Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

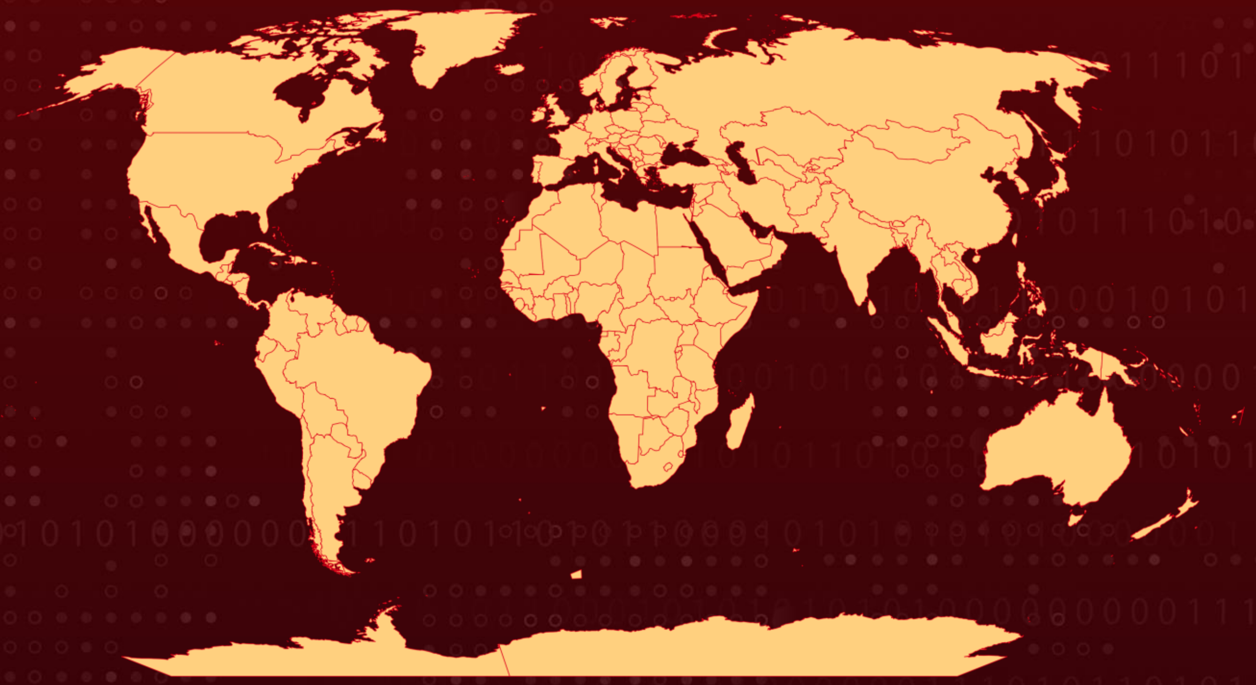
CherryTree Impostor Dubbed CherryLoader Makes Its Move

Date of Publication	Admiralty Code	TA Number
January 31, 2024	A1	TA2024039

Summary

Malware: CherryLoader
Attack Region: Worldwide
Attack: CherryLoader, a new Go-based downloader, has surfaced in cyber attacks, masquerading as the legitimate CherryTree note-taking app. This sophisticated threat infiltrates compromised hosts, delivering malicious payloads such as privilege escalation tools for exploitation and persistent control.

Attack Regions



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

Attack Details

#1 A novel downloader named CherryLoader, developed using the Go programming language, has become a tool in cyber attacks. Threat actors skillfully masked this loader by adopting the icon and name of the legitimate CherryTree note-taking application, deceiving unsuspecting victims in the process.

#2 CherryLoader's main objective is to introduce additional malicious payloads, such as privilege escalation tools, onto compromised hosts, enabling subsequent exploitation and ensuring persistence. While the method of CherryLoader distribution remains undisclosed, attack patterns indicate that CherryLoader and its associated files are contained within an RAR archive file hosted on the IP address 141.11.187[.]70.

#3 The RAR file functions as an executable, unpacking and launching the Golang binary only if the first argument matches a predetermined MD5 password hash. Upon execution, the loader decrypts "NuxtSharp.Data" and writes its contents to a disk file. This file employs a fileless technique known as "Process Ghosting," first identified in June 2021.

#4 Process Ghosting allows an attacker to covertly execute malicious code by writing malware to disk in a way that evades scanning or deletion. The deleted malware then operates as if it were a standard file on disk, providing a discreet method of operation. CherryLoader is utilized to drop one of two privilege escalation tools, namely PrintSpoofer or JuicyPotatoNG.

#5 Subsequently, a batch file is executed to establish persistence on the victim's device. This process includes creating an admin account in the system, whitelisting and excluding executable files in Windows Defender and Microsoft Defender, disabling AntiSpyware, and modifying firewall rules to allow remote connections, among other actions.

