



ArcSight Use Case on BlackCat/ALPHV Ransomware

Pavan Raja

Pre-Sales Team

Middle East & Africa

Contents

- 1. Introduction 3
 - Purpose and Scope 3
 - Background 3
- 2. BlackCat/ALPHV Ransomware Indicators of Compromise Summary 4
 - Recommended Mitigations 5
- 3. ArcSight Use Case for BlackCat/ALPHV Ransomware 7
 - Installing the Use Case Content [ARB package] 7
 - Use Case Contents & Resources 9
 - Active Channel 10
 - Dashboard 11
 - Filters 12
 - Active Lists 13
 - Field Set 15
 - Rules 16
 - Monitoring the Alerts 17
- 4. References 17

1. Introduction

Purpose and Scope

As of 19th April 2022, Federal Bureau of Investigation[FBI] – Cyber Division provided known indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) associated with ransomware variants identified through FBI investigations.

As of March 2022, BlackCat/ALPHV ransomware as a service (RaaS) had compromised at least 60 entities worldwide and is the first ransomware group to do so successfully using RUST, considered to be a more secure programming language that offers improved performance and reliable concurrent processing. BlackCat-affiliated threat actors typically request ransom payments of several million dollars in Bitcoin and Monero but have accepted ransom payments as initial ransom demand amount.

The purpose of this document is to provide information and capture any such communications by alerting using ArcSight ESM. So, the use cases are applicable to any infrastructure which has Microsoft implementation which involves Active Directory, Group Policy Object deployment and environment which leverage PowerShell Scripts

The document and its contents provide no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber actors

Background

The content was created by Pavan Raja, ArcSight Specialist for MEA.

Contact details are as follows:

Pavan Raja
ArcSight Specialist & Pre-Sales, MEA
+971 565381117
Pavan.Raja@microfocus.com

2. BlackCat/ALPHV Ransomware Indicators of Compromise Summary

BlackCat/ALPHV ransomware leverages previously compromised user credentials to gain initial access to the victim system. Once the malware establishes access, it compromises Active Directory user and administrator accounts. The malware uses Windows Task Scheduler to configure malicious Group Policy Objects (GPOs) to deploy ransomware. Initial deployment of the malware leverages PowerShell scripts, in conjunction with Cobalt Strike and disables security features within the victim's network.

BlackCat/ALPHV ransomware also leverages Windows administrative tools and Microsoft Sysinternals tools during compromise. BlackCat/ALPHV steals victim data prior to the execution of the ransomware, including from cloud providers where company or client data was stored.

The actors leverage Windows scripting to deploy ransomware and to compromise additional hosts. For example, the following batch and PowerShell scripts were observed:

- start.bat - launches the ransomware executable with required arguments
- est.bat - copies the ransomware to other locations
- drag-and-drop-target.bat - launches the ransomware executable for the MySQL

Server

- run.bat - executes a callout command to an external server using SSH - file names

may change

depending on the company and systems affected

- Runs1.ps1 - PowerShell script to disable McAfee

Recommended Mitigations

Payment does not guarantee files will be recovered. It may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities.

Below are some of the steps which can help mitigate this situation:

- 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.

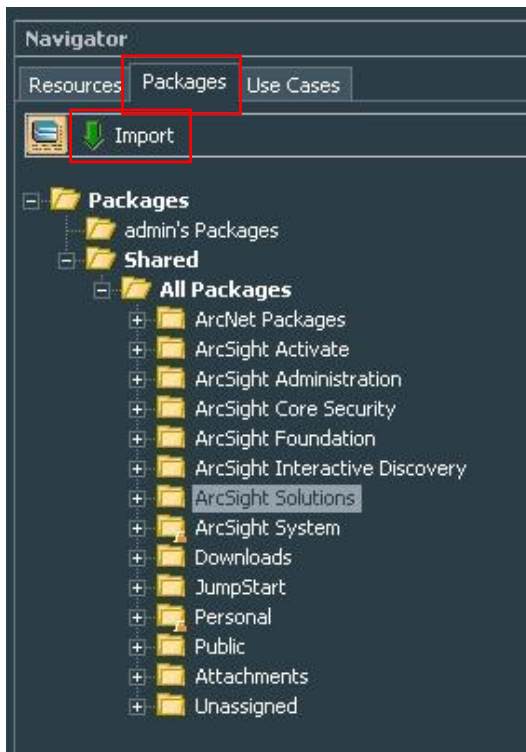
3. ArcSight Use Case for BlackCat/ALPHV Ransomware

The ArcSight Content has been created with ESM 7.6 Version and tested on the same platform. The content should be compatible with older versions of ESM/Express versions as well.

