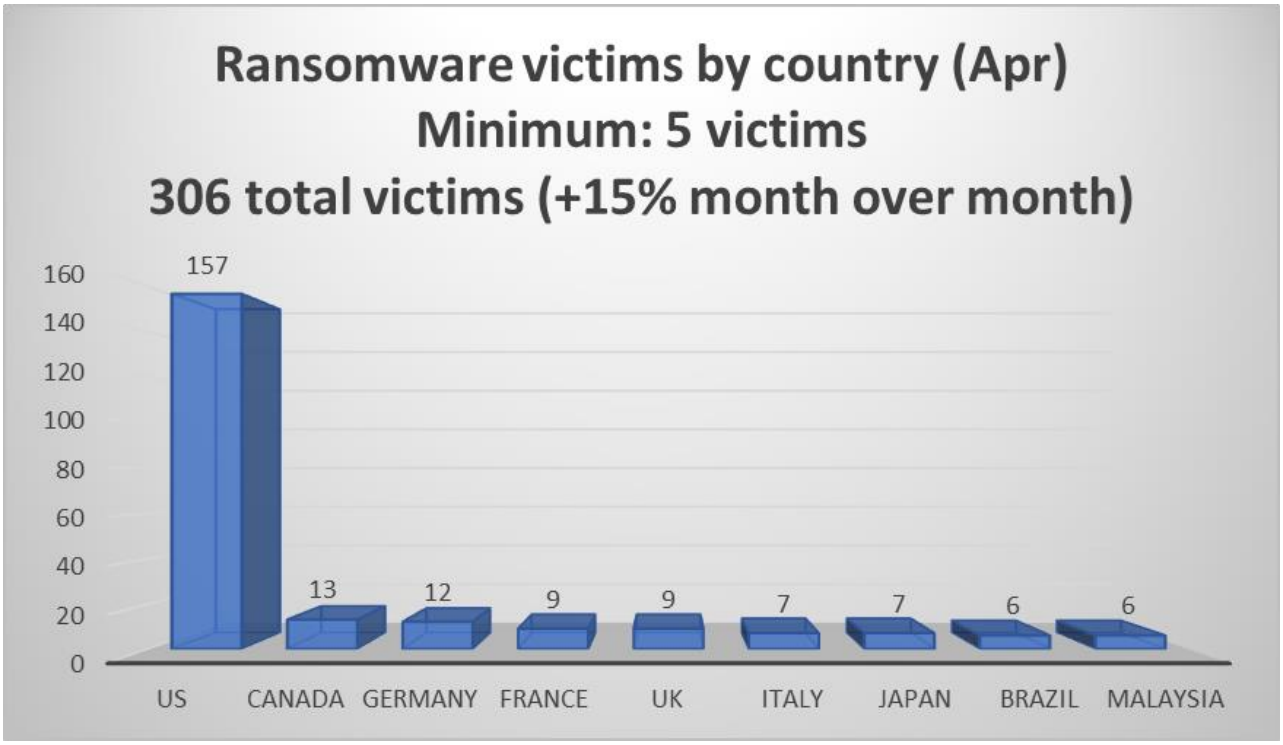
High-profile ransomware data dumps and dark web access sales identified in last thirty days.

