Securonix Threat Labs Monthly Intelligence Insights – September 2023

securonix.com/blog/securonix-threat-labs-monthly-intelligence-insights-september-2023/

Threat Research

SIEM

By Dheeraj Kumar, Ella Dragun, Securonix Threat Labs

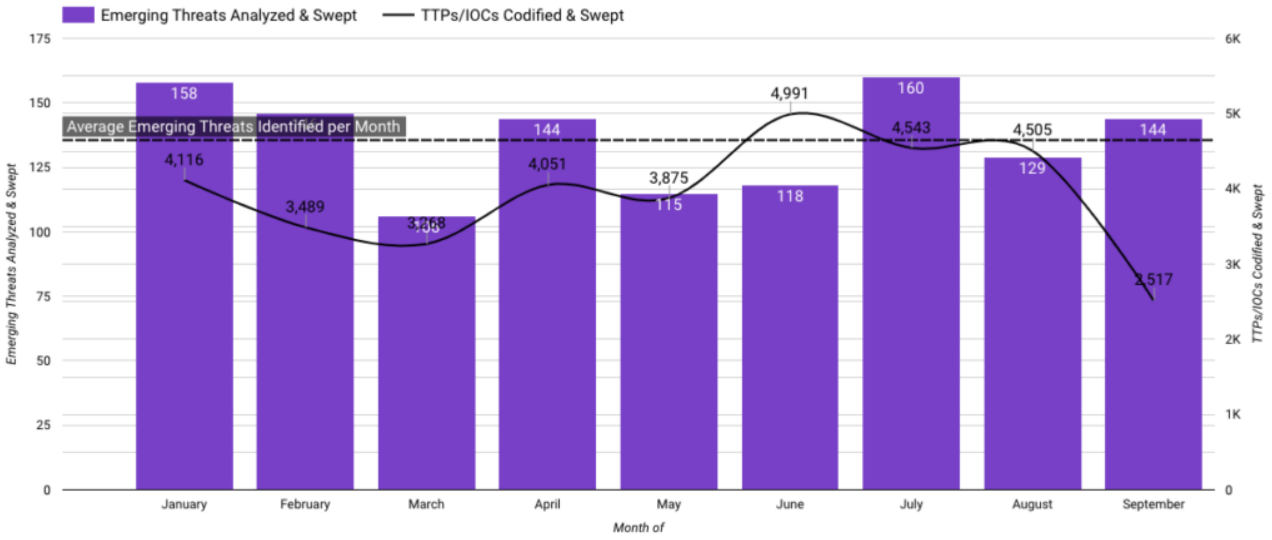
The Monthly Intelligence Insights provides a summary of top threats curated, monitored, and analyzed by Securonix Threat Labs in September. The report additionally provides a synopsis of the threats; indicators of compromise (IoCs); tactics, techniques, and procedures (TTPs); and related tags. Each threat has a comprehensive threat summary from Threat Labs and search queries from the Threat Research team. For additional information on Threat Labs and related search queries used via Autonomous Threat Sweeper to detect the below mentioned threats, refer to our Threat Labs home page.

In September 2023, Threat Labs analyzed and monitored major threat categories, including a brand-new ransomware family going by the name of 3AM. The ransomware is employed in a single attack by a ransomware affiliate that tried to install LockBit on a target's network but switched to 3AM after LockBit was blocked, according to Symantec researchers.

