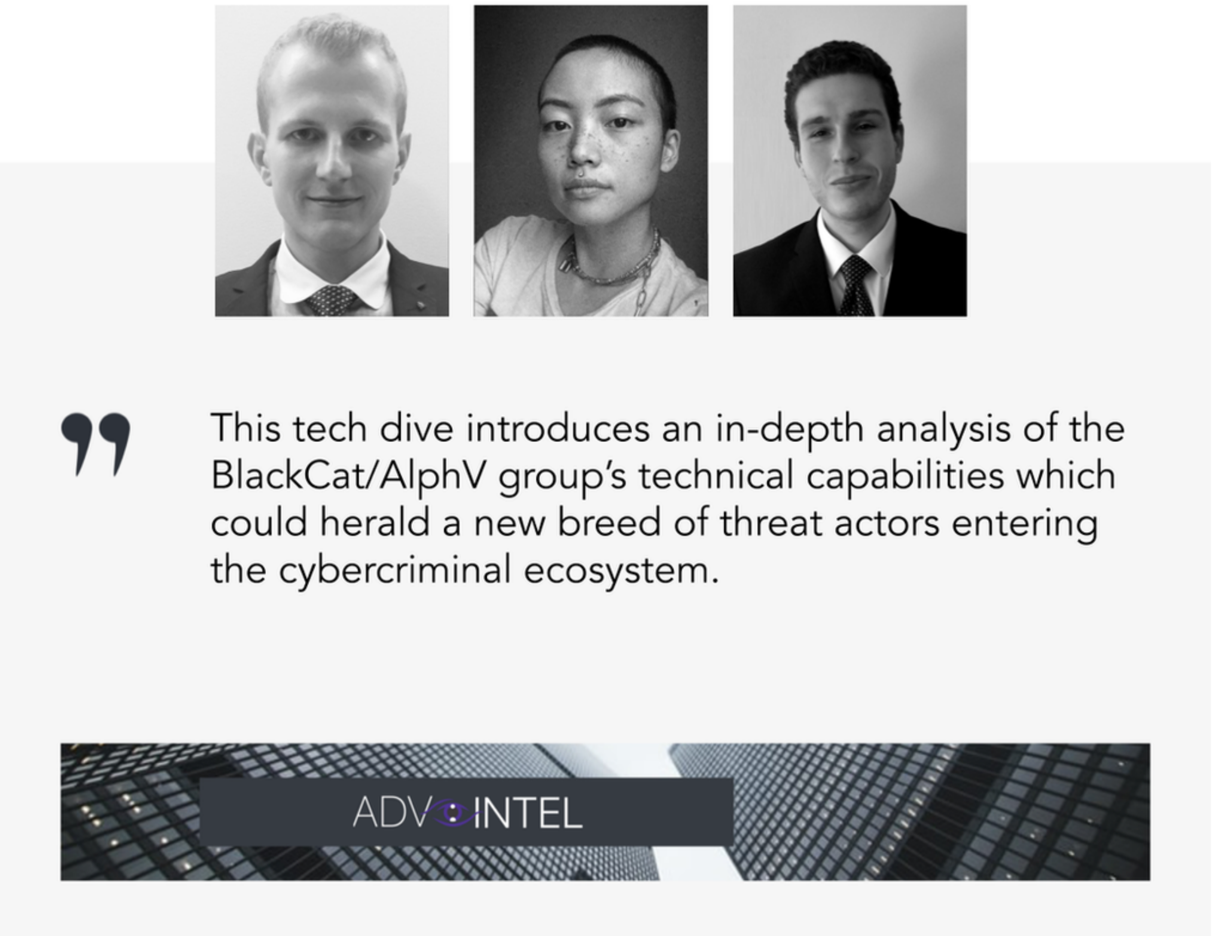
BlackCat — In a Shifting Threat Landscape, It Helps to Land on Your Feet: Tech Dive

By Vitali Kremez, Marley Smith & Yelisey Bogusalvskiy



This tech dive introduces an in-depth analysis of the BlackCat/AlphV group's technical capabilities which could herald a new breed of threat actors entering the cybercriminal ecosystem.

