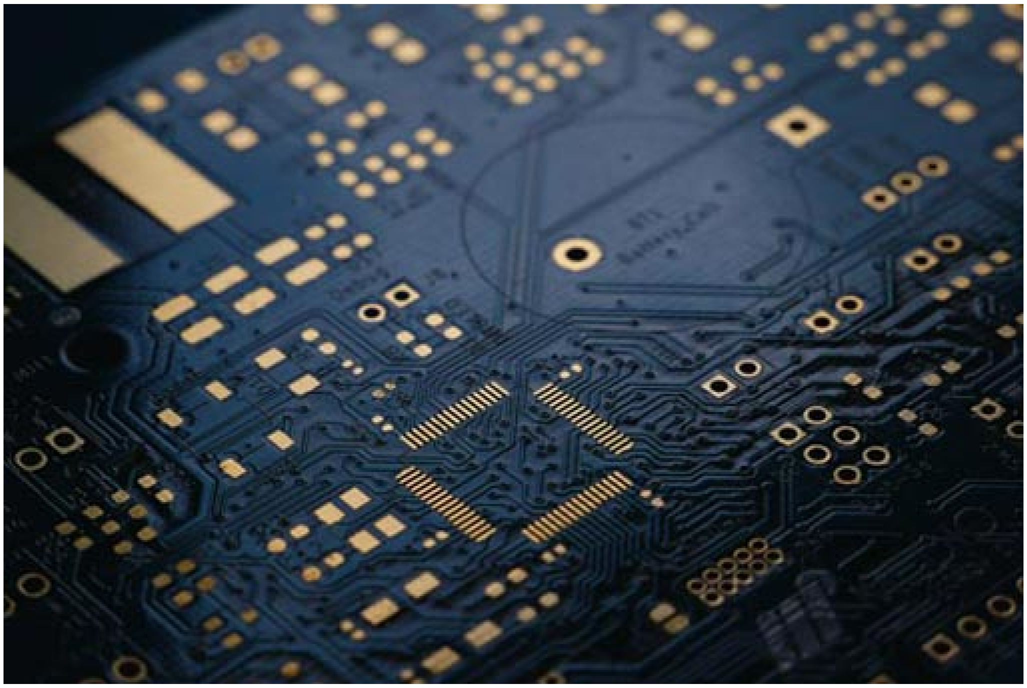
Trellix Global Defenders: BlackCat Ransomware as a Service - The Cat is certainly out of the bag!

trellix.com/en-us/about/newsroom/stories/threat-labs/blackcat-ransomware-as-a-service.html



Stories

The latest cybersecurity trends, best practices, security vulnerabilities, and more

By Arnab Roy · February 8, 2022

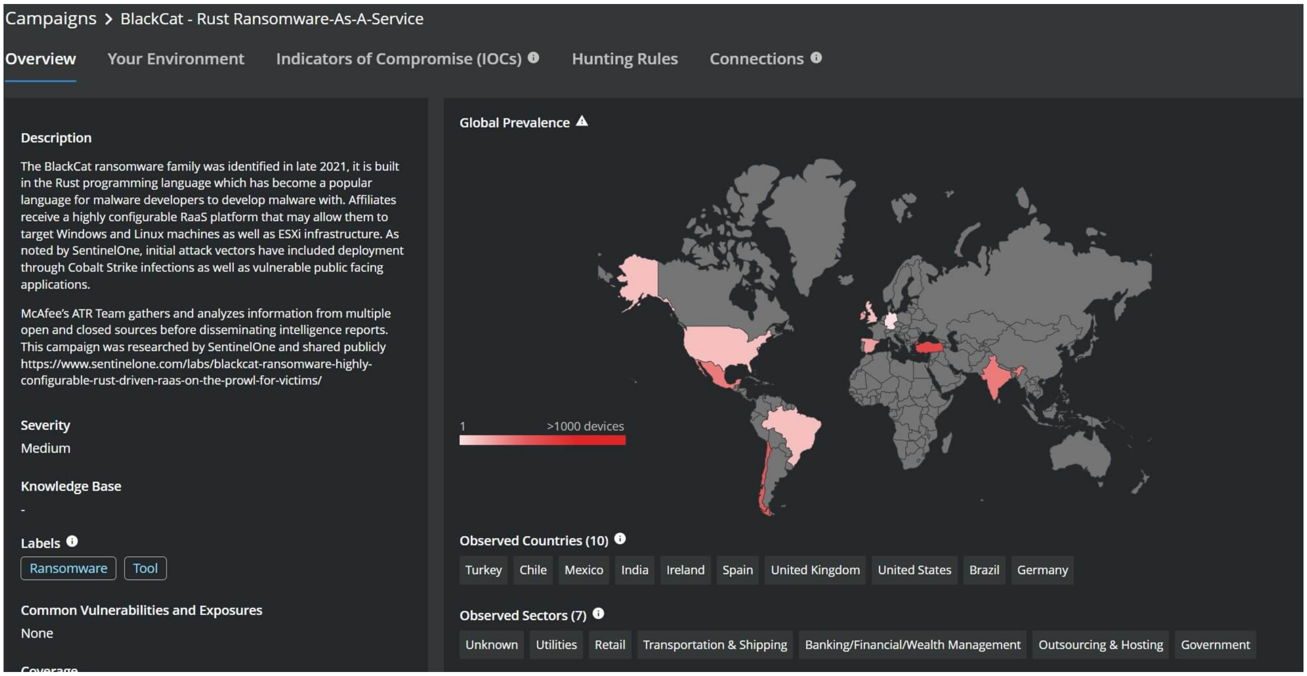
Research Contributions and Analysis: Filippo Sitzia

Threat Summary

Blackcat also known as ALPHV/Noberus is a Ransomware as a Service provider originally being detected around the end of November 2021. While analyzing the campaign we discovered several important aspects of this ransomware including operational similarity with previous ransomware families such as Darkside, Blackmatter and Revil. It is understood that Blackcat is potentially actively recruiting affiliates to increase proliferation and offering lucrative financial deals related to profit sharing of up to 90% in some cases.

Blackcat has potentially been attributed to a spate of recent attacks spread across various critical sectors such as energy, transportation and utilities.

This threat actor Is continuously updating their services and adding features and modifying their code to provide advanced penetration capabilities for It's affiliates. Keeping track of this threat groups activities Is extremely crucial and organisations can stay updated by keeping an eye on the IOC's and updates being provided by the Trellix ATR team via our Threat Dashboard and Trellix Insights platform.


