Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

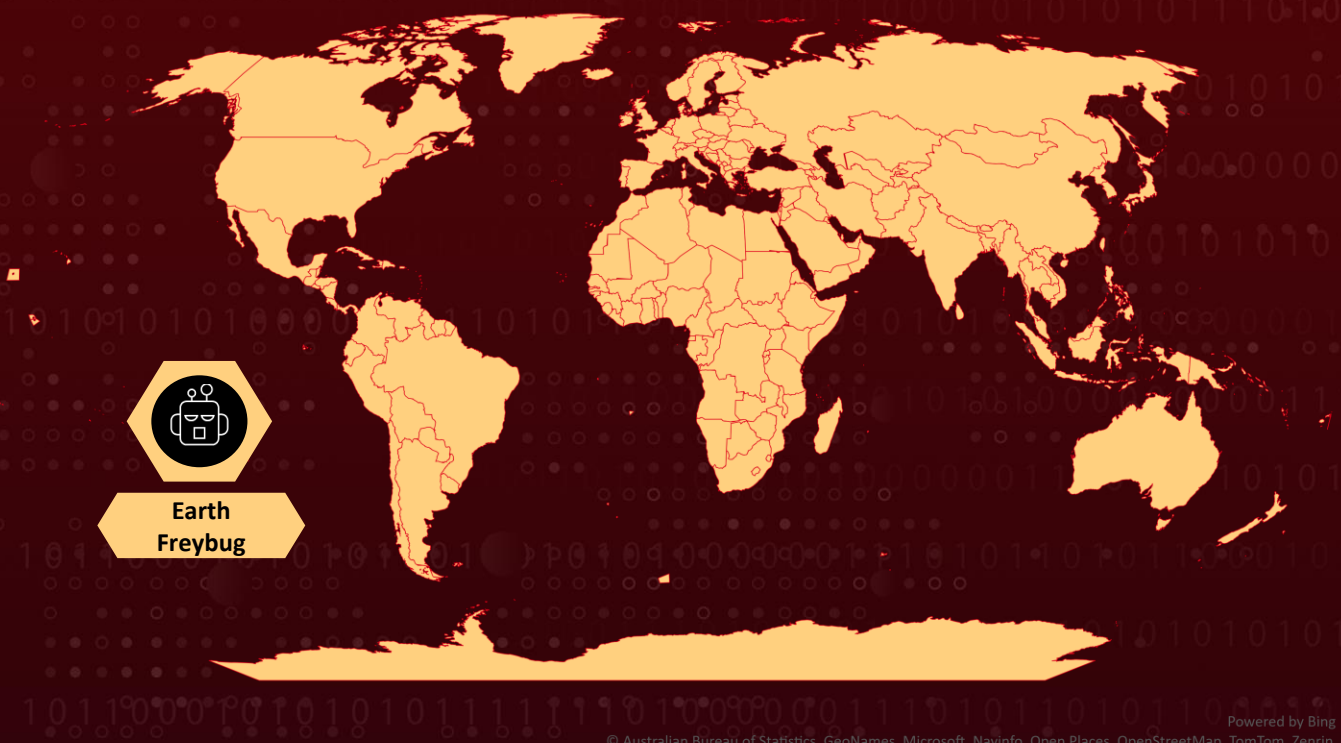
Unveiling Earth Freybug's New TTPs Adoption with UNAPIMON

Date of Publication	Admiralty Code	TA Number
April 3, 2024	A1	TA2024126

Summary

Attack Began: April 2024
Targeted Countries: Worldwide
Threat Actor: Earth Freybug
Malware: UNAPIMON
Affected Platform: Windows and VMware
Attack: Earth Freybug, a cyberthreat group, employs diverse tools for espionage and financial gain since 2012. Their recent attack involves UNAPIMON malware, evading detection by hijacking legitimate processes and unhooking critical APIs, highlighting the need for robust cybersecurity defenses against evolving threats.

Attack Regions



Attack Details

#1

Earth Freybug, also known as a subset of APT41, is a cyberthreat group that has been operational since at least 2012, engaging in espionage and financially motivated activities. They target organizations across various sectors and countries, utilizing a diverse array of tools and techniques, including LOLBins and custom malware. Recently Earth Freybug employed two techniques DLL hijacking and API unhooking, as observed in a new malware called UNAPIMON.

#2

The attack flow involves hijacking legitimate processes like vmtoolsd.exe and schtasks.exe to establish remote scheduled tasks and execute malicious batch files like cc.bat on target machines. These batch files gather system information and set up backdoors for further infiltration. Notably, the second cc.bat leverages DLL side-loading via the SessionEnv service to inject the UNAPIMON malware, which employs defense evasion tactics to avoid monitoring of child processes.

