THREAT REPORT:

XWorm malware is growing in popularity

Services Performed By:
UltraViolet Cyber
Johnathon Moyer
(443) 351-7630
info@uvcyber.com

Published Date:
9/18/2023

Doc ID: ECORP_SUM_07032023_v1.1

Contents

1 Executive Summary

XWorm, ironically, behaves like a Remote Access Trojan (RAT) and includes multiple defensive measures against inspection by security researchers. Over the past year, the XWorm malware has grown in popularity and has seen multiple improvements to its code. Once the malware has established itself on a victim host, it beacons out to a command and control (C2) server and awaits further instructions.

2 Technical Analysis

On August 24th, 2023, security researchers from ANY.RUN published an article regarding their in-depth analysis of the newest sample related to malware named 'XWorm.' The file was publicly submitted as a password protected .RAR archive file. Upon successful extraction, the payload will install XClient.exe on the endpoint in the public user folder, schedule a task to restart the service with the highest permissions, then call out to a remote server. The server is presumed to be the C2 server used by the threat actor to issue commands to the compromised host.

Researchers were able to reverse engineer the sample to confirm the software's source code. The given sample was based on the .NET framework. After the software is installed, the malware used WMI API calls to the 'Win32_ComputerSystem' field to identify whether the host system was a virtualized environment. Next, the sample checked the IP assigned to the given host via the site "http[://]ip-api[.]com/line/?fields=hosting". If the IP returns a 'true' finding for the IP, it is assumed that the IP belongs to a datacenter and is not a 'real' workstation. If either of these checks show that the host is a sandbox, the application crashes to avoid further detection.

Current Suricata filters can successfully identify the file as XWorm as soon as it is extracted from the file archive. Security engines based on behavioral analysis are usually able to identify and quarantine the file successfully. As the malware family continues to grow in popularity, organizations can expect to see a variant of this file show up in a user's inbox sometime soon.

3 What UltraViolet Cyber is Doing

- UltraViolet Cyber regularly updates our IOC database to ensure alerting is up to date
- Monitoring commands that are associated with malicious activity from threat actors
- Monitoring network logs for traffic to known malicious sites

4 What Customers Can Do

- User training should include specific instructions to not open files from unknown senders
- Ensure your endpoint detection and remediation software is up to date on all endpoints
- Verify that you have logging enabled on your Windows endpoints, which includes logs related to scheduled task creation and modification

5 References

Inside the Code of a New XWorm Variant. Retrieved September 22, 2023, from
https://thehackernews.com/2023/09/inside-code-of-new-xworm-variant.html

Malware sample from ANY.RUN, Retrieved September 22, 2023, from
https://app.any.run/tasks/da323bce-48aa-40c3-bf7f-c98625c9aa7c/

XWorm: Technical Analysis of a New Malware Version. Retrieved September 22, 2023, from
https://any.run/cybersecurity-blog/xworm-technical-analysis-of-a-new-malware-version/