Sentinel LABS

BlackCat (*aka* AlphaVM, AlphaV) is a newly established RaaS (Ransomware as a Service) with payloads written in Rust. While BlackCat is not the first ransomware

Sentinel LABS

First appearing in late November, BlackCat has reportedly been attacking targets in multiple countries, including Australia, India and the U.S, and demanding ransoms in the region of $400,000 to $3,000,000 in Bitcoin or Monero.

BlackCat Ransomware Overview

In order to attract affiliates, the authors behind BlackCat have been heavily marketing their services in well-known underground forums.

BlackCat operators maintain a victim blog as is standard these days. The blog hosts company names and any data leaked in the event that the victims do not agree to cooperate.

Current data indicates primary delivery of BlackCat is via 3rd party framework/toolset (e.g., Cobalt Strike) or via exposed (and vulnerable) applications. BlackCat currently supports both Windows and Linux operating systems.

BlackCat Configuration Options

Samples analyzed (to date) require an "access token" to be supplied as a parameter upon execution. This is similar to threats like Egregor, and is often used as an anti-analysis tactic. This 'feature' exists in both the Windows and Linux versions of BlackCat.

However, the BlackCat samples we analyzed could be launched with any string supplied as the access token. For example:

Sentinel LABS

The ransomware supports a visible command set, which can be obtained via the `-h` or `--help` parameters.

```
C:\Users\admin1\Desktop>worldwideStrata.exe --help

C:\Users\admin1\Desktop>

USAGE:
    [OPTIONS] [SUBCOMMAND]

OPTIONS:
        --access-token <ACCESS_TOKEN>              Access Token
        --child                                    Run as child process
        --drag-and-drop                            Invoked with drag and drop
        --drop-drag-and-drop-target                Drop drag and drop target batch file
    -h, --help                                     Print help information
        --log-file <LOG_FILE>                      Enable logging to specified file
        --no-net                                   Do not discover network shares on Windows
        --no-prop                                  Do not self propagate(worm) on Windows
        --no-prop-servers <NO_PROP_SERVERS>...     Do not propagate to defined servers
        --no-vm-kill                               Do not stop VMs on ESXi
        --no-vm-snapshot-kill                      Do not wipe VMs snapshots on ESXi
        --no-wall                                  Do not update desktop wallpaper on Windows
    -p, --paths <PATHS>...                         Only process files inside defined paths
        --propagated                               Run as propagated process
        --ui                                       Show user interface
    -v, --verbose                                  Log to console
```

BlackCat command line options

As seen above, the executable payloads support a variety of commands, many of which are VMware-centric.

```
--no-prop                               Do not self propagate(wor
--no-prop-servers <NO_PROP_SERVERS>     Do not propagate to defin
--no-vm-kill                            Do not stop VMs on ESXi
--no-vm-snapshot-kill                   Do not wipe VMs snapshots
--no-wall                               Do not update desktop wal
```

Sentinel LABS

```
:\Users\admin1\Desktop>worldwideStrata.exe --ui --access-token 12345 -v

:\Users\admin1\Desktop>18:37:13 [INFO] locker::core::stack: Starting Supervisor
8:37:13 [INFO] locker::core::stack: Starting Discoverer
8:37:13 [INFO] locker::core::stack: Starting File Unlockers
8:37:13 [INFO] locker::core::stack: Starting File Processing Pipeline
8:37:13 [INFO] locker::core::pipeline::chunk_workers_supervisor: spawned_workers=2
8:37:13 [INFO] locker::core::pipeline::file_worker_pool: spawned_file_dispatchers=2
8:37:13 [INFO] locker::core::pipeline::file_worker_pool: spawned_chunk_work_infastructure=2
8:37:13 [INFO] locker::core::stack: Detecting Other Instances
8:37:13 [INFO] locker::core::stack: Starting Cluster Service
8:37:13 [INFO] locker::core::stack: Connecting to Cluster
8:37:13 [INFO] locker::core::cluster: server=16992236885994352848
8:37:13 [INFO] locker::core::stack: This is a Master Process
8:37:13 [INFO] locker::core::stack: Starting Platform
8:37:13 [INFO] encrypt_app::windows: Bootstrap Routine
8:37:13 [INFO] locker::core::os::windows::privilege_escalation: win7_plus=true
8:37:13 [INFO] locker::core::os::windows::privilege_escalation: token_is_admin=false
8:37:13 [INFO] locker::core::os::windows::privilege_escalation: token_is_domain_admin=true
8:37:13 [INFO] locker::core::os::windows::privilege_escalation: masquerade_peb
8:37:13 [INFO] locker::core::os::windows::privilege_escalation: uac_bypass::shell_exec="worldwideStrata.exe",Some("\"--
i\" \"--access-token\" \"12345\" \"-v\""),Some("C:\\Users\\admin1\\Desktop")
8:37:14 [INFO] locker::core::os::windows::privilege_escalation: escalate=success
```

BlackCat ransomware run in verbose mode

BlackCat Execution and Encryption Behaviour

Immediately upon launch, the malware will attempt to validate the existence of the previously mentioned access-token, followed by querying for the system UUID (`wmic`).

