Date of Publication
February 27, 2023

Hive Pro

HiveForce Labs

WEEKLY
THREAT DIGEST

Actors, Attacks, and Vulnerabilities

20 to 26 FEBRUARY 2023

Summary

Threat Actors

HiveForce Labs has identified five active threat actors over the past week. The Earth Kitsune APT and Lazarus Group are North Korean-based cybercrime groups that focus on information theft and espionage activities. The other three actors named WIP26, Hydrochasma, and Clasiop are also well-known for their information theft and espionage capabilities. For more information, please refer to the "Actors" section for key takeaways

Attacks

Last week, we identified ten new strains of active malware. Three of them were information stealers: Stealc, DarkCloud, and Icarus. We discovered two new malware strains called SoulSearcher and Mylobot. Additionally, two were classified as backdoors: WhiskerSpy and WinorDLL64. We found two new RATs: Lilith RAT and Atharvan RAT. We also identified one new strain of ransomware called HardBit. For more information, please refer to the "Attacks" section for important highlights.

Vulnerabilities

Last week, we identified seven vulnerabilities that organizations should be aware of. One of these vulnerabilities affects VMware Carbon Black App Control and permits access to the underlying server. The remaining six vulnerabilities affect FortiWeb, FortiOS, FortiNAC, and FortiProxy, and allow local attackers to elevate privileges and execute unauthorized code or commands. For more information, please refer to the key takeaway section on vulnerabilities.

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Threat Actors

Earth Kitsune APT

Earth Kitsune, an advanced persistent threat (APT) actor known for targeting individuals interested in North Korea, also China, Brazil, and Japan and has been found to be using a new backdoor called "WhiskerSpy" in a recent campaign. The group used a social engineering tactic in a watering hole attack, luring visitors to a pro-North Korean website with a fake error message and offering a trojanized codec installer that loaded the WhiskerSpy backdoor on their systems.

WIP26

The WIP26 operation commences by precisely selecting employees to receive WhatsApp messages containing Dropbox links to a malware loader. The employees are enticed into downloading and executing the loader, which then deploys backdoors that employ Microsoft 365 Mail and Google Firebase instances as command-and-control servers.

Hydrochasma

Hydrochasma is a newly identified threat actor that has been targeting shipping companies and medical laboratories in Asia since October 2022. This group's primary focus appears to be on intelligence gathering, and they do not rely on custom malware in their attack campaign, instead using only publicly available and living-off-the-land tools.

Clasiopa

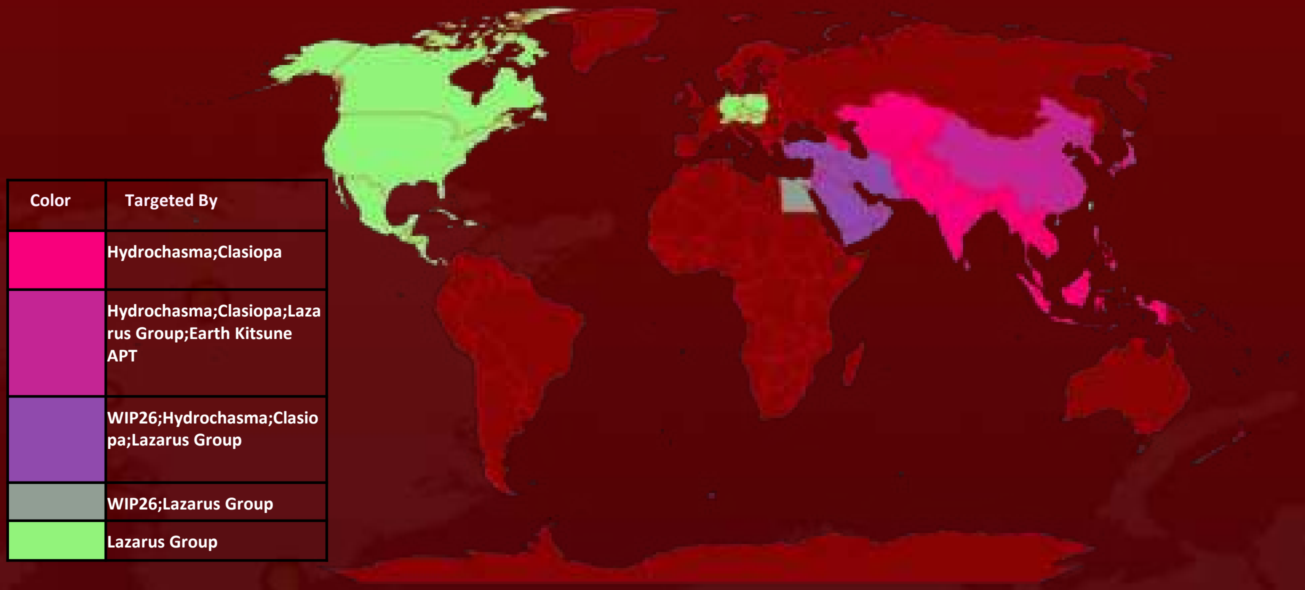
Clasiopa is a new attack group that has been observed targeting a materials research organization in Asia using a distinct toolset that includes a custom malware called Backdoor.Atharvan. It is unclear where Clasiopa is based or who they act on behalf of, although there are indications that imply the group may have links to India. The attackers gain access through brute force attacks on public-facing servers and use multiple backdoors to build lists of file names and exfiltrate them.

