KPMG Cyber Threat Intelligence Platform

StrelaStealer – Back with Revamped Tactics

StrelaStealer, active since 2022, intensifies its cyber threat via email campaigns, affecting over 100 organizations in the EU and U.S. The latest campaign, launched in January 2024, targets High Tech, Finance, and Utilities, using spam emails with malicious attachments to deploy the StrelaStealer DLL payload. The primary objective of the malware is to steal email credentials, particularly from Thunderbird and Outlook accounts. Notably, the distribution strategy has evolved, employing multilingual phishing emails for broader reach and deception.

StrelaStealer gains initial access via spear-phishing emails with ZIP attachments, which, when opened, drop a JScript file onto the system. Previous iterations of StrelaStealer infect systems through email attachments containing .iso files, containing .lnk files that execute HTML files. The JScript/HTML drops a Base64-encoded file and a batch file, decoded with certutil to create a PE DLL file. This DLL is placed in either %appdata%\temp or c:\temp and executed using rundll32.exe with the exported function "hello". Achieves persistence by dropping its payload DLL into the system, allowing it to remain on the infected machine even after a reboot. It masquerades as legitimate process, enhancing its DLL payload with advanced obfuscation. Furthermore, StrelaStealer likely discovers sensitive information by accessing and exfiltrating email login data from well-known email clients installed on the infected system. Communicates with its Command and Control (C2) server, StrelaStealer sends stolen email login data back to the attacker. The C2 server name is defined in the malware configuration.

StrelaStealer's continuous evolution in email campaigns and DLL payload highlights the imperative for robust cybersecurity measures to mitigate & prevent future attacks.

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.

The 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

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

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

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

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Associate Partner,
KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

StrelaStealer – Back with Revamped Tactics

Indicators of Compromise: IP Addresses	
91.215.85[.]209	193.106.191[.]166
193.109.85[.]231	

Indicators of Compromise: Hashes
301503edfb1ea723b231b416c2a81f0f
e2936de211b980bb9bc042c04348978e
ebb7cf1ce051a233b763f25ff52f5d56
830fc4d3eb1a57d969e2db2007a3f779
1096f27f41868601b382018c3daf895c
9499f14143b34ea7703c73b5f9b37013
95f51b48fb079ed4e5f3499d45b7f14e
97c4dc2b0307ce4aeb24e686fdee6b50
8d82b61263a52d999c346b335913b86e
26dbf856ee2a228a4eeb103408a356b0
6ab824fbb8b8b26fcb14b8791d2e2054
ce5b9bc6f56fe1950aa56534702df115
e00f53271b8af0b72fed60773547acb2
3c4bd5309143853848381c9eb0435d75
4d8cbe0df1737fd0aeecca940a3c1755
cf047f2182ee81f428d0d40d1d63d5f5
9fa8a7248878e07e20094d101d5f21d0
ba5281c2978e426605f4be767898b323
4ba67e2197ae88dadd7d7c5294d2c15c
5400922b47487d4a2e813445e6c518d0
57ec0f7cf124d1ae3b73e643a6ac1dad
27160a11f771cf3e2f84f59d3218494d
0e6c952cc1400d6efa57ee3d3f0ac759
d272381c1fd89d0eec233f607d6eecbb
dd41fda85637d2593ef4aad407371ec830fe171d
f16890fb143741ec118befd22f6903a18f8f1315
1d1d47e11c57cdc599649f07c2f026ee54a6f2f5
f9d4e1db530e27817d4c61b7a057567f6543df5f
e5ac5b229f0525c407e8d8eeec5abeda5af8ff25