Those pieces of data are concatenated together into what becomes the 'Access key' portion of their recovery URL displayed in the ransom note. In addition, on Windows devices, BlackCat attempts to delete VSS (Volume Shadow Copies) as well as enumerate any accessible drives to search for and encrypt eligible files.

Other configuration parameters are evaluated before proceeding to execute multiple privilege escalation methods, based on the OS identified by `wmic` earlier. These

Sentinel LABS

≡

It is at this point that BlackCat will attempt to terminate any processes or services listed within the configuration such as any processes which may inhibit the encryption process. There are also specific files and directories that are excluded from encryption. Much of this is configurable at the time of building the ransomware payloads.

The targeted processes and services are noted in the `kill_processes` and `kill_services` sections respectively. File and folder exclusions are handled in the `exclude directory_names` section.

To further illustrate, the following were extracted from sample `d65a131fb2bd6d80d69fe7415dc1d1fd89290394` / `74464797c5d2df81db2e06f86497b2127fda6766956f1b67b0dcea9570d8b683` :

Kill_Processes

backup	memtas	mepocs	msexchange
sql	svc$	veeam	vss

Kill_Services

agntsvc	dbeng50	dbsnmp	encsvc
excel	firefox	infopath	isqlplussvc

Sentinel LABS

onenote	oracle	outlook	powerpnt
sqbcoreservice	sql	steam	synctime
tbirdconfig	thebat	thunderbird	visio
winword	wordpad	xfssvccon	

Exclude_Directory_Names

$recycle.bin	$windows.~bt	$windows.~ws	386
adv	all users	ani	appdata
application data	autorun.inf	bat	bin
boot	boot.ini	bootfont.bin	bootsect.bak
cab	cmd	com	config.msi
cpl	cur	default	deskthemepack
diagcab	diagcfg	diagpkg	dll
drv	exclude_file_extensions:[themepack	exclude_file_names:[desktop.ini	exe
google	hlp	hta	icl
icns	ico	iconcache.db	ics

Sentinel LABS

mpa	msc	msi	msocache
msp	msstyles	msu]	nls
nomedia	ntldr	ntuser.dat	ntuser.dat.log]
ntuser.ini	ocx	pdb	perflogs
prf	program files	program files (x86)	programdata
ps1	public	rom	rtp
scr	shs	spl	sys
system volume information	theme	thumbs.db	tor browser
windows	windows.old]	wpx	

BlackCat also spawns a number of its own processes, with syntax (for Windows) as follows:

```
WMIC.exe (CLI interpreter)    csproduct get UUID
cmd.exe (CLI interpreter)     /c "reg add HKEY_LOCAL_MACHINE\SYSTEM\Cu

cmd.exe (CLI interpreter)     /c "wmic csproduct get UUID"
cmd.exe (fsutil.exe)          /c "fsutil behavior set SymlinkEvaluatio
fsutil.exe                    behavior set SymlinkEvaluation R2L:1
cmd.exe (fsutil.exe)          /c "fsutil behavior set SymlinkEvaluatio
```

```
fsutil.exe                    behavior set SymlinkEvaluation R2R:1
cmd.exe (vssadmin.exe)        /c "vssadmin.exe delete shadows /all
reg.exe (CLI interpreter)     add HKEY_LOCAL_MACHINE\SYSTEM\Current

cmd.exe (worldwideStrata.exe) /c "C:\Users\admin1\Desktop\worldwide
vssadmin.exe                  delete shadows /all /quietcmd.exe (AR
```

Some more recently-built copies have a few additions. For example, in sample

`c1187fe0eaddee995773d6c66bcb558536e9b62c` / `c3e5d4e62ae4eca2bfca22f8f3c8cbec1275`

`7f78107e91e85404611548e06e40` we see the addition of:

```
wmic.exe Shadowcopy Delete"
"iisreset.exe /stop"
bcdedit.exe /set {default} recoveryenabled No
```

Much like other fine details, all this can be adjusted or configured by the affiliates at the time of building the payloads.

BlackCat configurations are not necessarily tailored to the target operating system. In the Linux variants we have analyzed to date, there are Windows-specific process, service, and file references in the `kill_processes`, `kill_services`, and `exclude_directory_names`.

