# KPMG Cyber Threat Intelligence Platform

## Void Arachne - Infiltrating Chinese Users with Winos 4.0

Void Arachne, a newly identified threat actor group, has been actively targeting Chinese-speaking users since its discovery in early April 2024. It employs sophisticated techniques to distribute a command-and-control framework called Winos 4.0 through malicious MSI files. The campaign strategically focuses on sectors and countries where there is a high interest in AI technologies, VPN services, and Chinese-language software, to infiltrate system for covert operations.

Void Arachne utilizes SEO poisoning and leverages social media platforms to distribute malicious software, including compromised MSI files for popular VPNs and AI technologies. The attackers distribute backdoored MSI files and ZIP archives via Chinese-language Telegram channels, directly hosting them to exploit user trust. The malicious MSI installers utilize multiple DLLs to schedule tasks and modify firewall rules, crucial for maintaining C2 communication on public networks. Upon execution, the installer employs RC4 decryption to execute a second-stage payload. The loader uses a Visual Basic Script (VBS) to establish persistence through Windows Task Scheduler, ensuring the malware remains active across system reboots. The decrypted payload serves as a stager to connect to a remote C2 server, deploying the final payload, Winos 4.0. The stager in Winos 4.0 serves as the core plugin manager, executing tasks initiated by the operator and managing commands received from the C2 server as DLL plugins. Once activated, Winos 4.0 conducts various malicious tasks, including file management, DDoS attacks, disk searching, webcam control, screen capturing, microphone recording, keylogging, and remote shell access.

Void Arachne's strategic use of SEO poisoning and exploitation of the burgeoning interest in AI technologies highlight critical requirements for swift and effective mitigation efforts.

### 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

## Void Arachne - Infiltrating Chinese Users with Winos 4.0

| Indicators of Compromise: IP Addresses | |
|---|---|
| 98.159.98[.]114 | 103.214.147[.]14 |
| 156.248.54[.]11 | 103.214.147[.]101 |

| Indicators of Compromise: Domain |
|---|
| webcamcn[.]xyz |

| Indicators of Compromise: Hashes |
|---|
| 18b485a2a8cd14cd3bc7d274d2f12c43 |
| fe7aedab70a5a58efb84e6cb988d67a4 |
| 4bb1a0acbe947b77031dcd4b5089d483 |
| f361f91c2f2e8597bb579e8151e25bd7 |
| cf887bbb3a9932417094ec7eab362f5a |
| b07aff833c84c8f60c220898369a85f8 |
| d9263ad408e44848b4bd07b2fd99ef59 |
| f3dd6c11f7cf5f4a7fe6f883d2c0a79c |
| 7a00cac5f1e621ec3da5f781fd89f270 |
| 543785705c4402e8259acb4ea2b2449e |
| 493c700ef6a7fa679d3d3fda9089f348 |
| 233e65344c964ecac506962f289f9503 |
| 4a6027e2547fe1418fb4ff73ca81176d |
| 5a187185bd8ba9c5f7fe85cd125d99b5 |
| 562883ca2bc819790793756d02aeef8d |
| 9d3e4a459be46c901167e21194523236 |
| 00be3d2cc7bd3558a6ebf77a9cf3318e |
| 28df247b75475c9d885376ae80b1a452 |
| 09821c414416fa1257fc4731dd6008dc |
| bb1db03aad061ec90289ec51ecfed72c |
| 2eb7bb21074e8415b4196d7d2a8aa086 |
| a03af44394e1647f8e9e76f12355bacd |
| 6cd6f35229a4c3e1bea0d1b91b8c5141 |
| ef34d4346a513a1f817c60daaa86556a |
| 44e6acaffe3c643899dab6d05b9ba2b4 |

KPMG

# KPMG Cyber Threat Intelligence Platform

## Void Arachne - Infiltrating Chinese Users with Winos 4.0

| Indicators of Compromise: Hashes |
|---|
| 0df68344f8c36d7d947ead941bd35228 |
| 966fde900b1ad15c9bc323ef940e261c |
| cc23fe095909828e70952ebbc41c162d |
| ba948d3de73c37f14b87879893f6ee547ced764c |
| 2c01c74b4272ffb955afb52c3aa8ba770272d9d2 |
| 7cc287d886f8851caf987c4cd8238302b65eda09 |
| 678dca04bf40b208ed45854c0ed0849394a7aded |
| 705a80b4a9ab6a31395e89dab91b9ee3933ee6d0 |
| 87b6afe25c7fea846a871e22f222e4ceb32f8201 |
| df6ffd03639011d11fbea583c799e7b5c1893ce3 |
| 284560038b769a616c20057570e2d3e55497fa40 |
| 7c7f4ad223476ba94ad23166df1b07f590e9ee55 |
| 855a96bdb899d3f25956459895628ba4d8d044ab |
| 723a2bffd15e3f09278d52f14be36dce1ce91012 |
| ae09e14e3f911359903b0c296455607f1d0c8082 |
| e042cda405b691de00411359ce3405d1cbc0dde7 |
| 5d1ad6938e19ec1a2de86a504cda3d7be4719313 |
| 9a5c08300f03a8381cfe3f0e726a32141f885c79 |
| a219e064fd783758d3899b36e7c8a46fab57caa8 |
| 0dc3ef2cd2ffe3a4c52c6fd01a5501d7b84ae8d6 |
| 61cd40da9253a367e416c9ab67e73738f18948c3 |
| 6926da5cba7aed9eb370b338e38990c0268668ee |
| b665cb8cbb3cfd3253dc994102d579237b7dcc3a |
| 2cf5ddffbc85a3acce9be26568f7258c7ea3a46c |
| cd3ed212441f221a2f0c40f2b71f7bfec1349a9a |
| 5701fe1b8ab3b5d9c35cba743a391191127a9180 |
| 38219b6b966f397bce79cbd42f7bce5470709966 |
| b248af4accd5739f1e7c792efb6a13d1ba89dbe0 |
| 6183c00570b7ae8c93dd2e5f0a0289aaafc8df06 |
| 09d07ce52af499c3674185511258ad15c5424fa1 |
| d3cbc91e6d5c11303f5efc5994b0c681d7fdb4ba |
| 9cbfbc782b224037e935b8501c79185f296de27e |
| ec928c5fe6e249fc426b27633c0826dfb011071e |
| f921c710dada0f5efa61527c006301cac7b40e2a |

