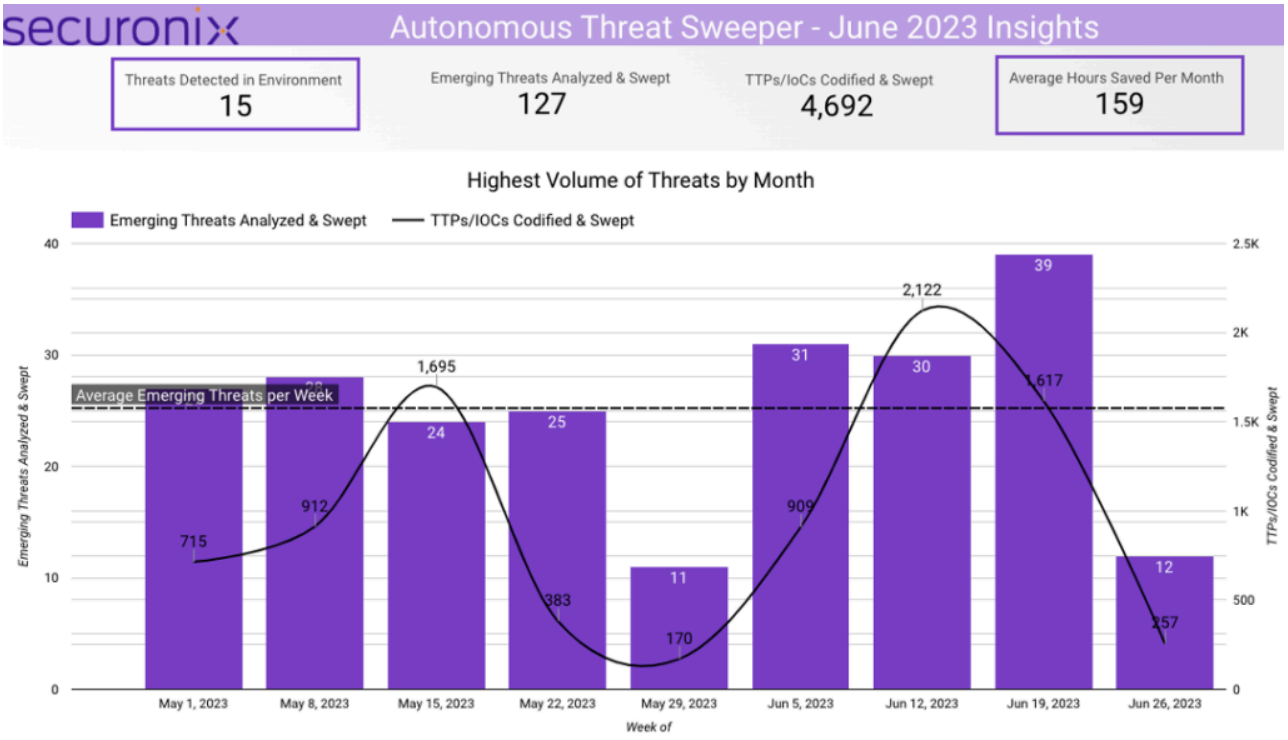
Securonix Threat Labs Monthly Intelligence Insights – June 2023