This report is part one of AdvIntel's new series on the *ALPHV (aka BlackCat) ransomware group. In the upcoming part two, AdvIntel will hold an analytical lens* on *BlackCat's organizational, recruitment, and operations process. This part introduces the context and offers a deep dive into the group's technical capabilities which could herald a new breed of threat actors entering the cybercriminal ecosystem.*

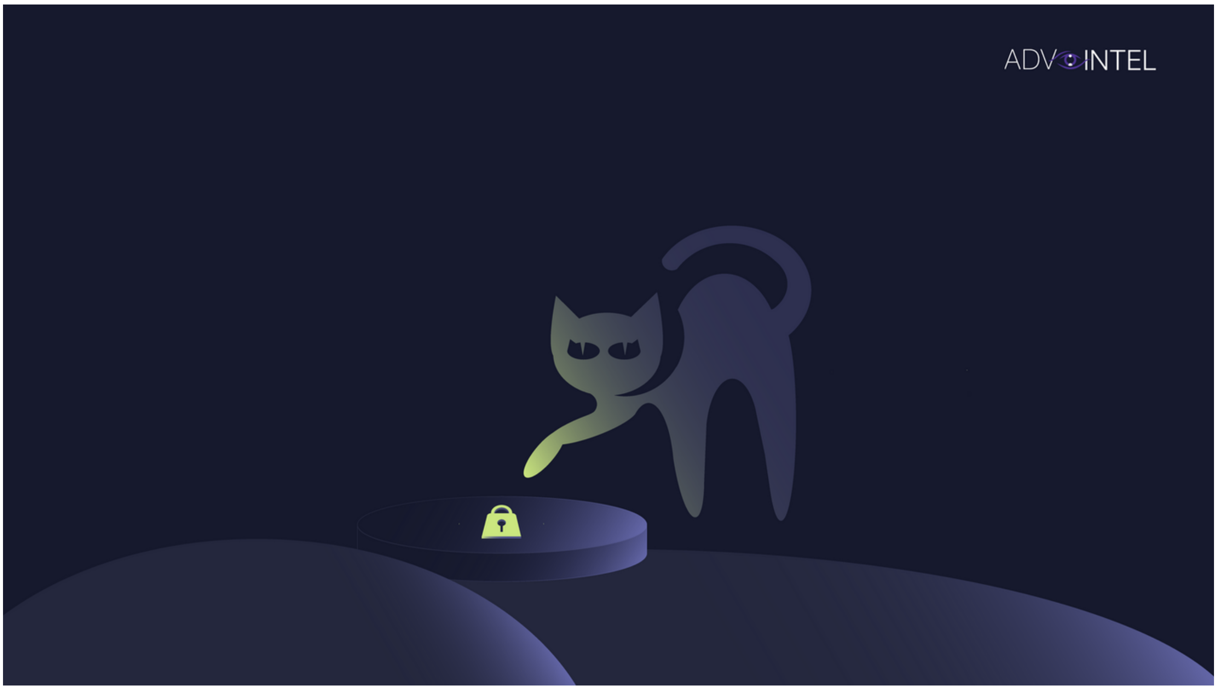
The intelligence analysis for this case originates in AdvIntel's direct adversarial visibility into the BlackCat group and is based on primary source intelligence and not tertiary evidence.

ALPHV: An Introduction

ALPHV (more commonly known as *BlackCat*), is a ransomware group known forits highly-customizable feature set and Rust-written malware locker, allowing forattacks on a wide range of corporate environments and the successful executionof a number of high-profile attacks, including the Italian luxury brand *Moncler*and the aviation company Swissport.

*BlackCat's ransomware includes many advanced technical features which set itapart from most ransomware operations—*these include the malware beingentirely *command-line driven, human-operated* and *adaptable,* as well as itsability to use different *encryption routines, spread between devices,* and *killhypervisors*, even wiping their snapshots to prevent recovery.

In short, BlackCat's unique strength seems to be in its *adaptability*, orwillingness to change to fit its own current needs. So what enablesBlackCat to set themselves apart from the rest?

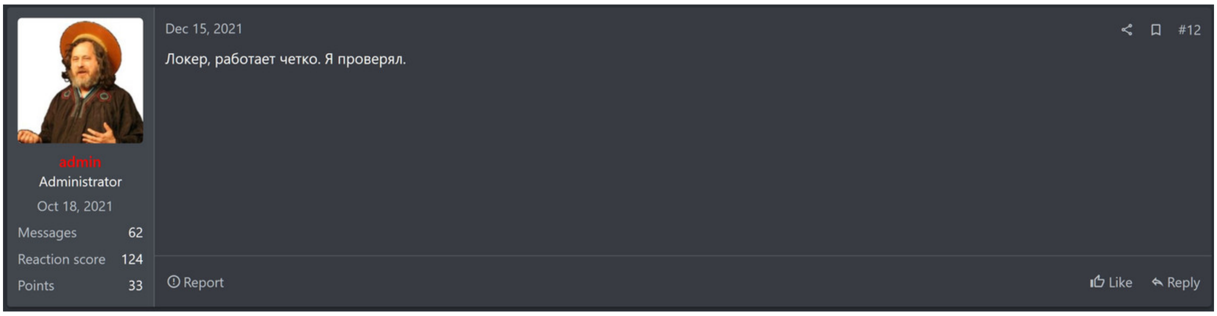


Starting from Square One

It has long been speculated that unlike other groups of its kind, BlackCat notonly uses an uncommon **Rust-based malware** (as opposed to the morecommonly used **C-based** variants), but also tend to avoid utilizing any of thesame tools common in ransomware operations (such as *Cobalt Strike,exploitations of Atera, Metasploit, etc*).