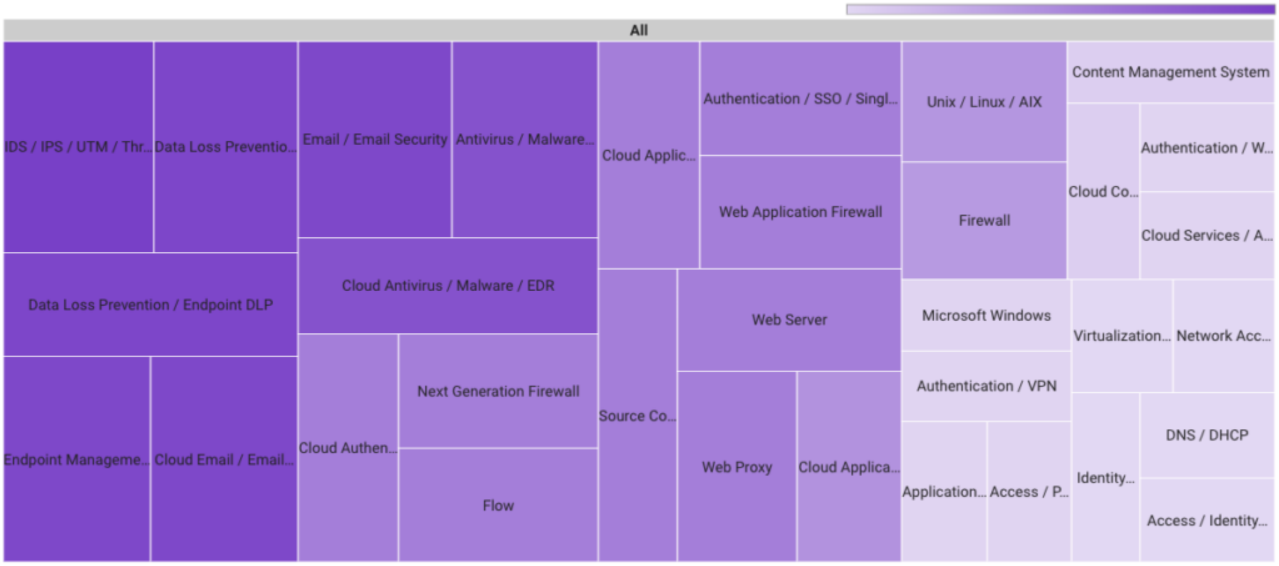
securonix Autonomous Threat Sweeper - September 2023

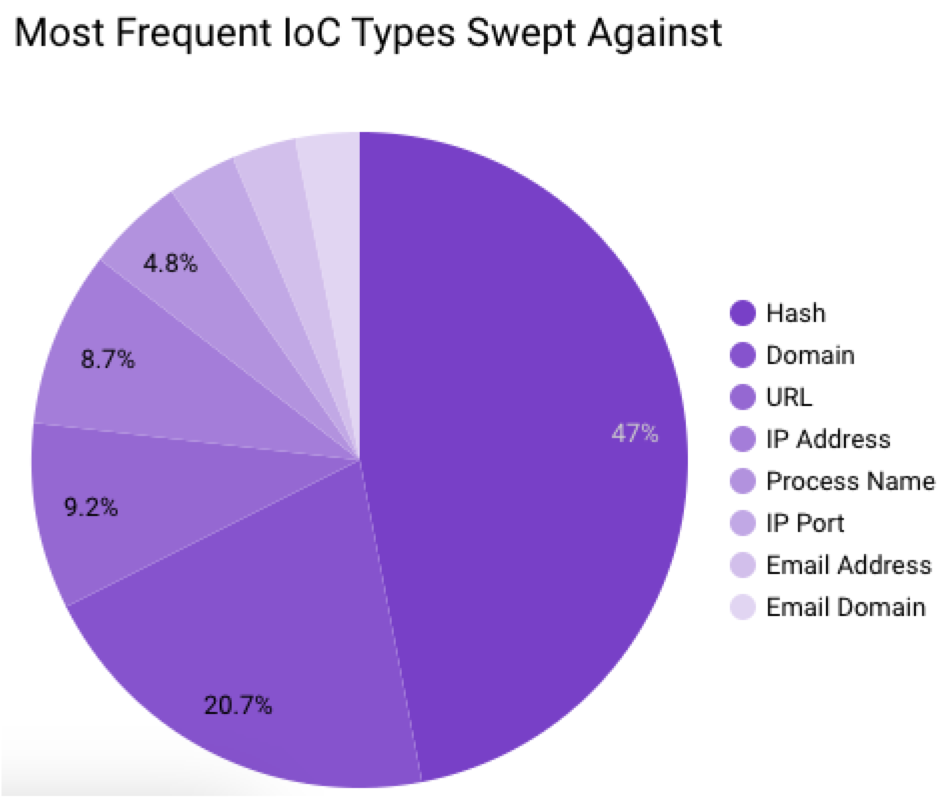
Emerging Threats Analyzed & Swept	TTPs/IoCs Codified & Swept	Threats Detected in Environments	Average Hours Saved Per Month
144	2,517	26	180

Volume of Threats by Month - 2023



Most Frequent Data Sources Swept Against





In September 2023, Securonix Autonomous Threat Sweeper identified **2,517 TTPs and IoCs, 144 distinct threats, and reported 26 threat detections**. The top data sources swept against include IDS/IPS/UTM/Threat Detection, Endpoint Management Systems, Data Loss Prevention, and Email/Email Security.