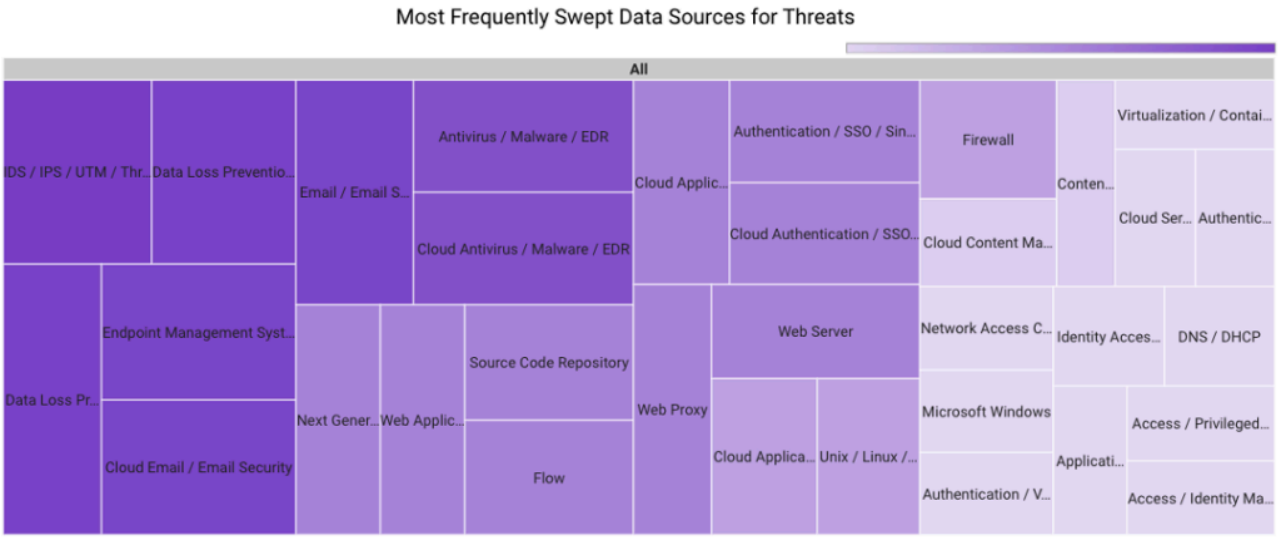
Authors: Dheeraj Kumar, Ella Dragun

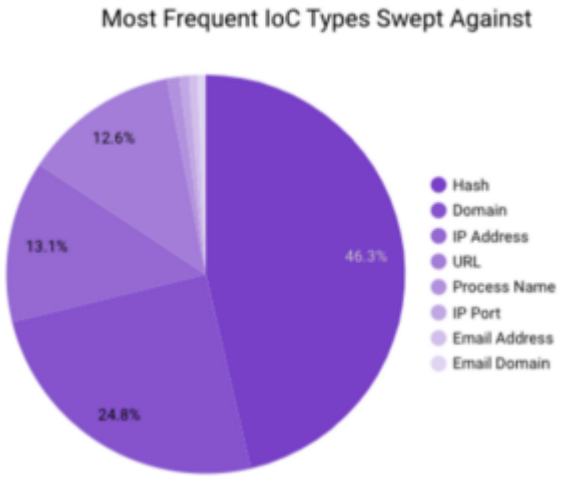
The Monthly Intelligence Insights provides a summary of top threats curated, monitored, and analyzed by Securonix Threat Labs in June. The report additionally provides a synopsis of the threats; indicators of compromise (IoCs); tactics, techniques, and procedures (TTPs); and related tags. Each threat 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 June 2023, Threat Labs analyzed and monitored major threat categories, including the ongoing zero-day vulnerability in the MOVEit Transfer campaign, Barracuda ESG zero-day vulnerability, MULTI#STORM attack campaign, North Korean TAG-71 Group, Cadet Blizzard a new Russian threat actor and Lancefly APT that targets governments, aviation, and organizations with custom backdoors.

In June 2023, Securonix Autonomous Threat Sweeper identified **4,692 TTPs and IoCs, 127 distinct threats, and reported 15 threat detections**. The top data sources swept against include IDS/IPS/UTM/Threat Detection, Endpoint Management Systems, Data Loss Prevention, and Email/Email Security.







Barracuda critical vulnerability (Originally published in June 2023)

Researchers from Barracuda have urged their customers who were impacted by a recently disclosed zero-day flaw in its Email Security Gateway (ESG) appliances to immediately replace them. More technical details on the Barracuda ESG zero-day vulnerability (CVE-2023-2868) is reported in Mandiant's blog.

During its investigation, Mandiant recognized a China-nexus actor, known as UNC4841, which tried to target a subset of Barracuda ESG appliances for espionage across regions and sectors. UNC4841 is most likely an espionage actor driving this global campaign in favor of the People's Republic of China.

