Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

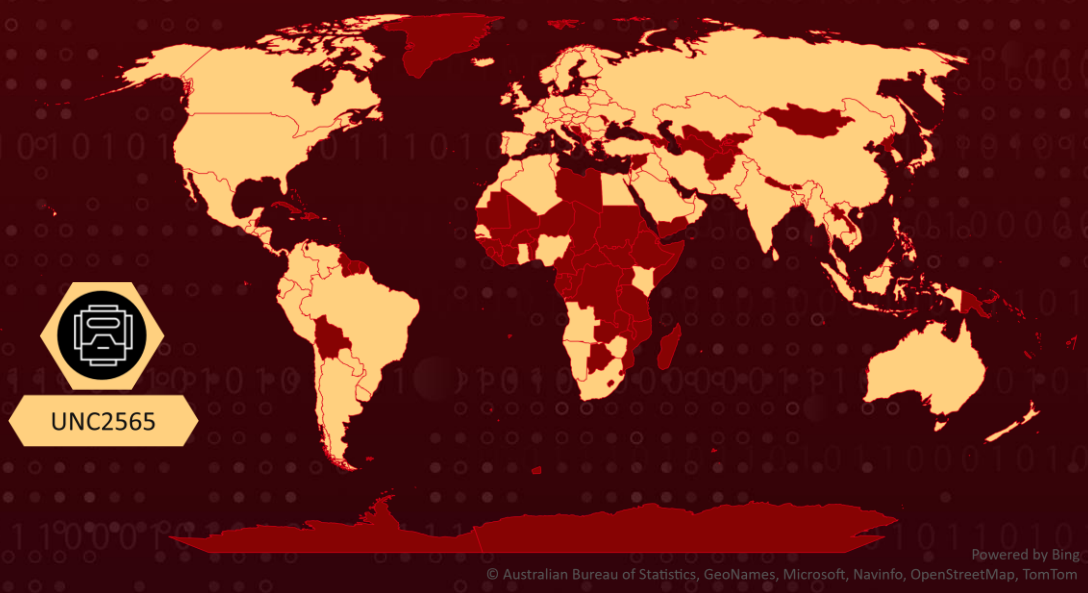
Infection and Evolution of the GOOTLOADER Malware

Date of Publication	Admiralty Code	TA Number
January 31, 2023	A1	TA2023054

Summary

First appeared: Late 2020
Threat Actor: UNC2565
Attack Region: United States, India, Canada, Japan, Russia, Thailand, Colombia, Belgium, Romania, Germany, Netherlands, Philippines, United Kingdom, Poland, South Africa, United Arab Emirates, France, Italy, Singapore, Switzerland, Algeria, Brazil, Turkey, Australia, Spain, Sweden, Hong Kong, Egypt, Ireland, Indonesia, Mexico, Ukraine, Saudi Arabia, Denmark, Croatia, Austria, Pakistan, Lithuania, Peru, Morocco, Malaysia, Vietnam, Czech Rep., Latvia, Finland, Nigeria, Argentina, Bulgaria, Kenya, Kazakhstan, Kuwait, Tunisia, Estonia, Hungary, Luxembourg, CÃ´te d'Ivoire, Taiwan, Bangladesh, Israel, Oman, New Zealand, Chile, Dominican Rep., Norway, Slovakia, Puerto Rico, Serbia, Qatar, Iran, South Korea, Sri Lanka, Panama, Portugal, Jamaica, Nicaragua, Costa Rica, Greece, Ecuador, Jordan, Slovenia, Ghana, Guatemala, Belarus, China, Honduras, Iraq, Mauritius, Uruguay, Cambodia, Myanmar, Senegal, El Salvador, Lebanon, Paraguay, Angola, Cyprus, Iceland, Malta, Namibia, Venezuela, Zimbabwe
Attack Sector: Government, Retail, Banking/Financial/Wealth Management, Healthcare, Outsourcing & Hosting, Technology/IT, Transportation & Shipping, Insurance, Automotive, Discrete Manufacturing, Wholesale
Attack: GOOTLOADER malware infects via malicious archive download, executing JavaScript and PowerShell, delivering FONELAUNCH, Cobalt Strike BEACON/SNOWCONE, with the latest variant writing JavaScript to disk and creating a task.