Recommendations

Anomaly Detection: Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

Ensure Software Authenticity: Exercise caution when downloading or updating software. Verify the authenticity of applications, particularly those that bear a resemblance to popular ones such as CherryTree.

Enhance Endpoint Security: Strengthen endpoint security by employing measures such as endpoint detection and response (EDR) solutions. These tools can help identify and respond to suspicious activities associated with CherryLoader.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	T1059 Command and Scripting Interpreter	T1136 Create Account
T1068 Exploitation for Privilege Escalation	T1055.003 Thread Execution Hijacking	T1543 Create or Modify System Process	T1574 Hijack Execution Flow
T1562 Impair Defenses	T1656 Impersonation	T1564 Hide Artifacts	T1140 Deobfuscate/Decode Files or Information
T1082 System Information Discovery	T1105 Ingress Tool Transfer	T1036 Masquerading	T1027.011 Fileless Storage

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	141.11.187[.]70
SHA256	50f7f8a8d1bd904ad7430226782d35d649e655974e848ff58d80eafedd377ee9, f9373383d2a1cea0179d016b4496475d44262945ab5fb6ff28cd156187c6ff6a, 8c42321dd19bf4c8d2ef11885664e79b0064194e3222d73f00f4a1d67672f7fc,

TYPE	VALUE
SHA256	7936b3d7d512c3a89914595c5048bce3c07bb872af59304fed95c567694230b0, e0f53fb3651caf5eb3b30603064d527b9ac9243f8e682e4367616484ec708976, 08b8d8f8317936dad4f34676823b2eeb4fe99b0f4c213224e035b403e1e76cc0, 92263e5085cb3fe58fd5803536c80c5c1084500c79fc026367a15b0f04ca0142, 9e6338674cd29066a4daad4ac54f01d272040d4947de39cfdf562e59af7c1318, 3641f3ddeb7583051f81ac15542850a1fba7591372389411a4b86363fdf02e78, 438c7ef49fbadd67bf809f7e3e239557e1d18d4c80e42c57f9479a89e3672fd9

References

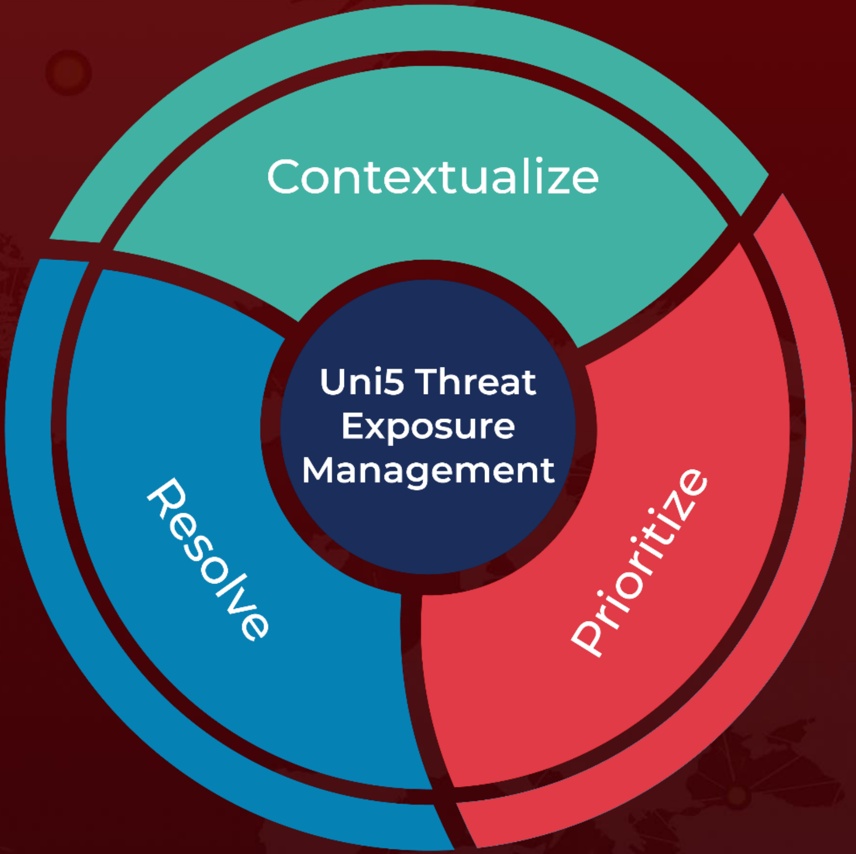
https://arcticwolf.com/resources/blog/cherryloader-a-new-go-based-loader-discovered-in-recent-intrusions/

https://www.elastic.co/blog/process-ghosting-a-new-executable-image-tampering-attack

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, 2024 • 3:00 AM

More at www.hivepro.com