Based on the evidence during the analysis, the first stage of compromises seemed to have happened on a small subset of appliances geo-located in China. The C2 communications were abused during this early stage of compromise, also using port 8080 while later compromises that occurred almost entirely leveraged port- 443 or port 25.

Threat Labs summary

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

- Review email logs to identify the initial point of exposure.
- Revoke and rotate all domain-based and local credentials that were on the ESG at the time of compromise.
- Revoke and reissue all certificates that were on the ESG at the time of compromise.
- Monitor the entire environment for the use of credentials that were on the ESG at time of compromise.
- Monitor the entire environment for use of certificates that were on the ESG at time of compromise.
- Review network logs for signs of data exfiltration and lateral movement.
- Barracuda reiterated guidance recommending that all impacted Barracuda customers immediately isolate and replace compromised appliances.
- 109 IoCs are available on our Threat Labs home page repository and have been swept against Autonomous Threat Sweeper customers.

Tags: Threat Actor: UNC4841 a China-nexus actor,| Threat Actor Location: China | Attack: Barracuda Email Security Gateway (ESG) appliances

Threat Activity Group 71 exploits (Originally published in June 2023)

Recorded Future researchers have discovered malicious cyber threat activity spoofing several financial institutions and venture capital firms in Japan, Vietnam, and the United States. They refer to the group behind this activity as Threat Activity Group 71 (TAG-71). They also identified 74 domains resolving to 5 IP addresses, as well as 6 malicious files, in the most recent cluster of activity from September 2022 to March 2023.

TAG-71 activities closely follow public reports on North Korea state-sponsored APT38 (also commonly known as Bluenoroff, Stardust Chollima, and BeagleBoyz) activity.

Last year, Insikt Group discovered 18 malicious servers tied to TAG-71 and linked to CryptoCore campaign to deliver malware, phishing, and malware command and control (C2). These servers and associated malicious documents compromised popular cloud services, cryptocurrency exchanges, and private investment firms and successfully targeted potential victims to open malicious content or provide their login credentials.

DEV-0586, another threat group that got Microsoft's attention this month is a distinct Russian state-sponsored threat actor that has now been given the name Cadet Blizzard. This group launched the destructive malware "Whispergate Wiper" in January 2022 against organizations affiliated with the Ukrainian government when Microsoft still identified it as DEV-0586.

While the group's activities may be less sophisticated than other threat actors, their destructive attacks have targeted government organizations and IT providers mainly in Ukraine, with occasional operations in Europe and Latin America.

From a technical perspective, Cadet Blizzard mainly achieved initial access by exploiting web servers and vulnerabilities in Confluence servers, Exchange servers and open-source platforms.

Cadet Blizzard reportedly ran lateral movement with obtained network credentials and modules from the Impacket framework, while command and control (C2) was achieved via socket-based tunneling utilities and occasionally Meterpreter.

Threat Labs summary

Securonix Threat Labs recommends leveraging our findings to deploy defensive measures against increased threats of Threat Activity Group 71 (TAG-71).

- Maintain consistent backup procedures and store those backups offline or on a different network.
- Review all authentication activity for remote access infrastructure, with a particular focus on accounts configured with single factor authentication, to confirm authenticity and investigate any anomalous activity.
- Enable multifactor authentication (MFA) to mitigate potentially compromised credentials
- 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.
- Avoid clicking on suspicious links and opening email attachments without first checking their legitimacy.
- 99 IoCs are available on our Threat Labs home page repository and have been swept against Autonomous Threat Sweeper customers

TTPs related to the Cadet Blizzard Group include but are not limited to the following:

- Monitor for PowerShell DownloadFile commandlet
- Check for WMIExec Impacket activity with common Cadet Blizzard commands
- Monitor for scheduled task creation, command execution and C2 communication

Tags: Campaign: North Korean state-sponsored cyber actor: 71 (TAG-71) and Russian state-sponsored: Cadet Blizzard | Target location: government organizations and IT providers mainly in Ukraine, with occasional operations in Europe and Latin America

Zero-Day vulnerability in MOVEit transfer (Originally published in June 2023)

The MOVEit Transfer web application has several SQL injection flaws that could let an unauthenticated attacker access the MOVEit Transfer database without authorization.