Lazarus Group

Lazarus Group is a notorious hacking group believed to be based in North Korea, although their true identity and location remain a matter of debate among cybersecurity experts. The group has been linked to a wide range of cyber attacks against financial institutions, government agencies, and other high-profile targets in various countries.

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Actor Map



Color	Targeted By
🟥	Hydrochasma;Clasiopa
🟪	Hydrochasma;Clasiopa;Lazarus Group;Earth Kitsune APT
🟪	WIP26;Hydrochasma;Clasiopa;Lazarus Group
⬜	WIP26;Lazarus Group
🟩	Lazarus Group

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Actor Details

ICON	NAME	ORIGIN	MOTIVE
🤖	Earth Kitsune APT	North Korea	Information theft and Espionage
🤖	WIP26	Unknown	Information theft and Espionage
🤖	Hydrochasma	Unknown	Information theft and Espionage
🤖	Clasiopa	Unknown	Espionage
🤖	Lazarus Group (Labyrinth Chollima,Group 77 ,Hastati Group,Whois Hacking Team,NewRomanic Cyber Army Team,Zinc,Hidden Cobra ,Appleworm,APT-C-26,ATK 3 ,SectorA01 ,ITG03 ,TA404 ,DEV-0139 ,Guardians of Peace ,Gods Apostles ,Gods Disciples)	North Korea	Information theft and espionage, Sabotage and destruction, Financial crime

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Attacks

WhiskerSpy (Earth Kitsune APT)

WhiskerSpy is a backdoor malware that was used by Earth Kitsune, an advanced persistent threat (APT) group known for its cyber espionage campaigns. In a recent campaign, Earth Kitsune was found to be using the WhiskerSpy backdoor as part of a watering hole attack targeting individuals interested in North Korea and other countries.

SoulSearcher malware (Unattributed)

SoulSearcher is a type of malware that serves as a second-stage loader, responsible for executing a payload known as the Soul module and parsing its configuration. It is well-crafted and has modular, multi-stage, reflectively executed payloads that make it difficult to detect and analyze. It has been observed in the wild since October 2017 and is a sign of a well-resourced group with advanced capabilities.

Stealc Malware(Unattributed)

Stealc is a newly discovered information-stealing malware that targets web browsers, desktop cryptocurrency wallets, and browser extensions for cryptocurrency wallets. It is a fully-featured malware that can be customized for specific purposes and has an administration panel that allows cybercriminals to maximize their chances of stealing valuable information.

Mylobot (Unattributed)

Mylobot is a Windows-targeting malware and was first discovered in 2017. It has not received much attention since then, but it is noteworthy for its ability to transform the infected system into a proxy. The number of unique infected systems per day has decreased from a peak of 250,000 in 2020 to currently observing over 50,000 unique infected systems daily.

DarkCloud Stealer (Unattributed)

DarkCloud Stealer is a multi-stage malware that is being distributed via spam emails with an order invoice phishing scheme. The malware has the ability to exfiltrate stolen data using various methods such as SMTP, Telegram, Web Panel, and FTP. It functions through a multi-stage process, with the final payload written in Visual Basic, which is loaded into the device's memory during the last stage.

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

HardBit Ransomware (Unattributed)

HardBit is a ransomware group that targets organizations and demands cryptocurrency payments for decrypting data. It first emerged in October 2022, and a newer version, HardBit 2.0, surfaced at the end of November of the same year. Recently, they have employed a new extortion tactic of demanding to know the victim's cyber insurance coverage in order to extort millions of dollars in ransom.

Icarus Stealer malware (Unattributed)

The Icarus Stealer malware is equipped with a Hidden Virtual network computing (hVNC) feature, which enables the attacker to generate a concealed desktop and traverse the compromised system without any contact with the primary desktop. Furthermore, Icarus Stealer is considerably less expensive than other widely used Info stealers available on the dark web.

Lilith RAT (Clasiopa)

Lilith RAT is a type of Remote Access Trojan (RAT) that has been observed in various cyberattacks. Lilith RAT is a particularly stealthy malware, as it has several features that make it difficult to detect and remove. Lilith RAT can be used to perform various malicious activities, such as stealing sensitive data, installing other malware, and taking screenshots.

Atharvan (Clasiopa)

Atharvan is a custom-built remote access Trojan (RAT) that is used by the Clasiopa attack group to gain unauthorized access to targeted systems. It is designed to run on Windows-based operating systems and has several features that allow attackers to take control of infected machines, steal data, and monitor user activity.

WinorDLL64 (Lazarus Group)

WinorDLL64 is a newly discovered backdoor associated with the malware downloader Wslink. It enables the manipulation of various files, executing further commands, and exfiltration or deletion of files. The backdoor is a DLL that is likely developed by the notorious Lazarus Group, a North Korea-aligned organization, and features encryption to ensure secure data exchange between the operator and the tool.

