Royal & BlackCat Ransomware: The Threat to the Health Sector

January 12, 2023

TLP:CLEAR, ID# 202301131300

https://nmlearning.net

Royal and BlackCat Ransomware

The U.S. health sector continues to be aggressively targeted by ransomware operators, and Royal and BlackCat are two of the more recent sophisticated ransomware threats.

- Royal Ransomware
  - Background
  - Targeting
  - Technical analysis
  - Encryption process
- BlackCat Ransomware
  - Background
  - Targeting
  - Technical analysis
  - Encryption process
- Defense and Mitigations
- References

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

https://t.me/learningnets

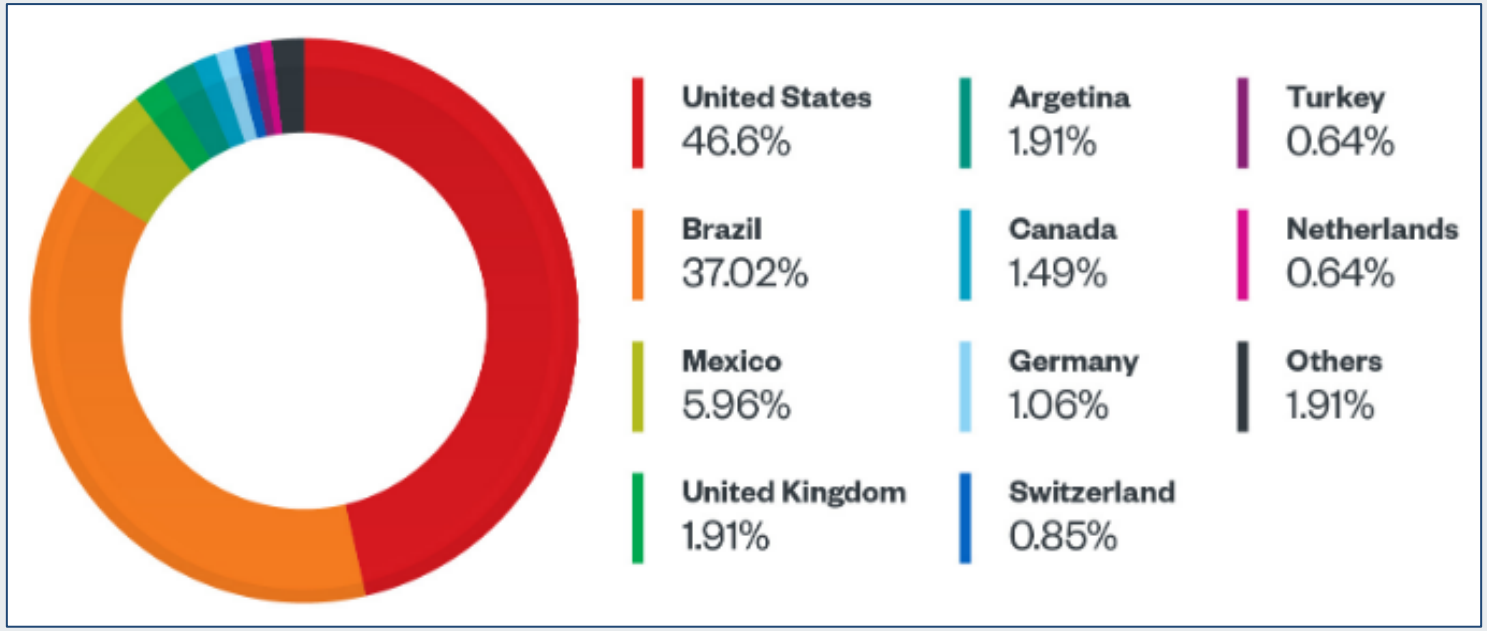
Royal Ransomware

A relatively new, but highly capable ransomware threat to the health sector

https://t.me/learningnets

What is Royal Ransomware?

- First observed in early 2022
- Believed to have very experienced operators, previously belonging to other infamous cybercriminal groups including Conti Team One
- The United States tops the victim list
- 64-bit executable
- Written in C++
- Targets Windows systems
- Encrypts files and appends ".royal or ".royal_w" extensions to filenames; creates "README.TXT" ransom note

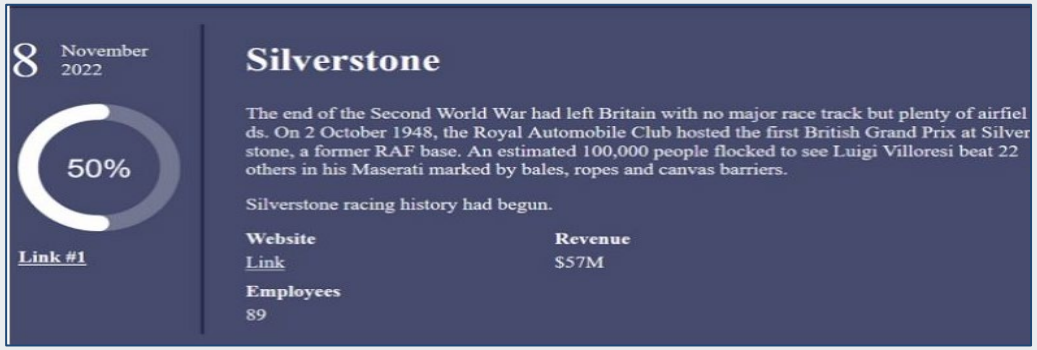


Percentage of Royal Ransomware Attacks by Country
Courtesy: Trend Macro

Background

Royal Ransomware attacks have surged across the globe, with U.S. entities as their top target. Some notable attacks by Royal are:

