Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

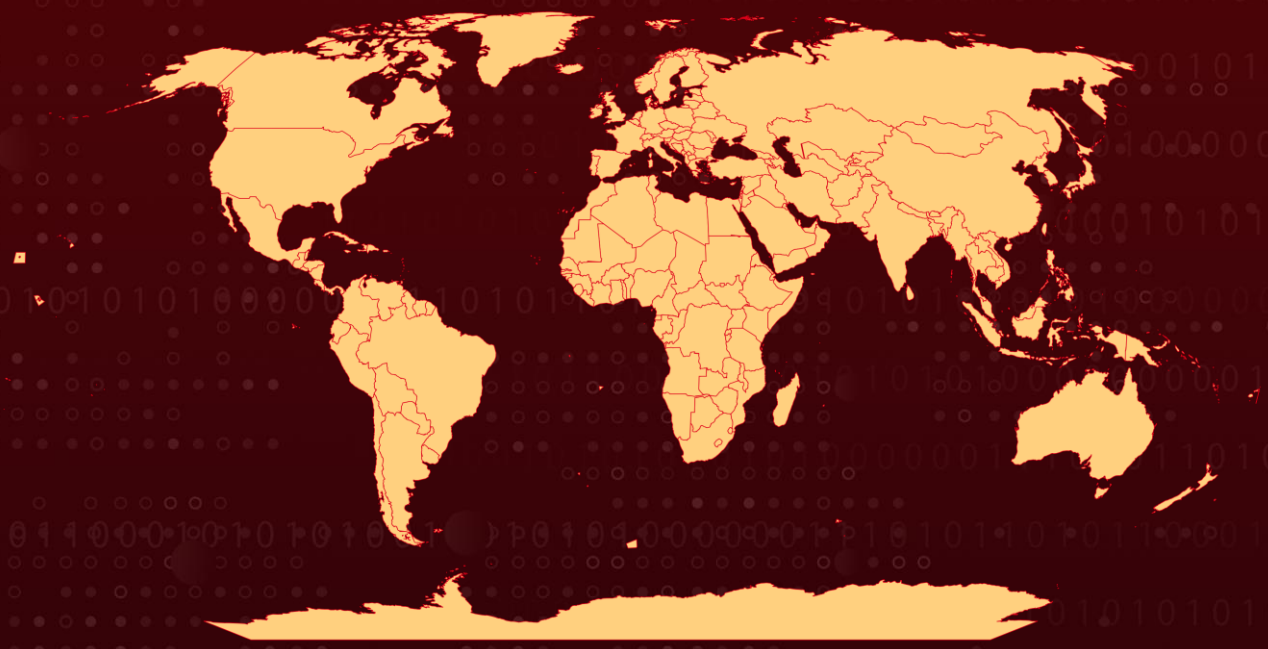
BlackCat Incorporates 'Munchkin' into Its Arsenal

Date of Publication	Admiralty Code	TA Number
October 20, 2023	A1	TA2023429

Summary

First Seen: November 2021
Attack Region: Worldwide
Ransomware: BlackCat (aka AlphaV, AlphaVM, ALPHV-ng, or Noberus)
Malware: Munchkin
Attack: The BlackCat ransomware group has introduced a new tool called 'Munchkin' in its operations. This tool employs virtual machines (VMs) to stealthily deploy encryptors on network devices. Munchkin allows the BlackCat group to run on remote systems and encrypt network file shares. Using VMs to deploy ransomware is a technique that enhances the stealth and reach of the attackers.

Attack Regions



Attack Details

#1 In November 2021, BlackCat, a highly skilled ransomware threat, drew attention due to its use of the Rust programming language and its Ransomware-as-a-Service (RaaS) business model. BlackCat is a major global threat since it started out targeting victims in the US and has now spread throughout the world, targeting victims in a variety of businesses and sectors.

#2 BlackCat is extremely customizable and can be tailored to create targeted executables, which makes it one of the most sophisticated RaaS operations to date. The BlackCat ransomware group has introduced a new tool called 'Munchkin' to its arsenal. This tool allows them to deploy BlackCat's latest variant Sphynx ransomware more stealthily over the network.

#3 Munchkin allows threat operators to run BlackCat on remote machines, as well as to deploy it for the purpose of encrypting remote SMB and CIFS network shares. Munchkin runs on customized version of Alpine Linux and delivered in the form of an ISO file.

#4 Upon gaining the initial access to a compromised device, the threat actors deploy VirtualBox and configure a new virtual machine using the Munchkin ISO. Munchkin VM contains a set of scripts and utilities that provide the threat actors with various capabilities, including password dumping, lateral movement within the network, building a tailored 'Sphynx' payload, and executing programs on network computers.

#5 When the Munchkin utility is booted, it initiates several actions to facilitate the deployment of Sphynx. These actions include changing the root password to one known only by the attackers. It then utilizes the 'tmux' utility to execute a Rust-based malware binary. Using this payload, custom Sphynx executables are generated in the /app/payloads/ directory. These executables are subsequently deployed over network and encrypts network file shares. The VM powers off once the malware is fully executed.

