Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

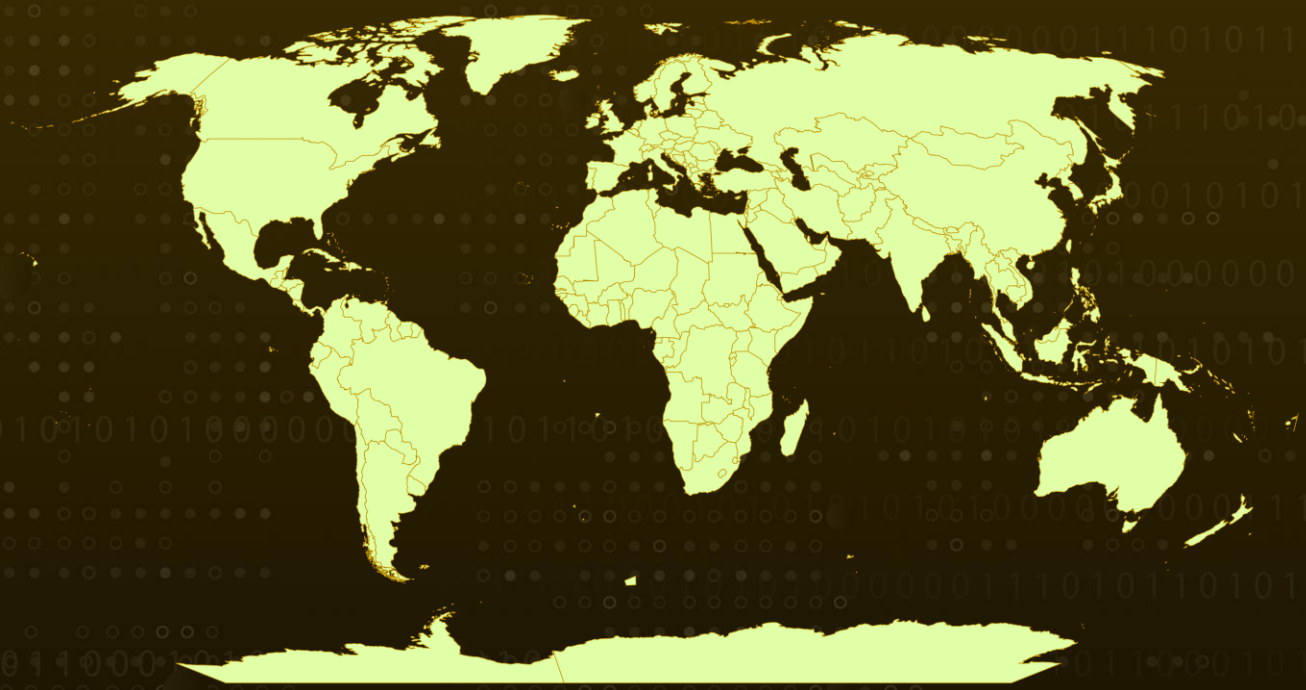
LummaC Stealer Enlists Amadey Bot to Unleash SectopRAT

Date of Publication	Admiralty Code	TA Number
August 16, 2023	A1	TA2023332

Summary

Malware: LummaC Stealer (aka LummaC2 Stealer), Amadey Bot, and SectopRAT (aka 1xxbot, ArechClient)
Attack Region: Worldwide
Attack: A fresh approach to spreading SectopRAT has surfaced. This method involves distributing the SectopRAT payload by utilizing the Amadey bot, which is sourced from the LummaC stealer.

Attack Regions



Attack Details

#1 A novel methodology for disseminating SectopRAT has emerged. This strategy involves distributing the SectopRAT payload by harnessing the Amadey bot sourced from the LummaC stealer (aka LummaC2). The propagation of the LummaC Stealer has occurred through tactics such as phishing websites, enclosed ZIP archives masquerading as legitimate software sources, and targeted spear-phishing emails.

#2 There are two different folders within a ZIP archive: "Common Files" and "HMService." These directories hold various legitimate DLL files, and the archive contains an executable named "Setup.exe." Notably, this "Setup.exe" acts as the central payload for the LummaC Stealer executable. After being successfully installed on a chosen target system, the LummaC Stealer carries out hidden operations to gather essential system details. Following this collection, the obtained data is encrypted and sent to the designated C&C server.

