KPMG

KPMG Cyber Threat Intelligence Platform

XWorm Malware: Leveraging Xlogger for Enhanced Keylogging

TLP : Clear

KPMG. Make the Difference.

XWorm malware, first discovered in 2022, primarily functions as a Remote Access Trojan (RAT) is capable of stealthily evading detection and collecting sensitive data like financial details, passwords and cryptocurrency wallet data. XWorm includes functionalities to track keystrokes, capture webcams and audio inputs and newer capabilities like plugin deletion and launching DDoS attacks. The countries targeted by XWorm includes UK, Spain, Russia, Ukraine, India, US and Germany.

Initial access being unclear, it is likely through phishing emails with malicious attachments. The victim opens an LNK file disguised as an invoice, which executes a hidden PowerShell command to copy and run a batch file in the background. The batch file distracts the victim by opening a fake tax invoice (PDF) in the browser while simultaneously executing PowerShell to download a malicious ZIP file. The ZIP file, containing Python setup files and scripts, is downloaded and extracted into the victim's Downloads folder. The extracted Python script decrypts embedded shellcode using Base64 and RC4 decryption, with a hardcoded key. The script modifies memory permissions using VirtualProtect and injects the decrypted shellcode into a newly launched notepad.exe process. The shellcode is executed using an Asynchronous Procedure Call (APC) to trigger the malicious code. The shellcode launches the XWorm payload, which includes the Xlogger module having keylogging functionality. It tracks user activities and exfiltrates data to the Command and Control (C2) server. XWorm establishes persistence by modifying registry settings or startup configurations, ensuring continued access to the system even after reboots.

XWorm malware's widespread campaigns and rapidly changing infection vectors highlight the critical need for security awareness and robust defenses to mitigate large-scale threats.

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.

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

B V, Raghavendra
Partner
T: +91 98455 45202
E: raghavendrabv@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

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.

KPMG

KPMG Cyber Threat Intelligence Platform

XWorm Malware: Leveraging Xlogger for Enhanced Keylogging

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses	
141.94.61[.]23	152.228.179[.]67
171.22.30[.]13	191.101.130[.]18

Indicators of Compromise: Domains	
ply[.]gg	portmap[.]host
myftp[.]biz	packetriot[.]net
duckdns[.]org	

Indicators of Compromise: Hashes
a21db5b6e09c3ec82f048fd7f1c4bb3a
4904329d091687c9deb08d9bd7282e77
0b426e8571f8d3e437b7a42e9b8fd808
ba41ffb3d8d33fc940d337c90f3fa129
57fec8de1cae9adfcdd8bd96a6f755df
2b7ba71d66acfabbc67099ea3b45560a
b8b6d0053cc3c7d9d58a19874b7807b1
dbaea36a3a89a62ed390b8b2e5782e30
0ae9d4d91bde4d050f899f917a56048c
12b9fd9acbc1ad0d11ea58a6930f119c
1a85ffae7660a7147e364ebd73a5a322
1cbca4b629db1d4f018c34ef73a5e30b
358e5b1466b74932897a1a20230ab58a
38dac2d34f499f649daf32e91097da5a
3f7913c73decfcac56e9f1c1bfb2779a

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.

This document is for e-communication only.

KPMG Cyber Threat Intelligence Platform

XWorm Malware: Leveraging Xlogger for Enhanced Keylogging

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
418ecfe44276b8cfa929f7ab2ec7837c
49253fe107d9edd9d8a92d69377975c5
4b6670807940844a62ce2777097ca39d
4da82753d48b6799fb2ff928878adc50
4eb04137b4fd24941e645c7fe7d0da00
65e054aa7b0524028da677ba90882713
850432e2797ef0864dd75af7dad0a8ee
868142ebdb38de361d4a3cba65dc84a0
871302d5688a0f95fe0d4c764eaf7e21
946d5227b4471d25d5c93dfe5e6a6376
95b3c12592ed7de85aeb86fe9c54e23a
96eb05963b8cf0f51fbb19f478a7aa86
99ac1041885d76a382b9a79e8c6cfe81
90a91116b24d6a273d07d1b516907fb8e0aebf56
1d457229c8f55b9eea85b0334f65fc2641144a41
148dd73b7a98df5a3990b016cdbed476e4320f13
87bb96efa520bdeea7cbee4559336610bc74d4f5
ae2e1e57a51229643b99519fc16a6df5ae7fa9d3
4355493bf39d0aed8faa64289903bcbea21012bf
505829777611a7ff257cfe1b0462394a97cad0a6
9c00c3b2163fa27b68f62366e02c68aec60f2ea5
1480393d5f36e017b5a98598742821ffb8a3ac5e
9a0019274f6950a35434b48846507cff6e65a01a
05b07466061e631e83f54d0eb4335067933f62c4
87ffb54fddbe132ecc10d61d2dbac21c5ba74e7a
241bbf93ea30dabf44324c7ef9b5714a8c3e010e

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.

This document is for e-communication only.

