Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

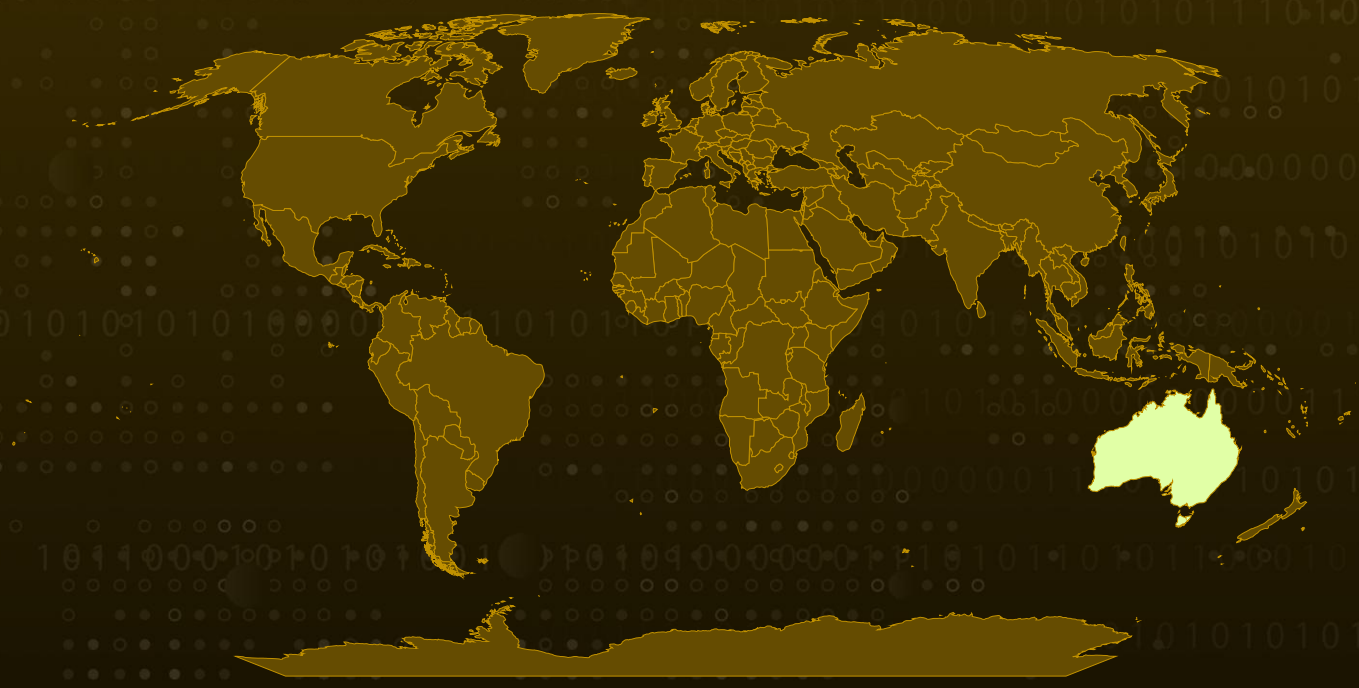
GootLoader's Evolution: From SEO Poisoning to Persistent Network Intrusions

Date of Publication	Admiralty Code	TA Number
November 12, 2024	A1	TA2024425

Summary

Attack Discovered: March 2024
Targeted Countries: Australia
Malware: GootLoader, GootKit
Attack: GootLoader has recently targeted Bengal cat enthusiasts in Australia with a new variant, leveraging SEO poisoning to manipulate Google search results and redirect users to malicious sites. Actively exploited in the wild, this variant exploits users' trust with a tailored approach to gain initial access. The campaign then delivers the GootKit RAT and an advanced information stealer, enabling persistent exploitation and further compromise.

Attack Regions



Attack Details

#1 Since early 2024, GootLoader has become a sophisticated access-as-a-service platform for information theft and ransomware deployment. Exploiting SEO poisoning, it redirects users to malicious sites, often under the guise of legitimate content. A recent variant targeted users searching for Bengal cat information in Australia, leading them to download a .zip archive containing an obfuscated JavaScript file. This file triggered the infection chain, redirecting the browser to a malicious site and facilitating the deployment of the GootKit RAT and info-stealer, establishing persistence for further attacks.

#2 The infection chain unfolds in multiple stages. The first stage executes an obfuscated JavaScript file from the .zip archive, setting up GootLoader. In the second stage, WScript.exe runs another JavaScript file, creating persistence through a scheduled task named “Business Aviation.” The third stage then attempts to use PowerShell to execute further tools, such as Cobalt Strike, though full deployment sometimes fails, halting additional exploitation.

#3 During static analysis, GootLoader’s evasion techniques were evident through dynamic filenames and generic licensing comments, marking the variant as GootLoader 3.0. Further highlighted the infection’s behaviors, such as file creation in the user’s AppData directory and persistence mechanisms via CScript.exe and PowerShell. Communication with C2 domains was observed, facilitating GootLoader’s call-back functions, establishing a base for potential follow-up exploitation or data theft.

#4 Organizations should bolster defenses, particularly in monitoring unusual file paths, restricting script execution, and raising user awareness about deceptive download sources.

Recommendations

- **Enhance Browser Security:** Use browser extensions that detect and alert users to potential SEO poisoning within search results related to niche or trending topics.
- **Restrict Access to Trusted Domains Only:** Implement web filters to block access to unauthorized domains and restrict access to high-risk or uncategorized websites. Limiting the ability to reach domains known for SEO poisoning can reduce exposure to malicious payloads.
- **Remain Vigilant:** Educate staff on identifying phishing risks and encourage them to avoid downloading attachments from unverified or unusual links.
- **Conduct Endpoint Detection and Response (EDR) Monitoring:** Implement EDR tools to detect unusual behaviors, such as unexpected use of PowerShell, scheduled tasks, and file creation in sensitive directories (e.g., AppData).