#3 Furthermore, the LummaC Stealer facilitates the retrieval of the Amadey bot, a 32-bit GUI-based .NET Reactor executable malware. The Amadey bot generates an LNK file strategically placed within the startup folder to ensure enduring persistence. As it operates, the Amadey bot establishes communication with its specified C&C server, periodically sending thorough system data while requesting instructions.

#4 The Amadey bot's defining feature is its ability to deliver auxiliary payloads, such as the SectopRAT, to compromised computer systems. SectopRAT (aka Arechclient,1xxbot) operates as a meticulously crafted Remote Access Trojan (RAT) developed using the .NET compiler, fortified with Anti-VM and Anti-Emulator mechanisms. When activated, the SectopRAT initiates its process of scanning directories, extracting vital information from various cryptocurrency wallets such as Atomic, Exodus, Electrum, and Daedalus Mainnet.

Recommendations

It is advisable to utilize robust email filtering solutions, as these tools have the capability to detect and prevent spam, phishing attempts, and harmful emails. Additionally, it is recommended to exercise caution when engaging with links and attachments from sources that are unfamiliar or untrusted.

Configure network infrastructure devices such as firewalls and routers with strict security specifications. Use application whitelisting or control mechanisms to only allow authorized applications to run on systems.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0011 Command and Control	T1204 User Execution	T1047 Windows Management Instrumentation	T1547 Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	T1055 Process Injection	T1497 Virtualization/Sandbox Evasion	T1027 Obfuscated Files or Information
T1562 Impair Defenses	T1027.002 Software Packing	T1140 Deobfuscate/Decode Files or Information	T1620 Reflective Code Loading
T1003 OS Credential Dumping	T1056 Input Capture	T1057 Process Discovery	T1012 Query Registry
T1082 System Information Discovery	T1083 File and Directory Discovery	T1518.001 Security Software Discovery	T1005 Data from Local System
T1071 Application Layer Protocol	T1573 Encrypted Channel	T1105 Ingress Tool Transfer	T1566.001 Spearphishing Attachment

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	507bddfabd74a3d024b2ad5f67d666ea, 952d825a264745bb52b6977ba5983568, f290ed868caae994bbfae1b63aca1d28
SHA1	78eac92e0040e033406e6786b58b8a367fe171fa, 627a0a841c2fe194dd54f9ec6b0c1231d7da135f, 5ac7b60e56281dc0c72f7c1125b165867df56ed9
SHA256	f85d8adf012c96a63fcb989b8b0e71894b12b769ce78f6a62064a4002954b144, d35d55bb74a7cf4349e2fa4a92839e2a88f17a1fee9725801d0d97b2bf0d311c, 501444c9d25c15ca62bafe062b6bb8a3b3f69f0ca13aff057e3b8b1a0595f3a4, ca21c5b129c001c2b51359d5f74c0a99667028810623b779190b13f0de86369e, 929f7b467d96d8d9c73bfa9b8adf758c1b3993c9438f23368c69e1201beea622, 515ab212127cc722326043d77dda60943145798bfe8b17178937a254989367f1, 0d8dee5e24500219f037e673324479f22cc5649c2aafdfe47b35375b6b76e60b, e0ac5909e219d4527691ea695185313376a0ccb075907b1deecd4e2aeae42cba, 9252e999b76b9628ad0942df2649e1203ca078d1b45dab6a8f1ede3e22b99625, 51cb8641ed75c5037fa657ed2aa33c71350e01f5f949054f17582ca41c260280, f819a1d2234c2755a8dc844f89e765de56c1c927f3964a1453961cec4fd38bae, 0539d46a6e61dd3ce32a4b41c0554f925f4b26054c49451accec7ccad0409846, 2c256a4a1ac022bcd3784d19e66934056015e20b49d58238ce4f3dfb37bfd98d, a3ceda3ef0a7b72145124def334dd3fa337614a1170960826016996151188fc5, 033cafb9fcd3d50d858164c117ee2a1c9e7fe95b4d027315bc9d1186e655d583, 81f4e0d6a70f14c3e07241196bd7f5318e302c28c64ca4bb876f4e25fbc3e5d2, ffd45c2b562d30113cb9a4823025a9a162503017e9d81fd96ddb5b98e5bb89bd, fb553e12381d42a612c713968078424201794a35fd13c681ae7faa77bf18e553,