Attack Regions



Attack Details

#1

GOOTLOADER infections have begun since late 2020, with threat actors spreading the malware widely, impacting various industry verticals and geographic regions. The group behind the malware and infrastructure is only attributed to UNC2565 and is believed to be exclusive to this group. In 2022, UNC2565 started incorporating changes to their tactics, techniques, and procedures, including the use of multiple variations of the FONELAUNCH launcher, the distribution of new follow-on payloads, and changes to the GOOTLOADER downloader and infection chain, including the introduction of GOOTLOADER.POWERSHELL.

#2

GOOTLOADER infections start with the victim downloading a malicious archive from a compromised website after searching for business-related documents. The archive contains a JavaScript file, GOOTLOADER, which downloads additional payloads, FONELAUNCH, and Cobalt Strike BEACON or SNOWCONE, and stores them in the registry. These payloads are executed using PowerShell in later stages. The typical infection chain was consistent until November 2022, when a new variant of GOOTLOADER, GOOTLOADER.POWERSHELL, was observed using a new infection chain. This new variant writes a second JavaScript file to disk and creates a scheduled task to execute it. This new chain reaches out to 10 hardcoded URLs and collects information about the victim's environment. The payloads are then written to the registry.

#3

Post-compromise activity of GOOTLOADER has mainly been limited to internal reconnaissance, as the intrusions have been quickly detected and mitigated.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.

- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
T1620 Reflective Code Loading	T1012 Query Registry	T1055 Process Injection	T1055.012 Process Hollowing
T1083 File and Directory Discovery	T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading	T1218 System Binary Proxy Execution
T1218.010 Regsvr32	T1218.011 Rundll32	T1056 Input Capture	T1082 System Information Discovery
T1518 Software Discovery	T1518.001 Security Software Discovery	T1071 Application Layer Protocol	T1036 Masquerading
T1010 Application Window Discovery	T1573 Encrypted Channel	T1018 Remote System Discovery	T1497 Virtualization/Sandbox Evasion
T1095 Non-Application Layer Protocol	T1129 Shared Modules	T1564 Hide Artifacts	T1564.003 Hidden Window
T1057 Process Discovery	T1105 Ingress Tool Transfer	T1562 Impair Defenses	T1562.001 Disable or Modify Tools
T1140 Deobfuscate/Decode Files or Information	T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1059.007 JavaScript
T1027 Obfuscated Files or Information	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1053 Scheduled Task/Job
T1053.005 Scheduled Task			

Indicator of Compromise (IOCs)