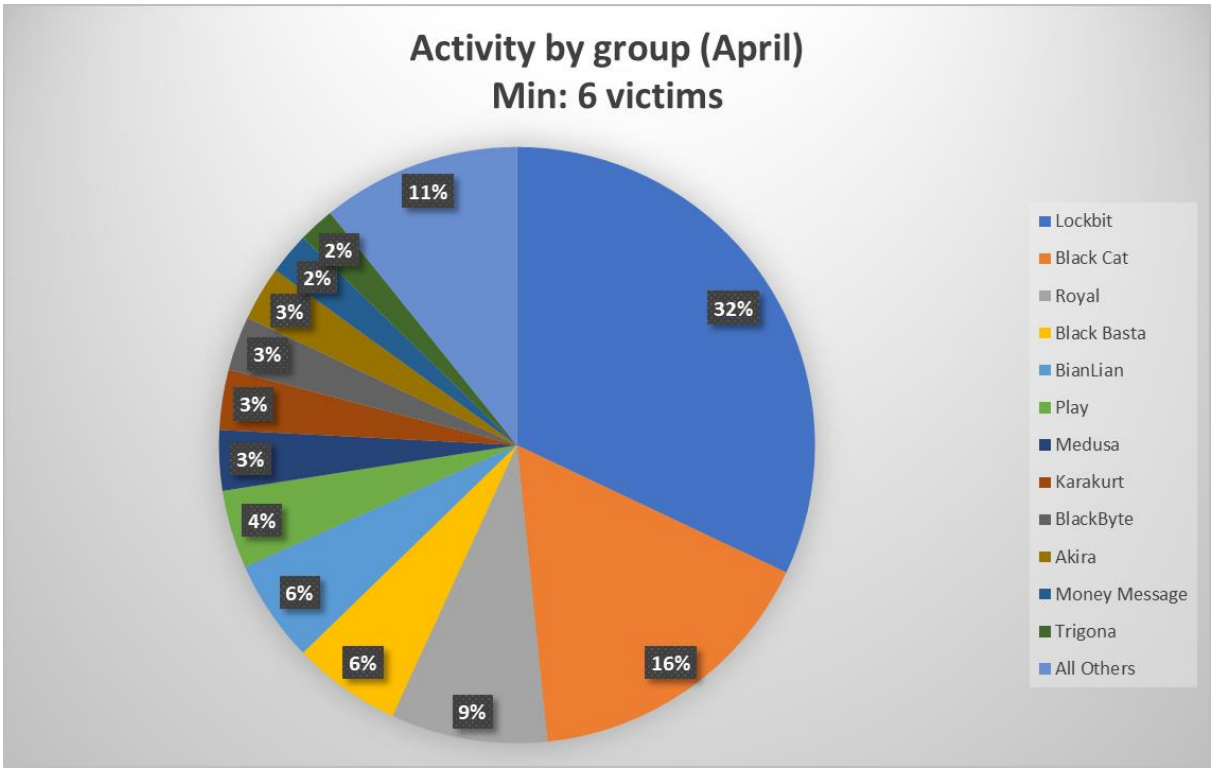
Activity	Note
Data Sale	An English-speaking actor on a public Russian language crime forum is selling caches of emails totaling more than 237,000 emails, with webmail access to dozens of victims for USD 7000. Some of the victims claimed by the actor included the California Department of Justice, the State of Wisconsin, the City of Baltimore, United Parcel Service (UPS), the City of San Antonio, and Oak Ridge National Laboratories (ORNL).
Data Sale	An English-speaking actor on a public Russian language crime forum is selling a package of items related to Equifax, including two Equifax certificate authority credentials, a valid Okta login, and FTP credentials for USD 750.
Tool Sale	An English-speaking actor on a prominent Russian language crime forum is selling a licensed version of Carbon Black for USD 350. He previously sold a licensed version of CrowdStrike Falcon. These are likely being utilized by actors to test their malware rather than hunting for vulnerabilities.
Access Sale	There were more than 40 companies for sale by initial access brokers in the Russian language crime forums, including nine with USD 1 billion or more in revenue. Some of the companies identified as potential victims included an unidentified UK based frozen food company with USD 1.2 billion in revenue, an unidentified Australian electronics manufacturer with USD 25.1 billion in revenue, the building materials manufacturer Masco Corporation (revenue USD 8.7 billion), Mexican outsourcing consulting company American Industries Group (revenue USD 2.9 billion), an unidentified electronics manufacturer that could be Zebra Technologies, Ricoh America, or Ohio-based data center manager Vertiv, Tennessee-based tool and die manufacturer Stamtec (revenue USD 407.4 million), and the Mississippi Department of Transportation.
Tool Sale	A criminal forum actor continues to sell licenses for EDRs, this time for Checkpoint Harmony EDR and Sophos EDR. The price is USD 350 each, or USD 600 for both. He wrote that these licenses are useful to malware developers to research evasion techniques.
Actor Developments	Pro-Russia hacktivist group KillMilk claimed they were teaming up with the developer of an infostealer called Titan Stealer, capable of stealing login passwords and browser cookies. Infostealers like Titan, such as Vidar or Redline, are used by many actors – including ransomware operators – to gain access to victims. They are also used to steal cryptocurrency wallets and consumer accounts to retailers, streaming services, and bank accounts. The incorporation of a stealer in KillMilk's arsenal suggests they may be pivoting to data stealing, or even destruction, and away from mostly ineffective DDoS attacks.

