Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

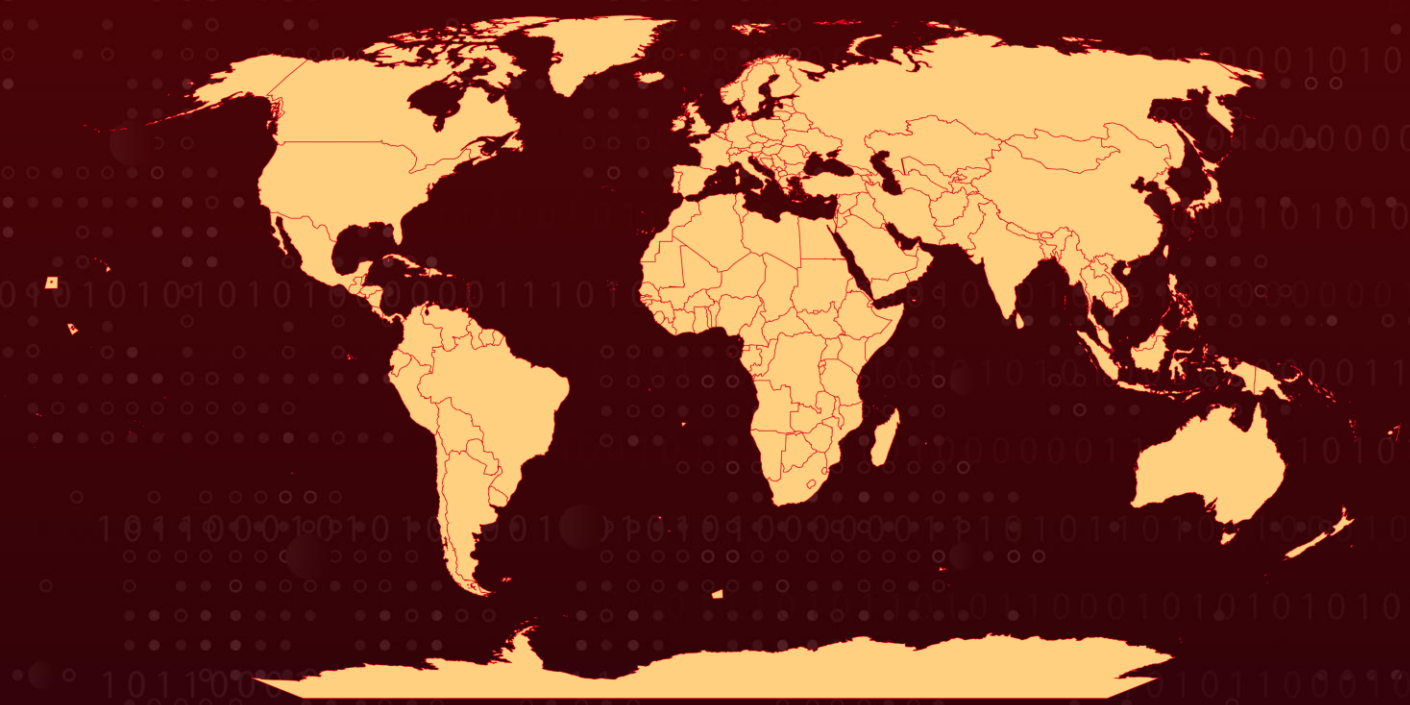
Maliciously Crafted Cracked Software Propagates Lumma Stealer via YouTube

Date of Publication	Admiralty Code	TA Number
January 12, 2024	A1	TA2024013

Summary

Attack Discovered: 2023
Attack Region: Worldwide
Malware: Lumma Stealer
Attack: In an attempt to deceive users into downloading the information-stealing virus Lumma, threat actors are exploiting YouTube videos featuring content related to cracked software. These videos typically include content related to the use of cracked software, accompanied by identical installation instructions. Furthermore, Lumma Stealer was recently discovered to incorporate a new feature, providing persistent Google OAuth access.

Attack Regions



Attack Details

#1 A threat group is utilizing YouTube channels as a distribution method for a variant of the Lumma Stealer. The videos typically feature content related to cracked applications, along with installation guides and malicious URLs. To evade web filter blacklists, the threat actors leverage open-source platforms such as GitHub and MediaFire. Users who follow the shared links can directly download a new private .NET loader, which, in turn, retrieves the final Lumma Stealer malware.

#2 Since early 2023, YouTube has been a focal point for promoting pirated software through consistent attack chains distributing various types of malware, including stealers, cutters, and crypto miners. In the latest attack sequence, viewers are directed to click on a link in the video's description, which results in the download of a ZIP file fake installer hosted on MediaFire.

#3 Upon extracting the contents of the ZIP installer, it exposes a Windows shortcut (LNK) that masquerades as a setup file. In reality, this Windows shortcut is designed to download a.NET loader from a GitHub repository. The loader is responsible for loading the Lumma Stealer payload, subjecting the execution to various anti-virtual machine and anti-debugging checks before proceeding. This multi-layered approach aims to enhance the malware's evasion and persistence capabilities.