- ***Silverstone Circuit*** – Researchers observed Royal using ransomware operation's encryptors, such as BlackCat, in September 2022. In November 2022, Royal claimed responsibility for the ransomware attack against Silverstone Circuit, the UK's most popular racing circuit.
- ***Travis Central Appraisal District*** – In December 2022, Royal struck again with a ransomware attack against this agency that provides appraisal values for properties, shutting down their website, email and servers for over two weeks.



Royal Ransomware website snapshot showing a victim organization.
Source: Cybereason

https://t.me/learningnets

Background, Part 2

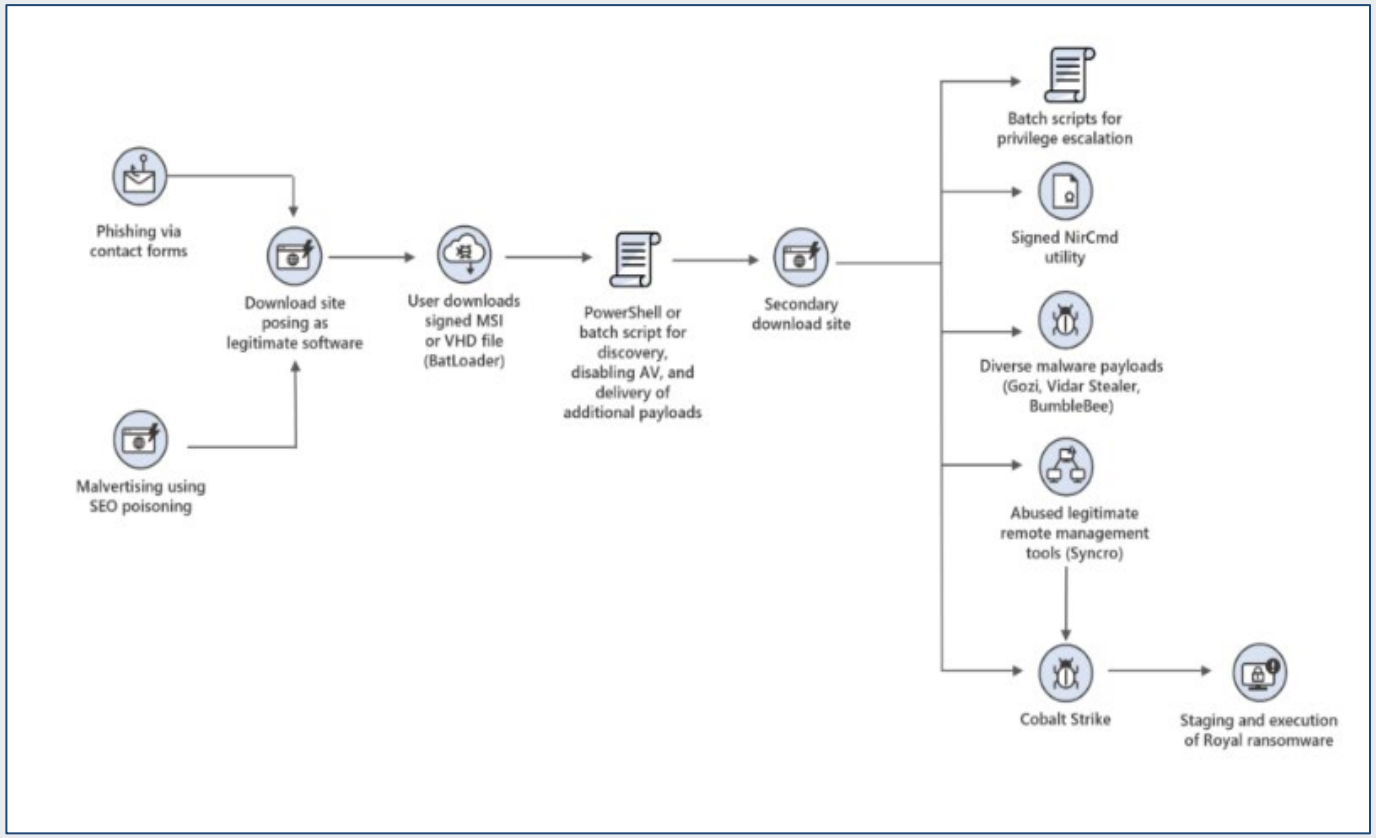
- *An unnamed U.S. telecom organization* – In December 2022, this company's internal documents, including employee passports and driver's licenses, were stolen through compromised work devices.
  - The initial breach by Royal Ransomware occurred on December 1st.
  - December 1st: The targeted U.S. telecom organization also experienced an outage that impacted all of their services, including Healthcare, Unified Communication Services, and Unified Communications as a Service.
  - Royal claimed responsibility for this attack and reportedly demanded $60 million.