Installing the Use Case Content [ARB package]

To install the content, you need to login to the thick client [JAVA console]

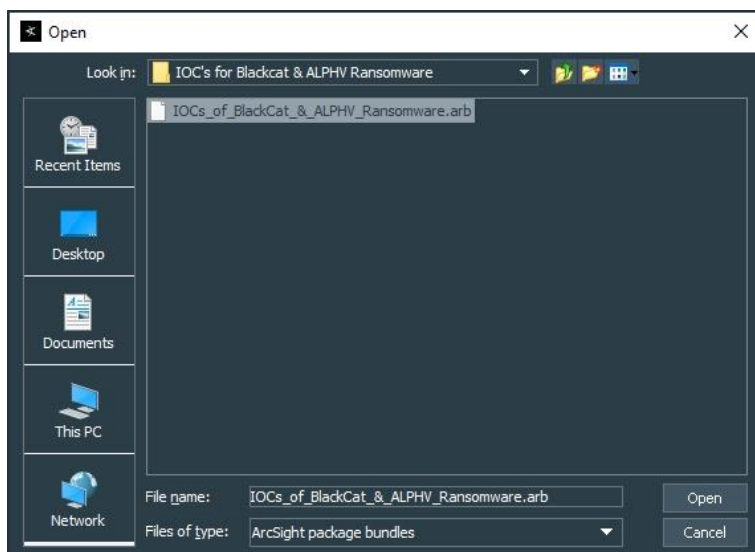
- Browse to Navigator and Select the “**Packages**” tab.
- Click on “**IMPORT**”



- The System Dialog Box opens up, where you can browse to the location where the “IOCs of BlackCat & ALPHV Ransomware.arb” file is stored and Select the file and Click on “**OPEN**”



IOCs_of_BlackCat_&
_ALPHV_Ransomwar



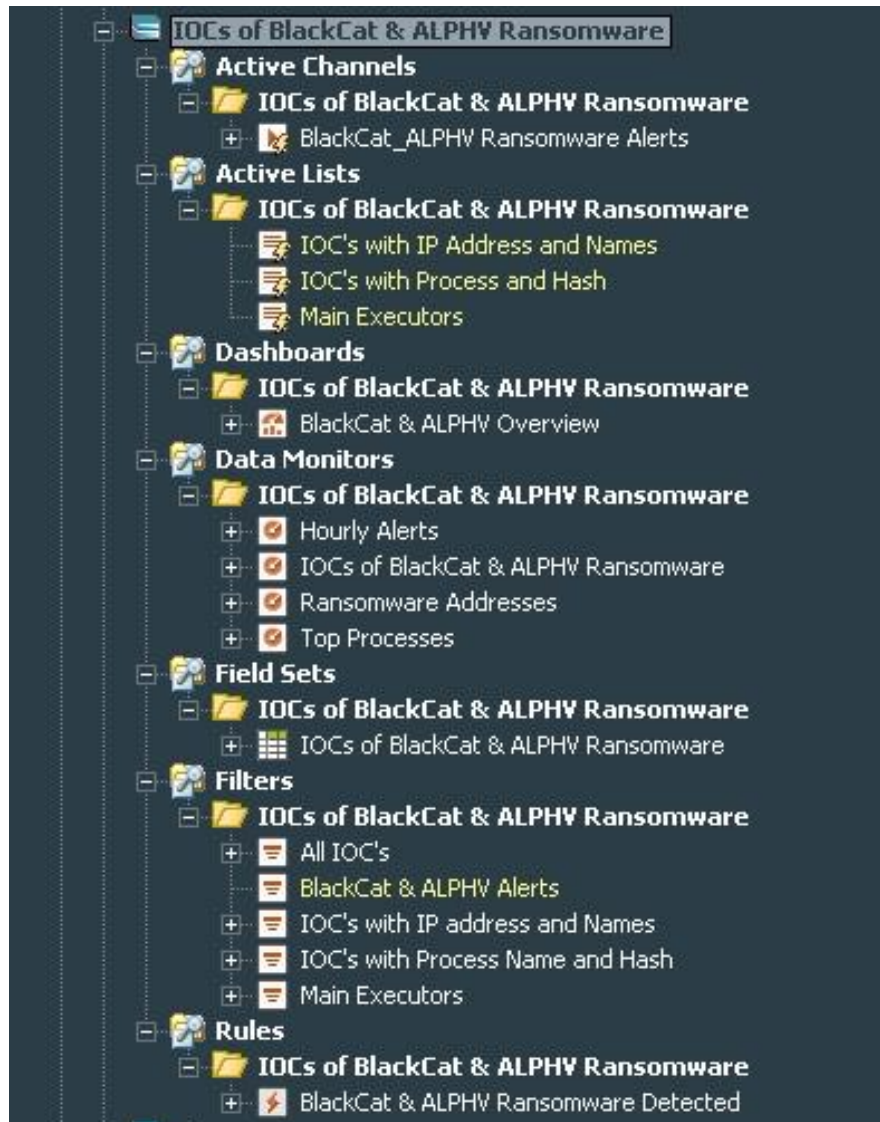
- This will now begin the process of importing the ARB file to the ArcSight Manager.



- Once the importing Packages summary report is shown, you can Click “OK” to close the window.