Prominent ransomware attacks (Originally published in September 2023)

Recent ransomware attacks have unveiled a concerning trend in the digital domain. Notably, major casino chains, Caesars Entertainment and MGM Resorts, have found themselves in the crosshairs. The dual-threat approach by cybercriminals has heightened the risks. They aren’t content with just encrypting data; they are also exfiltrating it, posing a dual threat to organizations. Furthermore, the focus on critical infrastructure components, as observed in the MGM attack where ESXi servers were encrypted, reveals a shift from traditional end-user targets. This surge in sophisticated attacks is reminiscent of the tactics employed by the notorious LockBit, Snatch, and Vidar ransomware groups in 2023, emphasizing a global trend in cyber threats.

The continuous evolution of ransomware tactics underlines the need for industries, especially data-rich sectors like casinos, to bolster their cybersecurity measures. With the recent activities of groups like LockBit, Snatch, and Vidar setting a menacing precedent, it’s imperative for organizations to adopt a multifaceted defense strategy. The recent willingness of entities like Caesars Entertainment to pay substantial ransoms also raises concerns about potentially emboldening cybercriminals for future attacks. In this fully digital environment, being proactive rather than reactive could be the difference between security and compromise.

Ransomware	Description
FreeWorld ransomware	A cyberattack operation that compromises vulnerable Microsoft SQL Server (MSSQL) databases and uses brute-force attacks to deliver Cobalt Strike and ransomware payloads has been identified. A recent Securonix analysis covers this campaign's typical attack sequence with brute forcing entry into the unprotected MSSQL databases. After initial infiltration, the attackers launch a number of payloads using MSSQL as a beachhead, including remote-access Trojans (RATs) and a new Mimic ransomware variant called "FreeWorld." The binary file names contain the word "FreeWorld," the ransom demand file is called FreeWorld-Contact.txt, and the ransomware extension is ".FreeWorldEncryption."
3AM ransomware	3AM was recently discovered by researchers. According to the analysis, this ransomware was first used in a failed attack when threat actors swapped it out for LockBit ransomware. This new strategy shows that ransomware affiliates can also carry several ransomware strains to pursue their targets until the very end and guarantee the success of their operations. Typically, ransomware affiliates carry a number of tools in their armory for use in attacks.
RedLine and Vidar	According to analysis by researchers, the threat groups behind RedLine and Vidar have started distributing ransomware using the same techniques they use to spread info-stealers. In one such instance, victims first encountered malware that was issued with Extended Validation (EV) code signing certificates and that stole information. However, over time, they also began acquiring ransomware using the same technique.
Snatch Ransomware	A combined cybersecurity advisory from the FBI and CISA has been released regarding the Snatch ransomware variant. The warning includes the tactics, techniques, and procedures (TTPs) used by the Snatch ransomware and offers insights into how it operates. The Snatch ransomware strain, which engages in data theft and extortion activities, was discovered through FBI investigations as recently as June 1, 2023, according to the advisory.

Threat Labs summary

Securonix Threat Labs recommends leveraging our findings to deploy protective measures against increased threats from these ransomware.

- Continually do backups, and store the results either offline or on a different network.
- On your computer, smartphone, and other connected devices, turn on automatic software upgrades whenever practicable and practical.

- Use a trusted antivirus and internet security software suite on all connected devices, including your computer, laptop, and mobile.
- Avoid opening email attachments without first verifying their legitimacy and clicking on dubious links.
- 88 IoCs are available on our Threat Labs home page repository and have been swept against Autonomous Threat Sweeper customers.

TTPs related to the **FreeWorld ransomware** include but are not limited to the following:

- Monitor for network-level authentication for RDP connection.
- Monitor for Mimikatz was executed through another batch file.

TTPs related to the **3AM ransomware** include but are not limited to the following:

Monitor for the presence of the following filenames in the directory – /usr/lib64/seahorses/

- – ‘kbioset’
- – ‘cpc’
- – ‘kkdmflush’
- – ‘soss’
- – ‘sshod’
- – ‘nethoogs’
- – ‘iftoop’
- – ‘iptraof’”

TTPs related to the RedLine and Vidar include but are not limited to the following:

Monitor for the rare installation path in TEMP folder which is later added to startup folder for establishing persistence.