The following excerpt is from sample

`f8c08d00ff6e8c6adb1a93cd133b19302d0b651afd73ccb54e3b6ac6c60d99c6`.

```
dows.~bt","public","msocache","windows","default","all users","tor browser","programdata","boot","config.msi","google","perflogs","appdata","windows.old"],"exclude_f
ile_names":["desktop.ini","autorun.inf","ntldr","bootsect.bak","thumbs.db","boot.ini","ntuser.dat","iconcache.db","bootfont.bin","ntuser.ini","ntuser.dat.log"],"excl
ude_file_extensions":["themepack","nls","diagpkg","msi","lnk","exe","cab","scr","bat","drv","rtp","msp","prf","msc","ico","key","ocx","diagcab","diagcfg","pdb","wpx"
,"hlp","icns","rom","dll","msstyles","mod","ps1","ics","hta","bin","cmd","ani","386","lock","cur","idx","sys","com","deskthemepack","shs","ldf","theme","mpa","nomedi
a","spl","cpl","adv","icl","msu"],"exclude_file_path_wildcard":[],"enable_network_discovery":true,"enable_self_propagation":true,"enable_set_wallpaper":true,"enable_
esxi_vm_kill":true,"enable_esxi_vm_snapshot_kill":false,"strict_include_paths":[
```

Linux variant configuration

Specific encryption logic is not necessarily novel either and is somewhat configurable by the affiliate at the time of building the ransomware payloads. BlackCat supports both ChaCha20 and AES encryption schemes.

Extensions on encrypted files can vary across samples. Examples observed include `.dkrpx75` , `.kh1ftzx` and `.wpzlbji` .

BlackCat ransomware execution chain (Windows version)

Post-Infection, Payment and Portal

Infected clients will be greeted with a ransom note as well as a modified desktop image.

BlackCat's modified desktop image

Infected uses are instructed to connect to the attackers' payment portal via TOR.

BlackCat ransom note

Sentinel LABS

Victim's are threatened with data leakage if they refuse to pay and provided with a list of data types that have been stolen.

In theory, once victims connect to the attacker's portal, they are able to communicate and potentially acquire a decryption tool. Everything on the BlackCat portal is tied back to the specific target ID, which must be supplied correctly from the URL in the ransom note.

Conclusion

In its relatively short time on the radar, BlackCat has carved a notable place for itself amongst mid-tier ransomware actors. This group knows their craft and are cautious when selecting partners or affiliates. It is possible that some of the increased affiliation and activity around BlackCat is attributed to other actors migrating to BlackCat as larger platforms fizzle out (Ryuk, Conti, LockBit and REvil).

Actors utilizing BlackCat know their targets well and make every attempt to stealthily compromise enterprises. Prevention by way of powerful, modern, endpoint security controls are a must. The SentinelOne Singularity Platform is capable of detecting and preventing BlackCat infections on both Windows and Linux endpoints.