This is a direct address to possibly the most pressing issue facing today'sransomware community—a **fatigue of attack methodologies** that has already contributed to the dissolution of established threat groups.

For years, only a few tools were being weaponized by cybercriminals to performnetwork penetration, with **Cobalt Strike** being the most common. This createdan entire generation of criminal pentesters who were working for ransomwaregroups and trapped within their own narrow toolboxes. This in turn allowedcyber-defense groups to focus on Cobalt Strike IOCs as a surefire warning sign,increasing the criminals' chance of being spotted and ultimately lowering theirattack persistences. Moreover, Cobalt Strike is a *legitimate pentesting tool, notoriginally conceived as a malware*, which makes the efficiency of cyber defensesaddressing CS-weaponized attacks even more effective—because the softwareis, in a sense, *designed to be beaten.*

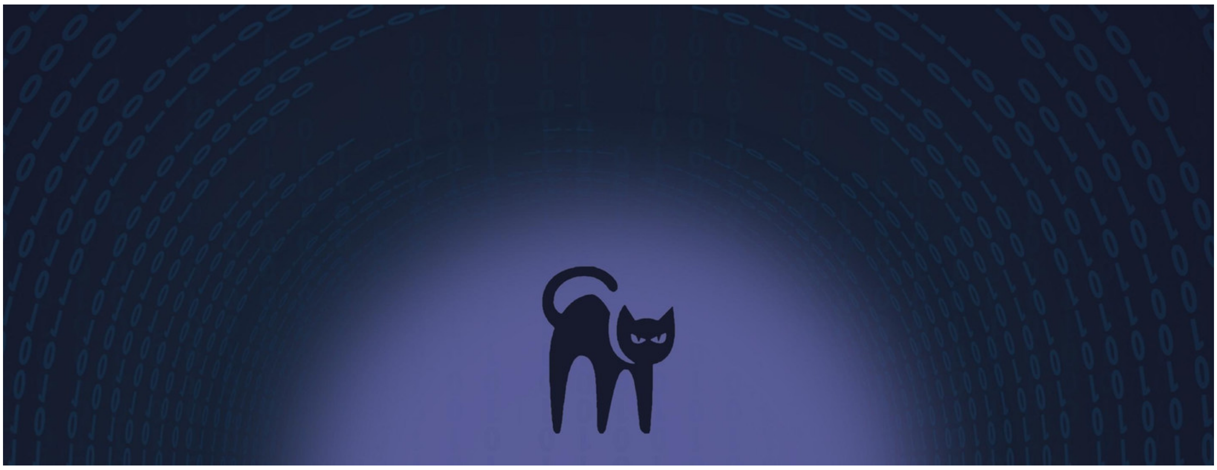


Локер, работает четко. Я проверял.

A short positive review of BlackCat from the RAMP's forum admin, a known ransomware developer with over a decade of cybercriminal experience.

As a result, ransomware collectives have been actively plotting an escape from the tunnel-vision of the toolbox mindset. The now-defunct **Conti, for instance,prepared a list of over a hundred different network penetration andoffensive alternatives, which included both legitimate tools as well asunderground malware.** But these initiatives never achieved actual execution.

BlackCat's case diverges from the mainstream narrative, however, as the group***has*** established an operation set around their own self-written offensive scripts.By creating entirely new tools to execute their operati ons, BlackCat has not onlyfound what seems like an effective way to *circumvent existing defensestrategies,* but also **to ensure their own *longevity*— by changing along withthe times.** This sets BlackCat leagues ahead of its competitors.



<u>BlackCat's Edge - Ransomware Binary Analysis: Tech Dive</u>

AdvIntel has observed BlackCat's ransomware binary to have quite a fewdifferent versions, different flavors for the variety of operating systemarchitecture it may come up against, including **ESXI.** Because of this range inransomware binaries, many opportunities have been provided for our team todissect AlphV's internal operations due to its use of the Rust programminglanguage.

AdvIntel has found the BlackCat deployment operation to involve one(1) ***directexecution using domain and enterprise administrator hard-codedcredentials.***

Additionally, the criminals launched the encryption operation via the *domaincontroller global policy update execution from SYSVOL directory* and *netlogonwith scheduled tasks,* followed with ***the following arguments from the primarydomain controller (PDC)***:

- `/c \\DOMAIN.LOCAL \netlogon\locker.exe --access-token CODE`
- `gpupdate /force`

Windows x64 Version

BlackCat's ransomware binary is written in Rust by mature and experiencedcoders, with each version of Windows or Linux library leveraging a usualcombination of private and public cryptography with *Salsa20/AES* and *RSA.* Themalware coder has left the compiler path as *"C:\Users\runneradmin"* for theWindows library. Interestingly, the binary has its own *full user graphical interface*launched via the access token, obtained by the affiliate from their ransomwarepanel.