Tags: Ransomware: FreeWorld, Mimic, 3AM, LockBit, Snatch Target: MS SQL server Target Sector: Infrastructure, IT, US Defense Industrial Base, Food and Agriculture Vertical

Ongoing phishing campaigns (Originally published in September 2023)

Group-IP claims that a custom phishing kit called W3LL Panel was available for purchase on the threat actor’s secret underground market, W3LL Store, which catered to a closed community of at least 500 other threat actors. W3LL Panel is made to get around MFA and 16 other completely customized tools for business email compromise (BEC) attacks. A previously undocumented “phishing empire” has been linked to more than 56,000 Microsoft 365 business email accounts over the past six years, according to firm Group-IB, who has identified a hidden underground market. W3LL’s major weapon, W3LL Panel, may be considered one of the most advanced phishing kits in class, featuring adversary-in-themiddle functionality, API, source code protection, and other unique capabilities. W3LL Panel does not have a variety of fake pages and it was designed to compromise Microsoft 365 accounts specifically. However, due to its high efficiency, the phishing kit became trusted by a narrow circle of BEC criminals.

Securonix Threat Labs experts have identified an ongoing phishing campaign that employs an ongoing cyber attack campaign, dubbed STARK#VORTEX, that is specifically targeting Ukraine's military. Orchestrated by the threat group UAC-0154, this campaign utilizes sophisticated techniques to evade detection. The attackers use a Microsoft Help file with an embedded obfuscated JavaScript code as a lure document, disguised as a manual for Pilot-in-Command (PIC) Drones, to deliver the MerlinAgent malware. The PowerShell-based malware is heavily obfuscated and downloads a payload from a remote server, giving attackers full control over compromised systems.

Threat Labs summary

Securonix Threat Labs recommends leveraging our findings to deploy defensive measures against this campaign.

- Fortify the authentication mechanism. Implement FIDO v 2.0 authentication solutions to disarm BEC adversaries that use W3LL tools or other phishing kits aimed at stealing OTPs or session cookies.
- Improve access policies. To prevent session cookies from being abused, organizations can implement stricter access policies such as IP whitelisting and trusted devices.
- Stay vigilant about any suspicious activity. Constantly monitor account activity, logins, forwarding rules, deleted emails, and other indicators potentially left by BEC threat actors
- Proactively detect and take down phishing domains. A proactive approach to hunting for phishing resources could also be part of a wider mitigation strategy. Leverage Group-IB Digital Risk Protection.
- Conduct regular training for your cybersecurity specialists and raise awareness with cyber security workshops for all of your employees.
- Even if there are no clear signs of an account compromise, it is important to leave threat actors no chance of going undetected. If there is doubt, a compromise assessment would be a necessary step to ensure that your cloud environment is secure.
- Review security policies. Following recommendations after a compromise assessment or implementing precaution measures listed above will help to decrease the likelihood of being a victim of BEC again.
- 15 IoCs are available on our Threat Labs home page repository and have been swept against Autonomous Threat Sweeper customers

TTPs related to the **STARK#VORTEX** include but are not limited to the following:

- Monitor for bxor, IO.StreamReader and Decompress command in PowerShell
- Monitor for STARK#VORTEX campaign, would be executed using the Windows binary hh.exe which is launched automatically when a user runs the .chm file.

Tags: Attack Type: Phishing | Threat Actor: W3LL, |UAC-0154 | Target Sector: companies in the US, the UK, Australia and Europe primarily operating in the manufacturing, IT, and financial services sectors.

Attacks by Iranian hackers (Originally published in September 2023)

Since February 2023, Microsoft researchers have seen that a threat group supported by Iran has been conducting password spray attacks against hundreds of businesses in the United States and around the world. The actor in these attacks was tracked as Peach Sandstorm (HOLMIUM). Peach Sandstorm is an Iranian nation-state threat actor who has targeted organizations in the satellite, defense, and pharmaceutical sectors around the globe.

In the initial phase of their campaign, Peach Sandstorm conducted password spray campaigns against thousands of organizations across several sectors and geographies. While Microsoft observed several organizations previously targeted by Peach Sandstorm, the volume of activity and range of organizations suggests that at least a subset of the initial activity is opportunistic. Microsoft observed Peach Sandstorm using two distinct sets of TTPs in the early stages of the intrusion lifecycle in 2023 attacks.

The second incident with Iranian hackers h was discovered by researchers from ESET. They reported the Iranian threat actor Charming Kitten is connected to a recent round of attacks that target targets in Brazil, Israel, and the United Arab Emirates using a hidden Ballistic Bobcat backdoor they have dubbed Sponsor. Victimology patterns suggest that the group primarily singles out education, government, and healthcare organizations, as well as human rights activists and journalists. The Sponsor backdoor uses configuration files stored on disk. These files are discreetly deployed by batch files and deliberately designed to appear innocuous, thereby attempting to evade detection by scanning engines. Sponsor was deployed to at least 34 victims in Brazil, Israel, and the United Arab Emirates.

