KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Hackers Disguise PlugX Trojan as Legitimate Windows Debugger Tool

Tracker ID: TN2334 **Date:** March 07, 2023 **Category:** Malware **Industry:** All **Region**: All

Overview

In an attempt to get through security measures and gain control of a target system, the PlugX remote access trojan has been observed disguising itself as an open source Windows debugger tool named x64dbg.Researchers from Trend Micro Buddy Tancio, Jed Valderama, and Catherine Loveria wrote in a report published last week: "This file is a legitimate open-source debugger tool for Windows that is generally used to analyze kernel-mode and user-mode code, crash dumps, or CPU registers.

PlugX, also referred to as Korplug, is a post-exploitation modular implant that is renowned for its various functionalities, including data exfiltration and the capacity to use the compromised machine for nefarious purposes.Early samples of the malware date back to February 2008, despite being initially detected over a decade ago in 2012, according to a Trend Micro report at the time. PlugX has been used over time by cybercrime groups as well as threat actors with Chinese nexus.DLL side-loading is a key tactic used by the malware to load a malicious DLL from a digitally signed software application, in this case the x64dbg debugging tool (x32dbg.exe).It's important to note that DLL side-loading attacks make use of Windows' DLL search order mechanism to load and then launch a legitimate application that executes a rogue payload. The researchers said that while x32dbg.exe is a legitimate application, its valid digital signature may confuse some security tools, enabling threat actors to avoid detection, maintain persistence, increase their level of privileges, and bypass file execution restrictions.

Palo Alto Networks Unit 42, which disclosed a new variant of the malware that hides malicious files on detachable USB devices to propagate the infection to other Windows hosts, disclosed the hijacking of x64dbg to load PlugX last month. Persistence is achieved via making modifications to the Windows Registry and establishing scheduled processes to maintain access even after a system restart. In addition, x32dbg.exe was used to deploy a backdoor, a UDP shell client that gathers system information and waits for further instructions from a remote server, as per Trend Micro's analysis of the attack chain. "Despite advances in security technology, attackers continue to use [DLL side-loading] since it exploits a fundamental trust in legitimate applications," the researchers said. "This technique will remain viable for attackers to deliver malware and gain access to sensitive information as long as systems and applications continue to trust and load dynamic libraries."

The fact that DLL side loading is still used by threat actors today shows that it is an effective way to get around protective measures and gain control of a target system. This has been demonstrated by the discovery and analysis of the malware attack using the open-source debugger tool x32dbg.exe. Attackers still utilize this method despite advances in security technologies as it takes control of users' inherent trust in reliable programmes. As long as systems and applications continue to trust and load dynamic libraries, this technique will continue to be a viable way for attackers to deliver malware and access sensitive information.

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 josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Hackers Disguise PlugX Trojan as Legitimate Windows Debugger Tool

Tracker ID: TN2334 **Date:** March 07, 2023 **Category:** Malware **Industry:** All **Region**: All

MITRE ATT&CK Tactics

Resource Development, Initial Access, Execution, Persistence, Defense Evasion, Command and Control, Exfiltration.

Indicators of Compromise *

Please refer to the attached sheet for IOCs.

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Allow only known and trusted applications to run on the system while blocking any suspicious or unknown ones.
- Ensure that all DLLs are signed with a trusted digital signature to ensure their authenticity and integrity.
- Monitor and control the execution of applications and their dependencies, including DLLs, to detect and prevent malicious activities.
- Use endpoint protection solutions that offer behavioral analysis and predictive machine learning for better security capabilities
- Enable biometric security features such as fingerprint or facial recognition for unlocking the mobile device to avoid unauthorized access obtained using malicious activities such as keylogging and screen recording.
- Use complex passwords and enforce multi-factor authentication wherever possible.
- Follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.

References

- Buddy Tancio, Jed Valderama, Catherine Loveria, the PlugX Trojan Disguised as Legitimate Windows Debugger Tool, February 24, 2023, External Link (www.trendmicro.com).
- Ravie Lakshmanan, PlugX Trojan Disguised as Legitimate Windows Debugger Tool in Latest Attacks, February 27, 2023, External Link (thehackernews.com).
- Alexandre Cote Cyr, Mustang Panda's latest backdoor treads new ground with Qt and MQTT, March 2 ,2023 , External link (www.welivesecurity.com).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