KPMG

# KPMG Cyber Threat Intelligence Platform

## Void Arachne - Infiltrating Chinese Users with Winos 4.0

| Indicators of Compromise: Hashes |
| --- |
| ff2d05a637d8da53ff460a0427ea952ceee561b7 |
| a2314cc7c245a276b0fce3a2f1d2de4bfbe5bd9b |
| 16d3c176ca94c84b60e26981231bf59ebe75057ac10dd6f583ce65a3bed11dd0 |
| 3ac0afec0ce29b69d57c54663c6e4fa6fee703696069cb5b8f00783b5504cf80 |
| ecf5394d78392b11daec1016c6b447f9da7eae69f7702ecf8c4d1d3f69e3fe64 |
| 2066dd040fe020ca32e5ebfeeb4fa75094d3ac43155c83fe222f380d4940df42 |
| f6216d72f4d9a7d46f3b878650b2f26982e4f05b8b5ce363a60c564159db781f |
| 81c30a63161d40fb6df55b6147b2d9577830f08bfc9121ba8574c8bb6ec3a2a2 |
| 41f827e6addfc71d68cd4758336edf602349fb1230256ec135121f95c670d773 |
| 11a96c107b8d4254722a35ab9a4d25974819de1ce8aa212e12cae39354929d5f |
| 186bf42bf48dc74ef12e369ca533422ce30a85791b6732016de079192f4aac5f |
| 202c378deb628a8104a1dd957bbd70b945beea8e11d55b9ce3e4787fbe496797 |
| 1dbb3d08931aac2a76c9a72fe38d038e172b29f898acaf5db1ec91e180f7ec22 |
| b022e0f0b2ae9e27847cfc909bfcdbc89a732fcdde6e473443aaab2592a84910 |
| 4b323ab024562e6f25eb91c7bbcd3f752f67ed5274dd83cf45b9d55aa0f37522 |
| c0aa7b470e2e76ba0aaa65de2257aec5ff23485115f38b7a7a1285067c69e0e8 |
| fae4f96beda54a1ed4914537b0542182d3a020dd9db9d9995df37d303b88e6df |
| 768881a43d2ffd9701bf2e241a1d59d8a0c116cf20e27a632a8b087bb81de409 |
| 7ed8c7ea5e2feeadb1966f53c48ab3a580f53a4d20725031d764db7e962607a9 |
| 49120dfcef430df1c90c9c370b92b969c876b9b4327d81eae720cd71fcd75b87 |
| 023822a8ad26f2d7330a2afa310ccf943058f2765b7cbc6975c51c144739b55f |
| bc01cf528086de6a1b231dee01c1624cf58911b171904bf7a6b08ddfba661d83 |
| 5759fc938f228579fc5e64e74cee083581a975d4054deb715c0f371b66b96263 |
| 976837663b25f793470f24925198b06e79a72ede014a84ba62311fadede5062f |
| 436499efe94c7a1bfefaa84c52f8187bffb3d4d1a49de1cbc8885e7807d11b42 |
| 5684fc4f33c168519b2fdcae59cc3be2e6db1f0b0f3718524ef57e0e7423f59d |
| 7a3841a5315c01df299d8844b62dc150b1c3e5b5ebe7547c1a211349879659af |
| 5abc2006c7a3a27e033075ba881a668aba5e70797677ed2220f7ab9fb36fc927 |
| 827ed4f36ea7032395bfa35da54c6e9d06d6633aa7396792e8511adf366c1fcc |
| c61c8ded2a9481c2e50b4872c8f7bcd8ecc33997a6004e62aa06b60742f54e57 |
| 409e09ac0fcf7d39044ef0b3eb798aea6dc0650e5214056760694c1340fc8488 |
| 61d73a8920c41483d0832c9a5c5bc9f57ac5f71146a98faefc0cb4d988e77bab |
| 4791c23aff8a09061b76a05bb88ee37149995584a87aade236ea4eebab79ed1c |
| 03669424bdf8241a7ef7f8982cc3d0cf56280a5804f042961f3c6a111252ffd3 |