KPMG Cyber Threat Intelligence Platform

XWorm V6.0 – Advanced Plugin Arsenal and Stealth Enhancements

TLP : Clear

KPMG. Make the Difference.

First observed in 2022, XWorm is a modular Remote Access Trojan (RAT) that uses a core client and plugin system to enable operators to execute additional payloads on compromised hosts. Following a surge in the use of version 5.6 in late 2024, XWorm version 6.0 emerged in mid-2025, reportedly linked to the threat actor "EvilCoder." XWorm is not restricted to any specific industry and has been observed targeting countries including Germany, France, the United Kingdom, the Netherlands, Italy, Spain, and Poland.

Initial access is gained via phishing emails delivering a malicious JavaScript file that executes a PowerShell script while displaying a PDF decoy. The script disables AMSI to evade detection and downloads both the XWorm client and a DLL injector, which embeds XWorm into trusted Windows processes like RegSvcs.exe for stealthy execution. Once deployed, the malware connects to its command-and-control (C2) infrastructure using a newly defined default encryption key to secure its traffic. It loads modular plugins directly from Windows registry entries and fetches missing ones dynamically, enabling malicious activities such as remote access, data theft, file manipulation, shell execution, webcam streaming, and ransomware deployment. The ransomware plugin uses AES-CBC encryption and alters system visuals and registry flags. For persistence, XWorm employs VBS or .wsf scripts to create scheduled tasks, registry run keys, and factory reset configurations. Cracked builder versions are also used, which not only distribute XWorm but contain embedded malware, creating a self-replicating threat. Version 6.0 leverages ILProtector-packed plugins, advanced injection techniques, and layered persistence, making it highly evasive and resilient.

XWorm V6.0 shows how modular malware can evolve into a persistent, multi-functional threat, capable of adapting across environments and sustaining long-term risk to organizations.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Patch your Windows environment with the latest version asper the OEM and secure it 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

XWorm V6.0 – Advanced Plugin Arsenal and Stealth Enhancements

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Address
94.159.113[.]64

Indicators of Compromise: Hashes
7de2e86da1f243e9c8230883b6c896ff
2a988ba96ffbae8f3935d3e9a89dd208
652f64fcf7c252f6bec01367fb50d8ef
cf7ce813fe97b99903bbccd0087ce0c0
06ca939eac30e7f1d789a9bd26586173
2561b457103e7e74f5e6d9dcf703bfe6
a11466bee082a37915c25b84f839a728
25e304f15acb97cab8a6b685d8c8ef05
56d0e1e06598562c8fa70c657464cf77
75f51daff0696bb59f14a9b3f12d3578
cbdfd0de5b3cda140b2213213218993e
0d6bdbccc1ff17a88a3ff3b5de642912
fef068d49d6bc853d465fd5723ff3f4c
ab7312c934601d868e0d73b82a324273
5656e51e048c8597aecacecccc99d43df
b606bf23628c8644cf1499279dea1d2b
74119cd82001c2edc64e276fb0b858bb
3f520c2d99f3d200267c2ce7004dc02f
7bb897ee78f56a59c82c457945a608db
c1dac1c03efe11a63fb986343e2707a5
62ecc01366698328ea524e0269776996
32e6e423f99580b0120bb3062ee9dcf2

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

XWorm V6.0 – Advanced Plugin Arsenal and Stealth Enhancements

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
ca73b9614022ed1c2f5552eec25fdf9d
4b6bfd7589b54468c38a9800ac70d781
b1242df7c14309c9ac6b8c645278b885
7267374f04eb27651b37a4c32c015e9e
1365149d2c36ddf23ba615c78f337476
42c76f1205d21eb41ccdc0cdd4f4fecf
10712db15771cae02ec607b75748b57cfc0cf7d9
626f0a6972e84db69f3ffbc326309797b1c8ea7a
3fc1723bd903875448476c0000b76c81addae934
4d7ca9c3af77e706ce4eae5308fb9face9499572
4ea5734e235b2a00dc91babb5131681f702016b1
bcde791850b3a547aee585ea8c8bf060b16512a9
0be606b363366742133a6c316736bab6bca54831
a96135197963d5022ab03b538adf587539e108fb
70ab393489e5924d64b99e15526ddfbaa749523d
45bd7a00225cf42644965e7f61f26f060ac56d98
43b5045c089b7ddca49352dc6cd883c1d9d76c9e
7999f7d5b0119e004d71dfd4d4368b8196391c41
e1a2b12412a1468e0b572ddb48c65f5ddffefdcd
3a6fc316778d4267d7771ed34b4d9cbffd8ef043
b952b8c706a1bccd353a7ea0e9c89bafd50e26b7
bdd772a15e9d7417ab5f0d0773a4d412d59fd133
7a154d082f294c73b8cd49d9919892f9f25d603e
3b7e75a11e53176e680363fae90c13b9b333ef6e
c587d2fbeb7509d1cf8b92b81abdba5afc60be05
f779aef8c46bccdb593ba1567b57aa1fdd30f202