Some of the notable malware features include self-propagationenumerating services and shares, *PsExec* for network-wide execution *("arp -a" enumeration*) alongside the leveraging of extensively safe boot functionality while modifying boot loader, establishing itself as 'service' in safeboot to enableit to *bypass certain antivirus and endpoint detection and response products.***The ransomware binary also *clears logs, removes volume shadow copiesand cleans up the Recycle Bin.***

The malware contains functionality to pass domain credentials to the "net use" function to allow system-wide access from a single machine with *UAC bypass,*leveraging the *process environment block (PEB) traversal technique* to obtainAPI calls*, as seen in the following:*

```
win7_plus=true
token_is_admin=
token_is_domain_admin=
masquerade_peb
Uac_bypass::
escalate=success
escalate=failure
```

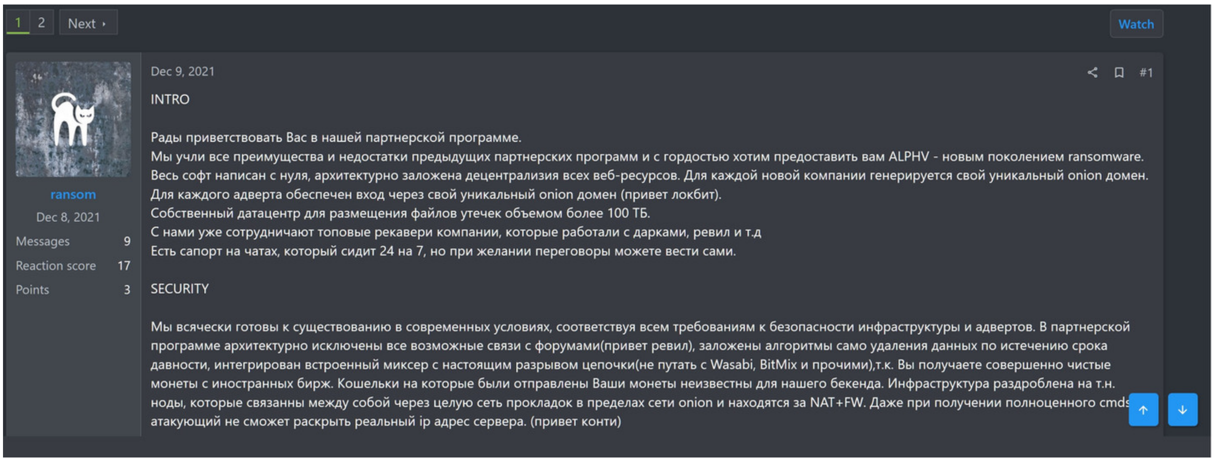
Additionally, the malware leverages the usual *Restart Manager API* for accessingcertain files, as well as the discovery of "hidden partitions".

Linux Debian x64 ESXI Version

The ESXI version of the malware contains the logic to *encrypt ESXI volumes in/ vmfs/volumes* as well as *renovating all virtual machines snapshots via thecommand line, as seen in the following:*

```
esxi/bin/esxclilog | | esxcli --formatter=csv --format-
param=fields=="WorldID,DisplayName" vm process list | awk -F
"\"*,\"*"
'{system("esxcli vm process kill --type=force --world-
id="$1)}'for i in `vim-cmd vmsvc/getallvms| awk '{print$1}'`;do
vim-cmd vmsvc/snapshot.removeall $i & done
```

The Mirror Worlds of Cybercriminals



ransom

Dec 8, 2021

Messages 9

Reaction score 17

Points 3

Dec 9, 2021

INTRO

Рады приветствовать Вас в нашей партнерской программе.
Мы учли все преимущества и недостатки предыдущих партнерских программ и с гордостью хотим предоставить вам ALPHV - новым поколением ransomware.
Весь софт написан с нуля, архитектурно заложена децентрализия всех веб-ресурсов. Для каждой новой компании генерируется свой уникальный onion домен.
Для каждого адверта обеспечен вход через свой уникальный onion домен (привет локбит).
Собственный датацентр для размещения файлов утечек объемом более 100 ТБ.
С нами уже сотрудничают топовые рекавери компании, которые работали с дарками, ревил и т.д
Есть сапорт на чатах, который сидит 24 на 7, но при желании переговоры можете вести сами.

