Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

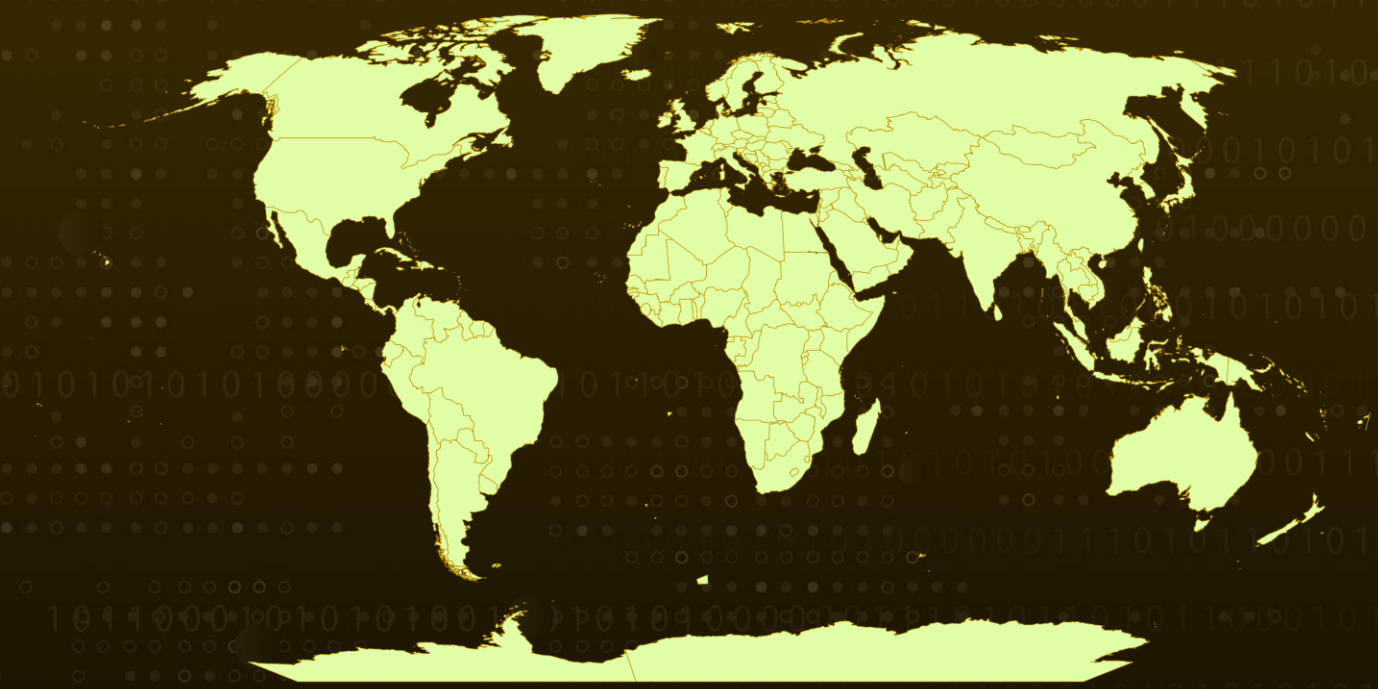
Stealing the Spotlight a Comprehensive Look at Stealers

Date of Publication	Admiralty Code	TA Number
May 23, 2024	A1	TA2024204

Summary

Malware: Acrid, ScarletStealer, Sys01
Attack Region: Worldwide
Attack: Stealers persist as a formidable threat in the malware ecosystem, frequently surfacing new variants. This analysis explores three distinct stealers: Acrid, ScarletStealer, and SYS01. The ongoing emergence of these diverse and increasingly sophisticated stealers underscores the enduring criminal market demand for such malicious tools.

Attack Regions



Attack Details

#1 Stealers pose a significant threat in the cybersecurity landscape. The narrative unfolds with the emergence of a familiar stealer and the introduction of two innovative counterparts, each with unique complexities.

#2 Acrid, revealed in December, though sharing a name with AcridRain, stands as an independent entity. Crafted in C++ for 32-bit systems—an unconventional choice in today's predominantly 64-bit landscape—Acrid employs the "Heaven's Gate" technique. This maneuver allows 32-bit applications to breach the 64-bit realm, evading specific security protocols.

#3 On the other hand, ScarletStealer diverges from the norm with its unorthodox approach. Predominantly reliant on external binaries, such as downloaded applications and Chrome extensions, this malicious entity scours designated file paths in pursuit of cryptocurrencies and crypto wallets. Upon detection, it executes a specified PowerShell command to procure additional executables. However, ScarletStealer's potential is hindered by its underdeveloped state, rife with errors, flaws, and redundant code.

#4 Meanwhile, **SYS01**—dubbed "Album Stealer" or "S1deload Stealer"—has lurked in obscurity since at least 2022. Its transformation from a C# framework to a PHP-based architecture is meticulously documented. Presenting a hybrid payload incorporating elements of both languages, SYS01 entices users through deceptive means, tempting them to download a malicious ZIP archive masquerading as adult content via deceptive Facebook pages.

#5 Despite evolving countermeasures, stealers persist as a menacing force. The continual emergence of novel variants, coupled with their diverse functionalities and growing sophistication, underscores an enduring demand within the criminal underworld for these malevolent tools.

Recommendations

Deep Packet Inspection (DPI): Employ DPI technologies to inspect network traffic at the packet level, enabling the detection of malicious payloads or command-and-control communications associated with stealers.

Continuous Monitoring and Analysis: Establish a robust system for monitoring and analyzing suspicious activities on networks and endpoints. Regularly review logs and conduct threat-hunting exercises to identify and neutralize potential threats before they escalate.