Access Sale	KillMilk also claimed to attack the European agency responsible for the safety of air navigation EUROCONTROL; however, judging from the activity as reflected by flight tracking apps, the attack appeared to be ineffective. KillMilk was also observed selling access to a small chain of Dunkin' Donuts franchises located in the upper east side of Manhattan, New York, for 1 BTC. It is unknown if they found a buyer.
Other Developments	Monti ransomware – a forked version of Conti ransomware described by the developer as "Conti on steroids" – is advertising for affiliates, hinting that there may be an uptick in Monti ransomware activity in the coming weeks. The operator announced that two of six available affiliate slots have been filled, and they are welcoming four more affiliates.
Other Developments	Russian Telegram news channels are reporting that the Russian Federal Security Service (FSB) are cracking down on local police officers who are selling the PII of Russian citizens to data brokers in criminal forums. In addition to PII, some officers are selling auto registration data, travel itineraries, passport data, and even security camera footage to data brokers in criminal forums. Western news organizations such as Bellingcat have used these illicit sources of data to identify Russian intelligence operatives in the West, as well as targeters in the Russian general staff who are coordinating the Russian bombing campaigns in Ukraine. The closures have raised concerns in the Russian language criminal forums, as several veteran actors have seemingly disappeared from the forums.
Data Sale	A criminal forum actor is selling what he claims is a "fresh from last week" 8.6 TB database of 300 million Kik users. In contravention of the rules, he did not specify a price and received a warning from the moderator. This product is different from what he usually sells; normally he is a well-regarded seller of stolen EV certificates.