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

XWorm V6.0 – Advanced Plugin Arsenal and Stealth Enhancements

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
19dfacb38c931b8d5ce1d5b151faf0ce22778f28
0d9dc66979374d8d18e98e44ca3b80c7b41ded39
80960663b19297b440bfe6290a50b0e759387bb9
940d574b867862491320b924e93b243755816282
b10ef5aa61b749f994e1f08224b67d0638a2bce7
cc9a12bb563fb4615d92c421ab10c1c1068873ca
881d9ee429514e127af290cf078cdf4e61daca9c
6890faa814977fca7b2d06d92c7e70956f2fe99c
c4c533ddfcb014419cbd6293b94038eb5de1854034b6b9c1a1345c4d97cdfabf
9dd4902099e23c380596e7061482560866e103d2a899b84e0b6ff98c44c494e4
4648ce5e4ce4b7562a7828eb81f830d33ab0484392306bc9d3559a42439c8558
e73f48fe634a0c767bd596bbd068a13be7465993633fd61ccda717a474ee2db2
52f489d47618db8dfb503d6da98cbd76d08b063cc7ce0aac02b03601b6cae6a1
99a0b424bb3a6bbf60e972fd82c514fd971a948f9cedf3b9dc6b033117ecb106
570e4d52b259b460aa17e8e286be64d5bada804bd4757c2475c0e34a73aeb869
6a0c1f70af17bd9258886f997bb43266aa816ff24315050bbf5f0e473d059485
000185a17254cd8863208d3828366ec25ddd01596f18e57301355d4a33eac242
d46bb31dc93b89d67abffe144c56356167c9e57e3235bfb897eafc30626675bb
1990659a28b2c194293f106e98f5c5533fdad91e50fdeb1a9590d6b1d2983ada
0c2bf36dd9ccb3478c8d3dd7912bcfc1f5d910845446e1adfd1e769490287ab4
2b507d3ae01583c8abf4ca0486b918966643159a7c3ee7adb5f36c7bd2e4d70e
31376631aec4800de046e1400e948936010d9bbedec91c45ae8013c1b87564d0
33ee1961e302da3abc766480a58c0299b24c6ed8ceeb5803fa857617e37ca96e
4ce4dc04639d673f0627afc678819d1a7f4b654445ba518a151b2e80e910a92c
4d225af71d287f1264f3116075386ac2ce9ee9cd26fb8c3a938c2bf50cca8683
5123b066f4b864e83bb14060f473cf5155d863f386577586dd6d2826e20e3988

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

XWorm V6.0 – Advanced Plugin Arsenal and Stealth Enhancements

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
5314c7505002cda1e864eced654d132f773722fd621a04ffd84ae9bc0749b791
64cbbbf90fe84eda1a8c2f41a4d37b1d60610e7136a02472a72c28b6acadc2fc
760a3d23ee860cf2686a3d0ef266e7e1ad835cc8b8ce69bfe68765c247753c6b
8106b563e19c946bd76de7d00f7084f3fc3b435ed07eb4757c8da94c89570864
8514a434b50879e2b8c56cf3fd35f341e24feae5290fa530cc30fae984b0e16c
8d04215c281bd7be86f96fd1b24a418ba1c497f5dee3ae1978e4b454b32307a1
995869775b9d43adeb7e0eb34462164bcfbee3ecb4eda3c436110bd9b905e7ba
b314836a3ca831fcb068616510572ac32e137ad31ae4b3e506267b429f9129b1
df0096bd57d333ca140331f1c0d54c741a368593a4aac628423ab218b59bd0bb
f279a3fed5b96214d0e3924eedb85907f44d63c7603b074ea975d1ec2fdde0b4
2d9107edad9f674f6ca1707d56619a355227a661163f18b5794326d4f81a2803