New SQL injection flaws impacting the file transfer solution have been patched by Progress Software, the developer of the MOVEit Transfer program, in order to prevent the theft of sensitive data.

The renowned Cl0p ransomware gang, which has a history of organizing data theft campaigns and utilizing zero-day weaknesses in several managed file transfer platforms since December 2020, has been blamed for the activity.

The earliest signs of exploitation, which led to the deployment of web shells and data theft, were discovered on May 27, 2023, according to a preliminary analysis by Mandiant incident response engagements. Data theft has occasionally happened within minutes after web shell deployment. Although the victims of this campaign did not originally receive any ransom demands, the campaign's appearance of opportunism and the eventual data theft are consistent with extortion actors' behavior. Then, on June 6, 2023, a post on the data leak site (DLS) CL0P_-LEAKS claimed ownership of this action and threatened to post stolen data if victims did not pay an extortion charge.

A web shell called LEMURLOOT was used to infect MOVEit Transfer web apps that were accessible to the public and steal data from the underlying MOVEit Transfer databases. A similar flurry of activity was launched by TA505 in early 2023 targeting Fortra/Linoma GoAnywhere MFT servers and Accellion File Transfer Appliance (FTA) devices in the form of zero-day exploit-driven attacks.

Threat Labs summary

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

- Update MOVEit Transfer to one of these patched versions:
  - MOVEit Transfer 2023.0.1
  - MOVEit Transfer 2022.1.5
  - MOVEit Transfer 2022.0.4
  - MOVEit Transfer 2021.1.4
  - MOVEit Transfer 2021.0.6
- Users should follow the steps which are provided in the MOVEit Security Advisory in order to successfully provide remediation. These steps include the following:
  - Disable all HTTP and HTTPS traffic to your MOVEit Transfer environment
  - Search for IoCs, delete, and reset account credentials
  - Apply the patch
  - Re-enable all HTTP and HTTPS traffic to your MOVEit Transfer environment
  - Verify all of the files have been successfully deleted, and no unauthorized accounts remain.
  - Continuously monitor network, endpoints, and logs for IoCs as listed in the advisory.
- 305 IoCs are available on our Threat Labs home page repository and have been swept against Autonomous Threat Sweeper customers.

TTPs related to the MOVEit vulnerability include but are not limited to the following:

- Monitor for specific requests to moveitisapi.dll, human2.aspx and guestaccess.aspx

Tags: Vulnerability: CVE-2023-34362 | Attack Type: SQL injection | Affect Product: MOVEit Transfer web application

New MULTI#STORM attack campaign (Originally published in June 2023)

Warzone RAT infections were recently discovered to be distributed using phishing emails by MULTI#STORM, an intriguing attack campaign using a Python-based loader malware.

The Securonix Threat Research Team recently examined an interesting phishing effort. The user clicks on a JavaScript file that has been extensively encrypted inside a password-protected zip file, which starts the attack. The MULTI#STORM campaign appears to have targeted certain victims in the US and India.

The victim computer is infected with numerous distinct RAT (remote access trojan) malware instances, including Warzone RAT and Quasar RAT, at the conclusion of the attack chain. For command and control at various points along the infection chain, both are utilized.

It's quite interesting to learn about the loader that led to the host's initial compromise. Although it utilizes similar TTPs as DBatLoader, this malware is written in Python, bundled with PyInstaller, and uses some quite advanced tactics to build persistence and evade detection before launching the RAT payloads.

Threat Labs summary

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

- Like so many previous attacks, this one begins with a phishing email that contains a link. The user is sent to a Microsoft OneDrive file for the victim to download when the link refers to a request for a quote.
- The OneDrive link in this instance downloads a 500KB password-protected zip file with the name "REQUEST.zip" and the password "12345".
- The target user gets shown a single JScript file called REQUEST.js after extracting the zip file. Surprisingly, no attempt was made to obscure the file using.LNK execution or, at the very least, a double extension to disguise it as a different file type.
- 18 IoCs are available on our Threat Labs home page repository and have been swept against Autonomous Threat Sweeper customers.

