KPMG Cyber Threat Intelligence Platform

UAT-11587 - Antino Backdoor Weaponizes Outlook & OneDrive

TLP : Clear

KPMG. Make the Difference.



UAT-11587 is a China-nexus cyberespionage group active since at least September 2025, known for multi-stage infection chains and tailored geopolitical lures. The group targets government administration, defense, diplomatic services, law enforcement, legislative, academic, and civil society organizations across Taiwan, India, the Philippines, Cambodia, Pakistan, Thailand, Myanmar, and Syria.

Initial access is gained via spearphishing emails with spoofed identities and decoy documents, including Gmail attachment-preview lures, directing recipients to Cloudflare-hosted Pages that deliver HTA or Windows Script File (WSF) stagers. The stager uses 'mshta.exe' to execute a JScript downloader, which retrieves encrypted resources hosted on Amazon CloudFront or Cloudflare R2. The second-stage JScript decrypts these resources and initiates a .NET BinaryFormatter deserialization chain using an 'ActivitySurrogateSelector' gadget chain to load and execute 'TestAssembly.dll' directly in memory within 'mshta.exe' process. 'TestAssembly.dll' opens a decoy lure document, stages the DLL bundle in a writable directory, and launches the Microsoft-signed 'GatherOsState.exe' to sideload the Antino backdoor. Antino establishes persistence via a Registry Run value and abuses the Windows Scripted Diagnostics framework to execute attacker-controlled PowerShell commands. For C2 communication, Antino uses Microsoft Graph and Outlook to retrieve commands and return results, while OneDrive stores heartbeat information and facilitates file transfers. It collects host and process information, lists directories, executes commands via cmd.exe/PowerShell, executes programs, and loads shellcode into memory. Data exfiltration occurs through the operator's OneDrive, blending malicious activity with legitimate Microsoft 365 traffic.

UAT-11587 abuses Outlook and OneDrive for stealthy C2 and data exfiltration, making cloud activity monitoring and restrictions on Windows Scripted Diagnostics abuse critical for mitigation.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Enforce browser extension approval policies through enterprise controls.
- 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

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

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

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

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

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 endeavour 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.

© 2026 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.

KPMG

KPMG Cyber Threat Intelligence Platform

UAT-11587 - Antino Backdoor Weaponizes Outlook & OneDrive

TLP : Clear

KPMG. Make the Difference.



Indicators of Compromise: IP Address

103.27.110[.]220

Indicators of Compromise: Domains

wps-cn[.]com	microsoft-flash[.]com

Indicators of Compromise: Hashes

8b6807b6a7479a2e770eb11a14de8e2e
a71774b0500f42b7b9ed658fa03ec874
ceb3158cee2b7d6b1dc829edc87eaf10
29a6d5c2c2bdf5a8baeb206f09a297b8
1a856063b368c7d4d4f13536b9ab7b42
cc648bee6b11ce487565ef67576eb1c6
80f759cdef77ce76d6b7cf4db20bcbe9
586dd64c038ebe36c39f38d0781ce81f
277529fc1204337be437c4459d743d34
a04eadb91762badff07709f7d01675c4
132268d8a6804f2d877b96ae082ae9de
ce0022848c660545b8dfb1a732957da2
28f754f64aeb80ba9e81f81c7b54bdd9
06967803198f1be4c67fbfc2d5176ce9
b7a58329428b68f2c108a0f77f1a78fc
a19ed0f912c2444f2fbe0ed82ab8d74b
46fa8f92dcfb524b1ee3796e1d79aa62
b4a4ef987e608ecce9c1e0d52f0dba2d
571d28a33cb18ddc5a467a6629ad49e9
c56fd048fdfc800a0a74ebe2cd5879bf

Follow us on:
kpmg.com/in/socialmedia

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 endeavour 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.

© 2026 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.

KPMG

KPMG Cyber Threat Intelligence Platform

UAT-11587 - Antino Backdoor Weaponizes Outlook & OneDrive

TLP : Clear

KPMG. Make the Difference.



Indicators of Compromise: Hashes
5510d33df957558bdde9a940d57a243f
f86a4cf2a1a18c83b1facba73de11315
78aef10e5ec0815abd5c0fbd21507b0e
764644ee9d2aaa263563619d6b1b3450
fca2d8e6bd9ed315c2324be2b3708bdc
f561360b382a7ef3f5c4e3b194d5d4d1
66b40330108e5f3fedc5b313584600f1
9a2dd009889b46218f1eb0ba34bbcefa
3f88687ca207a17f28eadfa3764c68dc
f74fa4907c89d54656110be02e1d5cd4
42260273521681 99e32509ee8dbddd478394372c
6c8561477c4b8fa035066538bce4f31c4b3b0870
e2fe11571f9f031fc1ce7b3a92b7163f9e34222b
eae2019bc39d11ed657472668ec3b426045a1ac8
d3a825a310d58a4d0498cf293aedf8edd945b2c4
3fe4bd14923975e5e934876903f2f0260e35b754
8d877dfbe3ee74a9b55e8695252ba50196826657
e3b2bba523c035177241f6f66168e60fa6abbaaf
0fa55930a5269a7fa8e7b7ea56f9daa4801a3bd6
da0f6a00624b21e1bff8dda95a5ac847a9c2b936
5fc2fc9f15d522d5ca88d99f4bbeb45884215cd6
b5abdd6c018abb160a0b331ab6f723cef646e932
c18515555b00b3e9fce9d43cc13cb0af9539f92c
dd4744dd39b9cc3c61b5fa52652f67a04b4c1aec
c89901f080718a78b41ebefd3f07972b0b382588
59a7956d8fcee8af30cff6adf5ee40ae24042296

Follow us on:
kpmg.com/in/socialmedia

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 endeavour 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.