Exercise Caution with Unsolicited Emails: Always exercise caution when receiving unexpected or urgent emails, especially those from unknown sources. Avoid downloading attachments from unsolicited emails to mitigate the risk of malware infections.

Content Filtering and Application Control: Enforce application control to prevent unauthorized app installations and executions, reducing the risk of downloading and running malicious files. This integrated strategy safeguards against downloadable threats like stealers by proactively blocking access to harmful content and preventing the execution of malicious code.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0011 Command and Control	TA0010 Exfiltration
T1204.002 Malicious File	T1204 User Execution	T1140 Deobfuscate/Decode Files or Information	T1555.003 Credentials from Web Browsers
T1555 Credentials from Password Stores	T1553 Subvert Trust Controls	T1566 Phishing	T1059 Command and Scripting Interpreter
T1574 Hijack Execution Flow	T1055 Process Injection	T1211 Exploitation for Defense Evasion	T1027 Obfuscated Files or Information
T1212 Exploitation for Credential Access	T1053 Scheduled Task/Job	T1070 Indicator Removal	T1083 File and Directory Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	abceb35cf20f22fd8a6569a876e702cb, 2b71c81c48625099b18922ff7bebbf51, b9b83de1998ebadc101ed90a6c312da8, 1d3c3869d682fbd0ae3151b419984771, c0cf3d6d40a3038966f2a4f5bfe2b7a7, f8b2b941cffb9709ce8f422f193696a0, 6e2b16cc41de627eb7ddcd468a037761, 21df3a69540c6618cfbdaf84fc71031c, 23ae473bc44fa49b1b221150e0166199
SHA1	99b356a98942d78f9a3f9f0c1d161435f78646d5, c2a4aee4fa2ca053c24c9e970741532427cd9f43, 116e20c95bf215fca276456a1d0e36c71192a3e4, 9120d7d680824a351f36312054fce5f398b92c77, 70565be6172fd0c6f914e86ca77bd74de1592b80, 18df1ca8e6551d8a280b28d44d737c9e9279bdd7, b22362a52d6c4ec9faf01fe122d576802202952f
SHA256	e8aeacf53531c3e4befc2c750f7592e7d22e0d6a0e728ea60566e798d148ea50, bf04f1095661a32fae746430ff31de02f686ddadd288d9ea3b58d4279e079c41, aae240697a9632cf70db2b77fe7117fdf3d6d5d63c60f67a86dffc681da14204, ce06ce31fe90d2f022b95efcdb3d07e02ae40f3addecac0ddce51a389f046144, 74dd00bc6672e3a03f457a090b88e9402dfc2b4725567fdbac040e58f8dd1d32, 73bd715184ebf17fc0ff19d98d070d7d72f4ca8164c8fa2eef462d8d8d20d100, c53d48985646e412d92e2c86b400082d19dd023d351417f9fa49182e27724c78

References

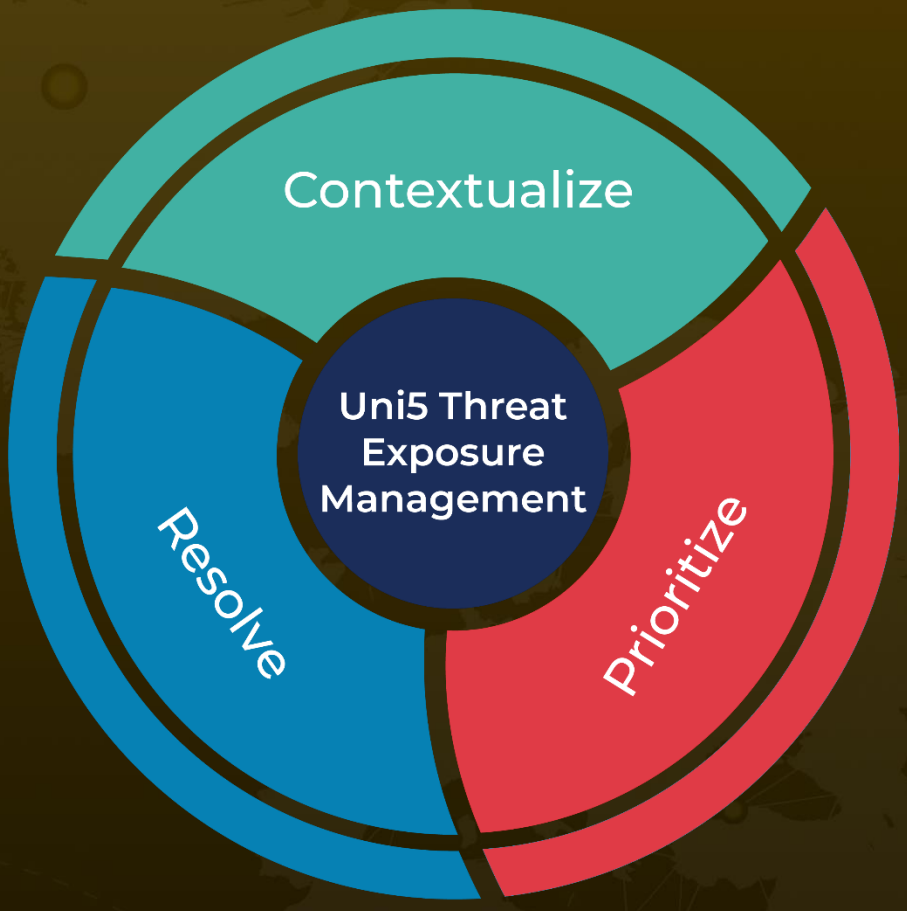
https://securelist.com/crimeware-report-stealers/112633/

https://www.hivepro.com/threat-advisory/sys01-stealer-targets-government-and-manufacturing-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

May 23, 2024 • 8:00 PM

More at www.hivepro.com