Use Case Contents & Resources

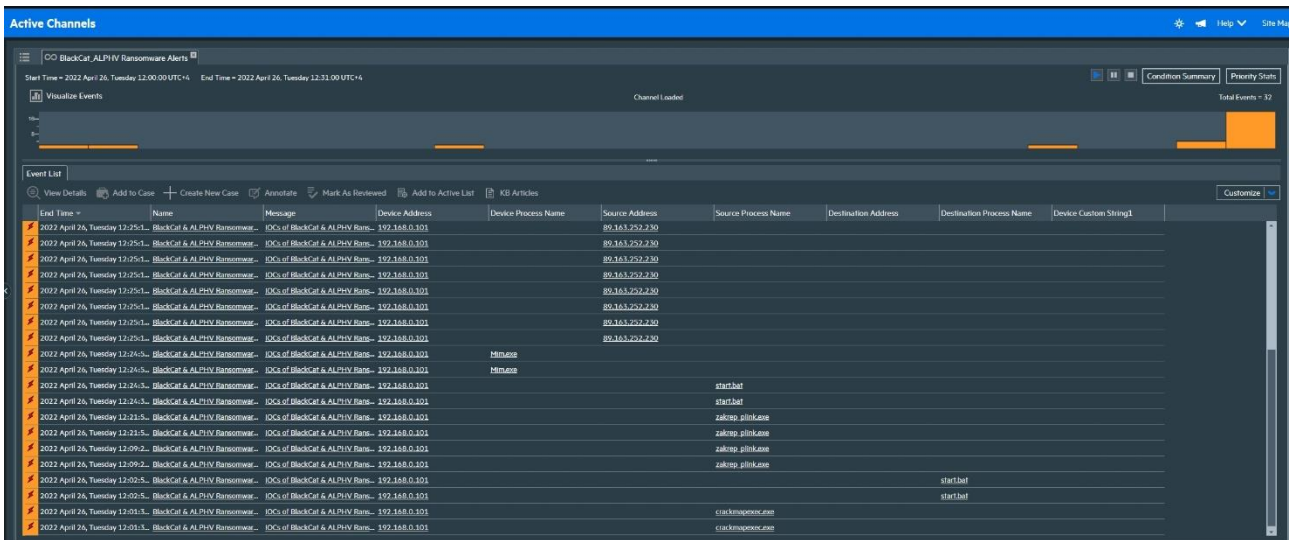
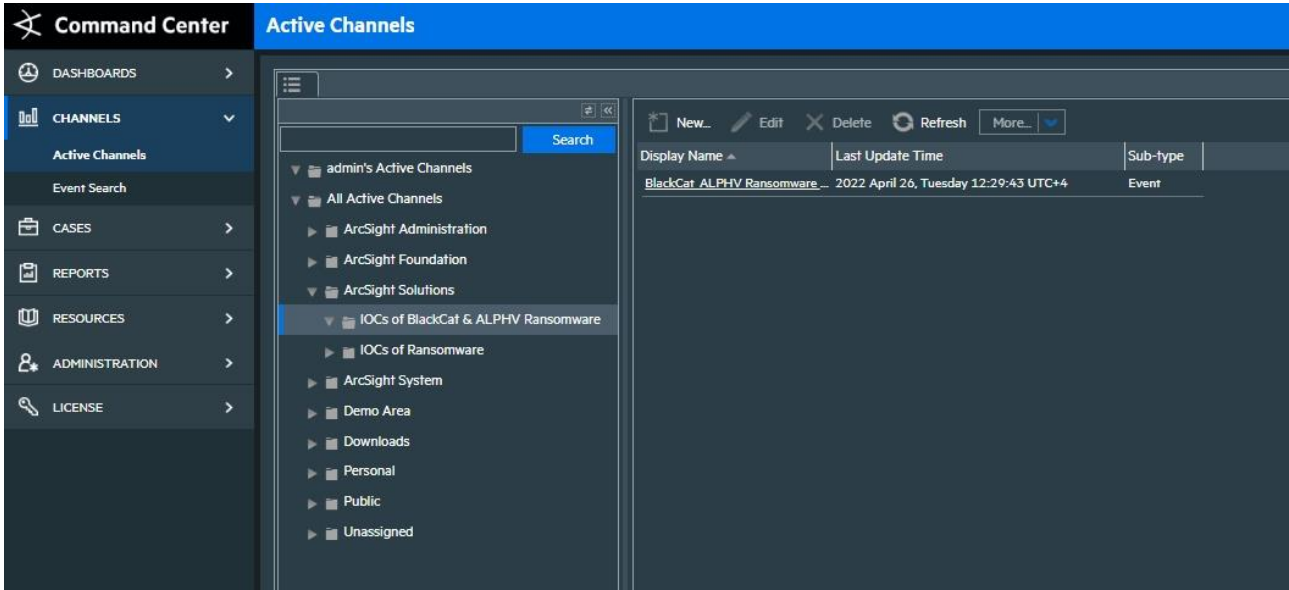
Once the Import has been successfully completed, you can validate by expanding the Package Content. The Package will install all the contents under “ArcSight Solutions\IOCs of BlackCat & ALPHV Ransomware”