SECURITY

Мы всячески готовы к существованию в современных условиях, соответствуя всем требованиям к безопасности инфраструктуры и адвертов. В партнерской программе архитектурно исключены все возможные связи с форумами(привет ревил), заложены алгоритмы само удаления данных по истечению срока давности, интегрирован встроенный миксер с настоящим разрывом цепочки(не путать с Wasabi, BitMix и прочими),т.к. Вы получаете совершенно чистые монеты с иностранных бирж. Кошельки на которые были отправлены Ваши монеты неизвестны для нашего бекенда. Инфраструктура раздроблена на т.н. ноды, которые связанны между собой через целую сеть прокладок в пределах сети onion и находятся за NAT+FW. Даже при получении полноценного cmds атакующий не сможет раскрыть реальный ip адрес сервера. (привет конти)

BlackCat update announcement post on the criminal forum RAMP.

What's important to note is that BlackCat's foundation for their clean start ismore about the group's mindset, rather than its toolkit. From the get-go,BlackCat has been searching for *outside-the-box* solutions to ransomware'sbiggest obstacles, both operationally and organizationally.

For years now, extortionist groups have mainly adhered to the *RaaS, orRansomware-as-a-Service* model, enabling their affiliates to rent *already-developed ransomware tools* to independently execute their attacks. Apart fromConti, Cl0p, and DoppelPaymer**, most ransomware collectives have tended tobe loosely organized, with very little internal structure holding them together— the cybercriminal ecosystem, due to the illegal nature of its existence, isinherently unstable and chaotic, with *groups disbanding and rebrandingconstantly within the trade's very young lifespan.*

This constant, kinetic movement is strangely reminiscent of the high attrition rateof *startup companies*— the cybercriminal community, specifically theransomware community, can sometimes be a black mirror of real-world crime syndicates or even legitimate businesses: the high turnover in startup companiesshows an above-ground parallel to the movement of threat actors in and out ofransomware collectives because both industries tend to suffer from similarissues: this can include *lack of regulation, high competition, "sniping" of talented members, structural issues, and general lack of dedication to maintaining growth and structure.*

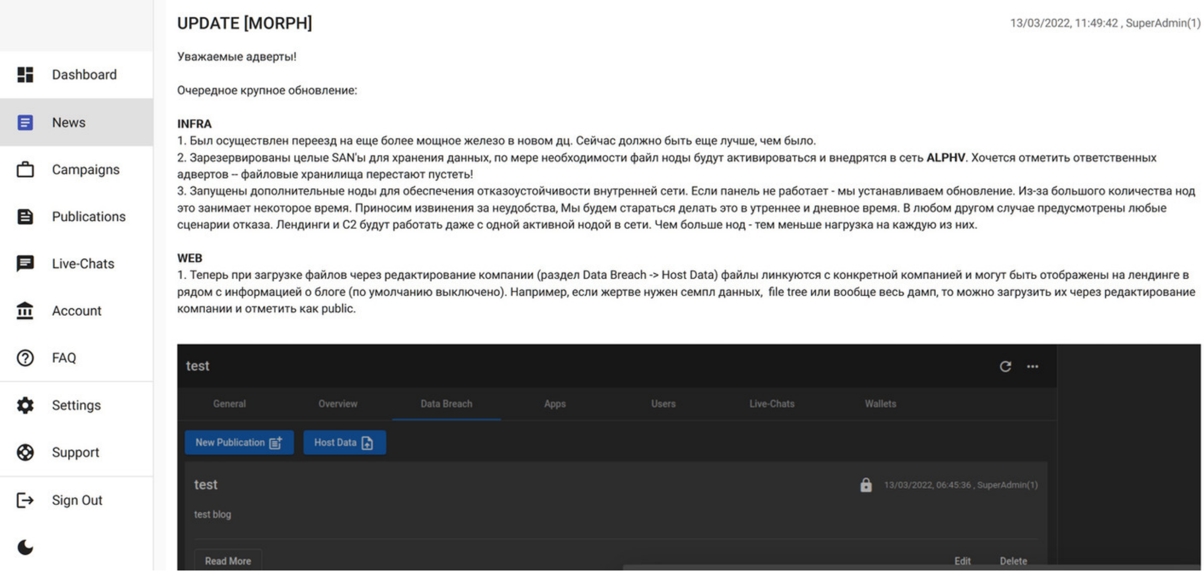
BlackCat & REvil: Avoiding the Mistakes of the Past

Conversely, the *RaaS* model is both named for and reflective of the[***Software-as-a-Service*** **model**](), which is used nigh-universally across the*enterprise software* industry.

Initially, the SaaS model of "*on-demand software*" was focused on *managing andhosting third-party software from independent vendors.* However, over time,*SaaS* vendors began to develop their *own proprietary software, cutting out themiddle-man in the arrangement.*

BlackCat has done the same with its operational model. The group's Admin(according to AdvIntel investigation) is a former member of **REvil**, which was dismantled after FSB raids in early 2022. However, when it came time to rebrand,instead of merely recreating REvil's payload, BlackCat instead decided to createtheir own.