Campaigns > BlackCat - Rust Ransomware-As-A-Service
Overview
Your Environment
Indicators of Compromise (IOCs)
Hunting Rules
Connections
Global Prevalence
1
>1000 devices

Description

The BlackCat ransomware family was identified in late 2021, it is built in the Rust programming language which has become a popular language for malware developers to develop malware with. Affiliates receive a highly configurable RaaS platform that may allow them to target Windows and Linux machines as well as ESXi infrastructure. As noted by SentinelOne, initial attack vectors have included deployment through Cobalt Strike infections as well as vulnerable public facing applications.

McAfee's ATR Team gathers and analyzes information from multiple open and closed sources before disseminating intelligence reports. This campaign was researched by SentinelOne and shared publicly https://www.sentinelone.com/labs/blackcat-ransomware-highly-configurable-rust-driven-raas-on-the-prowl-for-victims/

Severity
Medium

Knowledge Base
-

Labels
Ransomware Tool

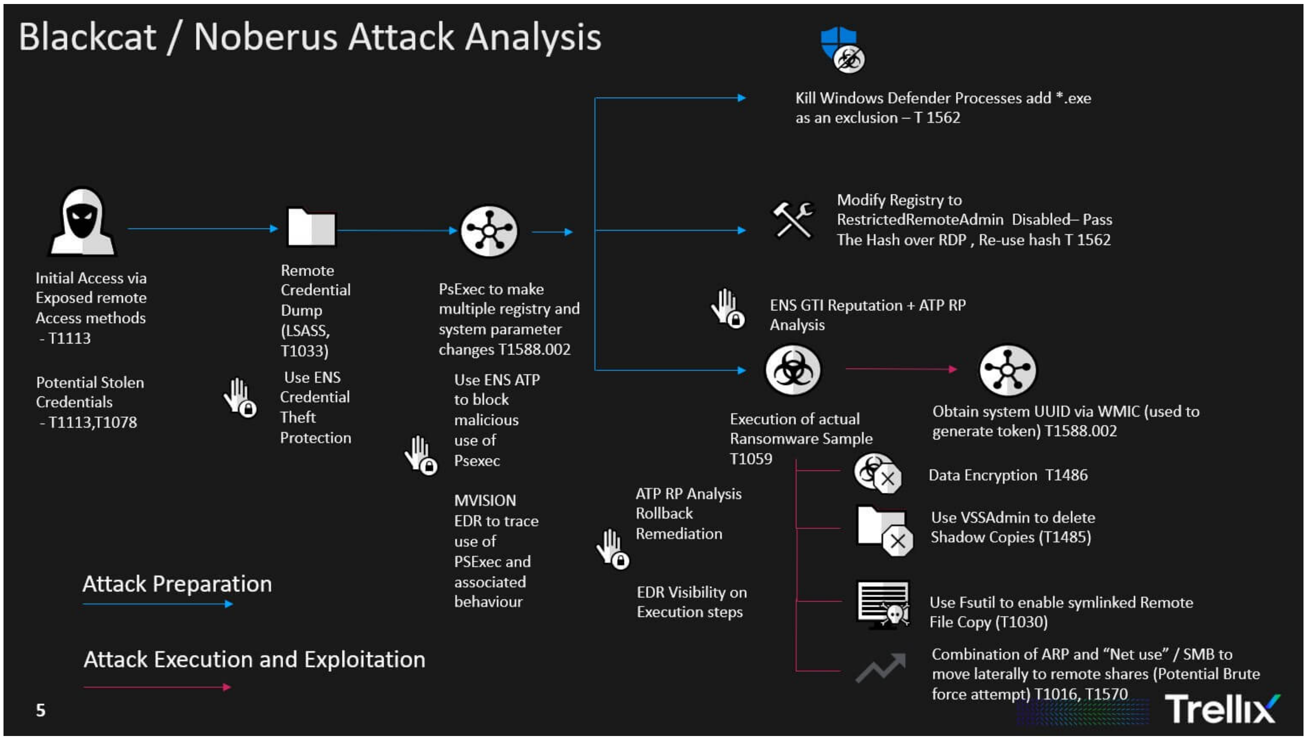
Common Vulnerabilities and Exposures
None

Coverage

Observed Countries (10)
Turkey Chile Mexico India Ireland Spain United Kingdom United States Brazil Germany

Observed Sectors (7)
Unknown Utilities Retail Transportation & Shipping Banking/Financial/Wealth Management Outsourcing & Hosting Government

Figure 1: Trellix Insights - Blackcat Campaign



Blackcat / Noberus Attack Analysis

Initial Access via Exposed remote Access methods - T1113

Potential Stolen Credentials - T1113,T1078

Remote Credential Dump (LSASS, T1033)

Use ENS Credential Theft Protection

PsExec to make multiple registry and system parameter changes T1588.002

Use ENS ATP to block malicious use of Psexec

MVISION EDR to trace use of PSExec and associated behaviour

Kill Windows Defender Processes add *.exe as an exclusion – T 1562

Modify Registry to RestrictedRemoteAdmin Disabled– Pass The Hash over RDP , Re-use hash T 1562

ENS GTI Reputation + ATP RP Analysis

Execution of actual Ransomware Sample T1059

Obtain system UUID via WMIC (used to generate token) T1588.002

ATP RP Analysis Rollback Remediation

EDR Visibility on Execution steps

Data Encryption T1486

Use VSSAdmin to delete Shadow Copies (T1485)

Use Fsutil to enable symlinked Remote File Copy (T1030)

Combination of ARP and "Net use" / SMB to move laterally to remote shares (Potential Brute force attempt) T1016, T1570

Attack Preparation

Attack Execution and Exploitation

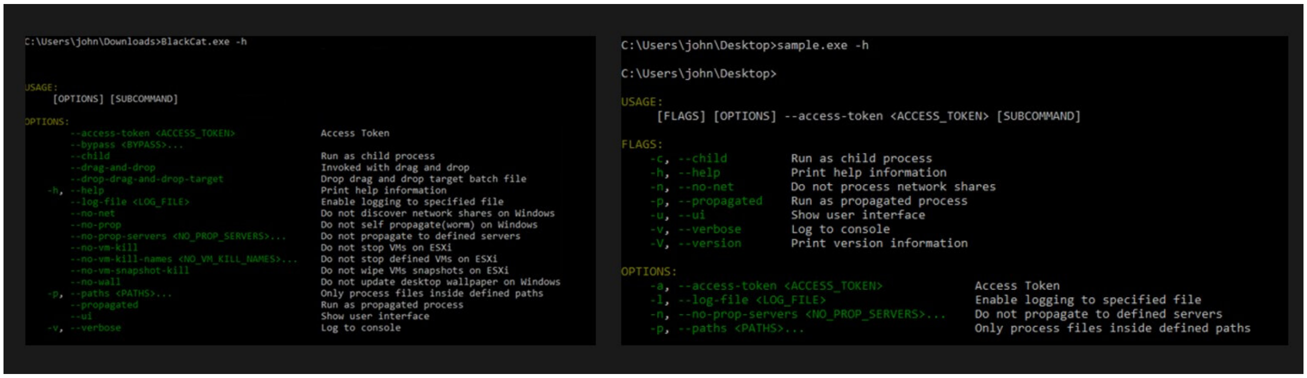
5

Figure 2: Attack Analysis

An analysis of the attack flow shows typical pre-execution and post execution stages of a ransomware incident. The initial access is gained either via leaked credentials or through exposed remote access software. Following this it is clear the threat actor spends a good amount of time compromising various defenses such as Windows Defender , enabling better data exfiltration by increasing connection limits on remote connections, discovering network shares etc. The actual encryption part seems to come at later stage similar to what we have seen with other Ransomware families such as Darkside etc.