#3

UNAPIMON is a straightforward DLL malware written in C++, designed to prevent monitoring of child processes. It achieves this by hooking into the CreateProcessW function and unhooking critical API functions in child processes, thereby allowing malicious activities to go undetected. Despite its simplicity, UNAPIMON showcases the ingenuity of its creators and the potential threat posed by seemingly basic techniques.

#4

Overall, Earth Freybug continues to evolve, refining their techniques to achieve their objectives. This attack underscores the importance of vigilance against both sophisticated and seemingly simple tactics in cybersecurity defense.

Recommendations

Implement Least Privilege Access: Restrict admin privileges to only those individuals who require them for their roles. Limiting admin access reduces the attack surface and minimizes the impact of potential breaches.

Frequent Password Rotation: Enforce regular password changes for all user accounts, especially those with elevated privileges. Implementing strong password policies and multi-factor authentication adds an extra layer of security.

Continuous Monitoring and Logging: Maintain thorough monitoring of system and network activities, and keep detailed logs of user actions, especially those involving critical processes and file access. Regularly review these logs for suspicious activities.

Enhance Endpoint Security: Deploy advanced endpoint protection solutions that can detect and prevent malicious activities, including DLL hijacking and API unhooking techniques employed by attackers like Earth Freybug. Ensure that endpoint protection software is regularly updated and configured properly.

Potential MITRE ATT&CK TTPs

TA0007 Discovery	TA0008 Lateral Movement	TA0001 Initial Access	TA0002 Execution
TA0040 Impact	TA0005 Defense Evasion	TA0003 Persistence	TA0004 Privilege Escalation
TA0043 Reconnaissance	T1574 Hijack Execution Flow	T1106 Native API	T1053.005 Scheduled Task
T1053 Scheduled Task/Job	T1592 Gather Victim Host Information	T1574.002 DLL Side-Loading	T1190 Exploit Public-Facing Application
T1059.001 PowerShell	T1059 Command and Scripting Interpreter	T1082 System Information Discovery	T1574.006 Dynamic Linker Hijacking
T1036 Masquerading	T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution	T1489 Service Stop

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	62ad0407a9cce34afb428dee972292d2aa23c78cbc1a44627cb2e8b945195bc2

References

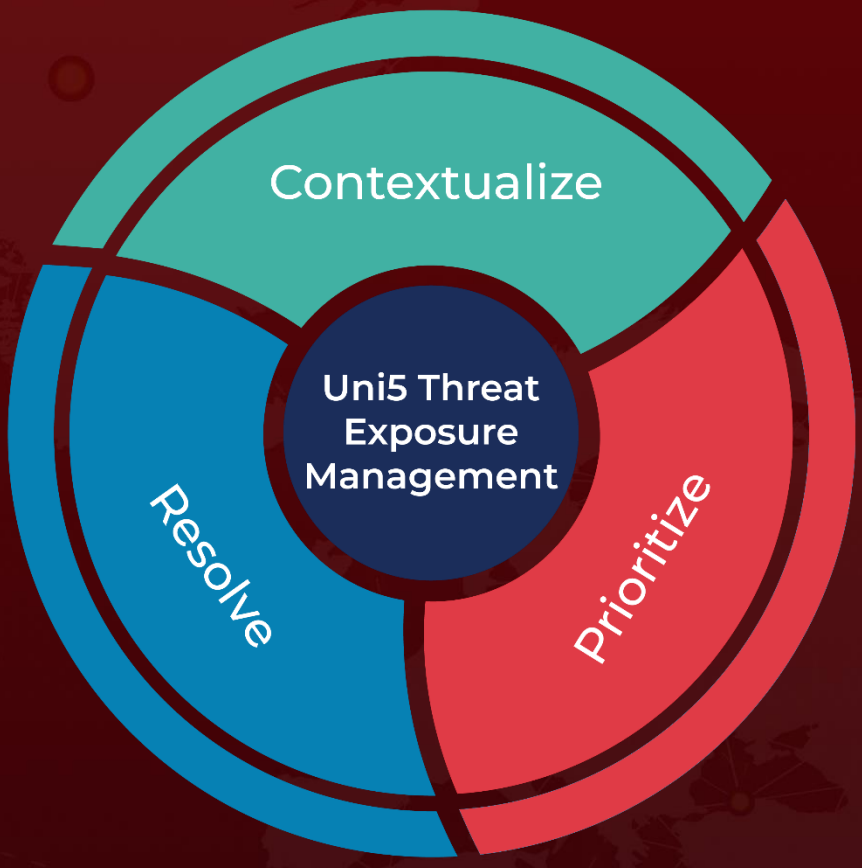
https://www.trendmicro.com/en_us/research/24/d/earth-freybug.html

https://www.hivepro.com/threat-advisory/blackfly-chinese-apt-targets-asian-conglomerate-in-materials-sector/

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.



REPORT GENERATED ON

April 3, 2024 • 4:30 AM

More at www.hivepro.com