Active Channel

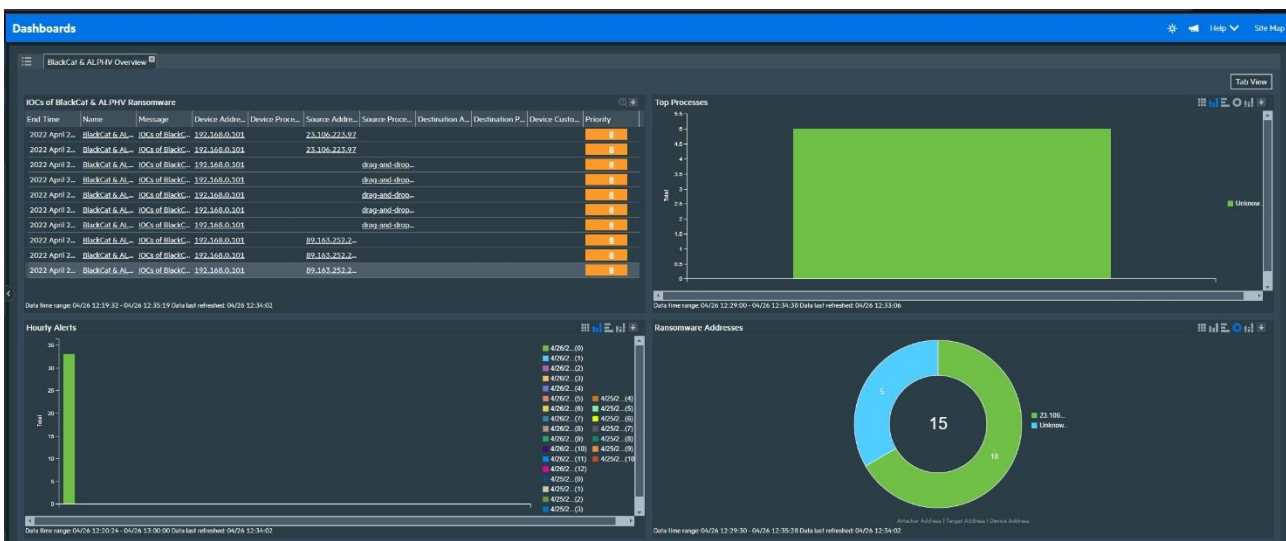
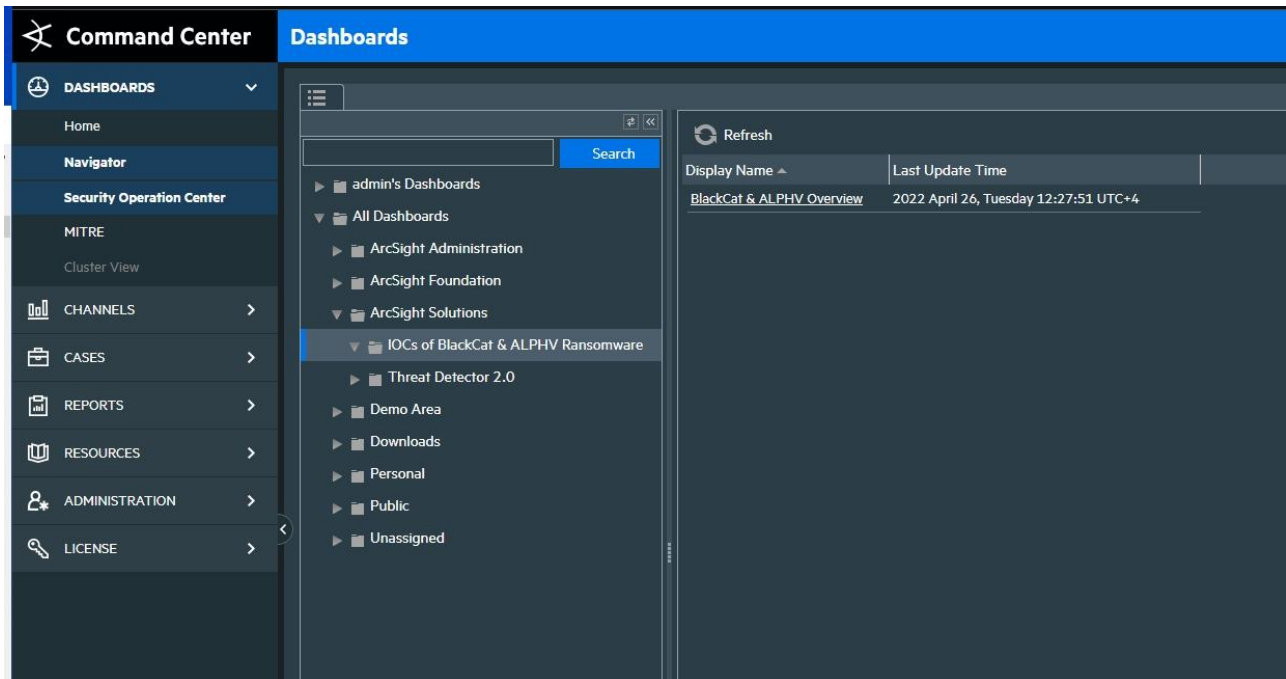
The channel has been created, to monitor the Alerts triggered by the Rules.