Indicators of Compromise

13828b390d5f58b002e808c2c4f02fdd920e236cc8015480fa33b6c1a9300e31

15b57c1b68cd6ce3c161042e0f3be9f32d78151fe95461eedc59a79fc222c7ed

1af1ca666e48afc933e2eda0ae1d6e88ebd23d27c54fd1d882161fd8c70b678e

28d7e6fe31dc00f82cb032ba29aad6429837ba5efb83c2ce4d31d565896e1169

2cf54942e8cf0ef6296deaa7975618dadff0c32535295d3f0d5f577552229ffc

38834b796ed025563774167716a477e9217d45e47def20facb027325f2a790d1

3d7cf20ca6476e14e0a026f9bdd8ff1f26995cdc5854c3adb41a6135ef11ba83

4e18f9293a6a72d5d42dad179b532407f45663098f959ea552ae43dbb9725cbf

59868f4b346bd401e067380cac69080709c86e06fae219bfb5bc17605a71ab3f

731adcf2d7fb61a8335e23dbee2436249e5d5753977ec465754c6b699e9bf161

74464797c5d2df81db2e06f86497b2127fda6766956f1b67b0dcea9570d8b683

7b2449bb8be1b37a9d580c2592a67a759a3116fe640041d0f36dc93ca3db4487

7e363b5f1ba373782261713fa99e8bbc35ddda97e48799c4eb28f17989da8d8e

bd337d4e83ab1c2cacb43e4569f977d188f1bb7c7a077026304bf186d49d4117

c3e5d4e62ae4eca2bfca22f8f3c8cbec12757f78107e91e85404611548e06e40

c8b3b67ea4d7625f8b37ba59eed5c9406b3ef04b7a19b97e5dd5dab1bd59f283

cefea76dfdbb48cfe1a3db2c8df34e898e29bec9b2c13e79ef40655c637833ae

f815f5d6c85bcbc1ec071dd39532a20f5ce910989552d980d1d4346f57b75f89

f8c08d00ff6e8c6adb1a93cd133b19302d0b651afd73ccb54e3b6ac6c60d99c6

SHA1

087497940a41d96e4e907b6dc92f75f4a38d861a

11203786b17bb3873d46acae32a898c8dac09850

2a53525eeb7b76b3d1bfe40ac349446f2add8784

5869820f261f76eafa1ba00af582a9225d005c89

5c6ca5581a04955d8e4d1fa452621fbc922ecb7b

655c2567650d2c109fab443de4b737294994f1fd

783b2b053ef034571ocd2487e5184f29116e367c

89060eff6db13e7455fee151205e972260e9522a

9146a448463935b47e29155da74c68d16e0d7031

94f025f3be089252692d58e54e3e926e09634e40

a186c08d3d10885ebb129b1a0d8ea0da056fc362

c1187fe0eaddee995773d6c66bcb558536e9b62c

ce5540c0d2c54489737f3fefdbf72c889ac533a9

d65a131fb2bd6d80d69fe7415dc1d1fd89290394

da1e4a09a59565c5d62887e0e9a9f6f04a18b5f4

e17dc8062742878b0b5ced2145311929f6f77abd

e22436386688b5abe6780a462fd07cd12c3f3321

f466b4d686d1fa9fed064507639b9306b0d80bbf

MITRE ATT&CK

T1027.002 – Obfuscated Files or Information: Software Packing

T1027 – Obfuscated Files or Information

T1007 – System Service Discovery

T1059 – Command and Scripting Interpreter

TA0010 – Exfiltration

T1082 – System Information Discovery

T1490 – Inhibit System Recovery

Sentinel LABS

T1486 – Data Encrypted For Impact

T1140 – Encode/Decode Files or Information

T1202 – Indirect Command Execution

T1543.003 – Create or Modify System Process: Windows Service

T1550.002 – Use Alternate Authentication Material: Pass the Hash

RAAS   RANSOMWARE

SHARE

X   f   in   reddit   ✉   PDF

Sentinel LABS

trends, actors, and tactics within the thriving ecosystem of cybercrime and crimeware. He specializes in the discovery and analysis of emerging cybercrime "services" and evolving communication channels leveraged by mid-level criminal organizations. Jim joined SentinelOne following ~4 years at a security start-up, also focused on malware research and organized crime. Previously, he spent over 17 years at McAfee/Intel running their Threat Intelligence and Advanced Threat Research teams.

🏠

PREV

Wading Through Muddy Waters | Recent Activity of an Iranian State-Sponsored Threat Actor

NEXT

Hacktivism and State-Sponsored Knock-Offs | Attributing Deceptive Hack-and-Leak Operations

RELATED POSTS

Sentinel LABS

Xeon Sender | SMS Spam Shipping Multi-Tool Targeting SaaS Credentials

📅 AUGUST 19 2024

NullBulge | Threat Actor Masquerades as Hacktivist Group Rebelling Against AI
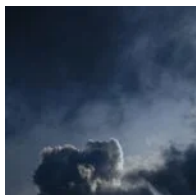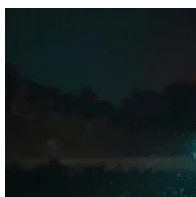
📅 JULY 16 2024

Search ...

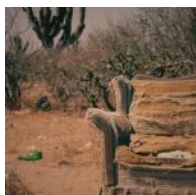SIGN UP

Sentinel LABS

RECENT POSTS

Cloud Malware | A Threat Hunter's Guide to Analysis, Techniques and Delivery

📅 OCTOBER 24, 2024

China's Influence Ops | Twisting Tales of Volt Typhoon at Home and Abroad

📅 OCTOBER 16, 2024

Kryptina RaaS | From Unsellable Cast-Off to Enterprise Ransomware

📅 SEPTEMBER 23, 2024

LABS CATEGORIES

Crimeware

Security Research

Advanced Persistent Threat

Adversary

LABScon

Security & Intelligence

Sentinel LABS

≡

SENTINELLABS

In the era of interconnectivity, when markets, geographies, and jurisdictions merge in the melting pot of the digital domain, the perils of the threat ecosystem become unparalleled. Crimeware families achieve an unparalleled level of technical sophistication, APT groups are competing in fully-fledged cyber warfare, while once decentralized and scattered threat actors are forming adamant alliances of operating as elite corporate espionage teams.

RECENT POSTS
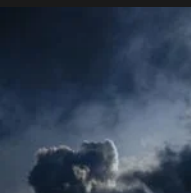
Cloud Malware | A Threat Hunter's Guide to Analysis, Techniques and Delivery

📅 OCTOBER 24, 2024

China's Influence Ops | Twisting Tales of Volt Typhoon at Home and Abroad

📅 OCTOBER 16, 2024

Kryptina RaaS | From Unsellable Cast-Off to Enterprise Ransomware

📅 SEPTEMBER 23, 2024

Sentinel LABS

Get notified when we post new content.

Twitter   LinkedIn