Why Is this Important?

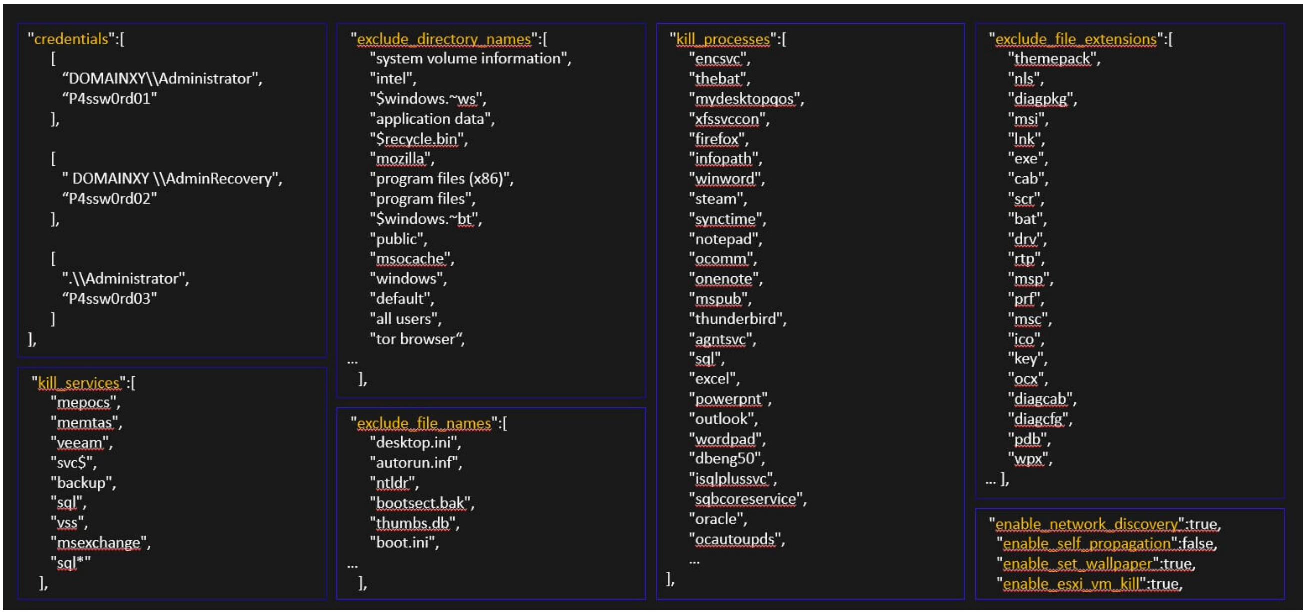
So what makes BlackCat different than previous ransomware as a service operators? the answer is many. This ransomware has been written using a programming language known as "Rust" diverging from common programing languages such as C/C++ in which previous ransomwares has been written in and is more widely understood and analyzed by threat researchers and defenders. The advantage of using "Rust" is maximum platform support in terms of OS that this ransomware can be executed on, potentially hugely widening the exposure for organisations. The next aspect is customization capabilities available in the malware and how it has embedded a lot of disparate capabilities in a modular self-contained package, it even has a help menu! Perfectly suitable for newbie affiliates. The notable capabilities include embedded PsExec, Powershell process migration capabilities and ability to infect VMWare ESXi services. The configuration options shown bellow allows the affiliates to customize how they execute the ransomware in the victims environment.



```
C:\Users\john\Downloads>BlackCat.exe -h


USAGE:
    [OPTIONS] [SUBCOMMAND]

OPTIONS:
        --access-token <ACCESS_TOKEN>                Access Token
        --bypass <BYPASS>...
        --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-kill-names <NO_VM_KILL_NAMES>...     Do not stop defined 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
```

```
C:\Users\john\Desktop>sample.exe -h

C:\Users\john\Desktop>

USAGE:
     [FLAGS] [OPTIONS] --access-token <ACCESS_TOKEN> [SUBCOMMAND]

FLAGS:
    -c, --child         Run as child process
    -h, --help          Print help information
    -n, --no-net        Do not process network shares
    -p, --propagated    Run as propagated process
    -u, --ui            Show user interface
    -v, --verbose       Log to console
    -V, --version       Print version information

OPTIONS:
    -a, --access-token <ACCESS_TOKEN>                Access Token
    -l, --log-file <LOG_FILE>                        Enable logging to specified file
    -n, --no-prop-servers <NO_PROP_SERVERS>...       Do not propagate to defined servers
    -p, --paths <PATHS>...                           Only process files inside defined paths
```

Figure 3: Two different Blackcat Samples showing different capabilities



```
"credentials":[
    [
      “DOMAINXY\\Administrator",
      “P4ssw0rd01"
    ],

    [
      " DOMAINXY \\AdminRecovery",
      “P4ssw0rd02"
    ],

    [
      ".\\Administrator",
      “P4ssw0rd03"
    ]
],

 "kill_services":[
    "mepocs",
    "memtas",
    "veeam",
    "svc$",
    "backup",
    "sql",
    "vss",
    "msexchange",
    "sql*"
  ],

"exclude_directory_names":[
   "system volume information",
   "intel",
   "$windows.~ws",
   "application data",
   "$recycle.bin",
   "mozilla",
   "program files (x86)",
   "program files",
   "$windows.~bt",
   "public",
   "msocache",
   "windows",
   "default",
   "all users",
   "tor browser“,
…
 ],

"exclude_file_names":[
   "desktop.ini",
   "autorun.inf",
   "ntldr",
   "bootsect.bak",
   "thumbs.db",
   "boot.ini",
…
 ],

"kill_processes":[
   "encsvc",
   "thebat",
   "mydesktopqos",
   "xfssvccon",
   "firefox",
   "infopath",
   "winword",
   "steam",
   "synctime",
   "notepad",
   "ocomm",
   "onenote",
   "mspub",
   "thunderbird",
   "agntsvc",
   "sql",
   "excel",
   "powerpnt",
   "outlook",
   "wordpad",
   "dbeng50",
   "isqlplussvc",
   "sqbcoreservice",
   "oracle",
   "ocautoupds",
   …
],

"exclude_file_extensions":[
   "themepack",
   "nls",
   "diagpkg",
   "msi",
   "lnk",
   "exe",
   "cab",
   "scr",
   "bat",
   "drv",
   "rtp",
   "msp",
   "prf",
   "msc",
   "ico",
   "key",
   "ocx",
   "diagcab",
   "diagcfg",
   "pdb",
   "wpx",
… ],

"enable_network_discovery":true,
 "enable_self_propagation":false,
 "enable_set_wallpaper":true,
 "enable_esxi_vm_kill":true,
```

