

blackCatConf

github.com/f0wl/blackCatConf

f0wl

f0wl/blackCatConf

Configuration Extractor for BlackCat Ransomware



1

Contributor

0

Issues

18

Stars

2

Forks



go report A+

blackCatConf is a static configuration extractor implemented in Golang for BlackCat Ransomware (targeting Microsoft Windows and GNU/Linux + VMware ESXi). By default the script will print the extracted information to stdout. It is also capable of dumping the malware configuration to disk as a JSON file with the `-j` flag.

Info: This tool does currently not support the new version of BlackCat/ALPHV ransomware.

Usage

```
go run blackcatconf.go [-j] path/to/blackcat_sample.bin
```

Screenshots

Sensitive victim information in the screenshot below and the example config file has been redacted.

```

Static Configuration Extractor for BlackCat Ransomware
Marius 'f0wL' Genheimer | https://dissectingmalwa.re

[bug]

File size (bytes): 3068928
Sample MD5: 173c4085c23080d9fb19280cc507d28d
Sample SHA-256: 731adcf2d7fb61a8335e23dbe2436249e5d5753977ec465754c6b699e9bf161

✓ Wrote 3995 bytes to blackCat_config-173c4085c23080d9fb19280cc507d28d.json

Config ID:
Public Key: MITBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApw3tWdMaWJvNf2MeJy5H0Y6kuj+1stNpwFyismGDEYhwKPPs9c68x1+84o6uLKfqpZnVnLnSx1Va6DitcJGeKJEQkz
File Extension:
Ransomnote Filename: RECOVER-$(EXTENSION)-FILES.txt
Default File Encryption Mode: Auto
Default File Encryption Cipher: Best
Compromised Credentials:
Services to be killed: [mepocs memtas veeam svc$ backup sql vss msexchange sql*]
Processes to be killed: [encsvc thebat mydesktopqos xfssvccon firefox infopath winword steam synctime notepad ocomm onenote mspub thunderbird agntsvc sql exc
Directories to be excluded: [system volume information intel $windows.~ws application data $recycle.bin mozilla program files (x86) program files $windows.~bt pu
Files to be excluded: [desktop.ini autorun.inf ntlldr bootsect.bak thumbs.db boot.ini ntuser.dat iconcache.db bootfont.bin ntuser.ini ntuser.dat.log]
Extensions to be excluded: [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
File Path Wildcards: []
Network Discovery: true
Self-Propagation: true
Set Wallpaper: true
ESXI VM Kill: true
ESXI Snapshot Kill: true
Strict Include Paths: []
ESXI VM Kill Exclude: []

Short Ransomnote:
Important files on your system was ENCRYPTED.
Sensitive data on your system was DOWNLOADED.
To recover your files and prevent publishing of sensitive information follow instructions in "${NOTE_FILE_NAME}" file.

Full Ransomnote:
>> Introduction
Important files on your system was ENCRYPTED and now they have have "${EXTENSION}" extension.
In order to recover your files you need to follow instructions below.

```

Configuration structure

With these novel BlackCat Ransomware samples this config extractor could easily be replaced by a bash one-liner (e.g. `strings ... | grep "{\"config_id\" > config.json`), but I expect that there will be config obfuscation/encryption added in future samples of BlackCat, similar to e.g. the changes made in Darkside Ransomware over time. If this is the case here as well having a structure to unmarshal the json config into will save me some time down the road.

Speaking of Darkside/BlackMatter: The configuration structure and values of BlackCat share significant similarities with those found in BlackMatter. The Korean Threat Intelligence company S2W Lab published [a thorough analysis of the similarities between these two Ransomware strains.](#)

Key	Value / Purpose	Type
config_id	Configuration ID, empty up until now (= Victim Identifier?)	unknown
public_key	RSA Public Key (Base64 encoded)	string
extension	Extension for encrypted files	string
note_file_name	Filename of the Ransomnote	string

Key	Value / Purpose	Type
note_full_text	Long version of the Ransomnote	string
note_short_text	Short version of the Ransomnote	string
default_file_mode	File Encryption Mode (observed: "auto" and "Smartpattern")	string or []int
default_file_cipher	File Encryption Cipher (observed: "Best")	string
credentials	Array of compromised credentials for escalation and propagation	[][]string
kill_services	List of services to be terminated	[]string
kill_processes	List of processes to be terminated	[]string
exclude_directory_names	Directories that are excluded from the encryption process	[]string
exclude_file_names	Files that are excluded from the encryption process	[]string
exclude_file_extensions	File extensions that are excluded from the encryption process	[]string
exclude_file_path_wildcard	Filepaths to be excluded via wildcard	[]string (?)
enable_network_discovery	Switch to enable/disable network discovery	bool
enable_self_propagation	Switch to enable/disable self propagation	bool
enable_set_wallpaper	Switch to enable/disable wallpaper change	bool
enable_esxi_vm_kill	Switch to enable/disable VM termination on ESXi Hosts	bool
enable_esxi_vm_snapshot_kill	Switch to enable/disable Snapshot deletion on ESXi Hosts	bool
strict_include_paths	Hardcoded filepaths (likely victim-specific)	[]string (?)
esxi_vm_kill_exclude	Exclusion list for virtual machines on ESXi Hosts	[]string (?)

Testing

This configuration extractor has been tested successfully with the following samples:

SHA-256	OS	Sample
59868f4b346bd401e067380cac69080709c86e06fae219bfb5bc17605a71ab3f	Windows	Malware Bazaar
731adcf2d7fb61a8335e23dbee2436249e5d5753977ec465754c6b699e9bf161	Windows	Malware Bazaar
5121f08cf8614a65d7a86c2f462c0694c132e2877a7f54ab7fcefd7ee5235a42	Linux	VX-Underground

SHA-256**OS****Sample**

f8c08d00ff6e8c6adb1a93cd133b19302d0b651afd73ccb54e3b6ac6c60d99c6

Linux

VX-
Underground

If you encounter an error with blackCatConf, please file a bug report via an issue. Contributions are always welcome :)