Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

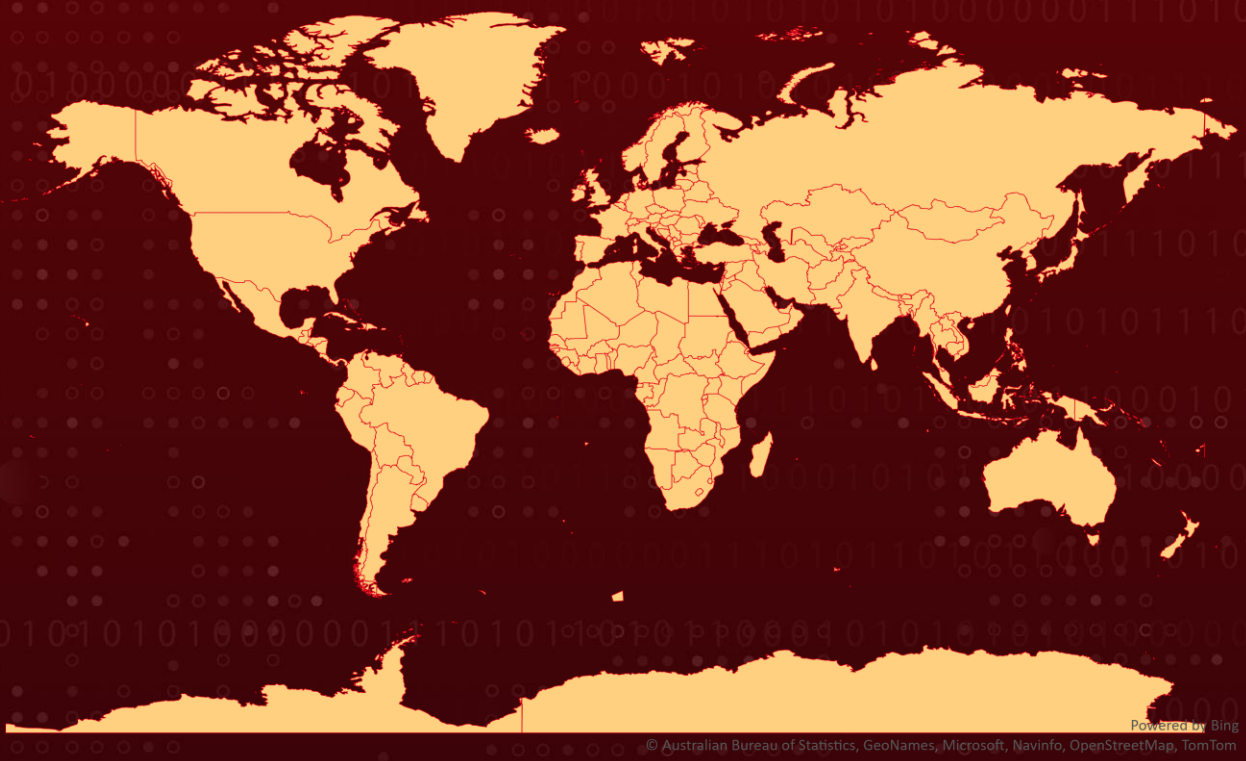
A New Emerging CatB Ransomware Using DLL Hijacking to Evade Detection

Date of Publication	Admiralty Code	TA Number
January 4, 2023	A1	TA2023004

Summary

First appeared: November 23, 2022
Attack Region: Worldwide
Attack: The CatB ransomware uses a DLL hijacking technique to evade detection by injecting itself into legitimate processes and using those processes to encrypt the victim's files.

Attack Regions



Attack Details

#1 CatB is a ransomware that uses a technique called DLL hijacking to evade detection. It does this by injecting itself into the Microsoft Distributed Transaction Coordinator (MSDTC) service, a legitimate Windows process, and using that process to encrypt the victim's files.

#2 This makes it more difficult for security scanners to detect the ransomware, as it is not running as a standalone process and may not exhibit the typical behavior of ransomware.

