BlackCat Climbs the Summit With a New Tactic

By Unit 42

Published: 2023-10-18 · Archived: 2026-04-05 16:41:02 UTC

Executive Summary

BlackCat operators recently announced new updates to their tooling, including a utility called Munchkin that allows attackers to propagate the BlackCat payload to remote machines and shares on a victim organization network. For the past two years, the BlackCat ransomware operators have continued to evolve and iterate their tooling as part of their ransomware-as-a-service (RaaS) business model.

As part of a recent investigation, Unit 42 researchers have acquired an instance of Munchkin that is unique, in that it is loaded in a customized Alpine virtual machine (VM). This new tactic of leveraging a customized VM to deploy malware has been gaining traction in recent months, allowing ransomware threat actors to use VMs to circumvent security solutions in deploying their malware payloads.

This publication details how this new utility works and sheds further light on the continued tactics used by BlackCat threat actors. In doing so, it is our sincere hope to motivate further effort by the information security industry to better defend against this evolving threat.

Palo Alto Networks customers receive protections against this specific threat through appropriate identification of the provided indicators as malicious.

Overview of BlackCat

The BlackCat ransomware threat was first made public when it surfaced in November 2021. This threat gained notoriety due to the sophistication employed within their malware, along with unique approaches such as the use of the Rust programming language.

BlackCat, similar to other ransomware threat actors, employs a RaaS business model. This model allows affiliates to leverage their tooling, in turn providing a portion of the profits to the operators. Based on historical reports, affiliates keep roughly 80-90% of the ransom payment, with the remainder being sent to the operators.

The BlackCat organization, including its affiliates, has historically focused on targeting victims in the United States. However, this focus has greatly broadened over time with increased popularity, and BlackCat has more recently been observed targeting victims worldwide across numerous industries and verticals.

The BlackCat tool set has continued to evolve over the years. Original versions provided an embedded JSON configuration with no obfuscation or encryption applied.

Over time, threat operators updated the malware family to obfuscate this underlying configuration. They also required a unique command-line parameter to execute the malware. In doing so, BlackCat prevented those within

the security community from gaining insight into the underlying payloads in the event this command-line parameter was unavailable.

The malware family has continued to evolve, with threat operators employing further capabilities and obfuscation mechanisms. In recent months, BlackCat has released a new tool named “Munchkin.”

This tooling provided a Linux-based operating system (OS) running Sphynx (the latest BlackCat variant). Threat operators can use this utility to run BlackCat on remote machines, or to deploy it to encrypt remote Server Message Block (SMB)/Common Internet File Shares (CIFS).

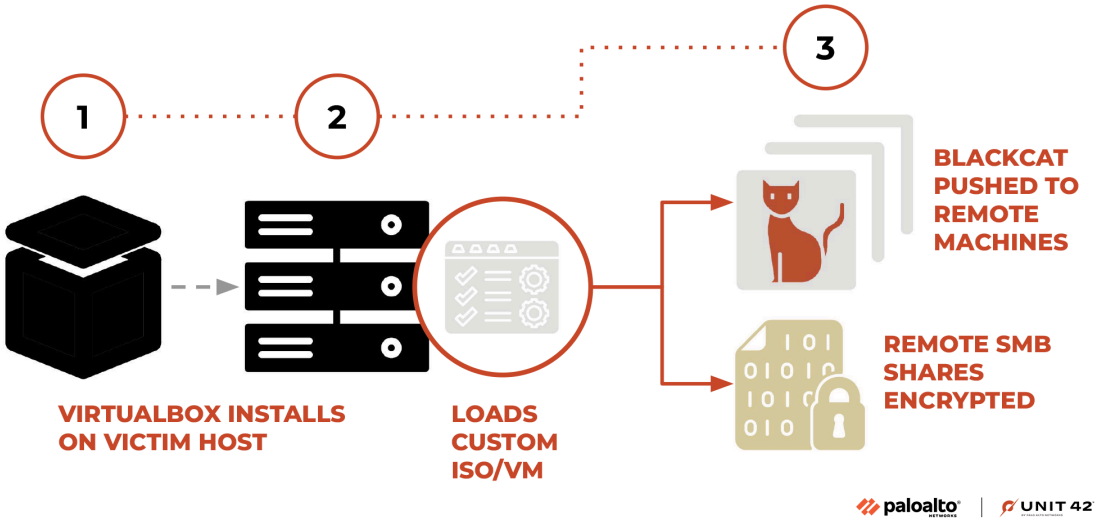

Figure 1. Diagram of Munchkin tool process.

The use of virtual machines to run malware is a growing trend within the ransomware community. Other ransomware organizations have been reported to leverage this new tactic as well.