TOP MITRE ATT&CK TTPS:

T1059
Command and Scripting Interpreter

T1055
Process Injection

T1012
Query Registry

T1204
User Execution

T1057
Process Discovery

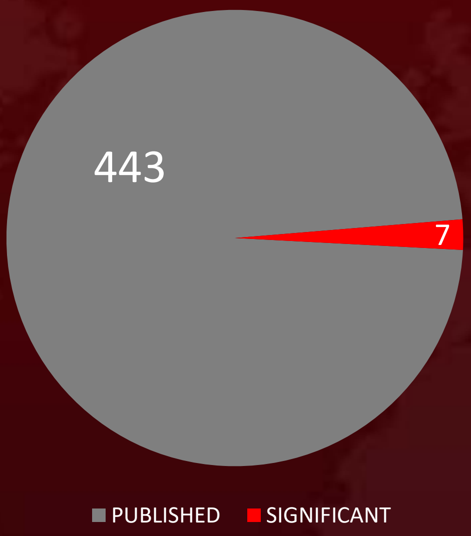
*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

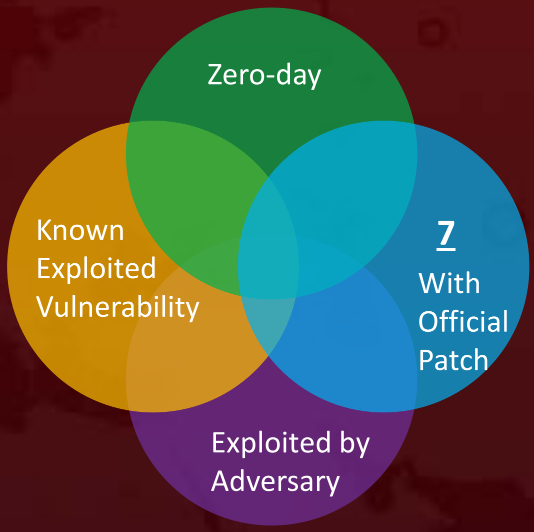
Key Takeaways

Vulnerabilities

Seven Notable Mentions

Out of the seven security vulnerabilities discovered, one (CVE-2023-20858) was found in the VMware Carbon Black App Control and this vulnerability allowing access to the underlying server. The remaining six vulnerabilities were found in FortiWeb, FortiOS, FortiNAC, and FortiProxy, enabling local attackers to escalate privileges and execute unauthorized code or commands. One of the vulnerabilities, CVE-2022-39952, affects FortiNAC and involves external control of the file name or path in the web server, allowing unauthenticated attackers to execute arbitrary writes. Another noteworthy flaw, CVE-2021-42756, involves multiple stack-based buffer overflow vulnerabilities in the proxy daemon of FortiWeb, which can lead to arbitrary code execution by an unauthenticated remote attacker using a specially crafted HTTP request.





*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **7 significant vulnerabilities** and block the indicators related to the threat actors **Earth Kitsune APT, WIP26, Hydrochasma, Clasiopa, Lazarus Group,** and malware, **SoulSearcher, Stealc, Mylobot, WhiskerSpy, WinorDLL64, DarkCloud, Icarus Stealer malware, Lilith RAT, Atharvan RAT,** and **HardBit Ransomware.**

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Running a Scan to discover the assets impacted by the **7 significant vulnerabilities**
- Testing the efficacy of their security controls by simulating the attacks related to and malware **SoulSearcher, Stealc, Mylobot, WhiskerSpy, WinorDLL64, DarkCloud, Icarus Stealer malware, Lilith RAT ,Atharvan RAT** and **HardBit Ransomware** in Breach and Attack Simulation(BAS).

Threat Advisories

Check out the links below for more extensive remediation and security precautions.

APT Earth Kitsune delivers new WhiskerSpy malware via watering hole attack

Multiple Fortinet products are vulnerable to unauthorized code execution flaws

The Intricate Evolution of SoulSearcher Loader for Multi-Stage Malware Execution

A New Info-Stealing Malware Named “Stealc” Targeting Cryptocurrency Wallets

WIP26 attacks Middle Eastern telecom service providers

Mylobot: A Sophisticated Botnet Malware Targeting Computers Worldwide

DarkCloud Stealer A Multi-Stage Malware That Pilfers Sensitive data

Injection vulnerability in VMware Carbon Black App Control

HardBit Ransomware: A Threatening Cyber Attack Targeting Organizations with New Version 2.0

Newly Identified Threat Actor Hydrochasma Targets Shipping Companies and Medical Laboratories in Asia

Icarus a Versatile Infostealer with Rootkit and hVNC Capabilities

New Attack Group Clasiopa Targets Materials Research Organization in Asia with Custom Malware

Exploiting ChatGPT's Popularity for Malware Distribution

Lazarus Strikes with WinorDLL64 Backdoor Discovered in Wslink Malware loader

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**:Threat Exposure Management Platform.

Contextualize
Uni5 Threat Exposure Management
Resolve
Prioritize

REPORT GENERATED ON

February 27, 2023 • 3:30 AM

More at www.hivepro.com