#3 CatB ransomware consists of two files: a dropper file called "version.dll," which is packed with UPX, and the actual ransomware payload called "oci.dll." The dropper file is responsible for verifying that the ransomware is not running in a virtual machine or sandbox, and then it drops and executes the payload file.

#4 CatB also uses several anti-virtual machine techniques to verify that it is running on a real machine before executing, and it will only encrypt specific hardcoded disks and folders, avoiding certain file types and the NTUSER.DAT file.

#5 The ransom note is added to the beginning of each encrypted file and the victim is asked to contact the ransomware group through a specified email address to pay the ransom and receive the decryption key.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0004 Privilege Escalation	TA0003 Persistence	TA0007 Discovery
TA0040 Impact	T1574 Hijack Execution Flow	T1036 Masquerading	T1027 Obfuscated Files or Information
T1497 Virtualization/Sandbox Evasion	T1082 System Information Discovery	T1518 Software Discovery	T1518.001 Security Software Discovery
T1574.001 DLL Search Order Hijacking	T1486 Data Encrypted for Impact		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	3661ff2a050ad47fdc451aed18b88444646bb3eb6387b07f4e47d0306aac6642 35a273df61f4506cdb286ecc40415efaa5797379b16d44c240e3ca44714f945b
Email ID	catB9991@protonmail[.]com

References

https://minerva-labs.com/blog/new-catb-ransomware-employs-2-year-old-dll-hijacking-technique-to-evade-detection/

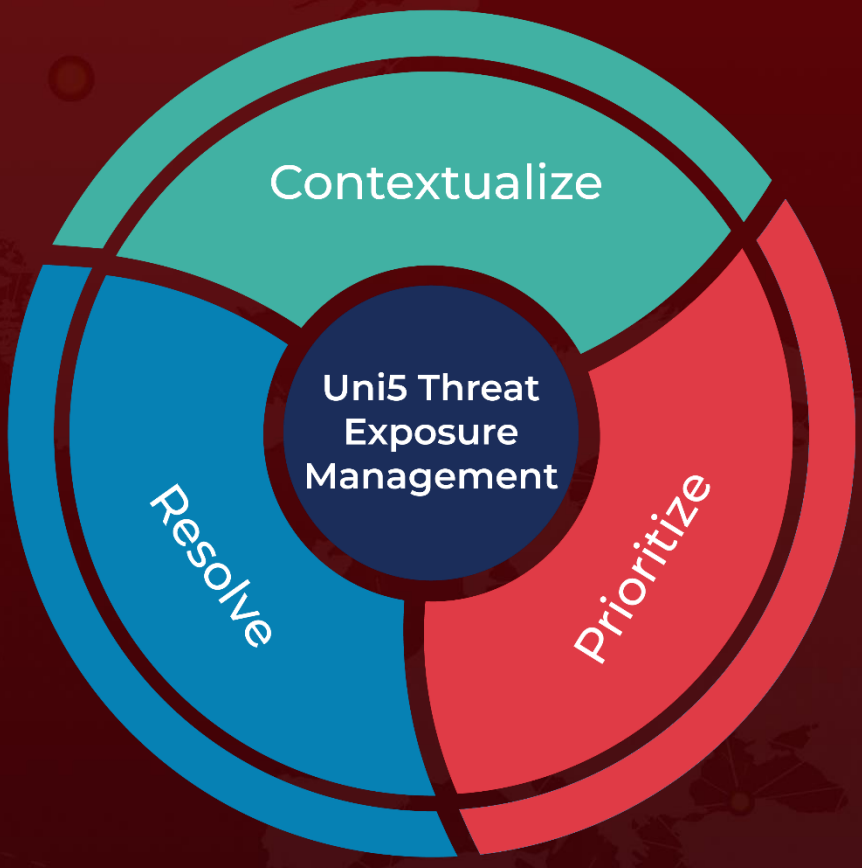
https://cyware.com/news/newly-found-catb-ransomware-uses-dll-hijacking-to-evade-detection-685dd2c8

https://attack.mitre.org/techniques/T1574/001/

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

January 4, 2023 • 5:40 AM

More at www.hivepro.com