The benefits of this approach include circumventing any security controls or protections set on the host OS, such as antivirus software. As these solutions often do not have the introspection within the embedded virtualized OS, malware will frequently bypass any checks that are present.

As part of a recent investigation, Unit 42 researchers were able to acquire a copy of this VM utility. As such, we can provide insights into how it works.

Climbing the Summit

The Munchkin utility is delivered as an ISO file, which is loaded in a newly installed instance of the VirtualBox virtualization product. This ISO file represents a customized implementation of the Alpine OS, which threat operators likely chose due to its small footprint. Upon running the operating system, the following commands are executed at boot:

```
echo -n "root:[password]" | chpasswd
```

```
tmux new-session -A -s controller \; send -t controller "/app/controller && poweroff" ENTER \; detach -s controller

eject
```

In doing so, the malware initially changes the root password of the VM to one chosen by the threat actors. It subsequently generates a new terminal session via the built-in tmux utility, which is used to execute the malware binary named controller. After the malware completes execution, it powers the VM off.

The controller malware is hosted within the /app directory, along with other related files. In addition, other related and notable files are included within the VM OS, as noted in Table 1 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.

Table 1. File path and description of the files included within the VM OS.

In addition to the files noted above, a large number of Python scripts are present within the /usr/bin directly, which the BlackCat operators can use in subsequent updates within the VM.

- DumpNTLMInfo.py
- Get-GPPPassword.py
- GetADUsers.py
- GetNPUsers.py
- GetUserSPNs.py
- addcomputer.py
- atexec.py
- changepasswd.py
- dcomexec.py
- dpapi.py
- esentutl.py
- exchanger.py
- findDelegation.py
- flask

- futurize
- getArch.py
- getPac.py
- getST.py
- getTGT.py
- goldenPac.py
- karmaSMB.py
- keylistattack.py
- kintercept.py
- ldapdomaindump
- ldd2bloodhound
- ldd2pretty
- lookupsid.py
- machine_role.py
- mimikatz.py
- mqtt_check.py
- mssqlclient.py
- mssqlinstance.py
- net.py
- netview.py
- nmapAnswerMachine.py
- normalizer
- ntfs-read.py
- ntlmrelayx.py
- pasteurize
- ping.py
- ping6.py
- pip
- pip3
- pip3.11
- psexec.py
- raiseChild.py
- rbcd.py
- rdp_check.py
- reg.py
- registry-read.py
- rpcdump.py
- rpcmap.py
- sambaPipe.py
- samrdump.py
- secretsdump.py
- services.py

- smbclient.py
- smbexec.py
- smbpasswd.py
- smbrelayx.py
- smbserver.py
- sniff.py
- sniffer.py
- split.py
- ticketConverter.py
- ticketer.py
- tstool.py
- wmiexec.py
- wmipersist.py
- wmiquery.py

Attackers can use many of the Python scripts above for lateral movement, password dumping and further execution of malware on the victim network.

The controller malware is written in the Rust programming language in a manner very similar to the BlackCat malware family. Upon execution, the controller will initially decrypt numerous strings using a unique single-byte XOR operation.

Figure 2. String decryption at runtime.

After the strings are decrypted, the threat will perform basic checks to ensure that the expected configuration and payload files reside within the /app directory. The threat will then deserialize and parse the /app/config file. In the event any of these files are not present or if they are unable to be parsed, the malware will exit with an error message.

The /app/config file contains a wealth of information including the following, which the controller malware sample subsequently uses:

- Access Token
- Task identifiers
- Victim credentials (including usernames, passwords and domains)
- BlackCat victim URLs
- Blocklisted file types and paths
- Hosts and shares to target for encryption

After the configuration is parsed, the controller creates and mounts the /payloads/ directory, which it uses to host subsequently created instances of BlackCat. The controller uses the previously noted /app/payload as a template for creating customized BlackCat samples. Within the template file, there are specific markers that the controller looks for and uses when it modifies this file.

