BlackCat ransomware uses new 'Munchkin' Linux VM in stealthy attacks

The BlackCat/ALPHV ransomware operation has begun to use a new tool named 'Munchkin' that utilizes virtual machines to deploy encryptors on network devices stealthily.

Manchkin enables BlackCat to run on remote systems or encrypt remote Server Message Block (SMB) or Common Internet File (CIFS) network shares.

The introduction of Munchkin to BlackCat's already extensive and advanced arsenal makes the RaaS more attractive to cybercriminals seeking to become ransomware affiliates.

Hiding in VirtualBox

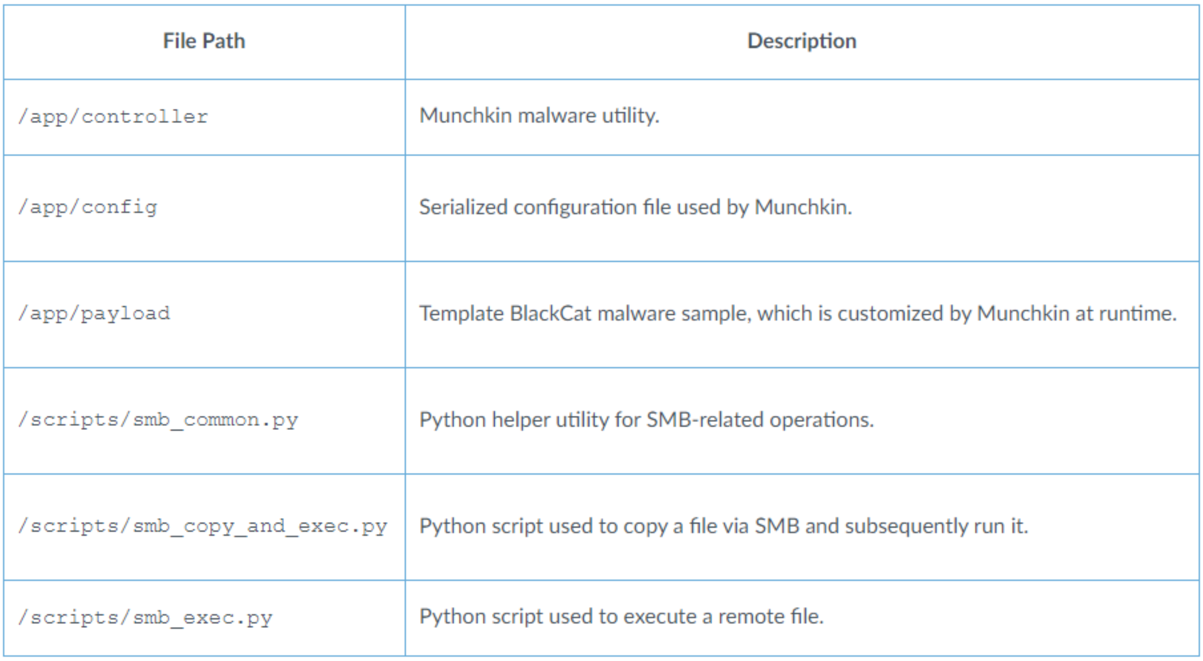
Palo Alto Networks Unit 42 has discovered that BlackCat's new Munchkin tool is a customized Alpine OS Linux distribution that comes as an ISO file.

After compromising a device, the threat actors install VirtualBox and create a new virtual machine using the Munchkin ISO.

This Munchkin virtual machine includes a suite of scripts and utilities that allow the threat actors to dump passwords, spread laterally on the network, build a BlackCat 'Sphynx' encryptor payload, and execute programs on network computers.

Upon boot, it changes the root password to one known only by the attackers and leverages the 'tmux' utility to execute a Rust-based malware binary named 'controller' that begins to load scripts used in the attack.

These scripts are listed below:



File Path	Description
/app/controller	Munchkin malware utility.
/app/config	Serialized configuration file used by Munchkin.
/app/payload	Template BlackCat malware sample, which is customized by Munchkin at runtime.
/scripts/smb_common.py	Python helper utility for SMB-related operations.
/scripts/smb_copy_and_exec.py	Python script used to copy a file via SMB and subsequently run it.
/scripts/smb_exec.py	Python script used to execute a remote file.

Structure of the image's filesystem

The 'controller' uses the bundled configuration file, which provides access tokens, victim credentials, and authentication secrets, as well as configuration directives, folder and file blocklists, tasks to run, and hosts to target for encryption.

This configuration is used to generate custom encBlackCatryptor executables in the /payloads/ directory, which are then pushed to remote devices to encrypt files or encrypt SMB and CIFS network shares.