TYPE	VALUE
SHA256	641710df66c792439f85b79879a268caa17b78ea0bf6924369fa6131fda01cd5
URLs	hxxp[:]//exitlife[.]xyz/c2sock, hxxp[:]//africatechs[.]com/Amdaygo[.]exe, hxxp[:]//45[.]9[.]74[.]182/b7djSDcPcZ/index[.]php, hxxp[:]//patriciabono[.]com/BRR[.]exe, hxxp://enfantfoundation[.]com/amday[.]exe, hxxp://fuji-iasi[.]ro/BRR[.]exe, hxxps://earthqik[.]co[.]za/BR[.]exe, hxxp://silversoft[.]in/BR[.]exe, hxxp://tbmcoats[.]com/BRRR[.]exe, hxxp://aviangas[.]co[.]ke/BRRRRAS[.]exe
IP:PORT	95.143.190[.]57:15648

References

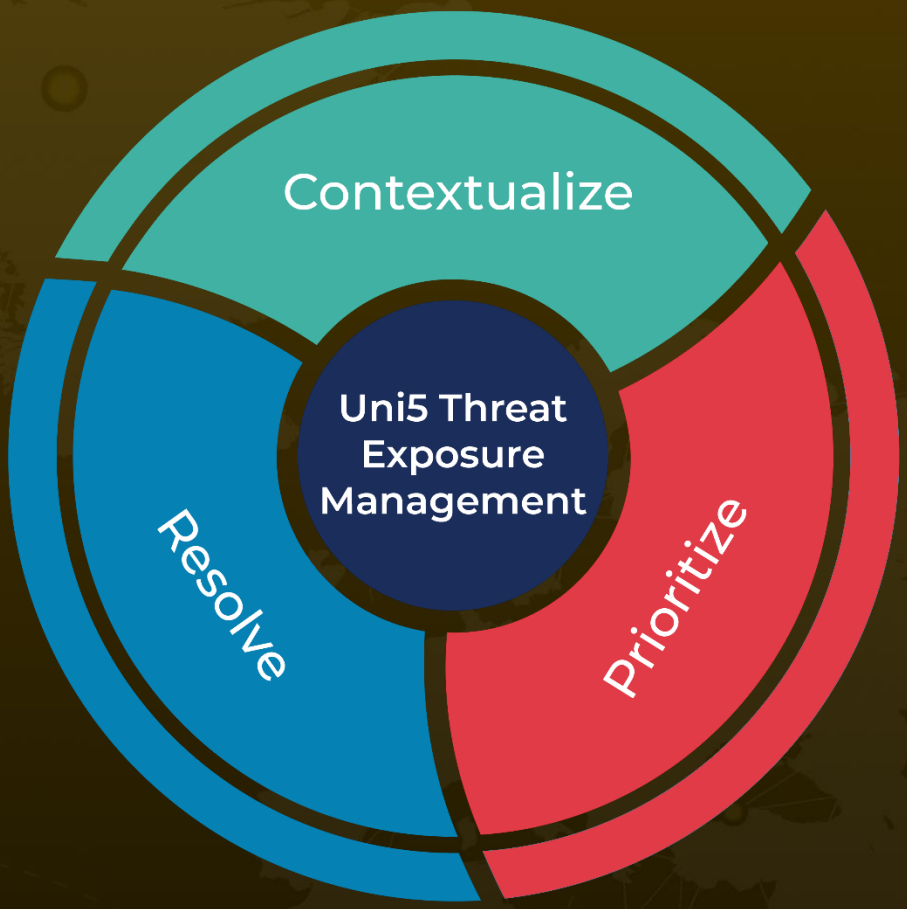
https://cyble.com/blog/lummac-stealer-leveraging-amadey-bot-to-deploy-sectoprat/

https://www.hivepro.com/information-stealer-lummac2-targets-browsers-and-crypto-wallets/

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

August 16, 2023 • 6:00 AM

More at www.hivepro.com