Threat Labs summary

Securonix Threat Labs recommends the following guidelines

- Implement network segmentation and maintain offline backups of data to ensure limited interruption to your organization.
- Apply the vendor patches immediately.
- Add users to the Protected Users Security Group
- 23 IoCs are available on our Threat Labs home page repository and have been swept against Autonomous Threat Sweeper customers.

TTPs related to the **Charming Kitten backdoor** include but are not limited to the following:

- Monitor for network traffic containing “info.php?name=”, “dn.php?name=” and “up.php?name=” in the request url.
- Monitor for the rare instance where rundll32.exe is executed with command line parameter – ”iiiiiiii“
  Example: cmd /c rundll32 “C:\Users\username\AppData\Local\Temp\wpnprv.dll”, IIIIIIII 4 “cmd /c del /f /q C:\Windows\system32\wpcsvc.dll”
- Monitor for rare command lines executed that contain all these parameters – “cd /d” and ”dir” and ”/a/o-d/s” and ”*.”
  Example: cmd /c cd /d “C:\Users” && dir /a/o-d/s *.*
- Monitor for cmd.exe spawning expand.exe to decompress the cab files.
  Example: cmd /c expand %TEMP%\1.cab -f:* %TEMP%
- Monitor the rare registry additions that contain either of the two combinations – “system\currentcontrolset\services” and “reg_expand_sz” or “software\microsoft\windows nt\currentversion\svchost” and “reg_multi_sz”.
  Example: reg add “HKLM\SYSTEM\CurrentControlSet\Services\wpcsvc\Parameters” /v ServiceDll /t REG_EXPAND_SZ /d “%windir%\System32\wpcsvc.dll” /f > nul
- Monitor the execution of process sc.exe wherein the commandlines contain the parameters ”failure”, ”reset=” and ”actions=”

Tags: Attack Type: password spray| Threat actor: Peach Sandstorm is an Iranian nation-state threat actor, Charming Kitten | Targeted organizations: education, government, and healthcare organizations, as well as human rights activists and journalists

Exploitation of CVE-2022-47966 and CVE-2022-42475 (Originally published in September 2023)

A U.S. aeronautical corporation was compromised by state-sponsored hacker gangs using exploits that targeted crucial Fortinet and Zoho ManageEngine vulnerabilities. Although the threat groups responsible for this breach have not yet been identified, USCYBERCOM’s press release links the malicious actors to Iranian exploitation efforts, but the joint alert did not link the attackers to a specific state.

Nation-state APTs used CVE-2022-47966 to acquire unauthorized access to a public-facing application (Zoho ManageEngine ServiceDesk Plus), establish persistence, and move laterally through the network, according to statements from CISA, FBI, and CNMF. The ManageEngine program is vulnerable and permits remote code execution. Additional APT actors were seen using CVE-2022-42475 to set up shop on the company’s firewall device.

Threat Labs summary

Securonix Threat Labs recommends leveraging our findings to deploy protective measures for increased threats from this campaign.

- The organization confirmed the user had been disabled before the observed behavior, but it was discovered that APT actors had stolen and used legal administrative account credentials from a previously engaged contractor.
- In addition to using legitimate credentials to jump from the firewall to a web server and deploy web shells for backdoor access, the attackers have been seen starting multiple transport layer security (TLS)-encrypted sessions to a number of IP addresses, indicating data transfer from the firewall device.
- In both situations, the adversaries allegedly deactivated administrative account credentials and erased logs from a number of important systems to try to cover their tracks forensically.
- 25 IoCs are available on our Threat Labs home page repository and have been swept against Autonomous Threat Sweeper customers

Tags: Vulnerability: CVE-2022-47966, CVE-2022-42475 | Target Sector: Aviation Organization | Target Location: United State | Exploit: Zoho ManageEngine, Fortinet

For a full list of the search queries used on Autonomous Threat Sweeper for the threats detailed above, refer to our Threat Labs home page. The page also references a list of relevant policies used by threat actors.

We would like to hear from you. Please reach out to us at [email protected].

Note: The TTPs when used in silo are prone to false positives and noise and should ideally be combined with other indicators mentioned.

Contributors: Sina Chehreghani, Dhanaraj K R