Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

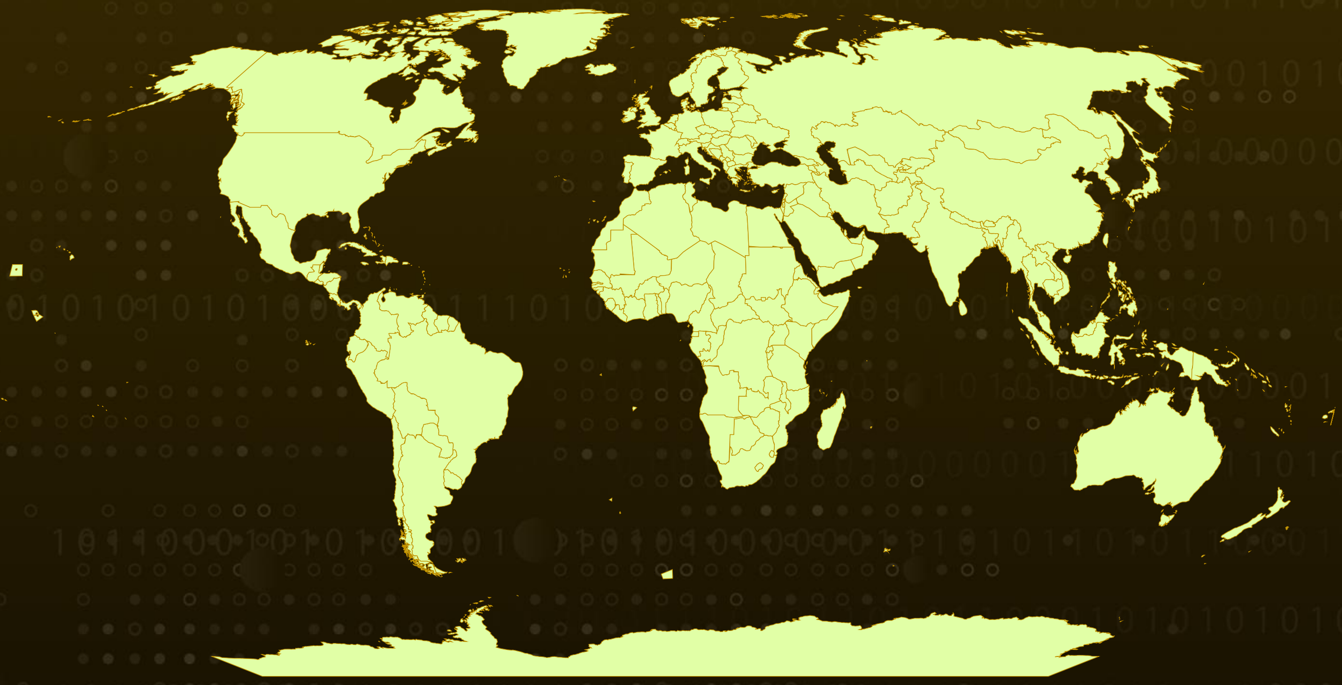
SnipBot: Unpacking the Latest RomCom Malware Variant

Date of Publication	Admiralty Code	TA Number
September 25, 2024	A1	TA2024372

Summary

First Seen: June 2024
Targeted Countries: Worldwide
Malware: SnipBot, RomCom
Targeted Industries: IT services, Legal and Agriculture
Affected Platforms: Windows
Attack: SnipBot, a newly identified variant from the RomCom malware family, employs advanced infection and evasion techniques. Typically delivered via phishing emails posing as PDF attachments, it downloads additional malicious payloads from remote command-and-control servers. This malware showcases capabilities for remote command execution and data exfiltration while using anti-sandbox methods to evade detection. Organizations should enhance their defenses with advanced threat detection and monitoring tools to counter this evolving cyber risk.

Attack Regions



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

Attack Details

#1 A new variant of the RomCom malware family, named SnipBot, is actively targeting IT services, legal and agriculture sectors. This variant employs advanced techniques and post-infection activities previously unseen in earlier versions. SnipBot is primarily based on RomCom 3.0, incorporating elements from its offshoot PEAPOD (RomCom 4.0), thus being classified as version 5.0.