Figure 4: Blackcat embedded configuration file with victim specific data preloaded

The most important aspect is possibly the fact that during analysis we discovered that each sample had configuration files embedded that included information such as Usernames and passwords for the target victims to facilitate lateral movement(potentially gathered from previous breaches or bought password dumps). We also noticed that a unique access token is used to generate an unique victim identifier and a unique link for Blackcat’s “Tor” webpage for the ransomware negotiations to take place. This is specifically designed to keep security researchers and law enforcement out of the conversations as well as defeating some automated sandboxing capabilities that does not inject sample specific attributes.

Defenders Guidance

One of the hardest part of this ransomware family is keeping track of prevalence information. The reason being that almost every sample has a different set of IOC's associated with it(hash, tor url , access tokens, config files). So this is where we have to resort to more advanced behavioral characteristics and properties of the malware.

Establishing relationship between the various samples might be extremely important at an early stage of an attack to understand the threat actor and their associated tactics, a new feature added to Trellix Insights provides just that:

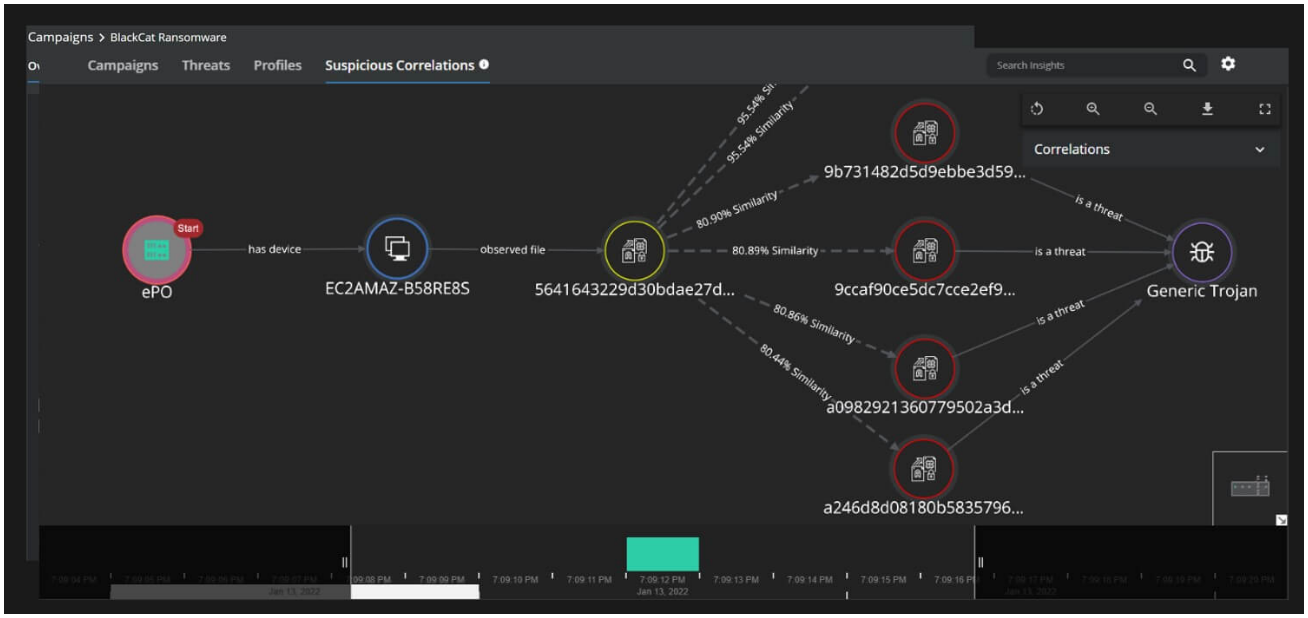
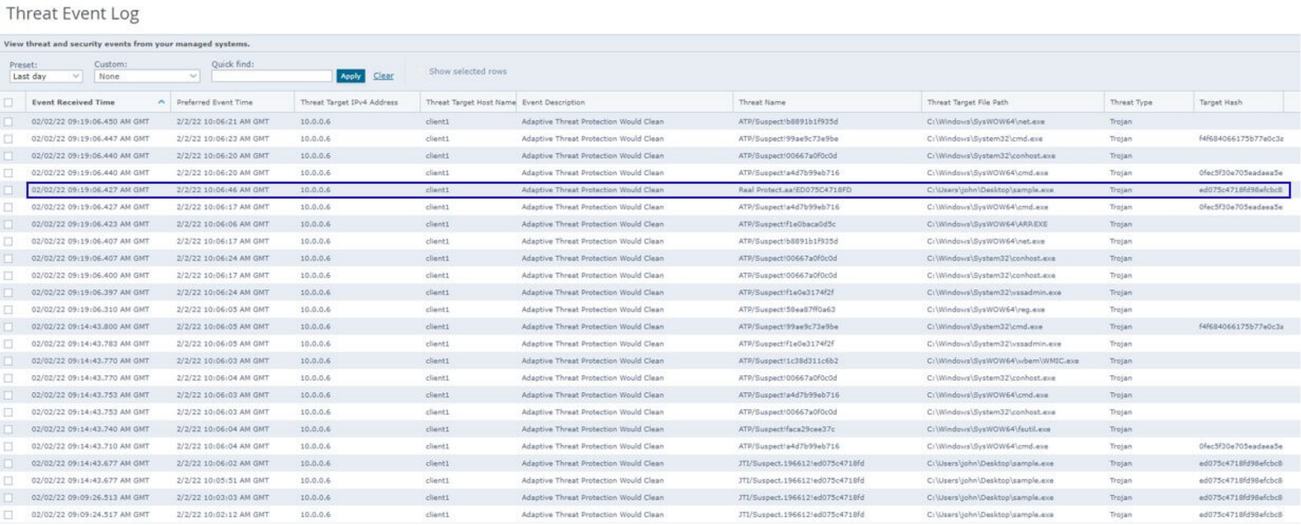


Figure 5: Sample relationship based on similarity and campaign relationship

Like with every ransomware attack the signs of the presence of the threat actor are visible In the early part of the attack lifecycle. Use of LOLBins and Dual Intent tools to land and expand are critical signals that should be captured by defenders, both EDR and ENS ATP provides early visibility Into the pre-execution phase of the attack as well as Post execution phases.

