KPMG Cyber Threat Intelligence Platform

Sticky Werewolf – Expanding threats in the Aviation Sector

Sticky Werewolf, a cyber threat group first detected in April 2023, initially focused on public organizations in Russia and Belarus. Over time, they have broadened their scope to include sectors such as pharmaceuticals, Russian research institutes specializing in microbiology and vaccine development, and the aviation industry. Their operations now aim at espionage and data exfiltration, reflecting an expanded and increasingly sophisticated threat landscape.

Initial access begins with phishing emails, previously containing links but now utilizing RAR archive attachments. Upon extraction, these archives reveal a decoy PDF and two LNK files. The decoy PDF serves to lower suspicion, while the LNK files execute the main payload. The first LNK file triggers actions including adding registry entries for persistence, displaying fake error messages, and copying decoy files locally. The second LNK executes a command which launches the same executable as the first, retrieved from a WebDAV server and is identified as a CypherIT crypter variant. This executable initiates a Batch script, which then launches an AutoIt script responsible for injecting the final payload. The Batch script delays execution, renames files to evade detection, and prepares for subsequent malicious activities. The AutoIT script employs anti-analysis measures, overrides ntdll.dll to remove hooks, establishes persistence via scheduled tasks/startup directory, and decrypts the payload using RC4, employing key scheduling and PRGA for seamless injection into a legitimate process. Final payloads include RATs and stealers like Rhadamanthys Stealer and Ozone RAT for espionage and data exfiltration.

Sticky Werewolf's advanced phishing and malware tactics illustrate its sophisticated approach to espionage and data exfiltration, highlighting the need for robust cybersecurity defenses.

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

KPMG Cyber Threat Intelligence Platform

Sticky Werewolf – Expanding threats in the Aviation Sector

Indicators of Compromise: IP Addresses	
185.12.14[.]32	79.132.128[.]47
94.156.8[.]166	194.61.121[.]167
94.156.8[.]211	

Indicators of Compromise: Domains	
diskonline[.]net	document-cdn[.]org
yandeksdisk[.]org	

Indicators of Compromise: Hashes
d4b75a8318befdb1474328a92f0fc79d
2bc840a360f3bc58788c32805c7c8849
6892abc8eb5833b7a142bb88dc0bc1c5
5132cbde40a752aa50a6b45e4b29512b
9ed5a7b6e69198eee0b1742c20141d3d
b57b13e9883bbee7712e52616883d437
e0f8d7ec2be638fbf3ddf8077e775b2d
2d165ee27f72773623d6820f651c5d32
43817fd79651402ea37ef0e922ad93fe
39d28ebb429ba8228e6a81e5d4d3fa04
bf3eafa83b3bdee1f42cc9fb3bd66eb0
d8c6199b414bdf298b6a774e60515ba5
b579010d05f9af4884d64d9ea74a10f1
75fd9018433f5cbd2a4422d1f09b224e
842f8064a81eb5fc8828580a08d9b044
613bbcc11ea7b72e6a9e1b0dc67ba67173e4a3e4
60de4d99d793c1180b46a1025adaf028453daee8
1fffe7b13151711bc2df8a2631f77a1c35ae8bec
db1deb3a5f1452935117a27134ffca86e3687dab
8d8dac4463c12d4fe106ca801f7c81874d4fb430
9dd1244e79c1a40606816f7498a67a6d0bd21bce
9038327e1ecece25917f07cae5f66c60c6daaf4d
5dc5b89af233c31517365448f1ebede4f63e7c45
96424f0f14daa3b3f412a010942be901ba5df3ab

KPMG

KPMG Cyber Threat Intelligence Platform

Sticky Werewolf – Expanding threats in the Aviation Sector

Indicators of Compromise: Hashes
cc3457b7d9475ee1c6beef98a9c7510734fa5309
ca65a505196383e9bd06500e2d80cd2219191969
3436370107bb02f0966acc2d104ed1edc99a1896
562b7eae0b178ba3ea502b10a5137af5049469e6
a70ae8967ba471d65a2946fa99cf0f055051eb02
5ee694301a0d8388f7dd35b1df3e7319fce4fab0
05880ff0442bbedc8f46076ef56d4d1ffeda68d9ef26b659c4868873fa84c1a9
03ee2011ad671b1781015024ea53edfbff92c28c2b123bba02d6a6f462e74105
1301ec3006ad03742bfaef047aa434320aa0e725a99be5d6be27b955a814fcf4
c3efbac8ebffcf3d8178ce23e59f3b4978f5a91bf93773889870d45cc1b554b0
ce2b6d3aad07d3dec2b24f676cc9d2022bab5a086c7e773f9cfa3e7b7dc6d66a
9eddffbef4d9d7329d062db0a93c933104d00f12106bf91fa3b58e8f8b19aa41
217196571088cfd63105ae836482d742befcb7db37308ce757162c005a5af6ab
3ccbd8bd7424506b26491e5ff5ff55b000adaab1074ccf3b7452d0883f668040
d6e6c786b793b46a1ee9b18b058e045d0aa1c83aa2b6aa493637f611d654d957
d973e7854f10b4d0a1060e55022dceadc51d038cee85d05e2c2c2fd3b40a42be
a015790f512784ec1e552402c60c402d6ff292143ab888811cd8bb70da572860
e50987f5f13de4a552778a691032d9fce3a102bfad3fb5b7edc4c48d2aa3b4f2
fe7c1337ecc319a62d325c720c24bd953f2ac51c72ba456aff16894b958f24b5
078859c7dee046b193786027d5267be7724758810bdbc2ac5dd6da0ebb4e26bb
9162ccb4816d889787a7e25ba680684afca1d7f3679c856ceedaf6bf8991e486