KPMG Cyber Threat Intelligence Platform

KimJongRAT - Dual-Variant RAT Targeting Sensitive Data

TLP : Clear

KPMG. Make the Difference.

KimJongRAT is a sophisticated Remote Access Trojan (RAT) first identified in 2013, believed to be attributed to the DPRK-linked threat actor Kimsuky. Over time, the malware has evolved significantly, adopting a dual-variant delivery mechanism that includes both Portable Executable (PE) files and PowerShell payloads. KimJongRAT latest operation targets government, defense, and research sectors in South Korea, with potential spillover to other regions.

Initial access is achieved via phishing emails impersonating trusted institutions such as the Ministry of Gender Equality and Family and the National Tax Service, directing recipients to a GitHub-hosted URL. The GitHub-hosted URL delivers a ZIP archive containing a decoy PDF and a malicious LNK file. Upon execution, the malicious LNK file triggers a VBScript that decodes and executes a Base64-encoded PowerShell script via mshta, which subsequently downloads and executes HTA and PE files. The HTA files perform system-level tasks like credential extraction, while the PE files inject DLLs into browser processes to harvest sensitive data such as passwords, cookies, and master keys. Persistence is established by modifying Task Scheduler and registry entries, ensuring the malware remains active across reboots. The malware performs anti-VM checks to detect virtualized environments and self-deletes if detected, evading analysis and sandbox detection. It decrypts stolen data using techniques like RC4 and AES, collects system information, and exfiltrates it to the attacker's command-and-control (C2) server over encrypted channels. Additionally, it includes keylogging and clipboard monitoring capabilities, continuously collecting user input, which is stored temporarily and later exfiltrated to the C2 server.

KimJongRAT's continued evolution and deployment highlight its persistence as a sophisticated threat, demanding robust detection, mitigation, and ongoing monitoring efforts.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the latest versions as per the OEM and is protected with multi-factor authentication.
- 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
Director
T: +91 99994 30277
E: rishabhd@kpmg.com

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

KimJongRAT - Dual-Variant RAT Targeting Sensitive Data

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses

142.11.248[.]98	27.102.113[.]107
27.102.113[.]20	27.102.113[.]170
27.102.113[.]209	183.111.226[.]13

Indicators of Compromise: Domains

daumcyd.ddns[.]net	yfews.mailhubsec[.]com
natezlx.myvnc[.]com	nid-naverbpk.onthewifi[.]com
yajxu.mailhubsec[.]com	

Indicators of Compromise: Hashes

2e8bf657d0301fb4c61e29f455d9058e
172dc997ca6022ec8dff0842e4c7b887
5441d8a79411a261546beb1021cb5052
1230b4160b399b84453fd15ed7a6f1e0
13d89e3f08197920230b521997135a6c
40e117a35c579a2f17eafaa728abdee3
425e7f14bfef366725fb806c93a0e94e
444f67d186136d3deaae17a7f27b879e
4593e0baa7e444537730c057b1a465f3
4aea7f8a80c27268bd68077621d69b68
5852e7911d0df2473d6ed34d1ce56ff7
5eb7a909d8e8e3773b2ccc780d8f765a
71a6e029ae3a56a1d5d244cdda0a93e0
95b0ee79eda2ea1857bda77aaaa71d92
9debce6651edac2a0e135a5b06f68a88