Access Sale	A public criminal forum access actor is selling access to a Czech bank with USD 21 million in revenue. They claim to have access to two databases and to be able to modify currency exchange rates. No prices were named. ZoomInfo lists the Czech PPF Banka as having USD 21 million in revenue.
Data Sale	A criminal forum actor is selling 240 GB of data belonging to a Croatia based arms trader. They claim to have internal emails and documents and correspondence with the ministries of defense of six countries and with the ministries of internal affairs of three more countries. They set the buy now price as USD 5000.

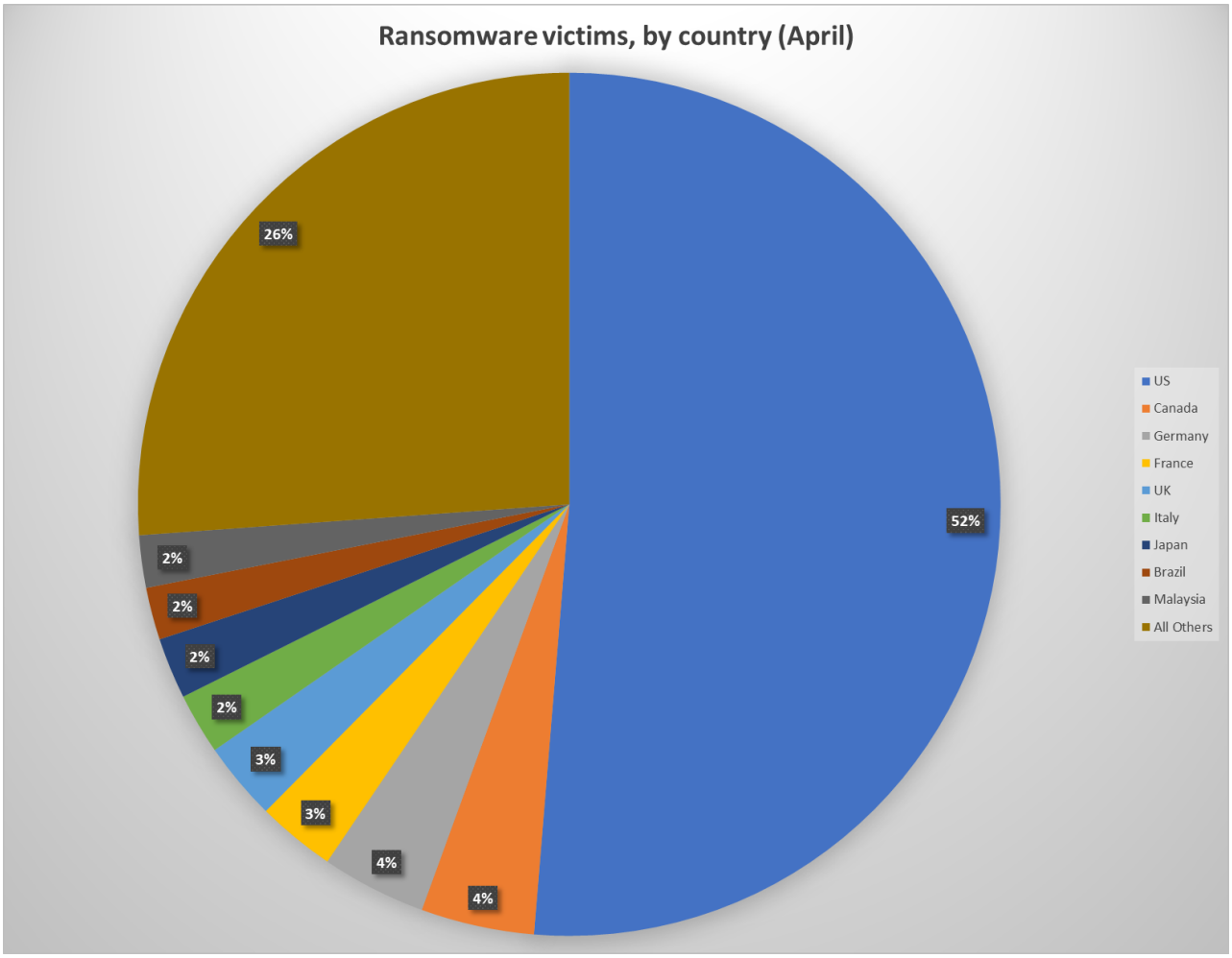
By The Numbers

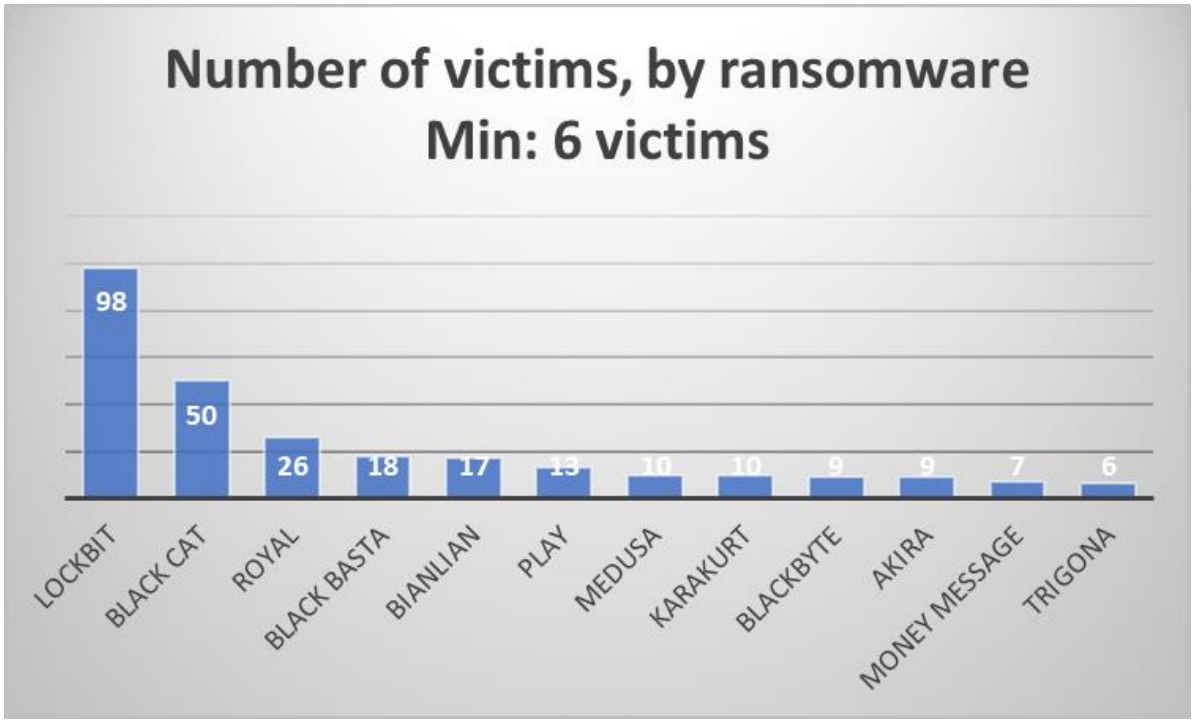
Summarizing incidents in graphical format



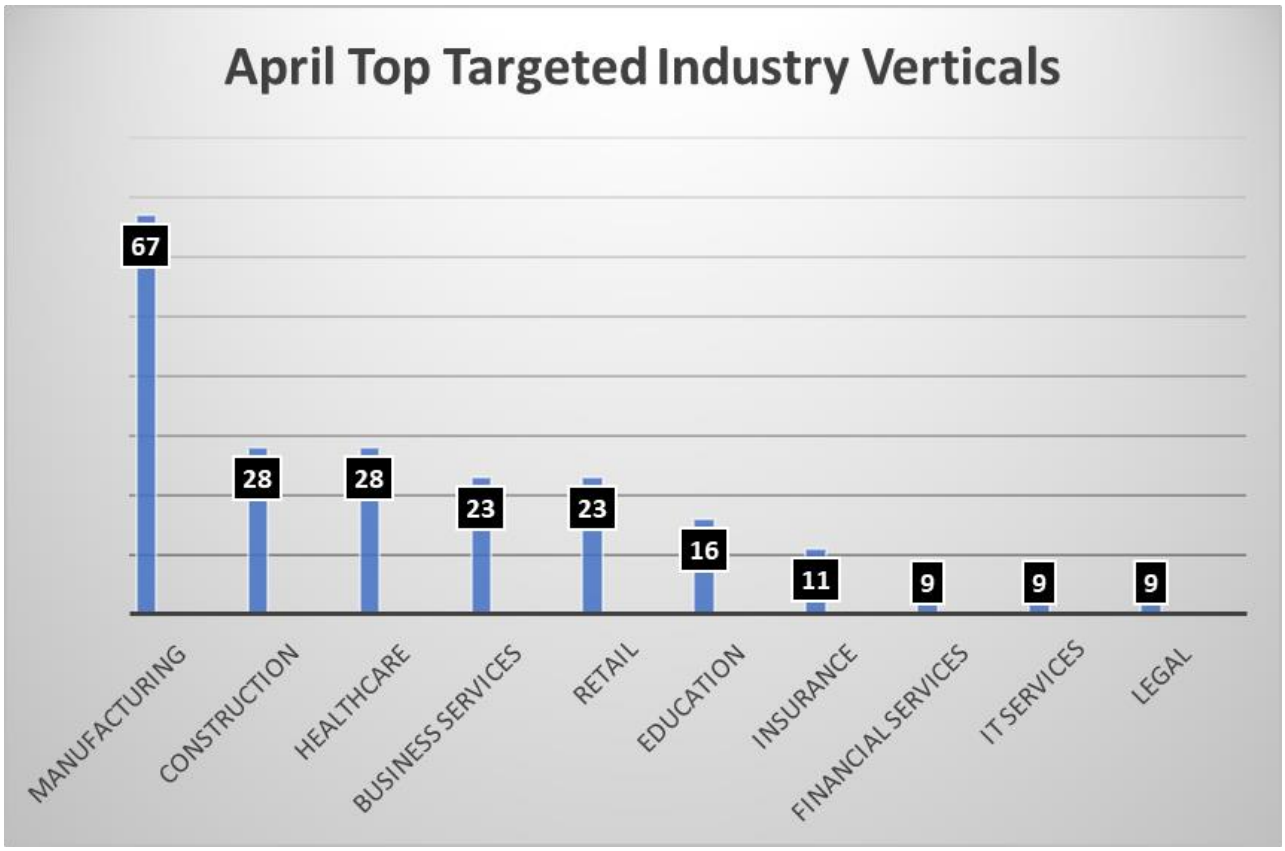


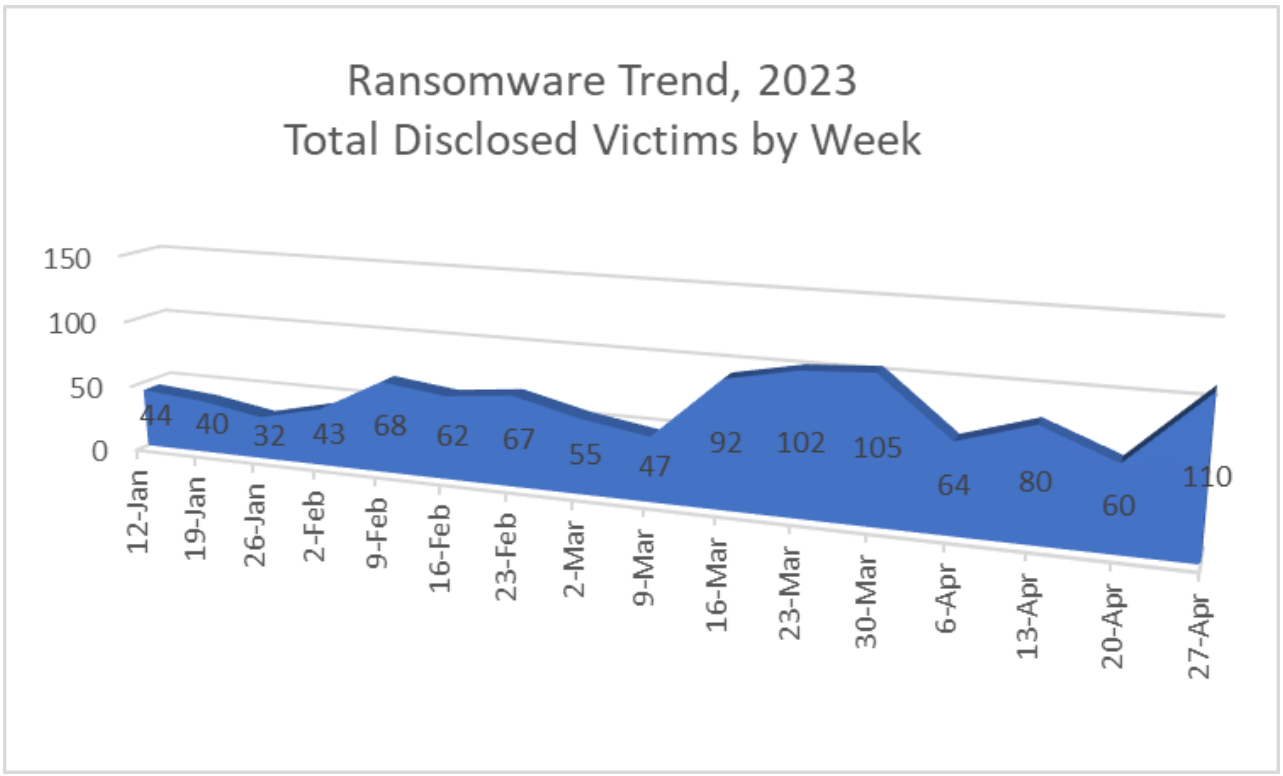
Explore more: deepseas.com





Explore more: deepseas.com





Explore more: deepseas.com

[i] https://thehackernews.com/2023/04/fbi-cracks-down-on-genesis-market-119.html
[ii] https://blog.cyble.com/2023/04/18/crosslock-ransomware-emerges-new-golang-based-malware-on-the-horizon/
[iii] https://labs.withsecure.com/publications/fin7-target-veeam-servers
[iv] https://research.checkpoint.com/2023/rorschach-a-new-sophisticated-and-fast-ransomware/
[v] https://blog.cyble.com/2023/04/06/demystifying-money-message-ransomware/
[vi] https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/, https://www.microsoft.com/en-us/security/blog/2023/04/11/dev-0196-quadreams-kingspawn-malware-used-to-target-civil-society-in-europe-north-america-the-middle-east-and-southeast-asia/
[vii] https://securityintelligence.com/posts/ex-conti-fin7-actors-collaborate-new-domino-backdoor/
[viii] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/play-ransomware-volume-shadow-copy
[ix] https://go.recordedfuture.com/hubfs/reports/cta-2023-0330.pdf
[x] https://www.microsoft.com/en-us/security/blog/2023/04/07/mercury-and-dev-1084-destructive-attack-on-hybrid-environment/
[xi] https://www.group-ib.com/blog/muddywater-infrastructure/
[xii] https://unit42.paloaltonetworks.com/alloy-taurus/#
[xiii] https://www.jamf.com/blog/bluenoroff-apt-targets-macos-rustbucket-malware/