The group seems to be avoiding a mere retread of REvil's footsteps, and forgood reason—as earlier stated, ransomware collectives based around "*on-demand software*" with no personal innovation model have a tendency toexplode into infamy before quickly burning out. For instance, **Avaddon, Maze,Egregor**, and **REvil**, who by all accounts were already on the verge of death bythe time its members were arrested.



UPDATE [MORPH]

13/03/2022, 11:49:42 , SuperAdmin(1)

Уважаемые адверты!

Очередное крупное обновление:

INFRA
1. Был осуществлен переезд на еще более мощное железо в новом дц. Сейчас должно быть еще лучше, чем было.
2. Зарезервированы целые SAN'ы для хранения данных, по мере необходимости файл ноды будут активироваться и внедрятся в сеть **ALPHV**. Хочется отметить ответственных адвертов -- файловые хранилища перестают пустеть!
3. Запущены дополнительные ноды для обеспечения отказоустойчивости внутренней сети. Если панель не работает - мы устанавливаем обновление. Из-за большого количества нод это занимает некоторое время. Приносим извинения за неудобства, Мы будем стараться делать это в утреннее и дневное время. В любом другом случае предусмотрены любые сценарии отказа. Лендинги и C2 будут работать даже с одной активной нодой в сети. Чем больше нод - тем меньше нагрузка на каждую из них.

WEB
1. Теперь при загрузке файлов через редактирование компании (раздел Data Breach -> Host Data) файлы линкуются с конкретной компанией и могут быть отображены на лендинге в рядом с информацией о блоге (по умолчанию выключено). Например, если жертве нужен семпл данных, file tree или вообще весь дамп, то можно загрузить их через редактирование компании и отметить как public.

test

test blog

13/03/2022, 06:45:36 , SuperAdmin(1)

AdvIntel's visibility into BlackCat's panel—a mimic of REvil's previous panel.

BlackCat's decision to "start from scratch", writing new, highly-configurable malware in a lesser-utilized programming language reflects aparallel demand within *RaaS* to its *SaaS* namesake: the demand for new,specialized tools that would allo

w BlackCat to corner the ransomwaremarket at a time when development is desperately needed in order forthreat groups to survive.

On Trend: Cornering the Black Market

Moreover, SaaS's more recent developments have recently seen another notabletrend: the shift from *horizontal SaaS,* or software that applies broadly to a widevariety of industries, to *vertical SaaS,* which targets specific industry niches andstandards.

RaaS's movement as a model within the threat landscape indicates that its nextsteps are similar: the most innovative threat groups, BlackCat included, seem tobe *honing in*, with a greater emphasis in their malware's *exclusivity,customization features,* and *ability to target specific entities.* As of right now,BlackCat's exclusive, highly-configurable Rust-based locker seemsunprecedented, with government agencies scrambling to classify IOCs for thegroup while their target count continues to rise.

The current threat landscape is now undergoing changes that have only becomemore pronounced in recent weeks, as larger and more established groups suchas Conti have quickly disintegrated, its **previous affiliates surreptitiouslyforming new groups, or joining existing ones.**

The new threat groups that result from this dispersion have the benefit ofutilizing their new members' *advanced capabilities* as former affiliates of *larger*and *more established* ransomware collectives. The novel groups have emergedfrom members who yield extremely niche operational skillsets, in turn making thegroups' functionalities increasingly specialized. If access brokerage trendsfurther towards the *specific targeting of organizations and industries,* **groupspecialization may even begin to influence what tools are used anddeveloped by different groups, as we are currently seeing with thebreakneck evolution of the BazarCall attack vector.**

Conclusions—RaaS: Resiliency-as-a-Service

Despite its innovations to the model, BlackCat, like its contemporaries, still fallsunder the category of a *Ransomware-as-a-Service* group. *RaaS* didn't take itstitle from *SaaS* merely as a joke; both models function "on-demand"—or as theirnames indicate, "*as-a-Service*". As the criminal ecosystem continues to evolveat an alarming pace, **BlackCat's methodologies may soon becomerepresentative of the scene as demand for specificity increases—** ***withbroader threat groups who fail to adapt left to become obsolete.***

Adversarial Assessment Summary [ALPHV/BlackCat]

ALPHV/BlackCat [Threat Group]

Malware Type: Ransomware

Origin: Eastern Europe

Intelligence Source: High Confidence

Functionality:

- Data encryption
- Data exfiltration
- Locker creation
- Malware configurability/adaptivity

MITRE ATT&CK Framework:

- T1070 - Indicator Removal on Host
- T1070.001 - Clear Windows Event Logs
- T1078.003 - Local Accounts
- T1562.001 - Disable or Modify Tools
- T1048 - Exfiltration Over Alternative Protocol
- T1048.002 -Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
- T1486 - Data Encrypted for Impact

Distribution:

- Proprietary Locker Malware (Rust-coded)
- Fortinet VPN Exploitation

Persistency: Very High

Infection Rate: High

Decrypter: Not Released

Threat Assessment: Critical

Recommendations & Mitigations [ALPHV/BlackCat]