#6 The introduction of the 'Munchkin' tool by the BlackCat ransomware group allows them to execute their latest BlackCat variant, Sphynx, on a Linux-based operating system. As BlackCat uses virtual machines, it adds an extra layer of isolation from the underlying operating system, making it more difficult for security solutions to detect and analyze the malware and the use of Alpine OS ensures a small digital footprint, reducing the chances of detection. These features collectively enhance the efficiency and effectiveness of the BlackCat ransomware attacks.

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.

Least Privilege: Assign the minimum necessary permissions to users and VMs to reduce the attack surface. Ensure that users and VMs only have access to the resources they need.

Network Segmentation: Use network segmentation to isolate critical systems and data from less critical areas, helping to contain the spread of ransomware.

Conduct Regular Data Backups: Implement a robust data backup strategy that includes regular backups of critical data and systems, ad hoc and periodic backup restoration test. In the event of a ransomware attack, having up-to-date backups will allow organizations to restore their systems and data without paying the ransom. Ensure backups are adequately protected, employ 3-2-1-1 back up principle and Deploy specialized tools to ensure backup protection.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0040** Impact	**TA0005** Defense Evasion
TA0007 Discovery	**TA0011** Command and Control	**TA0008** Lateral Movement	**TA0010** Exfiltration
T1021 Remote Services	**T1027** Obfuscated Files or Information	**T1059** Command and Scripting Interpreter	**T1059.006** Python
T1082 System Information Discovery	**T1486** Data Encrypted for Impact	**T1105** Ingress Tool Transfer	**T1098** Account Manipulation
T1570 Lateral Tool Transfer			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1a4082c161eafde7e367e0ea2c98543c06dce667b547881455d1984037a90e7d, b4dd6e689b80cfcdd74b0995250d63d76ab789f1315af7fe326122540cddfad2, 41c0b2258c632ee122fb52bf2f644c7fb595a5beaec71527e2ebce7183644db2, 2e808fc1b2bd960909385575fa9227928ca25c8665d3ce5ad986b03679dace90, b4dd6e689b80cfcdd74b0995250d63d76ab789f1315af7fe326122540cddfad2

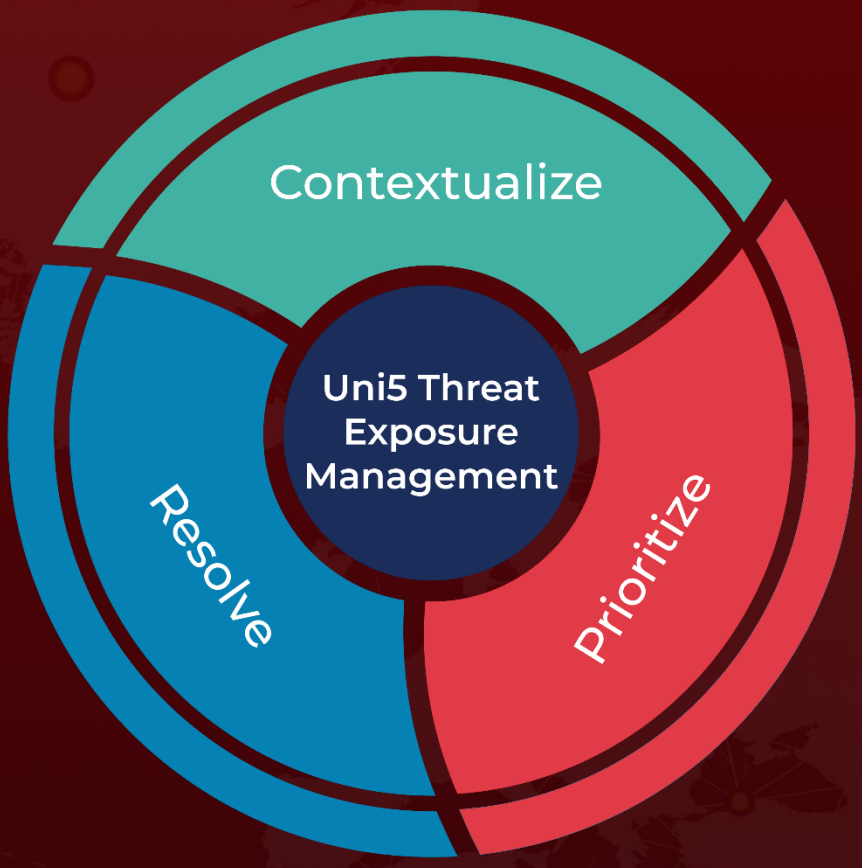
References

https://unit42.paloaltonetworks.com/blackcat-ransomware-releases-new-utility-munchkin/

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 20, 2023 . 6:05 AM

More at www.hivepro.com