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 josh

home.kpmg/in

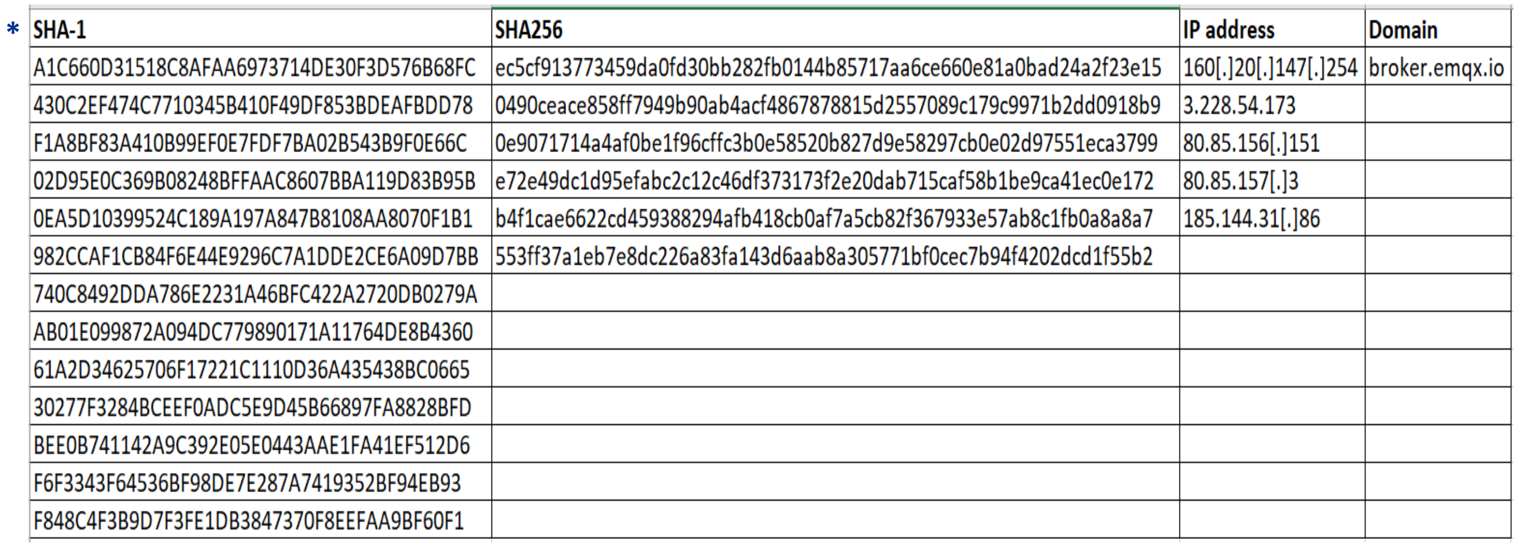
Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Hackers Disguise PlugX Trojan as Legitimate Windows Debugger Tool

Tracker ID: TN2334 **Date:** March 07, 2023 **Category:** Malware **Industry:** All **Region**: All



* SHA-1	SHA256	IP address	Domain
A1C660D31518C8AFAA6973714DE30F3D576B68FC	ec5cf913773459da0fd30bb282fb0144b85717aa6ce660e81a0bad24a2f23e15	160[.]20[.]147[.]254	broker.emqx.io
430C2EF474C7710345B410F49DF853BDEAFBDD78	0490ceace858ff7949b90ab4acf4867878815d2557089c179c9971b2dd0918b9	3.228.54.173	
F1A8BF83A410B99EF0E7FDF7BA02B543B9F0E66C	0e9071714a4af0be1f96cffc3b0e58520b827d9e58297cb0e02d97551eca3799	80.85.156[.]151	
02D95E0C369B08248BFFAAC8607BBA119D83B95B	e72e49dc1d95efabc2c12c46df373173f2e20dab715caf58b1be9ca41ec0e172	80.85.157[.]3	
0EA5D10399524C189A197A847B8108AA8070F1B1	b4f1cae6622cd459388294afb418cb0af7a5cb82f367933e57ab8c1fb0a8a8a7	185.144.31[.]86	
982CCAF1CB84F6E44E9296C7A1DDE2CE6A09D7BB	553ff37a1eb7e8dc226a83fa143d6aab8a305771bf0cec7b94f4202dcd1f55b2		
740C8492DDA786E2231A46BFC422A2720DB0279A			
AB01E099872A094DC779890171A11764DE8B4360			
61A2D34625706F17221C1110D36A435438BC0665			
30277F3284BCEEF0ADC5E9D45B66897FA8828BFD			
BEE0B741142A9C392E05E0443AAE1FA41EF512D6			
F6F3343F64536BF98DE7E287A7419352BF94EB93			
F848C4F3B9D7F3FE1DB3847370F8EEFAA9BF60F1			

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.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia