Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

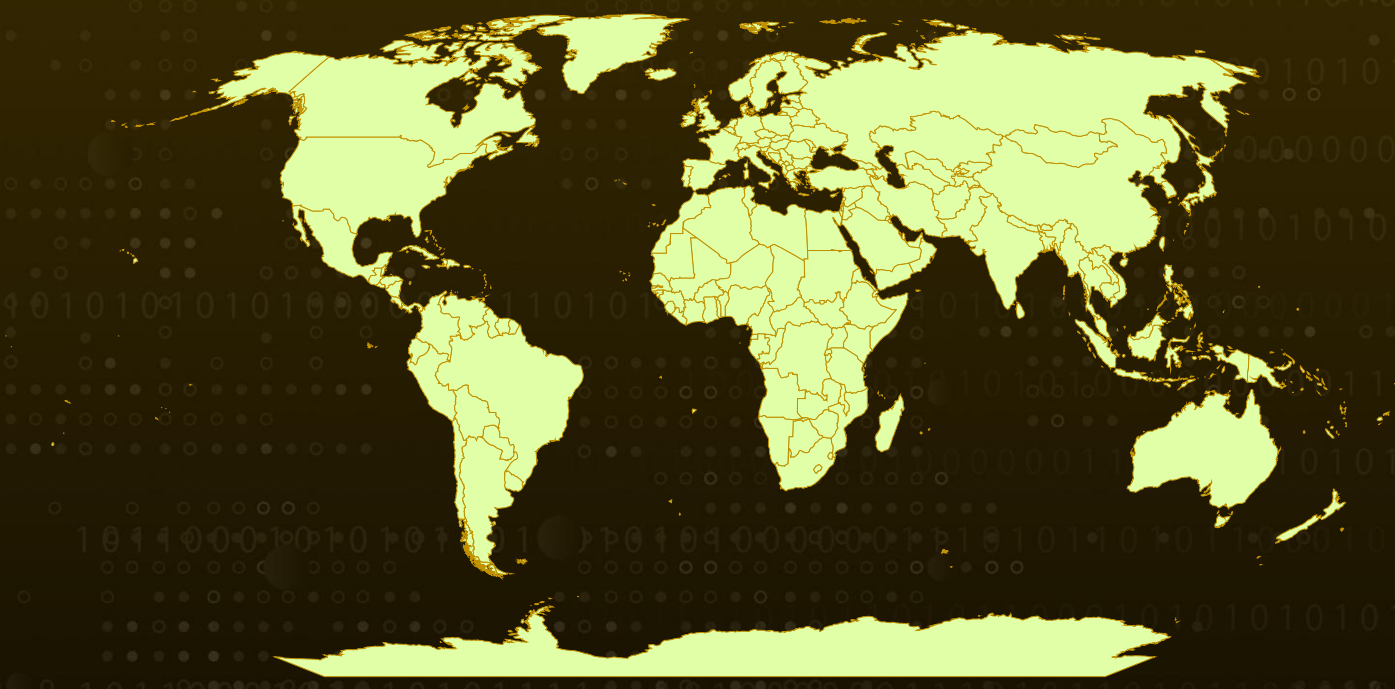
CoreWarrior Unleashed: A Stealthy Trojan Wreaking Havoc on Windows Systems

Date of Publication	Admiralty Code	TA Number
October 15, 2024	A1	TA2024394

Summary

Attack Discovered: October 2024
Targeted Countries: Worldwide
Affected Platform: Windows
Malware: CoreWarrior
Attack: A newly discovered malware, CoreWarrior, has emerged as a persistent trojan that aggressively spreads by creating multiple copies of itself across infected systems. It reaches out to numerous IP addresses and opens several network sockets to establish backdoor access. Additionally, CoreWarrior hooks into Windows UI elements to monitor user activities, enhancing its ability to evade detection and maintain control. This malware, targeting Windows machines, underscores the ongoing and serious threat that Windows-based environments face from sophisticated malware attacks.

Attack Regions



Attack Details

#1

A new malware named CoreWarrior has emerged as a highly persistent trojan, posing a serious threat to Windows environments. This malware spreads aggressively by creating multiple copies of itself while establishing backdoor connections to various IP addresses. It opens numerous network sockets to ensure continuous unauthorized access, making it challenging to detect and remove. Additionally, CoreWarrior hooks into Windows UI elements, allowing it to monitor and potentially manipulate user interactions stealthily. Its rapid replication and monitoring capabilities underscore its significance as a major security concern.

#2

CoreWarrior is delivered as a UPX-packed executable that has been manually altered, preventing it from being unpacked using standard UPX unpackers. Upon execution, it generates a copy of itself with a randomly chosen name, launches a command prompt, and uses curl to send POST requests to an external server. The parent process deletes the existing copy, creates a new one, and repeats this cycle generating over a 117 copies in under ten minutes during testing.

#3

CoreWarrior malware exhibits sophisticated techniques to maintain persistence and evade detection. It binds listeners on ports 49730-49777 and 50334-50679, creating multiple avenues for backdoor access. Additionally, it assigns a secondary IP address without generating noticeable TCP/UDP traffic, further concealing its activity. The malware actively monitors system drive changes and hooks into the command prompt window, allowing it to track modifications and respond accordingly. It includes several anti-analysis features, such as anti-debugging, VM environment detection, and evasion tactics. It can also use FTP, SMTP, and POP3 protocols for data exfiltration, further enhancing its potential for covert operations.

#4

CoreWarrior represents a sophisticated and persistent threat to Windows systems, characterized by its aggressive replication, stealthy backdoor connections, and robust monitoring capabilities. The malware's ability to evade standard analysis techniques, manipulate user interactions, and exfiltrate data using multiple protocols makes it a highly dangerous tool for cybercriminals. Immediate attention to detection and remediation strategies is crucial to prevent this trojan from causing significant damage to compromised environments. Strengthening monitoring and response mechanisms is vital for mitigating the risks posed by such advanced malware.

Recommendations

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Endpoint Protection and Monitoring: Deploy advanced endpoint detection and response (EDR) solutions that monitor system behavior for unusual activities, such as multiple processes being spawned rapidly or unauthorized network connections.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Regular Software Updates: Ensure all systems are consistently updated with the latest software patches to maintain security and enhance overall system protection. Regular updates help optimize performance, close security gaps, and ensure compatibility with newer technologies.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0005 Defense Evasion	TA0007 Discovery	TA0010 Exfiltration
T1027 Obfuscated Files or Information	T1027.002 Software Packing	T1070 Indicator Removal	T1053 Scheduled Task/Job
T1053.006 Systemd Timers	T1497 Virtualization/Sandbox Evasion	T1048 Exfiltration Over Alternative Protocol	T1082 System Information Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	85A6E921E4D5107D13C1EB8647B130A1D54BA2B6409118BE7945FD71C6C8235F, 8C97329CF7E48BB1464AC5132B6A02488B5F0358752B71E3135D9D0E4501B48D

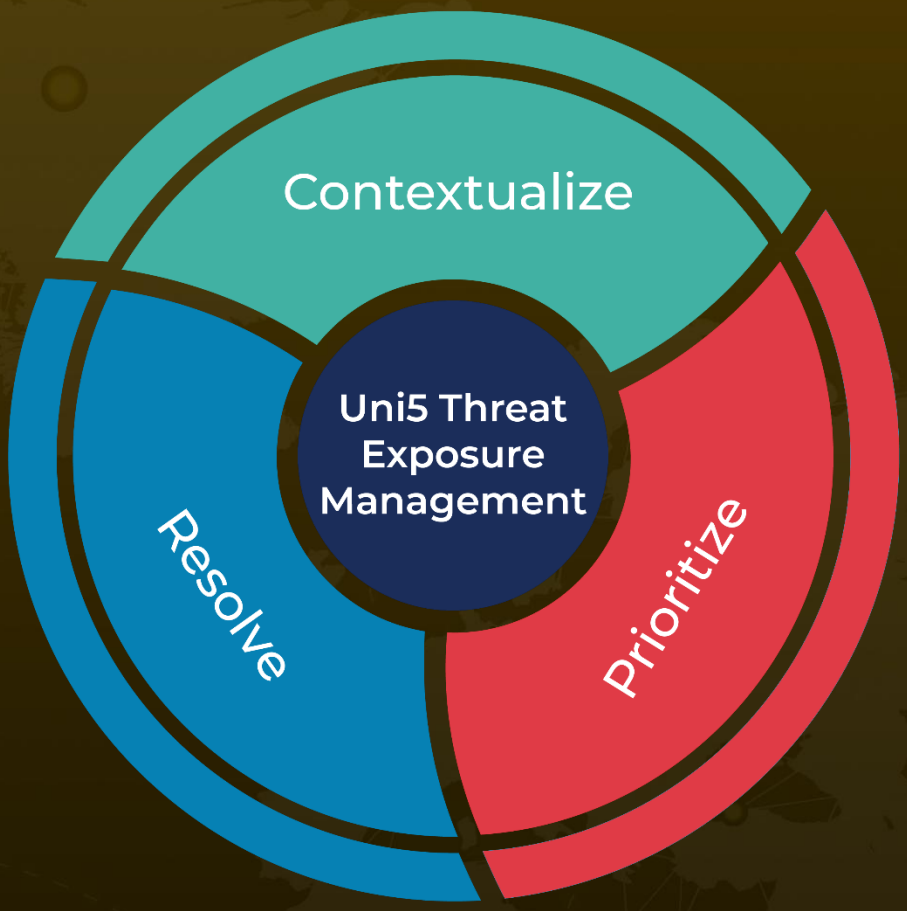
References

https://blog.sonicwall.com/en-us/2024/10/corewarrior-spreader-malware-surge/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 15, 2024 . 7:00 AM

More at www.hivepro.com