Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

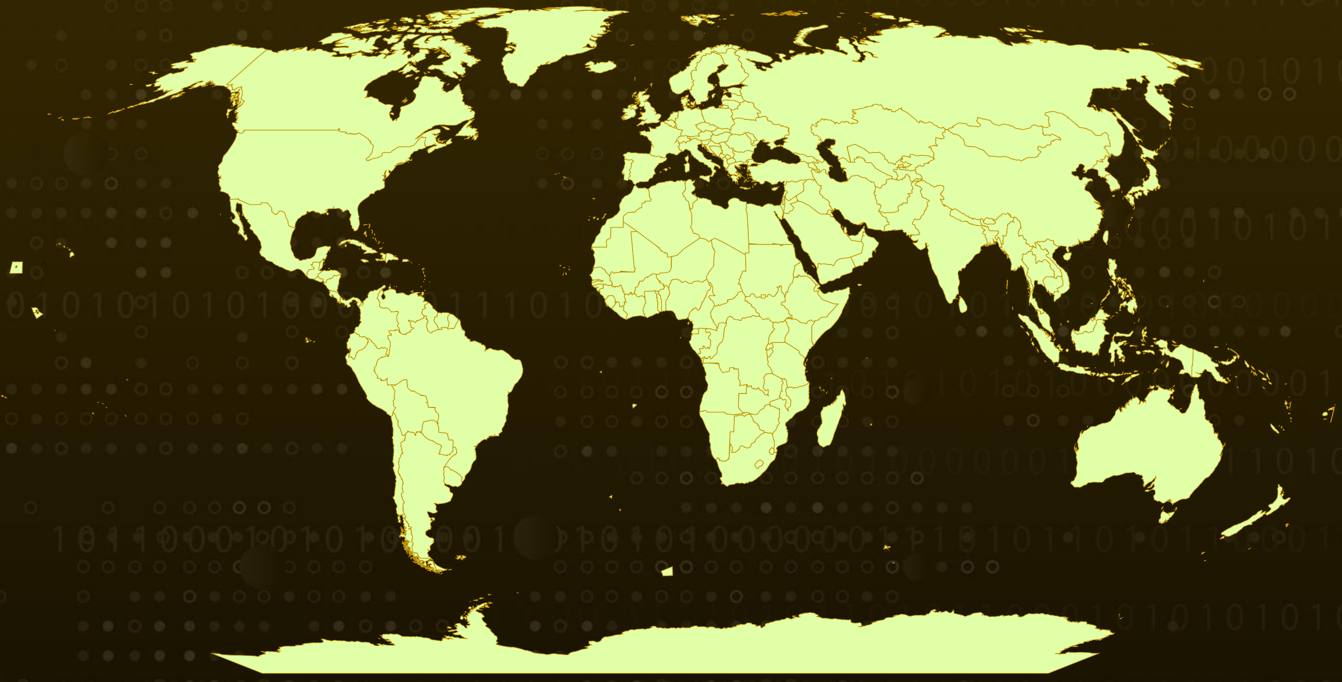
Gomorrah Stealer v5.1: A MaaS Malware with a Growing Arsenal

Date of Publication	Admiralty Code	TA Number
September 17, 2024	A1	TA2024359

Summary

First Seen: 2020
Targeted Countries: Worldwide
Malware: Gomorrah Stealer
Affected Platforms: Windows
Attack: The Gomorrah Stealer v5.1 is a sophisticated MaaS malware that targets sensitive data from browsers, cryptocurrency wallets, and more. It uses .NET-based IL code and JIT compilation to evade detection, exfiltrates data to a C2 server, and ensures persistence through Autorun registry entries. Distributed via Telegram, the malware continues to evolve, highlighting the need for enhanced cybersecurity measures.

Attack Regions



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

Attack Details

#1 Gomorrah Stealer v5.1 is a sophisticated information-stealing malware that operates within a malware-as-a-service (MaaS) framework. Its primary objective is to extract sensitive data from compromised systems, targeting information such as passwords, credit card details, and cookies from various applications, including web browsers and cryptocurrency wallets. The stealer employs advanced evasion techniques to avoid detection, making it a formidable tool for cybercriminals.

#2 The operational behavior of the Gomorrah Stealer is marked by its use of .NET-based pure Intermediate Language (IL) code, which is executed through Just-In-Time (JIT) compilation. This design choice facilitates evasion of static analysis techniques commonly employed by security software.

#3 The malware is typically distributed through drive-by-downloads, or infected websites. Upon execution, the malware collects extensive information about installed programs and system configurations by querying the Windows registry and other directories. It then organizes this data within a designated folder in the Temp directory before compressing it into zip files for exfiltration to a command-and-control (C2) server. The malware's persistence is ensured through the creation of Autorun registry entries that allow it to reactivate after system reboots.

#4 Key findings indicate that Gomorrah Stealer v5.1 targets a wide array of applications and data types. It not only extracts information from web browsers but also gathers sensitive data from messaging apps, VPN clients, and FTP clients. The malware's ability to capture configuration settings and authentication details from .ini files further enhances its data collection capabilities. Moreover, it has been observed to take screenshots of user activity, thereby broadening the scope of sensitive information at risk.

#5 The Gomorrah Stealer reflects a fast-changing cyber landscape where advanced malware is easily accessible, often via platforms like Telegram. The ongoing development of this malware, including announcements regarding new versions with enhanced features, highlights the persistent challenges faced by cybersecurity professionals.