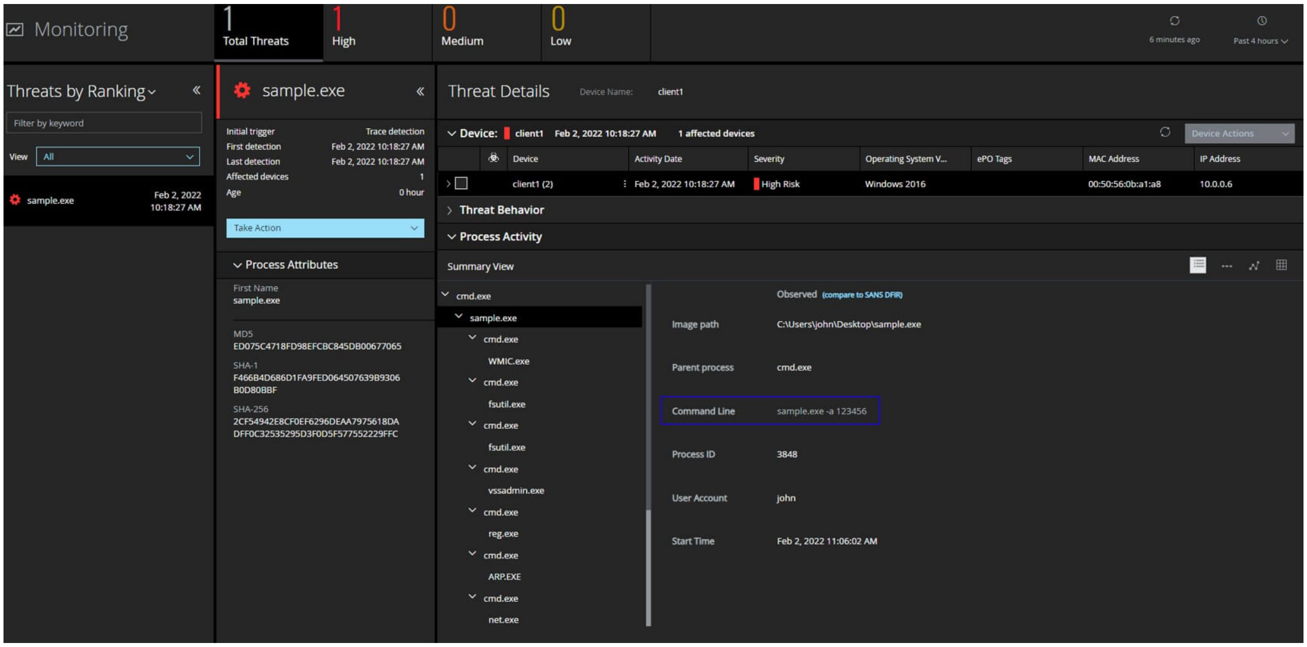

Threat Event Log

View threat and security events from your managed systems.

Preset: Last day
Custom: None
Quick find:
Apply
Clear
Show selected rows

□	Event Received Time	Preferred Event Time	Threat Target IPv4 Address	Threat Target Host Name	Event Description	Threat Name	Threat Target File Path	Threat Type	Target Hash
□	02/02/22 09:19:06.450 AM GMT	2/2/22 10:06:21 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	ATP/Suspect!b8891b1f935d	C:\Windows\SysWOW64\net.exe	Trojan	
□	02/02/22 09:19:06.447 AM GMT	2/2/22 10:06:23 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	ATP/Suspect!99ae9c73e9be	C:\Windows\System32\cmd.exe	Trojan	f4f684066175b77e0c3a
□	02/02/22 09:19:06.440 AM GMT	2/2/22 10:06:20 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	ATP/Suspect!00667a0f0c0d	C:\Windows\System32\conhost.exe	Trojan	
□	02/02/22 09:19:06.440 AM GMT	2/2/22 10:06:20 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	ATP/Suspect!a4d7b99eb716	C:\Windows\SysWOW64\cmd.exe	Trojan	0fec5f30e705eadaea5e
□	02/02/22 09:19:06.427 AM GMT	2/2/22 10:06:46 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	Real Protect.aa!ED075C4718FD	C:\Users\john\Desktop\sample.exe	Trojan	ed075c4718fd98efcbc8
□	02/02/22 09:19:06.427 AM GMT	2/2/22 10:06:17 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	ATP/Suspect!a4d7b99eb716	C:\Windows\SysWOW64\cmd.exe	Trojan	0fec5f30e705eadaea5e
□	02/02/22 09:19:06.423 AM GMT	2/2/22 10:06:06 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	ATP/Suspect!f1e0baca0d5c	C:\Windows\SysWOW64\ARP.EXE	Trojan	
□	02/02/22 09:19:06.407 AM GMT	2/2/22 10:06:17 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	ATP/Suspect!b8891b1f935d	C:\Windows\SysWOW64\net.exe	Trojan	
□	02/02/22 09:19:06.407 AM GMT	2/2/22 10:06:24 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	ATP/Suspect!00667a0f0c0d	C:\Windows\System32\conhost.exe	Trojan	
□	02/02/22 09:19:06.400 AM GMT	2/2/22 10:06:17 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	ATP/Suspect!00667a0f0c0d	C:\Windows\System32\conhost.exe	Trojan	
□	02/02/22 09:19:06.397 AM GMT	2/2/22 10:06:24 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	ATP/Suspect!f1e0e3174f2f	C:\Windows\System32\vssadmin.exe	Trojan	
□	02/02/22 09:19:06.310 AM GMT	2/2/22 10:06:05 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	ATP/Suspect!58ea87ff0a63	C:\Windows\SysWOW64\reg.exe	Trojan	
□	02/02/22 09:14:43.800 AM GMT	2/2/22 10:06:05 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	ATP/Suspect!99ae9c73e9be	C:\Windows\System32\cmd.exe	Trojan	f4f684066175b77e0c3a
□	02/02/22 09:14:43.783 AM GMT	2/2/22 10:06:05 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	ATP/Suspect!f1e0e3174f2f	C:\Windows\System32\vssadmin.exe	Trojan	
□	02/02/22 09:14:43.770 AM GMT	2/2/22 10:06:03 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	ATP/Suspect!1c38d311c6b2	C:\Windows\SysWOW64\wbem\WMIC.exe	Trojan	
□	02/02/22 09:14:43.770 AM GMT	2/2/22 10:06:04 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	ATP/Suspect!00667a0f0c0d	C:\Windows\System32\conhost.exe	Trojan	
□	02/02/22 09:14:43.753 AM GMT	2/2/22 10:06:03 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	ATP/Suspect!a4d7b99eb716	C:\Windows\SysWOW64\cmd.exe	Trojan	
□	02/02/22 09:14:43.753 AM GMT	2/2/22 10:06:03 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	ATP/Suspect!00667a0f0c0d	C:\Windows\System32\conhost.exe	Trojan	
□	02/02/22 09:14:43.740 AM GMT	2/2/22 10:06:04 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	ATP/Suspect!faca29cee37c	C:\Windows\SysWOW64\fsutil.exe	Trojan	
□	02/02/22 09:14:43.710 AM GMT	2/2/22 10:06:04 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	ATP/Suspect!a4d7b99eb716	C:\Windows\SysWOW64\cmd.exe	Trojan	0fec5f30e705eadaea5e
□	02/02/22 09:14:43.677 AM GMT	2/2/22 10:06:02 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	JTI/Suspect.196612!ed075c4718fd	C:\Users\john\Desktop\sample.exe	Trojan	ed075c4718fd98efcbc8
□	02/02/22 09:14:43.677 AM GMT	2/2/22 10:05:51 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	JTI/Suspect.196612!ed075c4718fd	C:\Users\john\Desktop\sample.exe	Trojan	ed075c4718fd98efcbc8
□	02/02/22 09:09:26.513 AM GMT	2/2/22 10:03:03 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	JTI/Suspect.196612!ed075c4718fd	C:\Users\john\Desktop\sample.exe	Trojan	ed075c4718fd98efcbc8
□	02/02/22 09:09:24.517 AM GMT	2/2/22 10:02:12 AM GMT	10.0.0.6	client1	Adaptive Threat Protection Would Clean	JTI/Suspect.196612!ed075c4718fd	C:\Users\john\Desktop\sample.exe	Trojan	ed075c4718fd98efcbc8