The FBI has recently released an official profile on BlackCat ransomware. The government agency recommends that victims of BlackCat ***do not pay requested ransoms if possible, and to report all BlackCat-related incidents to the agency itself.***

AdvIntel & the FBI both support the ***<u>following mitigations and prevention recommendations for ALPHV/BlackCat ransomware:</u>***

- **Review domain controllers, servers, workstations, and active directories** for new or unrecognized user accounts.
- **Regularly back up data, air gap, and password protect backup copies offline.** Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- **Review Task Scheduler** for unrecognized scheduled tasks. Additionally, manually review operating system defined or recognized scheduled tasks for unrecognized "actions" (for example: review the steps each scheduled task is expected to perform).
- **Review antivirus logs** for indications they were unexpectedly turned off.
- Implement **network segmentation.**
- Require **administrator credentials to install software.**
- Implement a **recovery plan** to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (e.g., hard drive, storage device, the cloud).
- **Install updates/patch operating systems, software, and firmware** as soon as updates/patches are released.
- Use **multifactor authentication** where possible.
- **Regularly change passwords** to network systems and accounts, and avoid reusing passwords for different accounts.
- Implement the **shortest acceptable timeframe for password changes.**
- **Disable unused remote access/Remote Desktop Protocol (RDP)** ports and monitor remote access/RDP logs.
- **Audit user accounts with administrative privileges** and configure access controls with least privilege in mind.
- **Install and regularly update antivirus** and anti-malware software on all hosts.
- **Only use secure networks** and avoid using public Wi-Fi networks. Consider installing and using a **virtual private network (VPN).**
- Consider adding an **email banner** to emails received from outside your organization.
- **Disable hyperlinks** in received emails.

YARA Signature:

```
rule crime_win64_blackcat_rust_ransomware
{
   meta:
       description = "Detects BlackCat/AlphaV Windows x64 RUST
Ransomware"
       author = "@VK_Intel"
       date = "2022-06-07"

   strings:

       // RUST SETUP
       $r0 = "app.rs" ascii fullword wide

       // RUST RANSOMWARE INJECT
       $func0 = "explorer.exe" ascii fullword wide
       $func1 = "ntdll.dll" ascii fullword wide
       // RUST LOCKER reference lib
       $func2 = "locker " ascii fullword wide

   condition:
       ( uint16(0) == 0x5a4d and $r0 and
       ( all of ($func*) )
       )
}

rule crime_lin64_blackcat_rust_ransomware
{
   meta:
       description = "Detects BlackCat/AlphaV RUST Linux/Debian
x64 ESXI Ransomware"
       author = "@VK_Intel"
       date = "2022-06-07"

   strings:

       // RUST SETUP
       $r0 = "app.rs" ascii fullword wide

       // RUST RANSOMWARE INJECT
       $func0 = "/vmfs/volumes" ascii fullword wide
       $func1 = "esxcli" ascii fullword wide
       // RUST LOCKER reference lib
       $func2 = "locker " ascii fullword wide
   condition:
       ( uint16(0) == 0x5a4d and $r0 and
       ( all of ($func*) )
       )
}
```

Appendix I: Windows x64 BlackCat Ransomware

Windows x64 / Binary:

```
/locker/src/core/os/windows/samba.rs
/locker/src/core/os/windows/file_unlocker.rs
/locker/src/core/os/windows/shutdown.rs
/locker/src/core/os/windows/shadow_copy.rs
/locker/src/core/os/windows/self_propagation.rs
/locker/src/core/os/windows/service.rs
/locker/src/core/pipeline/chunk_worker.rs
/locker/src/core/os/windows/desktop_note.rs
/locker/src/core/pipeline/chunk_workers_supervisor.rs
/locker/src/core/pipeline/file_worker_pool_core.rs
/locker/src/core/config.rs
/locker/src/core/os/windows/console.rs
/locker/src/core/os/windows/psexec.rs
/locker/src/core/pipeline/file_worker_pool.rs
/locker/src/core/cluster.rs
/locker/src/core/discoverer.rs
/locker/src/core/os/windows/safeboot.rs
/locker/src/core/os/windows/user.rs
/locker/src/core/pipeline/file_work.rs
/locker/src/core/os/windows/system_info.rs
/locker/src/core/os/windows/restart_manager.rs
/locker/src/core/os/windows/netbios.rs
/locker/src/core/os/windows/privilege_escalation.rs
/locker/src/core/os/windows/process.rs
/locker/src/core/os/windows/hidden_partitions.rs
/locker/src/core/os/windows/self_propagation.rs
```