TYPE	VALUE
MD5	1011b2cbe016d86c7849592a76b72853,80a79d0c9cbc3c5188b7a247907e7264,bee08c4481babb4c0ac6b6bb1d03658e,82607b68e061abb1d94f33a2e06b0d20,961cd55b17485bfc8b17881d4a643ad8,af9b021a1e339841cfdf65596408862d,d3787939a5681cb6d6ac7c42cd9250b5,ea2271179e75b652cafd8648b698c6f9,ab1171752af289e9f85a918845859848,d6220ca85c44e2012f76193b38881185,35238d2a4626e7a1b89b13042f9390e9,53c213b090784a0d413cb00c27af6100,7352c70b2f427ef4ff58128a428871d3,a0b7da124962b334f6c788c27beb46e3,a4ee41bd81dc3b842ddb2952d01f14ed,d401dc350aff1e3fd4cc483238208b43,ec17564ac3e10530f11a455a475f9763,f9365bf8d4b021a873eb206ec98453d9,aec78c1ef489f3f4b621037113cbdf81,08fa99c70e90282d6bead3bb25c358dc,aef6d31b3249218d24a7f3682a00aa10,04746416d5767197f6ce02e894affcc7,2eede45eb1fe65a95aefa45811904824,3d768691d5cb4ae8943d8e57ea83cac1,84f313426047112bce498aad97778d38,92a271eb76a0db06c94688940bc4442b,328b032c5b1d8ad5cf57538a04fb02f2,7a1369922cfb6d00df5f8dd33ffb9991
Domains	jonathanbartz[.]com jp[.]imonitorsoft[.]com junk-bros[.]com kakiosk[.]adsparkdev[.]com kepw[.]org kristinee[.]com lakeside-fishandchips[.]com
URLs	hxxps://108.61.242[.]65/dot.gif hxxps://108.61.242[.]65/submit.php hxxps://146.70.78[.]43/fwlink hxxps://146.70.78[.]43/submit.php hxxps://87.120.254[.]39/ga.js hxxps://87.120.254[.]39/submit.php hxxps://45.150.108[.]213/ptj hxxps://45.150.108[.]213/submit.php hxxps://92.204.160[.]240/load hxxps://92.204.160[.]240/submit.php

References

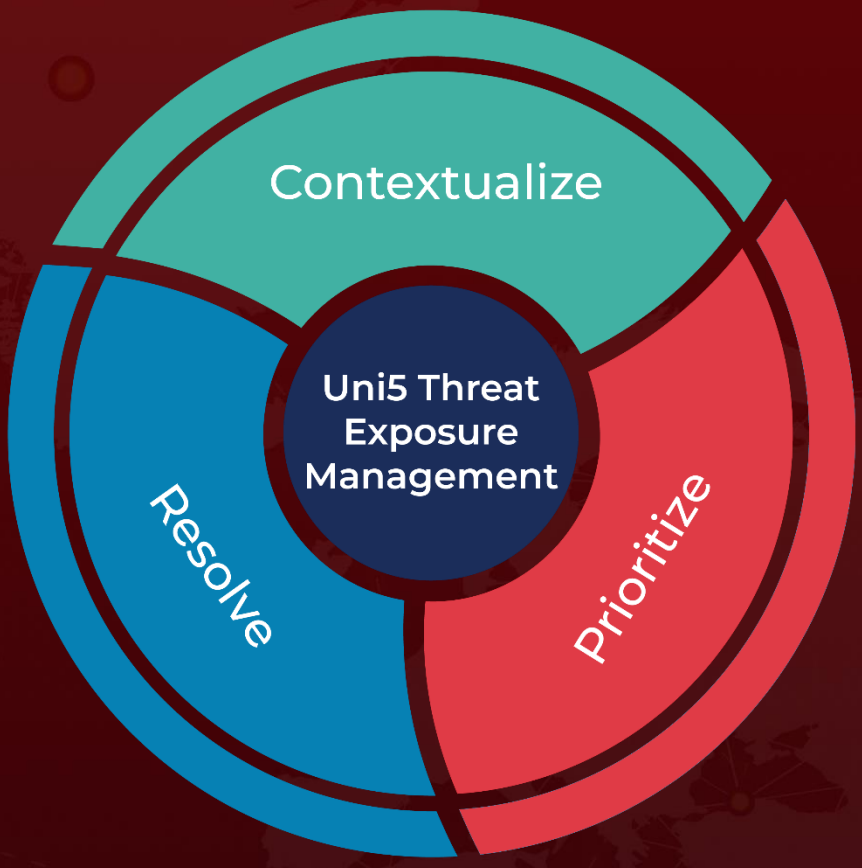
https://www.mandiant.com/resources/blog/tracking-evolution-gootloader-operations

https://www.hivepro.com/gootkit-loader-is-targeting-organizations-in-the-australian-healthcare-industry/

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

January 31, 2023 . 4:55 AM

More at www.hivepro.com