Figure 6: Post Execution ENS ATP Detections for RealProtect



View: All

sample.exe Feb 2, 2022 10:18:27 AM

sample.exe

Initial trigger	Trace detection
First detection	Feb 2, 2022 10:18:27 AM
Last detection	Feb 2, 2022 10:18:27 AM
Affected devices	1
Age	0 hour

Process Attributes

First Name: sample.exe

MD5: ED075C4718FD98EFCBC845DB00677065

SHA-1: F466B4D686D1FA9FED064507639B9306B0D80BBF

SHA-256: 2CF54942E8CF0EF6296DEAA7975618DADFF0C32535295D3F0D5F577552229FFC

Threat Details — Device Name: client1

Device: client1 Feb 2, 2022 10:18:27 AM 1 affected devices

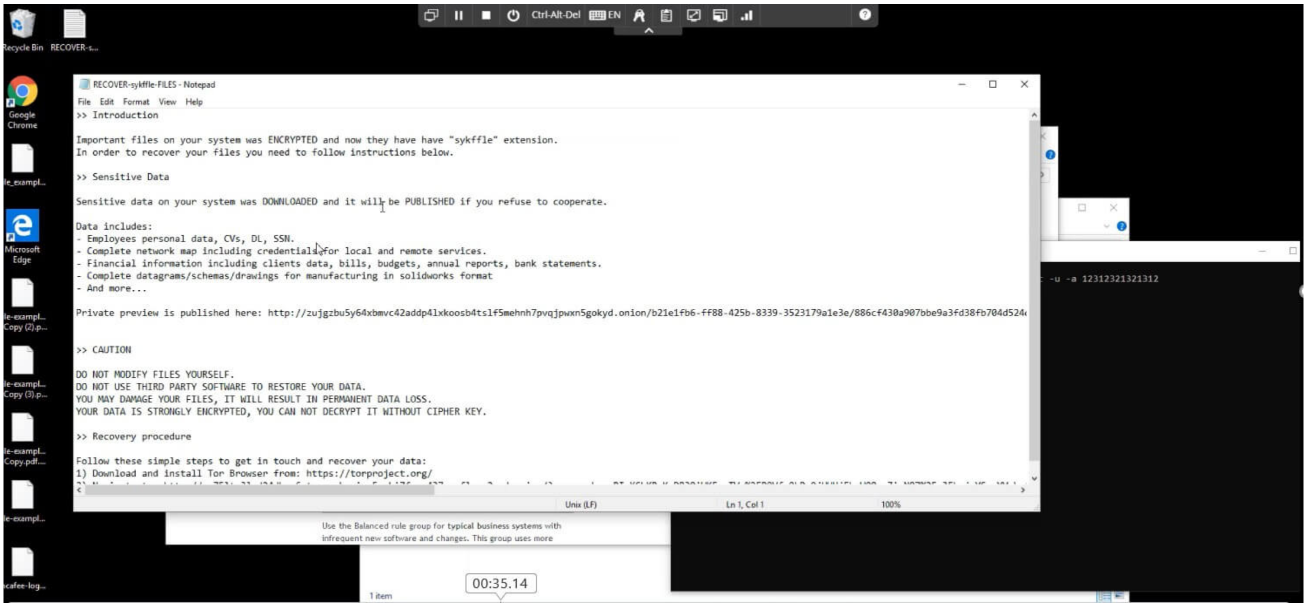
Device	Activity Date	Severity	Operating System V...	ePO Tags	MAC Address	IP Address
client1 (2)	Feb 2, 2022 10:18:27 AM	🟥 High Risk	Windows 2016		00:50:56:0b:a1:a8	10.0.0.6

```
cmd.exe
  sample.exe
    cmd.exe
      WMIC.exe
    cmd.exe
      fsutil.exe
    cmd.exe
      fsutil.exe
    cmd.exe
      vssadmin.exe
    cmd.exe
      reg.exe
    cmd.exe
      ARP.EXE
    cmd.exe
      net.exe
```

	Observed (compare to SANS DFIR)
Image path	C:\Users\john\Desktop\sample.exe
Parent process	cmd.exe
Command Line	sample.exe -a 123456
Process ID	3848
User Account	john
Start Time	Feb 2, 2022 11:06:02 AM