TTPs related to theMULTI#STORM attack campaign include but are not limited to the following:

- Monitor for PowerShell and .lnk files initiated by the explorer.exe process in an endpoint management system. It captures the conditions you specified, and the response actions suggest measures to mitigate and detect such behavior.
- Monitor for process creation events in an endpoint management system where the destination process starts with "C:\Windows\System32".
- Monitor for registry modifications in an endpoint management system related to the "Open" command for folders, specifically when the value is set to either cmd.exe or powershell.exe.

Tags: Malware: MULTI#STORM | Target Location: India, US | Attack Type: Phishing

Increased attacks on government organizations (Originally published in June 2023)

Numerous espionage operations were directed at governmental organizations in the Middle East and Africa. The attacks' primary objective, according to the results, was to acquire extremely sensitive and private information, particularly on political figures, military operations, and foreign affairs departments.

The attacks, which took place around the same time, included a number of strikingly identical tactics, techniques, and procedures (TTPs), some of which had never been seen before in the wild. Other TTPs, on the other hand, are rather uncommon, with just a few attackers having been known to use them and are identified as CL-STA-0043. The expertise, adaptability, and victimology of this activity group point to a highly skilled APT threat actor, and it is believed that this threat actor is a nation-state.

In South and Southeast Asia, the APT group Lancefly is targeting businesses in the government, education, telecom, and aviation sectors using a specially created backdoor. The potent backdoor, known as Merdoor, has been operational since 2018.

The campaign's perpetrators have access to the most recent ZXShell rootkit version. The latest version of ZXShell targets antivirus software to disable it while also being lower in size and having more features. The certificate 'Wemade Entertainment Co. Ltd,' which was connected to APT41 in August 2019, is used to sign the rootkit.

Threat Labs summary

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

- After breaking into the network, CL-STA-0043 engaged in reconnaissance, mapping out the system and locating vital assets. The attackers' primary objectives were locating administrator accounts and locating crucial servers, such as:
    - Domain controllers
    - Web servers
    - Exchange servers
    - FTP servers
    - SQL databases
- Merdoor is a fully functional backdoor with the following features that appears to have been available since 2018:
    - Installing itself as a service
    - Keylogging
    - A variety of methods to communicate with its command-and-control (C&C) server (HTTP, HTTPS, DNS, UDP, TCP)
    - Ability to listen on a local port for commands
- 76 IoCs are available on our Threat Labs home page and have been swept against Autonomous Threat Sweeper customers.

TTPs related to the CL-STA-0043 group include but are not limited to the following:

- Monitor for instances where the command line contains "JuicyPotato", "SharpEfsPotato", or "StickyKeys", or where the process name is "cmd.exe" and the command line contains "Iislpe.exe".

TTPs related to the Lancefly group include but are not limited to the following:

- Monitor detect PowerShell commands that launch rundll32.exe with MiniDump, Reg.exe commands dumping SAM and SYSTEM hives, Avast tool used for dumping LSASS memory, and the use of masqueraded WinRAR (wmiprvse.exe) for staging and encrypting files.
- Monitor for "LoadSys" export is executed and checks for the presence of files with the paths "[WindowsDirectory]\system32\drivers\TdiProxy.sys" or "[WindowsDirectory]\system64\drivers\TdiProxy.sys". It also detects the creation of the device

> "\Device\TdiProxy0" and the symbolic link "\DosDevices\TdiProxy0". Additionally, it checks for the presence of the PDB filename "c:\google\objchk_win7_amd64\amd64\Google.pdb".

Tags: Target Location: Middle East, Africa, South and Southeast Asia | APT Group: Lancefly, CL-STA-0043 | Target Sector: Government, Education, Telecom, and Aviation | Malware: Merdoor

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 scia@securonix.com.

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