Contents can be found under “ArcSight Solutions\IOCs of BlackCat & ALPHV Ransomware”



Dashboard

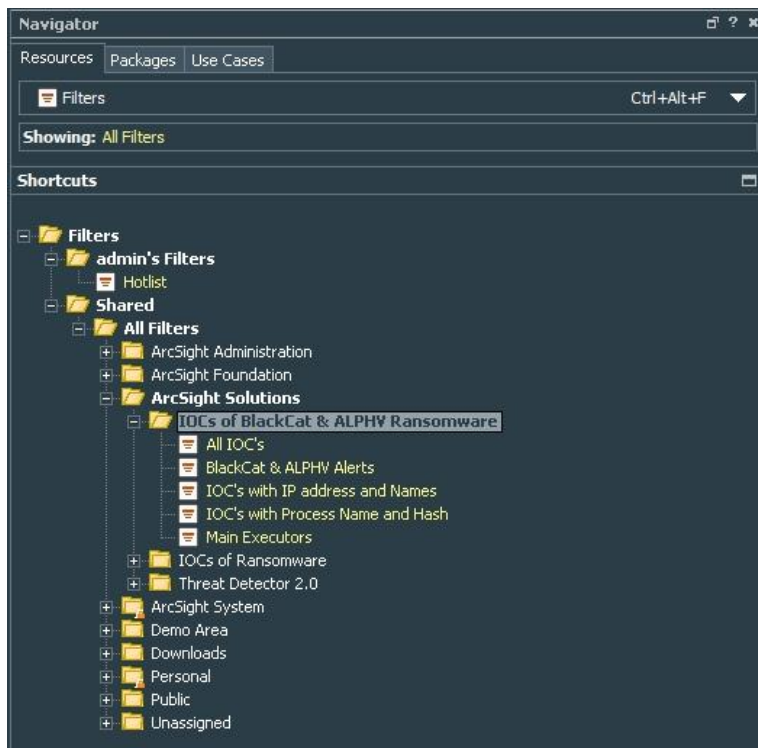
The dashboard and data monitors has been created, to monitor the Alerts triggered by the Rules. Contents can be found under “ArcSight Solutions\IOCs of BlackCat & ALPHV Ransomware”



Filters

The Filters created for referencing all the Ransomware Lists or specific Ransomware list can be found in this section.

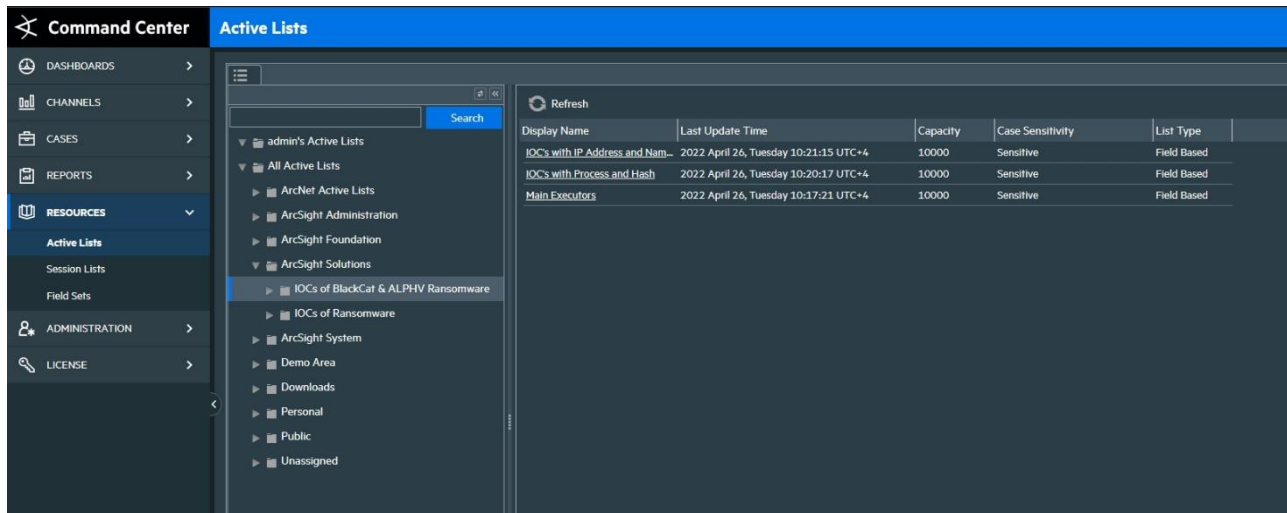
Contents can be found under “ArcSight Solutions\IOCs of BlackCat & ALPHV Ransomware”