Config:

```
${EXTENSION}${ACCESS_KEY}${NOTE_FILE_NAME}
```

```
ADMIN$IPC$Config
extension
public_keynote_file_namenote_full_textnote_short_textcredentialsd
efault_file_modedefault_file_cipherkill_serviceskill_processesexc
lude_directory_namesexclude_file_namesexclude_file_extensionsexcl
ude_file_path_wildcardenable_network_discoveryenable_self_propaga
tionenable_set_wallpaperenable_esxi_vm_killenable_esxi_vm_snapsho
t_killstrict_include_pathsesxi_vm_kill_excludestruct
```

Debugging Elements:

```
locker::core::stacklibrary/locker/src/core/stack.rsPreparing
Logger
Starting File Unlockers
/locker-app/library/locker/src/core/stack.rs
locker::core::os::windows::recycle_binlibrary/locker/src/core/os/
windows/recycle_bin.rsnV
locker::core::os::windows::sambalibrary/locker/src/core/os/window
s/samba.rsenum_servers_sync::server=
locker::core::os::windows::file_unlockerlibrary/locker/src/core/o
s/windows/file_unlocker.rsreg add
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer
\Parameters /v MaxMpxCt /d 65535 /t REG_DWORD /f
locker::core::os::windows::shutdownlibrary/locker/src/core/os/win
dows/shutdown.rsExitWindowsEx=
library/locker/src/core/renderer.rs
locker::core::renderer
library/locker/src/core/env.rs
locker::core::os::windows::shadow_copylibrary/locker/src/core/os/
windows/shadow_copy.rswmic.exe Shadowcopy
Deleteshadow_copy::remove_all_wmic=
locker::core::os::windows::self_propagationlibrary/locker/src/cor
e/os/windows/self_propagation.rspropagate::credentials=uGg
locker::core::os::windows::servicelibrary/locker/src/core/os/wind
ows/service.rsenum_services=
library/locker/src/core/pipeline/chunk_worker.rsxJg
library/locker/src/core/os/windows/desktop_note.rsset_desktop_ima
ge=
locker::core::os::windows::desktop_note
```

```
locker::core::pipeline::chunk_workers_supervisorlibrary/locker/sr
c/core/pipeline/chunk_workers_supervisor.rs
locker::core::pipeline::file_worker_pool_corelibrary/locker/src/c
ore/pipeline/file_worker_pool_core.rsCan't dispatch ->
[2JInvalid HeaderInvalid KeyInvalid RSA Private
Keylibrary/locker/src/core/config.rs-{
locker::core::os::windows::consolelibrary/locker/src/core/os/wind
ows/console.rsattach=
locker::core::os::windows::psexeclibrary/locker/src/core/os/windo
ws/psexec.rs-accepteula-nobannerpsexec_args::args=
locker::core::os::windows::safeboot
locker::core::pipeline::file_worker_poollibrary/locker/src/core/p
ipeline/file_worker_pool.rsspawned_chunk_work_infastructure=
locker::core::clusterlibrary/locker/src/core/cluster.rsRecv Path
-> [
locker::core::discovererlibrary/locker/src/core/discoverer.rsIgno
ring Symlink ->
Cant open filelibrary/locker/src/core/os/windows/netbios.rs
locker::core::os::windows::netbios
locker::core::os::windows::privilege_escalationlibrary/locker/src
/core/os/windows/privilege_escalation.rsimpersonate_spawn_trying:
:
library/locker/src/core/os/windows/process.rskill_all=
locker::core::os::windows::processkill=
Couldn't acquire process
Envlibrary/locker/src/core/os/windows/safeboot.rs
--safeboot-entry""library/locker/src/core/os/windows/user.rs
library/locker/src/core/pipeline/file_work.rs
library/locker/src/core/os/windows/hidden_partitions.rs
locker::core::os::windows::hidden_partitions
locker::core::os::windows::system_infolibrary/locker/src/core/os/
windows/system_info.rsdomain_name=
cmd/ccmd.exe /c  for /F "tokens=*" %1 in ('wevtutil.exe el') DO
wevtutil.exe cl "%1"iisreset.exe
/stoplibrary/locker/src/core/os/windows/restart_manager.rsRmStart
Session=
locker::core::os::windows::restart_managerRmStartSession::Error:
invalid key output
```

Appendix II: Ubuntu Debian Linux x64 BlackCat Ransomware

Config:

```
{EXTENSION}${ACCESS_KEY}${NOTE_FILE_NAME}ADMIN$drag-and-drop-
target.batextensionpublic_keynote_file_namenote_full_textnote_sho
rt_textcredentialsdefault_file_modedefault_file_cipherkill_servic
eskill_processesexclude_directory_namesexclude_file_namesexclude_
file_extensionsexclude_file_path_wildcardenable_network_discovery
enable_self_propagationenable_set_wallpaperenable_esxi_vm_killena
ble_esxi_vm_snapshot_killstrict_include_pathsesxi_vm_kill_exclude
struct
```