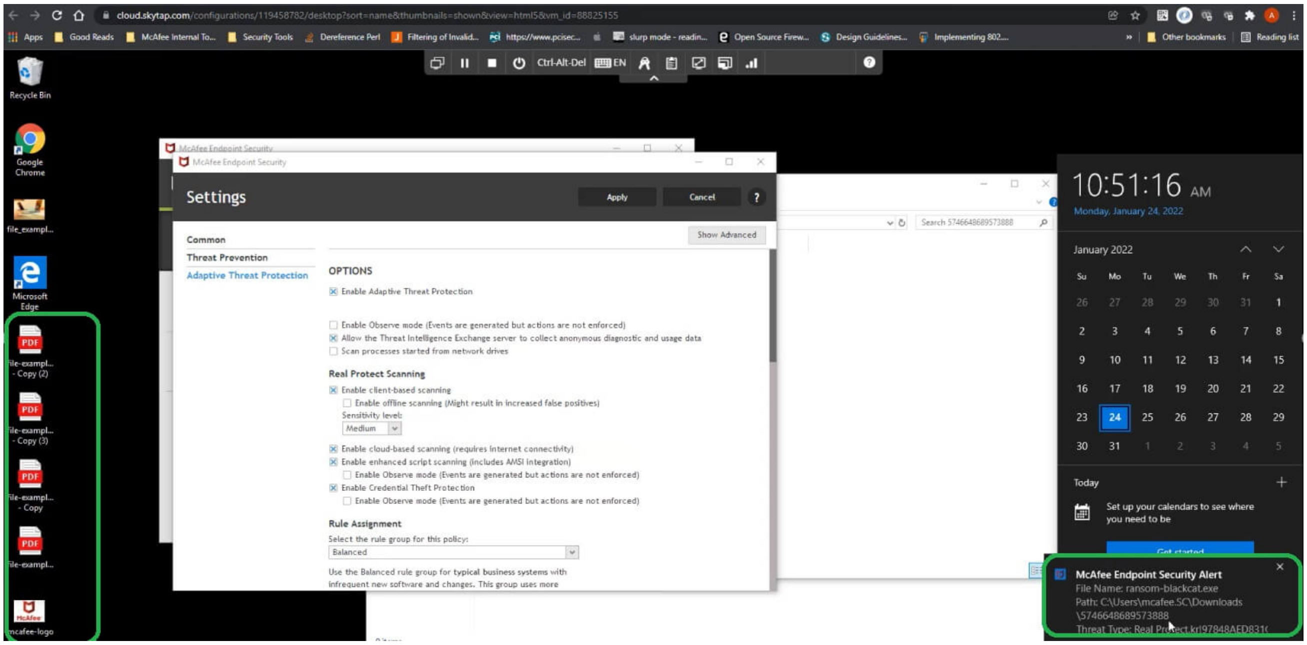
Figure 7: EDR Analysis of Blackcat Sample

Point to be noted here is that depending on the sample the data collected EDR trace analysis could appear differently. Having behavioral analysis and protection capabilities is critical for defenders during our testing both ENS Realprotect static and cloud got trigged and Enhanced remediation recovered the encrypted systems successfully.


Ctrl-Alt-Del
EN
Recycle Bin
RECOVER-s...
Google Chrome
Microsoft Edge
le-exampl...
le-exampl... Copy (2).p...
le-exampl... Copy (3).p...
le-exampl... Copy.pdf....
le-exampl...
cafee-log...
RECOVER-sykffle-FILES - Notepad
File Edit Format View Help
Unix (LF)
Ln 1, Col 1
100%
Use the Balanced rule group for typical business systems with infrequent new software and changes. This group uses more
00:35.14
1 item
-u -a 12312321321312

```
>> Introduction

Important files on your system was ENCRYPTED and now they have have "sykffle" extension.
In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your system was DOWNLOADED and it will be PUBLISHED if you refuse to cooperate.

Data includes:
- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Financial information including clients data, bills, budgets, annual reports, bank statements.
- Complete datagrams/schemas/drawings for manufacturing in solidworks format
- And more...

Private preview is published here: http://zujgzbu5y64xbmvc42addp4lxkoosb4tslf5mehnh7pvqjpwxn5gokyd.onion/b21e1fb6-ff88-425b-8339-3523179a1e3e/886cf430a907bbe9a3fd38fb704d524


>> CAUTION

DO NOT MODIFY FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.
YOUR DATA IS STRONGLY ENCRYPTED, YOU CAN NOT DECRYPT IT WITHOUT CIPHER KEY.

>> Recovery procedure

Follow these simple steps to get in touch and recover your data:
1) Download and install Tor Browser from: https://torproject.org/
```

Figure 8: Encrypted Endpoint



McAfee Endpoint Security

Settings

Apply | Cancel | ?

Common

Threat Prevention

Adaptive Threat Protection

Show Advanced

OPTIONS

☒ Enable Adaptive Threat Protection

□ Enable Observe mode (Events are generated but actions are not enforced)
☒ Allow the Threat Intelligence Exchange server to collect anonymous diagnostic and usage data
□ Scan processes started from network drives

Real Protect Scanning

☒ Enable client-based scanning
□ Enable offline scanning (Might result in increased false positives)
Sensitivity level:
Medium

☒ Enable cloud-based scanning (requires internet connectivity)
☒ Enable enhanced script scanning (includes AMSI integration)
□ Enable Observe mode (Events are generated but actions are not enforced)
☒ Enable Credential Theft Protection
□ Enable Observe mode (Events are generated but actions are not enforced)

Rule Assignment

Select the rule group for this policy:
Balanced

Use the Balanced rule group for typical business systems with infrequent new software and changes. This group uses more

Today

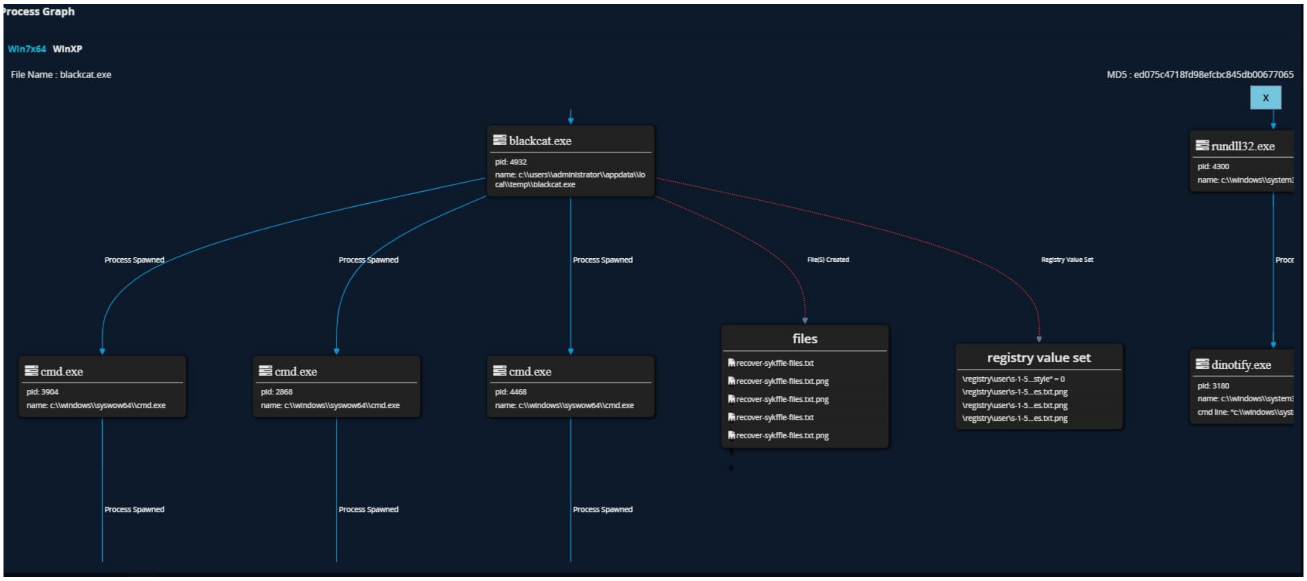
Set up your calendars to see where you need to be