Active Lists

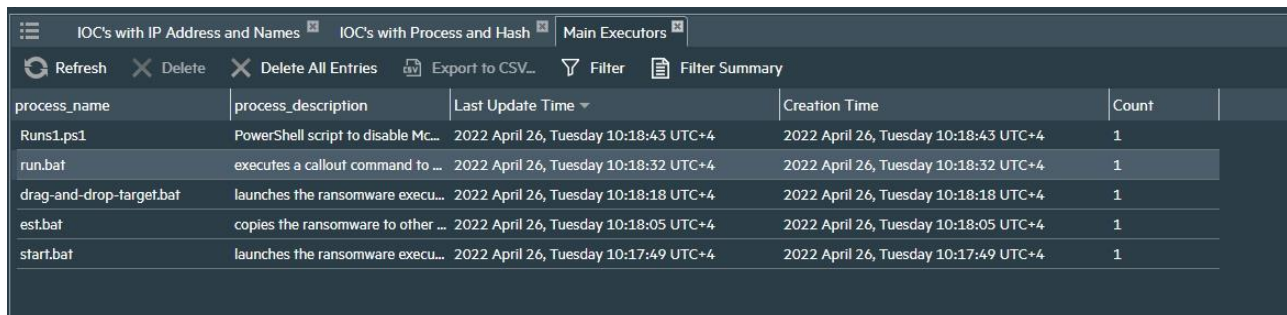
These are the dynamic lists which are configured to store Process Names and IP Addresses and can be updated with new IOC's at later stage.

Contents can be found under “ArcSight Solutions\IOCs of BlackCat & ALPHV Ransomware”



Display Name	Last Update Time	Capacity	Case Sensitivity	List Type
IOCs with IP Address and Nam...	2022 April 26, Tuesday 10:21:15 UTC+4	10000	Sensitive	Field Based
IOCs with Process and Hash	2022 April 26, Tuesday 10:20:17 UTC+4	10000	Sensitive	Field Based
Main Executors	2022 April 26, Tuesday 10:17:21 UTC+4	10000	Sensitive	Field Based

All the Active Lists are configured with TTL value 0, meaning the data within the Active List shall live forever unless manually removed or cleared.



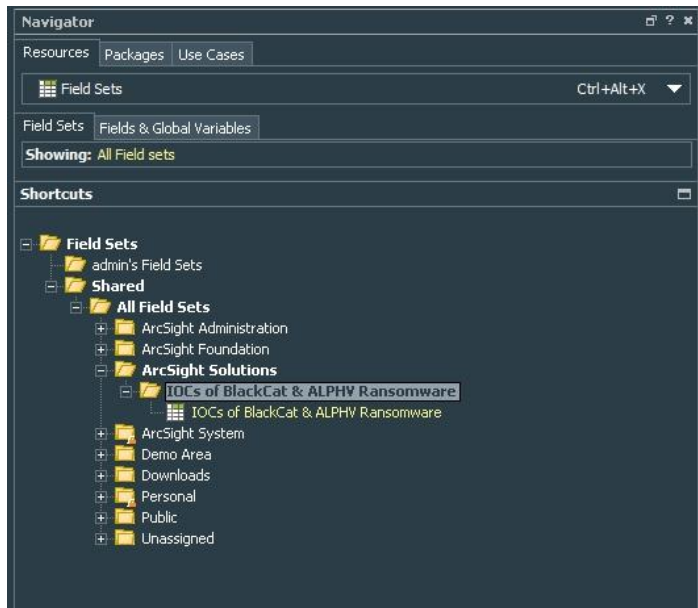
process_name	process_description	Last Update Time	Creation Time	Count
Runs1.ps1	PowerShell script to disable Mc...	2022 April 26, Tuesday 10:18:43 UTC+4	2022 April 26, Tuesday 10:18:43 UTC+4	1
run.bat	executes a callout command to ...	2022 April 26, Tuesday 10:18:32 UTC+4	2022 April 26, Tuesday 10:18:32 UTC+4	1
drag-and-drop-target.bat	launches the ransomware execu...	2022 April 26, Tuesday 10:18:18 UTC+4	2022 April 26, Tuesday 10:18:18 UTC+4	1
est.bat	copies the ransomware to other ...	2022 April 26, Tuesday 10:18:05 UTC+4	2022 April 26, Tuesday 10:18:05 UTC+4	1
start.bat	launches the ransomware execu...	2022 April 26, Tuesday 10:17:49 UTC+4	2022 April 26, Tuesday 10:17:49 UTC+4	1