#2 SnipBot typically spreads through email phishing campaigns, where the initial payload is often disguised as a PDF file. Victims are tricked into downloading an executable that acts as the downloader for the malware. Upon execution, SnipBot connects to command-and-control (C2) servers to download additional malicious payloads. The downloader is consistently signed with a legitimate certificate, likely obtained through theft or fraud, while subsequent modules are unsigned.

#3 The malware allows attackers to execute commands remotely, download further modules, and exfiltrate files from the victim's system. It uses sophisticated anti-sandbox techniques to evade detection and includes encrypted strings to complicate static analysis. SnipBot's main module supports various commands for data collection and manipulation, including file uploads, command execution, and system information retrieval. The malware can also create hidden processes to maintain persistence on infected systems, ensuring continuous access for further exploitation or espionage.

#4 The RomCom variant showcases a high degree of sophistication, evolving its techniques to remain stealthy and potent. Its use of trusted software channels makes it particularly dangerous, as it can evade traditional security defenses.

Recommendations

Download Software from Verified Sources: Ensure all software, updates, and installers are downloaded exclusively from trusted and official sources. Avoid downloading software from third-party websites or unverified links, as RomCom malware often impersonates legitimate tools like Veeam or KeePass to gain access to systems.

Implement Multi-Layered Security: Deploy multi-layered security solutions such as endpoint detection and response (EDR), network security monitoring, and next-gen firewalls. These can help detect suspicious activities related to malware execution and communication with external Command and Control (C2) servers.

Conduct Regular Security Audits: Perform regular system and network audits to identify potential vulnerabilities that could be exploited by malware. Pay special attention to systems handling sensitive data or those with frequent software updates, as they are prime targets for this kind of malware.

Monitor for Unusual Network Activity: Regularly monitor network traffic for anomalies that may indicate remote command execution or unauthorized data exfiltration. Implement tools that can detect abnormal communication between endpoints and external servers.

Potential MITRE ATT&CK TTPs

TA0009 Collection	TA0005 Defense Evasion	TA0001 Initial Access	TA0002 Execution
TA0011 Command and Control	TA0042 Resource Development	TA0010 Exfiltration	TA0003 Persistence
TA0007 Discovery	T1036 Masquerading	T1566.001 Spearphishing Attachment	T1059 Command and Scripting Interpreter
T1566 Phishing	T1027 Obfuscated Files or Information	T1140 Deobfuscate/Decode Files or Information	T1598.003 Spearphishing Link
T1204 User Execution	T1204.002 Malicious File	T1588 Obtain Capabilities	T1574.001 DLL Search Order Hijacking
T1082 System Information Discovery	T1574 Hijack Execution Flow	T1588.003 Code Signing Certificates	T1083 File and Directory Discovery

T1070.004 File Deletion	**T1070** Indicator Removal	**T1560.001** Archive via Utility	**T1560** Archive Collected Data
T1497 Virtualization/Sandbox Evasion	**T1041** Exfiltration Over C2 Channel	**T1046** Network Service Discovery	**T1027.007** Dynamic API Resolution
T1053.005 Scheduled Task	**T1053** Scheduled Task/Job		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	0be3116a3edc063283f3693591c388eec67801cdd140a90c4270679e01677501, 1cb4ff70f69c988196052eaacf438b1d453bbfb08392e1db3df97c82ed35c154, 2c327087b063e89c376fd84d48af7b855e686936765876da2433485d496cb3a4, 5390ba094cf556f9d7bbb00f90c9ca9e04044847c3293d6e468cb0aaeb688129, 57e59b156a3ff2a3333075baef684f49c63069d296b3b036ced9ed781fd42312, 5b30a5b71ef795e07c91b7a43b3c1113894a82ddffc212a2fa71eebc078f5118, 5c71601717bed14da74980ad554ad35d751691b2510653223c699e1f006195b8, 60d96087c35dadca805b9f0ad1e53b414bcd3341d25d36e0190f1b2bbfd66315, 92c8b63b2dd31cf3ac6512f0da60dabd0ce179023ab68b8838e7dc16ef7e363d, a2f2e88a5e2a3d81f4b130a2f93fb60b3de34550a7332895a084099d99a3d436, b9677c50b20a1ed951962edcb593cce5f1ed9c742bc7bff827a6fc420202b045, cfb1e3cc05d575b86db6c85267a52d8f1e6785b106797319a72dd6d19b4dc317, e5812860a92edca97a2a04a3151d1247c066ed29ae6bbcf327d713fbad7e79e8, f74ebf0506dc3aebc9ba6ca1e7460d9d84543d7dadb5e9912b86b843e8a5b671