Get started

McAfee Endpoint Security Alert
File Name: ransom-blackcat.exe
Path: C:\Users\mcafee.SC\Downloads\5746648689573888
Threat Type: Real Protect.krl97848AED831(

Figure 9: Endpoint Rolled Back

Being able to analyze threats fully and understand its behavior is crucial especially in a malware that is changing its attributes rapidly, Trellix Detection on Demand provides additional sampling capability along with endpoint integration to further enhance defenses and detection capabilities.



Process Graph
Win7x64
WinXP
File Name : blackcat.exe
MD5 : ed075c4718fd98efcbc845db00677065
X
blackcat.exe
pid: 4932
name: c:\\users\\administrator\\appdata\\local\\temp\\blackcat.exe
rundll32.exe
pid: 4300
name: c:\\windows\\system3
Process Spawned
Process Spawned
Process Spawned
File(S) Created
Registry Value Set
Proce
cmd.exe
pid: 3904
name: c:\\windows\\syswow64\\cmd.exe
cmd.exe
pid: 2868
name: c:\\windows\\syswow64\\cmd.exe
cmd.exe
pid: 4468
name: c:\\windows\\syswow64\\cmd.exe
files
recover-sykffle-files.txt
recover-sykffle-files.txt.png
recover-sykffle-files.txt.png
recover-sykffle-files.txt
recover-sykffle-files.txt.png
registry value set
\registry\user\s-1-5...style" = 0
\registry\user\s-1-5...es.txt.png
\registry\user\s-1-5...es.txt.png
\registry\user\s-1-5...es.txt.png
dinotify.exe
pid: 3180
name: c:\\windows\\system3
cmd line: "c:\\windows\\syst
Process Spawned
Process Spawned
Process Spawned

Figure 10: Trellix Detection on Demand analysis providing additional details, dropped payloads and registry changes as well as complete behavioral analysis

Summary

Organisations need to build resilient defenses against ransomware threats and not rely on single control/defenses, we can expect to continue to see more innovation from threat actors such as the ones highlighted here, fundamentally the following provides an effective security strategy against ransomware threats

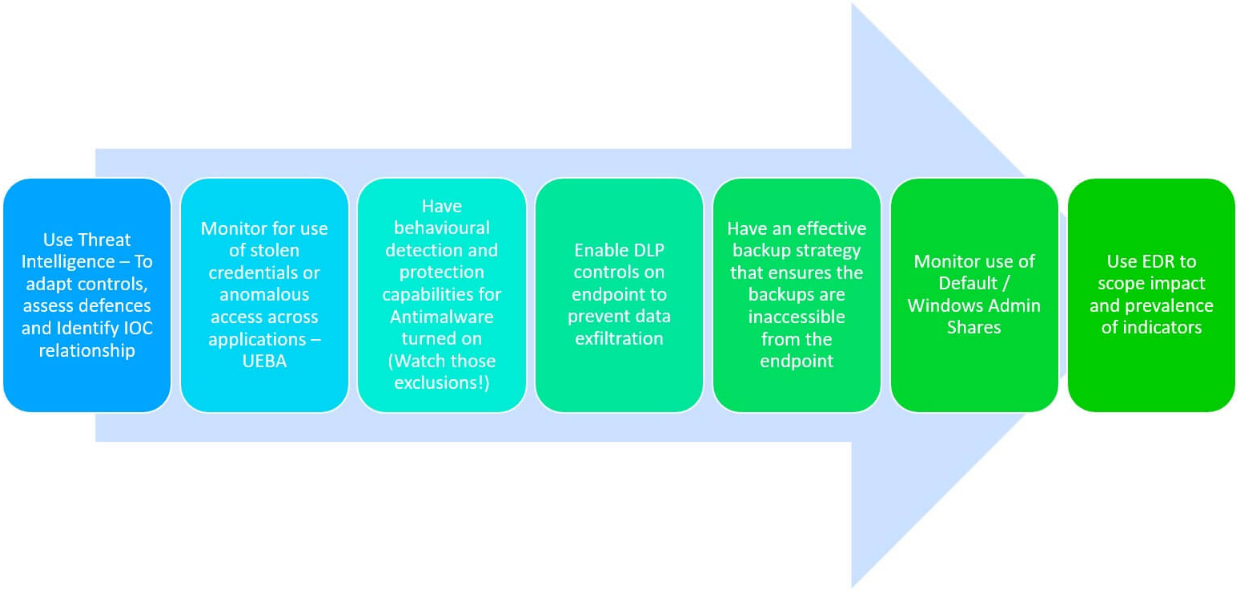

Use Threat Intelligence – To adapt controls, assess defences and Identify IOC relationship
Monitor for use of stolen credentials or anomalous access across applications – UEBA
Have behavioural detection and protection capabilities for Antimalware turned on (Watch those exclusions!)
Enable DLP controls on endpoint to prevent data exfiltration
Have an effective backup strategy that ensures the backups are inaccessible from the endpoint
Monitor use of Default / Windows Admin Shares
Use EDR to scope impact and prevalence of indicators

Figure 11: Ransomware Defense Strategy

Featured Content

PERSPECTIVES

Our CEO On Living Security

By Bryan Palma · January 19, 2022

Trellix CEO, Bryan Palma, explains the critical need for security that's always learning.

Read More

XDR

Time to Drive Change by Challenging the Challengers

By Michelle Salvado · January 19, 2022

Dynamic threats call for dynamic security – the path to resiliency lies in XDR.

Read More

THREAT LABS

2022 Threat Predictions

By Trellix · January 19, 2022

What cyber security threats should enterprises look out for in 2022?

Read More