IOC's with IP Address and Names ² IOC's with Process and Hash ² Main Executors ²				
Refresh Delete Delete All Entries Export to CSV... Filter Filter Summary				
device_address	device_hostname	Last Update Time ▾	Creation Time	Count
146.0.77.15		2022 April 26, Tuesday 10:25:59 UTC+4	2022 April 26, Tuesday 10:25:59 UTC+4	1
89.163.252.230		2022 April 26, Tuesday 10:25:43 UTC+4	2022 April 26, Tuesday 10:25:43 UTC+4	1
185.220.102.253		2022 April 26, Tuesday 10:25:38 UTC+4	2022 April 26, Tuesday 10:25:38 UTC+4	1
139.60.161.161		2022 April 26, Tuesday 10:25:33 UTC+4	2022 April 26, Tuesday 10:25:33 UTC+4	1
198.144.121.93		2022 April 26, Tuesday 10:25:28 UTC+4	2022 April 26, Tuesday 10:25:28 UTC+4	1
45.134.20.66		2022 April 26, Tuesday 10:25:23 UTC+4	2022 April 26, Tuesday 10:25:23 UTC+4	1
23.106.223.97		2022 April 26, Tuesday 10:25:19 UTC+4	2022 April 26, Tuesday 10:25:19 UTC+4	1
152.89.247.207		2022 April 26, Tuesday 10:25:14 UTC+4	2022 April 26, Tuesday 10:25:14 UTC+4	1
142.234.157.246		2022 April 26, Tuesday 10:25:08 UTC+4	2022 April 26, Tuesday 10:25:08 UTC+4	1
94.232.41.155		2022 April 26, Tuesday 10:25:03 UTC+4	2022 April 26, Tuesday 10:25:03 UTC+4	1
45.153.160.140		2022 April 26, Tuesday 10:24:59 UTC+4	2022 April 26, Tuesday 10:24:59 UTC+4	1
37.120.238.58		2022 April 26, Tuesday 10:24:55 UTC+4	2022 April 26, Tuesday 10:24:55 UTC+4	1
89.44.9.243		2022 April 26, Tuesday 10:24:49 UTC+4	2022 April 26, Tuesday 10:24:49 UTC+4	1

IOC's with IP Address and Names ² IOC's with Process and Hash ² Main Executors ²				
Refresh Delete Delete All Entries Export to CSV... Filter Filter Summary				
process_name	process_hash	Last Update Time ▾	Creation Time	Count
zakrep_plink.exe	fce13da5592e9e120777d82d2...	2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
[#].ps1		2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
mimikatz.exe	d241df7b9d2ec0b8194751cd5...	2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
run.exe	4831c1b113df21360ef68c450...	2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
[compromised company].exe	1b2a30776df64fbd7299bd588...	2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
Mim.exe		2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
beacon.exe	3f85f03d33b9fe25bcfac61118...	2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
psexec.ps1		2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
RCE-Exploit-RunAsUser.bat	6c6c46bdac6713c94debbd454...	2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
Run1.ps1		2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	2
PsExec64.exe		2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
crackmapexec.exe		2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
xxxw.exe		2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
spider_32.dll	82db4c04f5dcda3bfcd75357a...	2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
[###].ps1		2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
plink.exe		2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
est.bat	e7ee8ea6fb7530d1d904cdb2d...	2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
win1999.exe	37178dfaccbc371a04133d26a...	2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
ipscan.ps1	9f60dd752e7692a2f5c758de4...	2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
rpcdump.exe	91625f7f5d590534949ebe08c...	2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
http_x64.exe	6c2874169fdb30846fe7ffe34...	2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
CME.ps1		2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
Services.exe		2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
powershell.dll	fcf3a6eeb9f836315954dae034...	2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
[##].ps1		2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
test.exe		2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
System.ps1		2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1
amd - Copy.ps1	861738dd15eb7fb50568f0e39...	2022 April 26, Tuesday 10:22:58 UTC+4	2022 April 26, Tuesday 10:22:58 UTC+4	1

Field Set

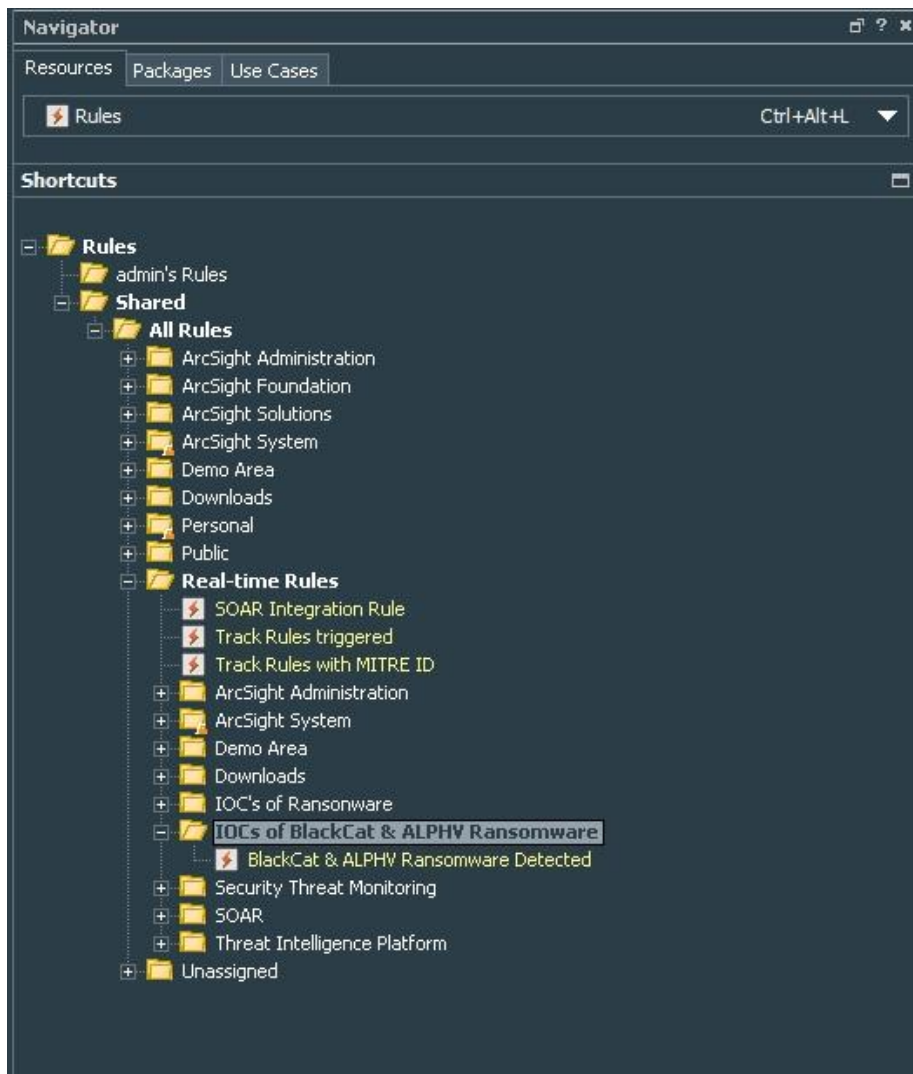
Field Set to specifically view and use in other resources has been created for future use.