Recommendations

Strengthen Authentication: Implement multi-factor authentication (MFA) to protect against credential theft. Regularly rotate passwords for privileged accounts, especially for remote services like VPNs. Continuous monitoring of login attempts is essential to detect suspicious activity early.

Implement Robust Endpoint Protection: Deploy advanced endpoint security solutions with real-time threat detection capabilities to identify and block malware like Gomorrah Stealer. Ensure that antivirus and anti-malware software are up-to-date and configured to perform regular scans.

Enhance Network Security: Implement firewalls and intrusion detection systems (IDS)/ Intrusion Prevention System (IPS) to monitor and block suspicious activities and communications to and from known malicious domains. Use network segmentation to limit the spread of malware and protect sensitive data.

Monitor and Manage Autorun Entries: Regularly review and manage autorun entries and startup programs to identify and remove unauthorized or suspicious entries. Use tools to detect and clean any modifications made to the Windows registry related to persistence mechanisms.

Potential MITRE ATT&CK TTPs

TA0007 Discovery	TA0005 Defense Evasion	TA0011 Command and Control	TA0043 Reconnaissance
TA0002 Execution	TA0010 Exfiltration	T1071 Application Layer Protocol	T1041 Exfiltration Over C2 Channel
T1592 Gather Victim Host Information	T1204 User Execution	T1622 Debugger Evasion	T1497 Virtualization/Sandbox Evasion
T1140 Deobfuscate/Decode Files or Information	T1204.002 Malicious File	T1622 Debugger Evasion	T1083 File and Directory Discovery
T1071.001 Web Protocols			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	E02089570b24b11d6350337069b7e823, 201fb3d8b93205488e1a6a408ce18539, B479fa60615c730d0417b67c1a26274f, 3afd64484a2a34fc34d1155747dd3847
IPV4	172[.]93[.]223[.]99
SHA256	2f8a79b12a7a989ac7e5f6ec65050036588a92e65aeb6841e08dc228ff0e21b4, 62c6aebb6bcc4d2faf985a4af59b111ae1e162419acfae7e7f126189073bddf1, dc33943da400ea506484952ba242737460c73dd2b3e88c16f0f18a0fd6dc459c, Bf78263914c6d3f84f825504536338fadd15868d788bf30d30613ca27abeb7a9
Domain	rougecommunications[.]org

References

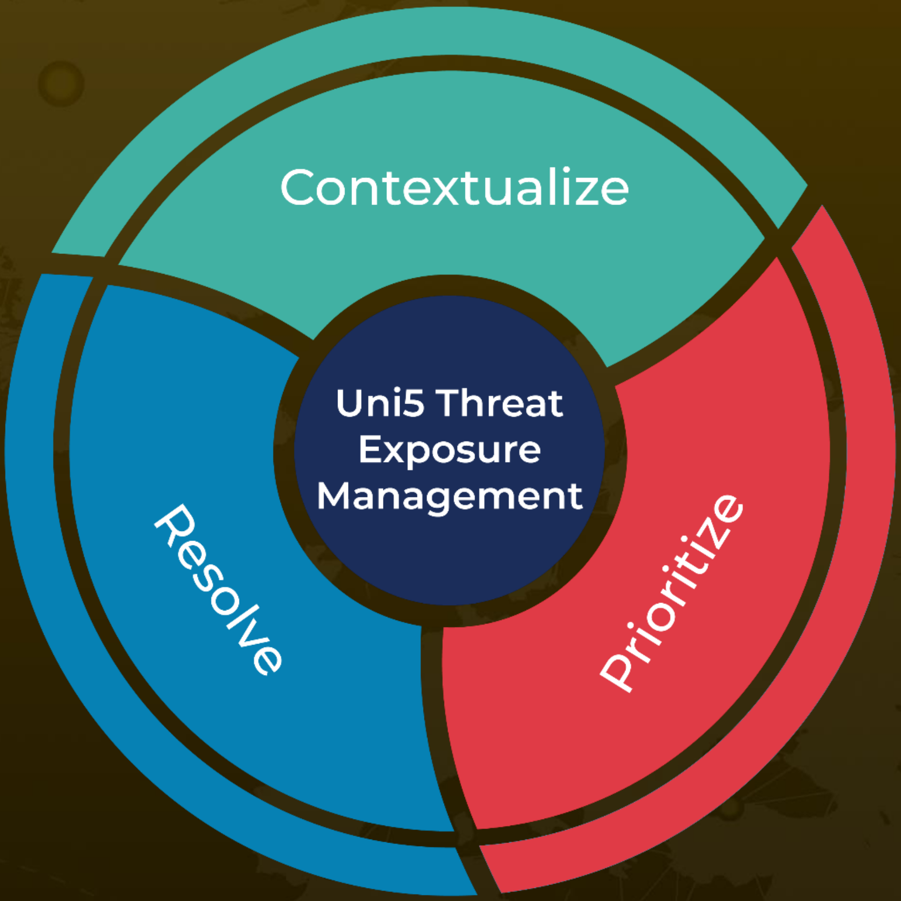
https://www.cyfirma.com/research/gomorrah-stealer-v5-1-an-in-depth-analysis-of-a-net-based-malware/

https://www.broadcom.com/support/security-center/protection-bulletin/gomorrah-stealer-v4-0-activity-observed

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

September 17, 2024 • 6:30 AM

More at www.hivepro.com