#4 Lumma Stealer, developed in C Language, is designed to target browsers, cryptocurrency wallets, system data with the goal of stealing sensitive information from users' computers. It employs various obfuscation techniques and is actively promoted on dark web forums. The malware establishes communication with a C2 server through a POST request using a Lumma ID and a hardcoded User-Agent. It has recently transitioned its data exfiltration method to leverage HTTPS.

#5 Recently, a number of malware programmes, such as Lumma, have brought attention to a new feature that allows for persistent **Google OAuth** access. Users should only download software from reliable and safe sites due to the risks involved with using cracked software and the spread of malware such as Lumma.

Recommendations

Avoid cracked software: It is strongly advised to refrain from using cracked or free software obtained from unofficial sources, as these versions often come with hidden malware like Lumma Stealer. Opt for legitimate and licensed software from official vendors to ensure the integrity and security of your systems.

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Download from Official Websites: Always download software from the official website of the developer or the project. Check the URL to make sure it's legitimate. If the software is open source, consider downloading it from well-known repositories like GitHub, GitLab, or Bitbucket.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0005** Defense Evasion
TA0007 Discovery	**TA0010** Exfiltration	**TA0011** Command and Control	**T1566** Phishing
T1033 System Owner/User Discovery	**T1608** Stage Capabilities	**T1027** Obfuscated Files or Information	**T1204** User Execution
T1036 Masquerading	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell	**T1048** Exfiltration Over Alternative Protocol
T1048.002 Exfiltration Over Asymmetric Encrypted Non-C2 Protocol			

Indicators of Compromise (IOCs)

TYPE	VALUE
IP	176[.]113[.]115[.]224, 176[.]113[.]115[.]226, 176[.]113[.]115[.]227, 176[.]113[.]115[.]229, 176[.]113[.]115[.]232
Hostnames	Netovrema[.]pw opposesicknessopw[.]pw politefrightenpowoa[.]pw chincenterblandwka[.]pw
SHA256	48cbeb1b1ca0a7b3a9f6ac56273fbaf85e78c534e26fb2bca1152ecd7542af54, 483672a00ea676236ea423c91d576542dc572be864a4162df031faf35897a532, 01a23f8f59455eb97f55086c21be934e6e5db07e64acb6e63c8d358b763dab4f, 7603c6dd9edca615d6dc3599970c203555b57e2cab208d87545188b57aa2c6b1

References

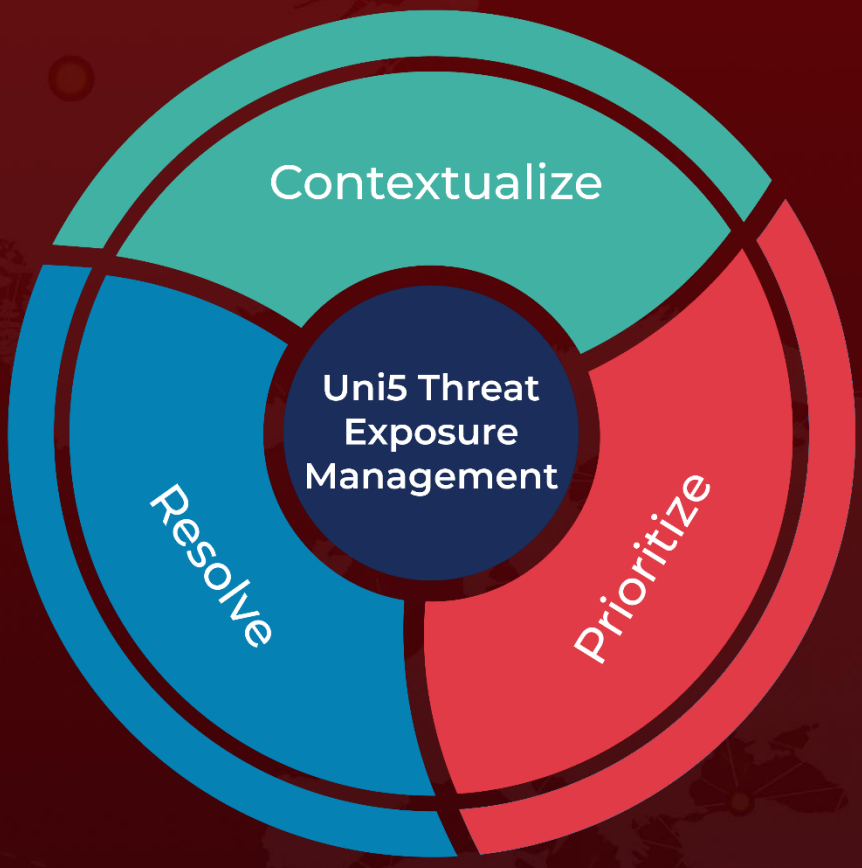
https://www.fortinet.com/blog/threat-research/lumma-variant-on-youtube

https://www.hivepro.com/threat-advisory/malware-leveraging-google-oauth-for-persistent-account-access/

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 12, 2024 . 4:50 AM

More at www.hivepro.com