Rules

The Correlation Rules is configured to validate any traffic towards these Process Names, Asset Names and IP Addresses.

Contents can be found under “ArcSight Solutions\IOCs of BlackCat & ALPHV Ransomware”



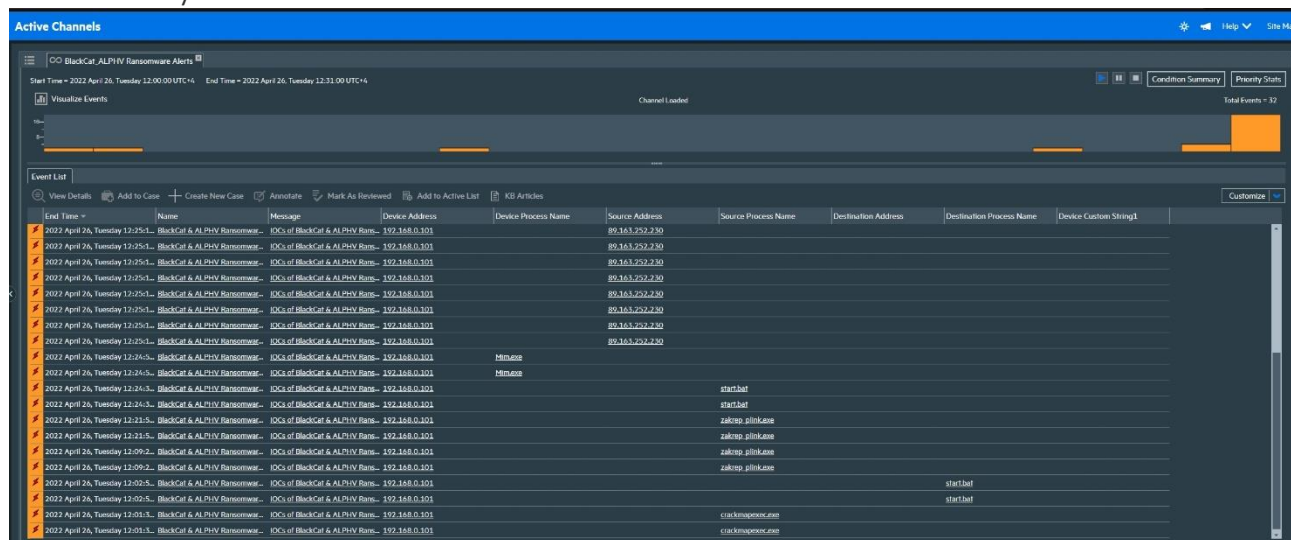
TIP: This RULE can be used in conjunction with other alerts related to Windows Events and SYSMON Events. They provide more details about the RDP sessions.

Monitoring the Alerts

After the content has been deployed, the Rules needs to be deployed to make it work in REAL TIME.

You can deploy by Right Click on the “IOCs of BlackCat & ALPHV Ransomware” group which can be found under “ArcSight Solutions\IOCs of BlackCat & ALPHV Ransomware” and then Click on Deploy Real Time Rule(s)

Once its deployed under Real Time, the rule will start monitoring for active session towards any of the ROUGE Assets.



The same can be validated using the Active Channel.

For Historical Correlation, you can use the Rule to Verify Rule(s) with Events and choose older Time frame where you wish to validate the events against the rule.

4. References

The document has been created in reference to the FBI FLASH article CU-000167-MW issued March 2022.