© 2026 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.

KPMG

KPMG Cyber Threat Intelligence Platform

UAT-11587 - Antino Backdoor Weaponizes Outlook & OneDrive

TLP : Clear

KPMG. Make the Difference.



Indicators of Compromise: Hashes
be4d124725649e689322c156ea5bdc3e44e58c1f
dec714a632190e0a6868dd4b2c67fba89d020aba
7f8f95988ee6d8b08e79e3138f853b4e66365032
e8b4a1ec9ca53688fb62e29c44d631f1cbc54d9a
5171f2578109edac2a6ee918b484d24d0bfd17c2
a80c082d42756c41b73bf29b08389a286b55e201
d3b22101fe3e29640fe6b8d6aefe7708a2209cec
46c30044e001ec3f3715d046d39c1572ef330cb2
33d222dfb62374413761e0c92b3a9e5360f4134c
0e56303743a81d4bb15cbf771fdc631f9b7f267c
3869e740a3188954c0ea74d448f806b9ff65285f
9632a6985a5f05c5db1e02e34388ce7bec88bbc0
40852f063eb49722219bd6f817392a8f6d3da33d
829a3aa7be1245bc25aaf7811e1bad044dd751b1
01b5c6acb20e41799a0e96d9d1d6e1c44791883706b6285e874fcb15cc93b31a
077bd873217d8abfbb6482d11966ca34f3fef7ad5166f24fbc5dc3ddefe894a1
079acd58a74479ac8b108b618d2a4da8a8bd560a04459cd90e2fec9da5027513
0a6fb71ab1362d065c7ec2678c1e73d9a0721b0e7099d392ba7559bb2eec4970
0b4e5e017c0f0ccac79e13ca5d580a75af67a24ca0763f9ebfdaaeb1ba4fc739
0c39264337a1186b2e765e24073399cbdcba118306614eb411e315887af578bd
09ef7c736bccfafefc44d9910d499173b88063b73b221fc0dc9e9105107e5cff
17b53ffa8e005f0e82491d3f9c0a4984c44da52e1668a855c11a137f627c5b4b
1fadc90b61ce536abda78eb387a7f3d745f00c16775d3f762845ccc0fde567da
23d5f1af8581ae200615d9a66d539f2043c3248b649e862557b379d7e8b7a3ac
2f1513c822af0c6635dd3c69dc38f0b2f6e02012ea36415fff111a5d4d5fae05
3a94910eb8022592ce030e6861359f7e980fc1b5a6ccd290cbb071d3e95ed02a

Follow us on:
kpmg.com/in/socialmedia

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 endeavour 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.

© 2026 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.

KPMG

KPMG Cyber Threat Intelligence Platform

UAT-11587 - Antino Backdoor Weaponizes Outlook & OneDrive

TLP : Clear

KPMG. Make the Difference.



Indicators of Compromise: Hashes
e809da86bd81463347fa7f922d3e088755a94a331889d32acb55aa8f57778a34
40e7e77aff603f4c2ef17b3bc8ea836e714d0734a1e5b946e52f95536ec5c91d
9b7df409c9a89f7536d3ba7b6d43fb6dbac618c8bb52615ba34cc971ad71bbf3
47f98dfe01759a464e22d5ec55d012dccb38ce010dd73e3ba8d7ffefca12b4b2
484ab497072ea09f12187b349f5b1c80754e4942408a009cccb20a2a3c8c6506
4b614e5c37abaddca162119e42a969945caa681305e246e0ed0060ea9984008b
5168a2696a0ed858f996f388bfe94f952d475158f4ee6206816608936db005ca
e2eb7703047b37b28dc34e6990205d758a2454b39bc655b460606745fadcb530
f1ef5fe4c0cdcff13cc750c867728b89719f81437bdc49041edd1ae1f3edb4e8
5555e904101689351a2a1359c9c06da0a57139a9470df7d26823c1b75db55041
5a35fcd4458e808ab0fa52bb2a92923b60566ee4d7aaadaac7c95cad3d839562
5c5c060b272cd4a5c3767edc0e9478bd35b7e1756e183d0446a5491bd65519cb
61a8f5add6c35f99c389012dbb2343061fd0b54611b40490b9a7f0b49d707da0
65f4b9292e91abfa5adf42a03526932930c1c0a436bb186a7948fe6770295788
e7e3b0bcd6798634adf8b49d305f3a7b7682e4b76db549682a183c5a186df4bb
6a1dbbfcfe6867ac83d35012b2717084388b4a34707efd0b725466dfd0e8fa56
747b1d13bdf06956b5da5f47250fefd5284ebcf7961971732c3d348aa1a2d533
75c12795016ae48b1bddd34a9f5adea63a12f58701eae01e1b4ab3d9dfa1513c
7969ae5f11fc163049c8eadba06f814f5edece13a707e6087c1c49011a45b838
7fa98efba59614cec0b7291aedee98764f8dc037b6cc798c93951a31208e9e32
8e1d68906d6de92f359945d3a95da1480e72773a3e8dea7682d6bf0f6699f75f
971cb2448b5d67dcc1f5eaa10d12e77f213035ad31230dc2ac7a510610a2059d
a0e91085f08956a9a7034ace73cee60cb211f5d96f02bc91a026601bde8f2221
ad0bd2b45e2416fb1384bf30af068d857e7c06b4226615d66b55b610a34c5670
ae1b45fb56b9f1b9cb3ee30d2bb1279c9b90b70bb62f8de305d198c6a4e0585e
aea5e9029f9212d05bde10f7806d1f2819be45d167e6fd877b9fb1b11088ac90

Follow us on:
kpmg.com/in/socialmedia

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 endeavour 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.

© 2026 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.