KPMG Cyber Threat Intelligence Platform

SnipBot Malware – A New RomCom Malware Variant

TLP : Clear

KPMG. Make the Difference.

SnipBot, part of the RomCom malware family, was first identified in December 2023, developed using C++ and employs email vectors and masquerading executables to reach its targets. As the fifth iteration of the RomCom malware, SnipBot introduces several advanced features, like remote command execution capabilities and data exfiltration mechanisms. SnipBot primarily targets sectors such as IT services, legal firms, and agricultural businesses.

Initial access is achieved through a phishing email containing an executable file disguised as a PDF or an actual PDF file, which prompts the victim to download the SnipBot downloader. The downloader, signed with a legitimate code-signing certificate, uses a window message-based control-flow obfuscation algorithm to split the code into multiple unordered blocks. The downloader employs Anti-Sandbox techniques, such as checking the hashed process name against a hard-coded value and verifying at least 100 entries in the RecentDocs registry key. Upon execution, the downloader contacts various C2 domains to retrieve a PDF file and subsequent payloads. The first payload is a DLL file, which executes in memory and downloads the next stage COM DLL from another C2 server. This DLL uses COM hijacking to register itself as the thumbnail cache library in the user's registry hive. It is then injected into Explorer, which stores additional payloads in the registry. The malware sets up a network listener on port 1342 to receive commands from the attacker, decrypting and executing encrypted payloads stored in the registry. It collects victim's system information, such as computer/domain name, MAC address, and Windows build number, and sends it to the C2 server. The collected data is then packed using WinRAR and exfiltrated using PuTTY.

SnipBot's capabilities and sophisticated techniques, combined with its ability to exfiltrate data, highlight the need for robust security measures and proactive threat management.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/ TAXII/ MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

KPMG in India Cyber Response Hotline: 1800 2020 502

KPMG in India contacts:

Atul Gupta
Partner
Head of Cyber Security
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Partner
T: +91 98181 99432
E: mtembhurkar@kpmg.com

Rishabh Dangwal
Director
T: +91 99994 30277
E: rishabhd@kpmg.com

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

SnipBot Malware – A New RomCom Malware Variant

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses	
23.184.48[.]90	79.141.170[.]34
38.180.5[.]251	91.92.250[.]104
91.92.242[.]87	91.92.250[.]106
91.92.254[.]54	91.92.250[.]240
185.225.74[.]94	91.92.254[.]234
212.46.38[.]222	23.137.249[.]182
23.137.249[.]14	23.137.248[.]220

Indicators of Compromise: Domains	
dns-msn[.]com	drvmcprotect[.]com
sitepanel[.]top	publicshare[.]link
ilogicflow[.]com	fileshare[.]direct
fastshare[.]click	adobe.cloudcreative[.]digital
mcprotect[.]cloud	

Indicators of Compromise: Hashes
7f2e4a44445b977ef8917cc0fb79035b
c0e499402acb6c302228b4a7923d5db6
524dda2410cc7ee8cc326ca42cebd7dd
fa400cb70d13cb329d05877b8fe73ed5
0cd8736a915e8e32ddeda21ed462670b
5d3e1102a61fc139018465a844b83652
d69cf309cb0e5d91237c6454e0e0dc45
6fa6dd331844ee5cfe20c74353c1e442
36d4903ffafa75c00460292881b5dad7

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

SnipBot Malware – A New RomCom Malware Variant

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
43cc1f2f07c1c1c7f69075d81332f95e
983332a5660ec6c28123e745023b41105775ab6f
cb3d3a7e39e7cdc8501ae0eff77d02a1c995bc31
42673214d773b6af23944a65f47d2841bad75de7
0fa5bfed7dafbe248f436a6b6ca4b08e7e859fd4
94fe1c6de60134ca6c0b9a36bba72aeb6c27bf6b
8cee4097fab131c00659cea09ff4c920be823a19
b37640cc1ef9354808562ced599a5ff0923156ac
16572311d9007d226f2e6d0abc3b980ffbc7521d
55aa2f684faa55b69fd559a142acee593ddf863c
520be5d84f7831854e5cb6eeebcafd55c3954aa6
0be3116a3edc063283f3693591c388eec67801cdd140a90c4270679e01677501
57e59b156a3ff2a3333075baef684f49c63069d296b3b036ced9ed781fd42312
a2f2e88a5e2a3d81f4b130a2f93fb60b3de34550a7332895a084099d99a3d436
b9677c50b20a1ed951962edcb593cce5f1ed9c742bc7bff827a6fc420202b045
cfb1e3cc05d575b86db6c85267a52d8f1e6785b106797319a72dd6d19b4dc317
f74ebf0506dc3aebc9ba6ca1e7460d9d84543d7dadb5e9912b86b843e8a5b671
2c327087b063e89c376fd84d48af7b855e686936765876da2433485d496cb3a4
5390ba094cf556f9d7bbb00f90c9ca9e04044847c3293d6e468cb0aaeb688129
5c71601717bed14da74980ad554ad35d751691b2510653223c699e1f006195b8
5b30a5b71ef795e07c91b7a43b3c1113894a82ddffc212a2fa71eebc078f5118
e5812860a92edca97a2a04a3151d1247c066ed29ae6bbcf327d713fbad7e79e8
60d96087c35dadca805b9f0ad1e53b414bcd3341d25d36e0190f1b2bbfd66315
92c8b63b2dd31cf3ac6512f0da60dabd0ce179023ab68b8838e7dc16ef7e363d
1cb4ff70f69c988196052eaacf438b1d453bbfb08392e1db3df97c82ed35c154