KPMG

KPMG Cyber Threat Intelligence Platform

StrelaStealer – Back with Revamped Tactics

Indicators of Compromise: Hashes
ceff6b19826c9a4e9b9e8cbcc512d5241a27825e
ecb4c122a3b91c92e3212dc06a05f7491cac2ac4
0d89a517f48732bb04744da77985fa48c70e2ef3
375fe4ca442ce93af496a4a59408bccd66f60b60
e585f349c464c4b3d0b034a4e53995a13279edc2
b001cdc9f6735555de8a3b843c4c7d867c197f28
ce32ec5af2676eeba165464f0c35641a120a57d7
19747fae33d23284424f00b38ba625170175b614
ebc1cbd8e5ceaff0dd941fd044d106997eba846f
f6ff5b25198d09dcde2cfa8efbebe98f14927d6b
533ed45fcfce6f982559b96dcc90ee1c4f95d138
fe1765890ba7546b91faf7f09f962a326b0644cb
bc986f48c82b840c7196377f1c0a106865068892
41593f320327e258d8f08230d84e2147ab766877
c1b1731d7be1f182b845d787cd67b0d15ed2b92e
213c548e0a5e3fefe37bb857f0f6e3230d29675c
4139e4d85e67f094eb98f13e16183075475dc1dc
60d510de7ebb381aa046f755374d3c9d411684ac
cdeca357a30d4c889ad85430984a6a29b4bc8a86
544887bc3f0dccb610dd7ba35b498a03ea32fca047e133a0639d5bca61cc6f45
3189efaf2330177d2817cfb69a8bfa3b846c24ec534aa3e6b66c8a28f3b18d4b
b8e65479f8e790ba627d0deb29a3631d1b043160281fe362f111b0e080558680
f95c6817086dc49b6485093bfd370c5e3fc3056a5378d519fd1f5619b30f3a2e
aea9989e70ffa6b1d9ce50dd3af5b7a6a57b97b7401e9eb2404435a8777be054
e6991b12e86629b38e178fef129dfda1d454391ffbb236703f8c026d6d55b9a1
c02bb26582576261645271763a17de925c2d90d430e723204baec82030dc889a
1e7277d2aef459eea9646a76032f1bd4384f7cedac8f4cff3670a601307ab25a
4e46e03a43a1b2805de578d2d0e11f7570f477072cee9ee4843fc7273906a5a3
52f0abd242c20a6cc7d5a03b5cf4759020f567a23530eaddf91699b52a1f433d
6e8a3ffffd2f7a91f3f845b78dd90011feb80d30b4fe48cb174b629afa273403
ae0bcf31bcebbc675af18fa7dbdfc805ad3b18d6baa427e70f77a6f3c6a0b684
c440c52855ad12a16785caea2bc8bd54f4b62786f8eb3809f52e1c081d5d4fa2
d3197dd9aec8f204f12ac85207ee1df2a6693b6c217a3d74ccbcb3098916ebe6
df529dfbb2ebd2ccd7b13a98bf78b6fa7d24ac5ca56dc6eb16aa7d1d7a92977b

KPMG

KPMG Cyber Threat Intelligence Platform

StrelaStealer – Back with Revamped Tactics

Indicators of Compromise: Hashes
ee6f823f197dbdc24995071c710b478e771ee3eb5386829ef8d6eaa83719acb9
f3fe692959c5078378e8221aa1da93b566c99737586291f2e2de88218d4df166
bcb5800437344387248c6297e393de63d9330899a040efee11fe70e6938e8df3
fa1295c746e268a3520485e94d1cecc77e98655a6f85d42879a3aeb401e5cf15
c8eb6efc2cd0bd10d9fdd4f644ebbebdebaff376ece9e48ff502f973fe837820
8b0d8651e035fcc91c39b3260c871342d1652c97b37c86f07a561828b652e907
879ddb21573c5941f60f43921451e420842f1b0ff5d8eccabe11d95c7b9b281e
b7e2e4df5cddcbf6c0cda0fb212be65dea2c442e06590461bf5a13821325e337
d8d28aa1df354c7e0798279ed3fecad8effef8c523c701faaf9b5472d22a5e28
ac040049e0ddbcb529fb2573b6eced3cfaa6cd6061ce2e7a442f0ad67265e800
bfc30cb876b45bc7c5e7686a41a155d791cd13309885cb6f9c05e001eca1d28a
c69bac4620dcf94acdee3b5e5bcd73b88142de285eea59500261536c1513ab86
be9f84b19f02f16b7d8a9148a68ad8728cc169668f2c59f918d019bce400d90e
1437a2815fdb82c7e590c1e6f4b490a7cdc7ec81a6cb014cd3ff712304e4c9a3
90b124755902204fa4b5ffd3cb6b1c334de6aca39b9a3bbc85e50b46a6b7a342