KPMG Cyber Threat Intelligence Platform

XWorm Malware: Leveraging Xlogger for Enhanced Keylogging

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
3effcf9674ad5c86c159f084ba0d7344aa53281e
70922950bc904c5fe9f8794fee4f2e01a642f36c
b3e711dff7690b47684ebaecb1efcfbd73c2f767
4b66acc8e4bd32fdbde3190a2d84f642f21a6dd5
ded312d465a891612e55ffeef71dbf6466d2f5f9
0873eb46e1450f5f70d05a0c2409089998ed79c4
4a6f7b46d077ad0e1dabea9f30efa95c52f79f3d
7a66dfb762362dc1a16615778a08d717eeac5342
1e32ee6a17e9526d41832177ed2d765fac9b8753
009c4ce76467e2b98bec20740dffefeecc365154
d528b7db179d7331823be2579763bd174f1fddad
5d53c734aa5ea76ebcd57cffa2236dab0c6ee252
f5279fab9888b810cbdebebb8eab8d8025228023
8a5ec3a2e03553d23a3327a1667908737851f114
219fbd1ffc17146d7a3297c4e1f7dc68d6ff28e1
67d9b4b35c02a19ab364ad19e1972645eb98e24dcd6f1715d2a26229deb2ccf5
e92707537fe99713752f3d3f479fa68a0c8dd80439c13a2bb4ebb36a952b63fd
ea9258e9975b8925a739066221d996aef19b4ef4fc91524f82e39d403f25579
aa8f8d093a10f1b25cb99ac059f30f056d2bb5924114a00a02cf83b0de04fae3
43812885c033ef342d147df053715761886fbec06d08e901419fcc9c969088e
9c1a4e3a1c90d013a9465ab585ad7a9cfc378ebdbe77fc1548cb81c791e6914e
6dc37cfbcc9f41c8854ce46505f0ca6e09d15c3147510e5e15f95dcfdf941108
b91b1d4d7f7d3010a2005aa20fb460e984e1fb4f0cd8d041626a0616c88579c9
090c22833f899dc6b0eaaf8511c0bdf7e638e0f905b224ae9e7db706063b2f90
8d3ef63171708962ad31c6328c418eab7f6f0f3bf97660d7c8b863cfa6282a9c
f0b72304c04c20c2fd7656fd43b3c916d92c7c89382a2e9a2ece614a90e61a10

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.

This document is for e-communication only.

KPMG

KPMG Cyber Threat Intelligence Platform

XWorm Malware: Leveraging Xlogger for Enhanced Keylogging

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
cbfb37a30549dfc3b45cb0619d9f810f8ea32c59e63aa91a21ab8d4192f74c72
83b91f098157b5ba0147972c1d5c4d751d66fc59d7645e2e643ce863101f6d52
ecfe634b75153c27d0e4bcaf3bf931aca1b64189254c8e08ffb04dc603915a55
979d8beb1cdb03b48e13beb8034136aeb2899bf437ce1483cff67976a0706db2
038806df1542419d8fff8f288bc2159a80c0a1c8f62e3df7c426bfd985b3d1d2
d9c88ab29f40ca6865aa0b0a99e8fe0ad9e00d57c88e084e94d70bf2ecf53b62
a088b9f3b8936f8fc7ef1c26a30e38b6fed5a08f20aad35a69733f2b83b9bffd
52d48762de1d1b88a9d5b1edb26ef678a1d5899e5521f1b49de0fdc159db899c
ea87bdca84791d7b13f4fae8744f3ef3ec81261be2b57f4dde80d9a2bcebdb2d
9b6eecaa9a316a2f4363b98691c52d775ba9c641fc13e9a2d0cde7ae725dd3b0
90e01d9e7329b5ece0778944afd455fa2cc55b27e4d78d7bc3f6a884a3b01c3d
9c8f662c94fb5178feb1af27980f736069689b039b32640df39c39e9438b0651
0b04d44318591e8dde1ac1cdd2ae725f97932aac7a471eacecf604bb1b76c898
0e775d8ad0dede1acec67508e6bdc2b6940a63c937e3131262889ddb3beb309a
87b2797f05debda5a97abab75511afdb42a2992fd8ca45e094b26bef558397cf
3d3e6df58bc4c81e9ba397b70246ec535b8e50cc01170b6be392566ccabaa7a4
72e72897d0386da8763e998e2b32cc996e500fe3db22556880cfb7b53f66199d
50a3d3508c4b826b4e36678dd91b374c339b0c57a89a31cd3e9f5a4441772dc0
a7da92a8f1dde21271b0e4ca6dab609c97cde7d659582eef25e373fc9dd44610
001e2be0b431a33fbc7d0eb1fabd07d5c1cdba26ebef12e85b2a7ba58bdd995c
853141ecab59614b4bd0e5ecd204a79e5856cd2aaa8464a6084b4c1ba2960610
cf479eb23e6252acce467b8cfc14182ac725659ef8fa5c28b9271a067756955c
f995d58bbe6383947308e35ffc36eba0fe3e357c2d4d9612dbf4bb2fa0f992b4
50cc18e65b1e6ca61f84eb2e255af53d1088db17585675c7eccc7a2236c13606
21432bcec2d1df855e85a64b3bfbcae8f5031ce449f2c4652076db7bdea375a2
7a61fcf00b368d4e5efe55c3d5b09b417422f081b4154a5b264a211c30959ed2

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.

This document is for e-communication only.