



# KPMG Cyber Threat Intelligence Platform

## Asylum Ambuscade – Straddling between Cybercrime and Cyber Espionage



Asylum Ambuscade is a crimeware group that has been engaging in both cybercrime and cyber espionage activities since 2020. In March 2022, they gained attention after targeting 4,500 victims worldwide along with some European governmental entities involved in helping Ukrainian refugees. Overlap between campaigns of Asylum Ambuscade & TA445/UAC-0051 have been noted, however the attribution is still unclear. The group targets banking customers, small & medium businesses & specific government agencies across Central Asia, US, Europe & Africa.

Initial access is achieved by spear-phishing emails with maldocs to run malicious VBS code or to exploit Follina vulnerability to download an MSI installer. Another attack path involves redirecting victims via Traffic Distribution Systems & Google Ads to download obfuscated malicious JavaScript payload, to finally download an MSI installer. First stage downloader (written in Lua / Tcl / VBS) is dropped by the MSI installer to deploy heavily obfuscated next stage payload – SunSeed malware. SunSeed creates a LNK shortcut in the startup folder to establish persistence, then proceeds to download AHKBOT & AutoHotKey interpreter from C2 via HTTP GET requests. It further downloads & execute additional Lua code. The group leverages another variant of AHKBOT written in Node.js, dubbed NODEBOT to evade detection. AHKBOT & NODEBOT take advantage of various plugins to perform password stealing from browsers, keylogging, capturing screenshots, exfiltration of sensitive files, deploy hVNC application, Rhadamanthys info-stealer, launch commercial RATs, etc.

The occurrence of a cybercrime group engaged in cyber espionage operations is rather uncommon. With attribution and detection of such groups becoming harder, it is crucial to closely monitor the activities of Asylum Ambuscade to stay informed about their TTPs.

### 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.

<b>We offer a wide-range of services, including:</b>
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: raghavendrabbv@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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2023 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.



home.kpmg/in

Follow us on home.kpmg/in/socialmedia





# KPMG Cyber Threat Intelligence Platform

Asylum Ambuscade – Straddling between Cybercrime and Cyber Espionage



## Indicators of Compromise: IP Addresses

84.32.188[.]96	46.151.24[.]226
45.132.1[.]238	84.32.188[.]141
46.17.98[.]190	157.230.104[.]79
5.255.88[.]222	212.113.106[.]27
62.84.99[.]195	91.245.253[.]112
80.66.88[.]155	104.248.149[.]122
185.123.53[.]49	176.124.214[.]229
45.61.137[.]231	212.113.116[.]147

## Indicators of Compromise: Domains

snowzet[.]com	namesilo.my[.]id
---------------	------------------

## Indicators of Compromise: Hashes

5150efe55280f3a6b2a043a84ef13bdb
a49c1b7743822ca0c36fe9e9128c20bf
3557d72a837ce1a90353eda8ba9ae758
66fc612cd5bbf780ef6b3cfc3f801418
a07fe3121c9cd1e11df062cf5629b4ff
eed618dd87e77cd343bcaaf43fd9b7f
a48ba472f31deccacbb759fb8401085d
69eab91a34647d8ef0ff0152391160f2
426dfd5ece3b41970773031637cd5539
24b6950afd8663a46246044e6b09add8
24a0d2ef5b931a2a13341a2503b1de80
d5f8acad643ee8e1d33d184daea0c8ea8e7fd6f8
57157c5d3c1bb3eb3e86b24b1f4240c867a5e94f
7db446b95d5198330b2b25e4ba6429c57942cfc9
5f67279c195f5e8a35a24cbea76e25bad6ab6e8e
c98061592de61e34da280ab179465580947890de
519e388182de055902c656b2d95ccf265a96ceab
ac3afd14ad1aea9e77a84c84022b4022df1fc88b
3e38d54cc55a48a3377a7e6a0800b09f2e281978