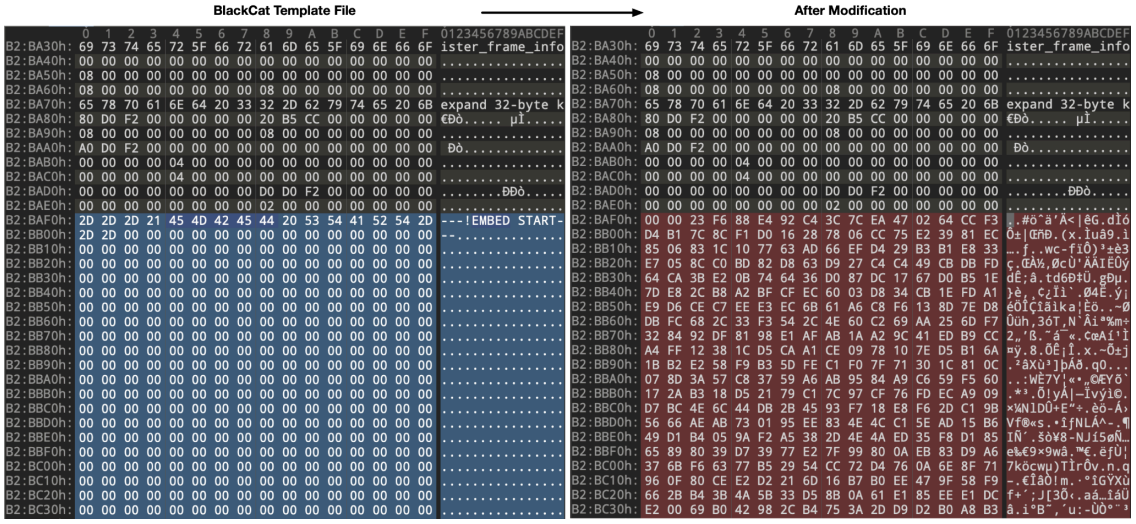

Figure 3. Creation of a new BlackCat sample based on template and configuration.

The created files are based on the provided configuration. However, they are named as follows, with incremental values:

- /payloads/0
- /payloads/1

After these payloads have been created, the malware proceeds to iterate through the provided configuration with the intent of infecting any SMB/CIFS drives that are specified. These attempts are outlined in various outputs written to STDOUT, an example of which is shown below.

(Note: The actual IP addresses and share names have been redacted in the output below.)

1	05:21:40 [INFO] Loading Config
2	05:21:40 [INFO] Initializing System
3	05:21:40 [INFO] Initializing Array
4	05:21:40 [INFO] Pass #1

5	05:21:40 [INFO] Executing tasks
6	05:21:40 [INFO] Task [ip_address]
7	05:21:40 [INFO] Encode Shares [ip_address] -> [share_path]
8	05:21:40 [INFO] Scanning [ip_address]
9	05:21:40 [INFO] Task [ip_address]
10	05:21:40 [INFO] Encode Shares [ip_address] -> [share_path]
11	05:21:40 [INFO] Scanning [ip_address]
12	05:21:40 [INFO] Task [ip_address]
13	05:21:40 [INFO] Encode Shares [ip_address] -> [share_path]
14	05:21:40 [INFO] Scanning [ip_address]
15	05:21:40 [INFO] Task [ip_address]
16	[TRUNCATED]
17	05:21:40 [INFO] Pass #2
18	05:21:40 [INFO] Executing tasks
19	05:21:40 [INFO] Task [ip_address]
20	05:21:40 [INFO] Encode Shares [ip_address] -> [share_path]
21	05:21:40 [INFO] Scanning [ip_address]
22	05:21:40 [INFO] Task [ip_address]
23	05:21:40 [INFO] Encode Shares [ip_address] -> [share_path]
24	05:21:40 [INFO] Scanning [ip_address]
25	05:21:40 [INFO] Task [ip_address]
26	05:21:40 [INFO] Encode Shares [ip_address] -> [share_path]
27	[TRUNCATED]
28	05:21:40 [INFO] Done!

After the malware executes fully, the VM powers off and performs no further actions.

We found the following message embedded within the malware sample itself. It is not used; it was presumably included at a certain stage of development but was later removed from use.

> 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.

This message appears to be a message from the BlackCat creators to their affiliates urging them to remove this file from a compromised environment. It would seem that the affiliate in question failed to heed this advice.

Conclusion

Malware authors, especially those behind the BlackCat ransomware threat, continue to iterate and evolve their techniques and tactics. This is fully apparent in their recent release of Munchkin, which they've developed and provided to their affiliates.

This tool follows a continued trend of leveraging VMs in an attempt to thwart security controls present on a host and to stay ahead of the security community in defending against these threats.

Palo Alto Networks customers receive protection from the threats discussed above through the following products:

- Next-Generation Firewalls with cloud-delivered security services including WildFire detect the files mentioned within this report as malicious.