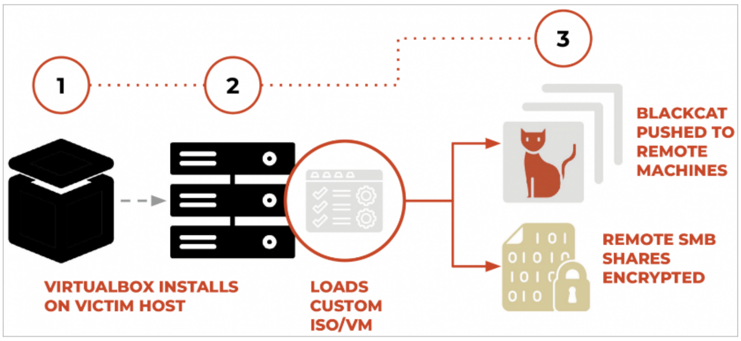

1
2
3
VIRTUALBOX INSTALLS ON VICTIM HOST
LOADS CUSTOM ISO/VM
BLACKCAT PUSHED TO REMOTE MACHINES
REMOTE SMB SHARES ENCRYPTED

FIG: Munchkin attack diagram

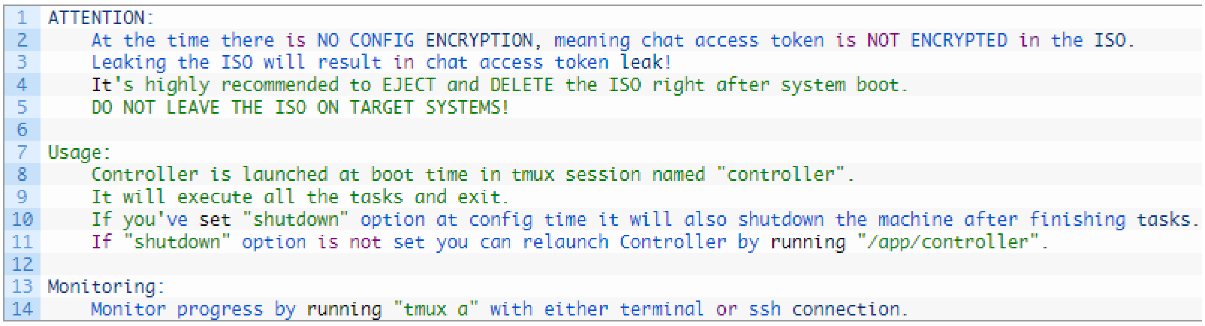
In this digram a message in the malware's code from BlackCat's authors to their partners, warning against leaving the ISO on target systems due to the lack of encryption for the configuration, especially highlighting the risk of chat access token leakage.

A common problem affecting ransomware victims and cybercriminals is that samples commonly get leaked through malware analysis sites. Analyzing the ransomware samples allows researchers to gain full access to the negotiation chat between a ransomware gang and its victim.

To prevent this, affiliates provide Tor negotiation site access tokens at run-time when launching. Therefore, it's impossible to gain access to a victim's negotiation chat, even if they have access to the sample used in the attack.

Due to this, the threat actors warn affiliates that they must delete the Munchkin virtual machines and ISOs to prevent these access tokens from leaking.

The developers also include instructions and tips on using 'Controller' to monitor the attack's progress and launch tasks.



```
ATTENTION:
    At the time there is NO CONFIG ENCRYPTION, meaning chat access token is NOT ENCRYPTED in the ISO.
    Leaking the ISO will result in chat access token leak!
    It's highly recommended to EJECT and DELETE the ISO right after system boot.
    DO NOT LEAVE THE ISO ON TARGET SYSTEMS!

Usage:
    Controller is launched at boot time in tmux session named "controller".
    It will execute all the tasks and exit.
    If you've set "shutdown" option at config time it will also shutdown the machine after finishing tasks.
    If "shutdown" option is not set you can relaunch Controller by running "/app/controller".

Monitoring:
    Monitor progress by running "tmux a" with either terminal or ssh connection.
```

Note contained in the malware

Munchkin makes it easier for BlackCat ransomware affiliates to perform various tasks, including bypassing security solutions protecting the victim's device. This is because virtual machines provide a layer of isolation from the operating system, making detection and analysis more challenging for security software.

Additionally, the choice of Alpine OS ensures a small digital footprint, and the tool's automated operations reduce the need for manual interventions and noise from command feeds.

Finally, the modularity of Munchkin, featuring a variety of Python scripts, unique configurations, and the ability to swap payloads as needed, makes the tool easy to adjust to specific targets or campaigns.

BlackCat still evolving

BlackCat emerged in late 2021 as a sophisticated Rust-based ransomware operation as the successor to BlackMatter and Darkside.

The RaaS has followed a successful trajectory thus far, regularly introducing advanced features like highly configurable intermittent encryption, data leak API, Impacket and Remcom embedding, encryptors with support for custom credentials, signed kernel drivers, and upgrades on the data exfiltration tool.

Notable BlackCat victims in 2023 include the Florida Circuit Court, MGM Resorts, Motel One, Seiko, Estee Lauder, HWL Ebsworth, Western Digital, and Constellation Software.

Author - Himangshu Sarkar
Github - https://github.com/Himangshu30
LinkedIN - https://www.linkedin.com/in/himangshu-sarkar-b4ba3a22a