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

KimJongRAT - Dual-Variant RAT Targeting Sensitive Data

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
acdf153ab1211ebc840a18d2ff2221fb
dcb9bcd4971167905a6924c4c2cef12e
e45606ec936210f3830f29d0e12108c8
03794685a12ce0dd7b69e70ced8568f9
17b2412c1c74db7e83482a544fefacdc
1a2164d9fea343bd5a5fc31a0849bb6e
373fce7c6fa68ad9afa22bcbf8c15f5d
851910eb3c05738de97d66078acc32bc
baaa2dd6942f582cd7f684b5ebc447f0
003ea91e9f52ecfdc3aadb2732e9b54c
66c4e2dd235c4d8d31abaf96e051585e
677e77265c7ba52e825fc62023942213
76d2cbad8502dce9e70e501c2378d3ff
77f131bc8f660f85812c0d2e0da8e77e
8b6580e14b8164e28e684d48691ddf4d
c0ee9a9046d82b294b3bf3bec997fc45
c69909ea3c131181fa7ae12155bcae17
d69fbf23e7492618cadc63d171010cd8
d9ecf148c88bfd9791758b3be1a9f459
e3a937869322cc4cd765fcbf16d5b9ea
f000df00a424cefcd8efff48ab167169
83dfa760ca4087d7320afc224089898dfe508b21
f254b3f809f2a866d41b3fac5e51a150ddf98b5c
85b1ec1efa49cbc9078017c0d9eabe51107d60b1
ccf44533aa41ebf0e666fad703c0be424aab16e5
e0847f233cfb02f575714ac685c52a2f7af1353e

KPMG

KPMG Cyber Threat Intelligence Platform

KimJongRAT - Dual-Variant RAT Targeting Sensitive Data

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
f6a09f9d525ae992ce8548b9053dd8f0d901bf28
717bd6595a1fe3e708cabca7b27fee872d969cac
b1c9fe1c7d0b7d6b51fa25d17bc0afcd092094ba
d9c47f8c80ed44feecd1676416572a397e73e6df
33038fabd6ebff363aea81c51b9490e510cce379
18c3c459e4546c0e987dea32f7a788469d3a36e5
7f8122a81da4f478078608b6169d12ee84e6b9b2
d3b3fb0a0f7876d9d17862e69050a15f7d8d452b
255858877ba0c68af03892c1b8da2373bacff6fd
75dd5870b5a5a364727d01b2ce442180b350866c
3b4dae483a2c44fa1fbd2a9da2780d40dd1aeea3
6043e11b02c5b5075e46e66b9330ad8ff4ef0b05
82c7a8a50b14985acc106f13cdfcda88ecaad7a7
3d053af7a7c8a14af8ec85fc12a66e8444e7e775
7f4fc97870f4442477c9aafdb2523187b3026d73de30e9f90593b1ab0ce31da3
c24353e61826eb7187d1acabbd857ddb694ddfe130eb1f5195aadd39701565ca
748b45f59a2b02f41d001f2d71dea9a1a5b4ef0e49c9d5a7a14ea3867c7be81c
0ff0ca772477fe4558bd75c1471b9e945d8580213121993fefb52e79f0793789
cecfa6dce05f3a71923fd0ffa6e1ef45e1da8802134e52e74cdce1fd96f64dc6
1f34b194259beb09bd8812313880aa3d1967d112d7fb3f0e55b1072c36d611d7
1d01eab612da7d635e6b92395ead126e3e07b7987b3a38c8831e25cbcd5456b7
64b48a4b186301cd18045126cf87343fd4c46d9efa04cfdfc6df69cfbf6c0293
746249913d1f6e944fe1a70ea1b3684d1ca1431596bc89fca31168e141cf20c1
092c2607c9f60360bac8eb22059ac51330dce71080ab99f494f96523b7e177ef
cb9c24ee556d0aabdcaaedbcd5dd8e6f8ee324156507af84399256fa09d8b542
1b1431e7f18038103235558d4461bb3ab319b28a22ccad8a3b5607a4f09099a3

KPMG Cyber Threat Intelligence Platform

KimJongRAT - Dual-Variant RAT Targeting Sensitive Data

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
6d9854b69ce9cdee79b723bc7632eeb4edb74b466514cbc184738dbc01be4b38
d4a63c97ade3bcca8913f50bc1b130f924f929c879b45b839a9b2779c50d327e
4739393bd6dd1d938dc1dc3ee7e9e06bd6df1eedeed4cffca44dd1cd11a37073
941ac1e6728aab61a303e0f8e7ef815ed3b9c69a20bec424ab4accfc46145549
7a1577516f7b8c45c92f65bb458c9e481e1d43d44d32ff0efa34ace3da10a19c
6730d86c8e24e0c2ae0bb1fb65d15b5c303855927719d5f572fdc0ff1f623de3