If you think you might have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

/app/controller - Munchkin Binary

- 1a4082c161eafde7e367e0ea2c98543c06dce667b547881455d1984037a90e7d

/app/payload - BlackCat Stub

- b4dd6e689b80cfcdd74b0995250d63d76ab789f1315af7fe326122540cddfad2

/scripts/smb_common.py - Python SMB Classes

- 41c0b2258c632ee122fb52bf2f644c7fb595a5beaec71527e2ebce7183644db2

/scripts/smb_copy_and_exec.py - Python SMB Copy/Exec Script

- 2e808fc1b2bd960909385575fa9227928ca25c8665d3ce5ad986b03679dace90

/app/payload - BlackCat Stub

- b4dd6e689b80cfcdd74b0995250d63d76ab789f1315af7fe326122540cddfad2

YARA Rules

```
1  rule u42_crime_nix_munchkin
2  {
3      meta:
4          author = "Unit 42 Threat Intelligence"
5          date = "2023-10-12"
6          description = "Identifies a scanning utility leveraged by the BlackCat operators that is used to
7  propagate the malware payload to additional hosts via SMB."
           hash = "1a4082c161eafde7e367e0ea2c98543c06dce667b547881455d1984037a90e7d"
```

```
        reference = "https://unit42.paloaltonetworks.com/blackcat-ransomware/"
    strings:
        $str0 = "At the time there is NO CONFIG ENCRYPTION, meaning chat access token is NOT ENCRYPTED in the ISO." xor(1-255)
        $str1 = "Leaking the ISO will result in chat access token leak!" xor(1-255)
        $str2 = "It's highly recommended to EJECT and DELETE the ISO right after system boot." xor(1-255)
        $str3 = "DO NOT LEAVE THE ISO ON TARGET SYSTEMS!" xor(1-255)
        $str4 = "Controller is launched at boot time in tmux session named \"controller\"." xor(1-255)
        $str5 = "It will execute all the tasks and exit." xor(1-255)
        $str6 = "If you've set \"shutdown\" option at config time it will also shutdown the machine after finishing tasks." xor(1-255)
        $str7 = "If \"shutdown\" option is not set you can relaunch Controller by running \"/app/controller" xor(1-255)
        $str8 = "Monitor progress by running \"tmux a\" with either terminal or ssh connection" xor(1-255)
        $str9 = "controller::smb" xor(1-255)
        $str10 = ": Failed, either no credentials or no ADMIN$ share found" xor(1-255)
        $str11 = "bin/controller/src/program.rs" xor(1-255)
        $str12 = "/scripts/smb_exec.py" xor(1-255)
        $str13 = "No payload configs provided!" xor(1-255)
        $str14 = "Can't deserialize config" xor(1-255)
        $str15 = "controller::program" xor(1-255)
    condition:
        any of them
}
```

```
rule u42_crime_win_blackcat
{
```

```
    meta:
        author = "Unit 42 Threat Intelligence"
        date = "2023-10-12"
        description = "Identifies the BlackCat ransomware malware family, which is written in the Rust programming language."
        hash = "b4dd6e689b80cfcdd74b0995250d63d76ab789f1315af7fe326122540cddfad2"
        reference = "https://unit42.paloaltonetworks.com/blackcat-ransomware/"
    strings:
        $str0 = "paths_file" xor(1-255)
        $str1 = "override_credentials" xor(1-255)
        $str2 = "disable_recursion" xor(1-255)
        $str3 = "disable_network" xor(1-255)
        $str4 = "disable_elevate_to_system" xor(1-255)
        $str5 = "disable_self_propagation" xor(1-255)
        $str6 = "self_destruct" xor(1-255)
        $str7 = "The following required argument was not provided: Path to resource to be processed." xor(1-255)
        $str8 = "Resource is one of:" xor(1-255)
        $str9 = "Path to local or remote File" xor(1-255)
        $str10 = "Path to local or remote Directory" xor(1-255)
        $str11 = "Path to remote server, i.e. \"\\10.0.0.1\"" xor(1-255)
        $str12 = "If no paths provided:" xor(1-255)
        $str13 = "A full scan in all available resources will be performed." xor(1-255)
        $str14 = "(you can provide multiple, single or no paths, i.e.: \"-p /home -p /opt\")" xor(1-255)
        $str15 = "Override config credentials:\n\nFormat:\n\nusername:password\n\n" xor(1-255)
        $str16 = "If Resource is a directory and this option is defined, only direct children of that directory will be processed" xor(1-255)
```

```
        $str17 = "disable-recursion" xor(1-255)
        $str18 = "DISABLE_NETWORK" xor(1-255)
        $str19 = "Disable automatic network discovery" xor(1-255)
        $str20 = "disable-network" xor(1-255)
        $str21 = "DISABLE_ELEVATE_TO_SYSTEM" xor(1-255)
        $str22 = "Do not attempt to elevalte access token to system" xor(1-255)
        $str23 = "disable-elevate-to-system" xor(1-255)
        $str24 = "DISABLE_SELF_PROPAGATION" xor(1-255)
        $str25 = "Disable network self propagation" xor(1-255)
        $str26 = "Network propagation is disabled by default in case you provided <" xor(1-255)
        $str27 = "Attach to parent console instead of allocating new one" xor(1-255)
        $str28 = "If no command provided an interactive client will be launched, otherwise client will send provided command and exit." xor(1-255)
    condition:
        3 of them
}
```

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