# KPMG Cyber Threat Intelligence Platform

Asylum Ambuscade – Straddling between Cybercrime and Cyber Espionage



## Indicators of Compromise: Hashes

441369397d0f8db755282739a05cb4cf52113c40
117ecfa95be19d5cf135a27aed786c98ec8ce50b
d24a9c8a57c08d668f7d4a5b96fb7b5ba89d74c3
95edc09600c5b8da7c8f93867f736928ea32575
62fa77daef21772d599f2dc17dbba0906b51f2d9
a9e3acfe029e3a80372c0bb6b7c500531d09edbe
ee1cfedd75cba9028904c759740725e855aa46b5
c554100c15ed3617ebfaab00c983ced5fec5db11
ad8143de4fc609608d8925478fd8ea3cd9a37c5d
f2948c27f044fc6fb4849332657801f78c0f7d5e
7aa23e871e796f89c465537e6ece962412cda636
384961e19624437eb4eb22b1bf45953d7147fb8f
64f5ac9f0c6c12f2a48a1cb941847b0662734fbf
557c5150a44f607ec4e7f4d0c0ed8ee6e9d12adf
f85b82805c6204f34db0858e2f04da9f620a0277
2b42fd41a1c8ac12221857dd2df93164a71b95d7
7fdb9a73b3f13dbd94d392132d896a5328daca59
7f8742778fc848a6fbcffec9011b477402544171
29604997030752919ea42b6d6cee8d3ae28f527e
7a78af75841c2a8d8a5929c214f08eb92739e9cb
d0fe14f8dab89aaddac8b1c89b1cee48396ec636
8c5f94da03e5653bc534394b2866c7a539d3b25b
752b16c7159b9706ac0a1c872de2e44c568a6f04
6444dab57d93ce987c22da66b3706d5d7fc226da
6201347d1ded92d365126a1225768e11c33ee818
518bd23ab095bfb4cf8577d8f216281199b57c55
fbb221ee4b17929bddc95beac7d2736709cf1a5c161c3139a1cd90c3f2044420
53e4bfd27474f6e4829ac4d625d3d914452456baf5da2c1c51e2e6df35ab634a
b59686a8ead6491bce8633f5e774fd5c3f52bc0f733cd168f113729dfdfa702f
ba0f32914a940acc18cda37781a6302cfb667a9c241c1f4e185509267f91dc95
253fe2c0c721a5d539f0e3ffbcfb0bfab11ed1d984750eff72a8595f2cd0e079
7bf33b494c70bd0a0a865b5fbc0c58fa9274b8741b03695b45998bcd459328
fbbe7ee073d0290ac13c98b92a8405ea04dcc6837b4144889885dd70679e933f
f97f26f9cb210c0fcf2b50b7b9c8c93192b420cddb946226ec2848fd19a9af2c



# KPMG Cyber Threat Intelligence Platform

Asylum Ambuscade – Straddling between Cybercrime and Cyber Espionage



## Indicators of Compromise: Hashes

e9167e0da842a0b856cbe6a2cf576f2d11bcedb5985e8e4c8c71a73486f6fa5a
d10fbef2fe8aa983fc6950772c6bec4dc4f909f24ab64732c14b3e5f3318700c
b1864aed85c114354b04fbc9b3f41c5ebc4df6d129e08ef65a0c413d0daabd29
a8fd0a5de66fa39056c0ddf2ec74ccd38b2ede147afa602aba00a3f0b55a88e0
9aa3ca96a84eb5606694adb58776c9e926020ef184828b6f7e6f9b50498f7071
976b7b17f2663fee38d4c4b1c251269f862785b17343f34479732bf9ddd29657
737f08702f00e78dbe78acbeda63b73d04c1f8e741c5282a9aa1409369b6efa8
5b317f27ad1e2c641f85bef601740b65e93f28df06ed03daa1f98d0aa5e69cf0
3694f63e5093183972ed46c6bef5c63e0548f743a8fa6bb6983dcf107cab9044
343afa62f69c7c140fbbf02b4ba2f7b2f711b6201bb6671c67a3744394084269
31d765daea26fb5cb506635754c700c57f9bd0fc643a622dc0911c42bf93d18f
303e004364b1beda0338eb10a845e6b0965ca9fa8ee16fa9f3a3c6ef03c6939f
2e1de7b61ed25579e796ec4c0df2e25d2b98a1f8d4fdb077e2b52ee06c768fca
269526c11dbb25b1b4b13eec4e7577e15de33ca18afa70a2be5f373b771bd1ab
20180a8012970453daef6db45b2978fd962d2168fb3b2b1580da3af6465fe2f6
15fd138a169cae80fecf4c797b33a257d587ed446f02ecf3ef913e307a22f96d
1561ece482c78a2d587b66c8eaf211e806ff438e506fcef8f14ae367db82d9b3