TYPE	VALUE
Domains	fastshare[.]click, docstorage[.]link, publicshare[.]link, xeontime[.]com, drvmcprotect[.]com, mcprotect[.]cloud, cethernet[.]com, sitepanel[.]top, ilogicflow[.]com, webtimeapi[.]com, dns-msn[.]com, certifysop[.]com, drv2ms[.]com, olminx[.]com, linedrv[.]com, adobe.cloudcreative[.]digital, 1drv.fileshare[.]direct
IPv4	91[.]92[.]250[.]104, 52[.]72[.]49[.]79, 212[.]46[.]38[.]222, 52[.]72[.]49[.]79, 91[.]92[.]250[.]240, 91[.]92[.]254[.]54, 185[.]225[.]74[.]94, 91[.]92[.]254[.]234, 91[.]92[.]254[.]234, 79[.]141[.]170[.]34, 91[.]92[.]250[.]106, 23[.]184[.]48[.]90, 91[.]92[.]242[.]87, 91[.]92[.]242[.]87, 23[.]137[.]248[.]220, 38[.]180[.]5[.]251, 23[.]137[.]249[.]182, 23[.]137[.]249[.]14
Registry key	HKCU\SOFTWARE\AppDataSoft, HKCU\SOFTWARE\AppDataHigh

References

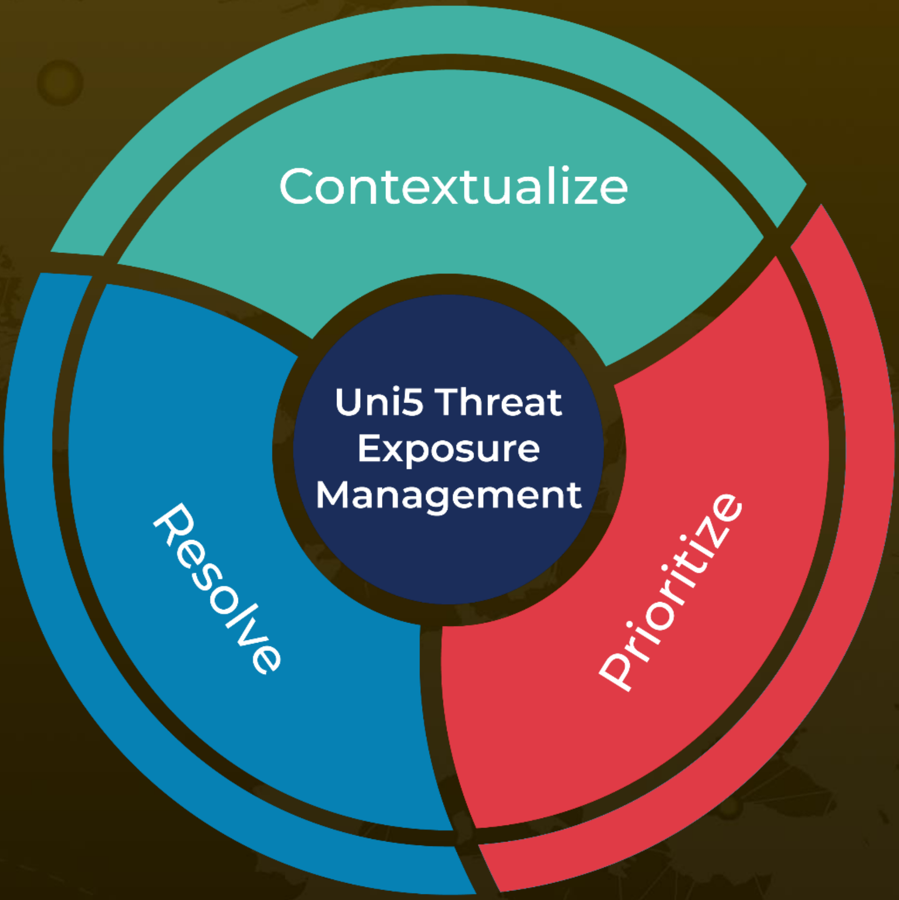
https://unit42.paloaltonetworks.com/snipbot-romcom-malware-variant/

https://hivepro.com/threat-advisory/storm-0978-unleashes-peapod-to-target-women-political-leaders/

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 25, 2024 • 6:30 AM

More at www.hivepro.com