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0007 Discovery	TA0010 Exfiltration	T1608 Stage Capabilities
T1608.001 Upload Malware	T1608.006 SEO Poisoning	T1189 Drive-by Compromise	T1059 Command and Scripting Interpreter
T1059.007 JavaScript	T1053 Scheduled Task/Job	T1053.005 Scheduled Task	T1027 Obfuscated Files or Information
T1027.009 Embedded Payloads	T1082 System Information Discovery	T1567 Exfiltration Over Web Service	T1036 Masquerading
T1204 User Execution	T1204.001 Malicious Link		

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps[:]//ledabel[.]be/en/are-bengal-cats-legal-in-australia-understanding-the-laws-and-regulations/#:~:text=In%20most%20cases%2C%20you%20do,a%20Bengal%20cat%20in%20Australia, hxxps[:]//www[.]chanderbhushan[.]com/doc[.]php, hxxps[:]//serviciilaser[.]ro/xmlrpc[.]php, hxxps[:]//metropole[.]com[.]au/xmlrpc[.]php, hxxps[:]//fannisho[.]com/xmlrpc[.]php, hxxps[:]//gobranded[.]com/xmlrpc[.]php, hxxps[:]//climatehero[.]me/xmlrpc[.]php, hxxps[:]//wyantgroup[.]com/xmlrpc[.]php, hxxps[:]//rkbaienfurt[.]de/xmlrpc[.]php, hxxps[:]//beezzly[.]com/xmlrpc[.]php, hxxps[:]//playyourbeat[.]com/xmlrpc[.]php, hxxps[:]//wowart[.]vn/xmlrpc[.]php
Files	Are_bengal_cats_legal_in_australia_33924.zip, Are_bengal_cats_legal_in_australia_33924.js, Rehabilitation Services.js, Huthwaite SPIN selling.dat, Small Units Tactics.js
SHA256	435f48667b32c3ab8bb806a8783c0fc40af86e6c5cbf6f621d6e1a3f331483ed, ea781eef1da03ea2c3b5250ce26b00445d8a5123bbb0575c583211cca53c61db, 9a7e79d4ff235feb12672979dfc073d2b4572233772ae500ef6b69c670a9820e, 5f2c97499943878d853332da541138bd6ccbafca7e00d6f90d06545b27b66ca3

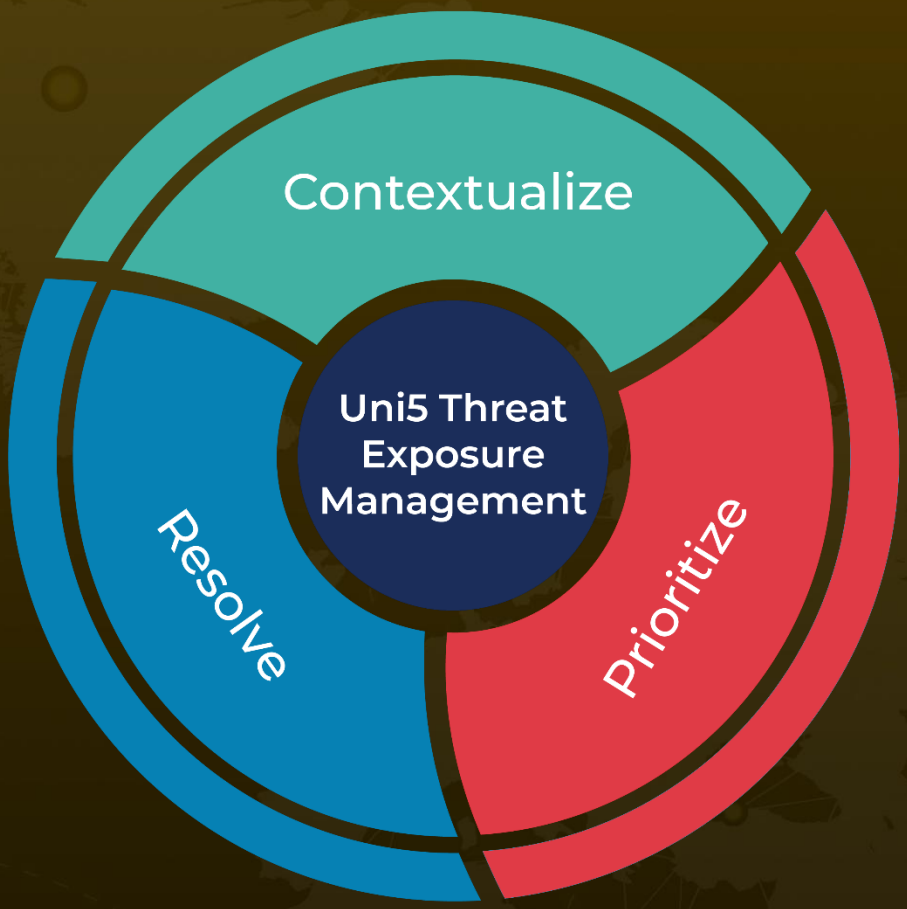
References

https://news.sophos.com/en-us/2024/11/06/bengal-cat-lovers-in-australia-get-psspsspssd-in-google-driven-gootloader-campaign/

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

November 12, 2024 . 7:30 AM

More at www.hivepro.com