Royal Ransomware website snapshot showing a U.S. telecom company as a victim. *Source: Bleeping Computer*

https://t.me/learningnets

Background, Part 3

- Since September 2022, Royal has begun deploying its own ransomware.
- In November 2022, Royal surpassed Lockbit to become the most notorious ransomware.
- Royal Ransomware operations start in various ways, including through phishing campaigns using common cyber crime threat loaders, such as BATLOADER and QBot.
- Following initial infection, Royal often leverages Cobalt Strike, QBot and BlackBasta for multi-stage attacks.
- Reports identified resemblances between the Royal Ransomware group and Conti, including the use of callback phishing attacks and both groups' ransom notes (in Royal's early stages).



High-level view of observed DEV-0569 infection chains between August – October 2022.
Source: Microsoft

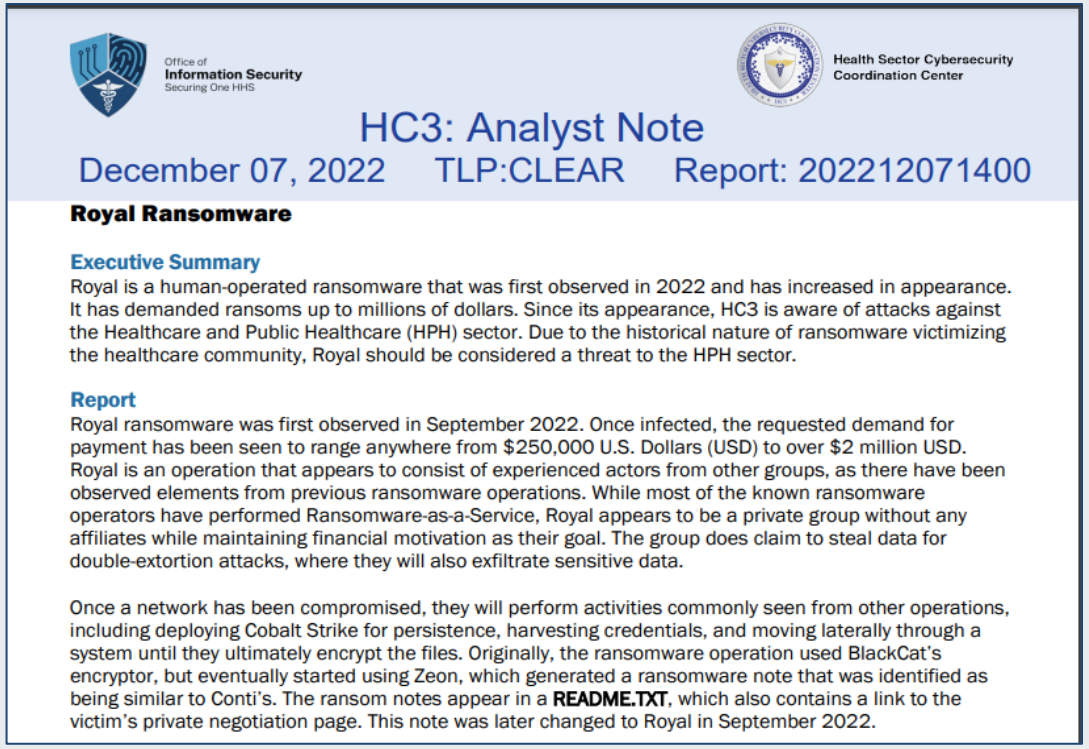
https://t.me/learningnets

Impact on Healthcare

Royal ransomware is a significant threat to the Healthcare and Public Health (HPH) sector due to the group victimizing the healthcare community.

HC3's Royal Ransomware Analyst Note:

- Royal appears to be a private group without any affiliates, maintaining financial motivation as their goal.
- Ransom demands range from $250,000 to over $2 million USD.
- The group will conduct methods seen from other operations, including deploying Cobalt Strike for persistence, harvesting credentials, and moving laterally through a system until files are encrypted.



Office of Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

HC3: Analyst Note

December 07, 2022 TLP:CLEAR Report: 202212071400

Royal Ransomware

Executive Summary

Royal is a human-operated ransomware that was first observed in 2022 and has increased in appearance. It has demanded ransoms up to millions of dollars. Since its appearance, HC3 is aware of attacks against the Healthcare and Public Healthcare (HPH) sector. Due to the historical nature of ransomware victimizing the healthcare community, Royal should be considered a threat to the HPH sector.

Report

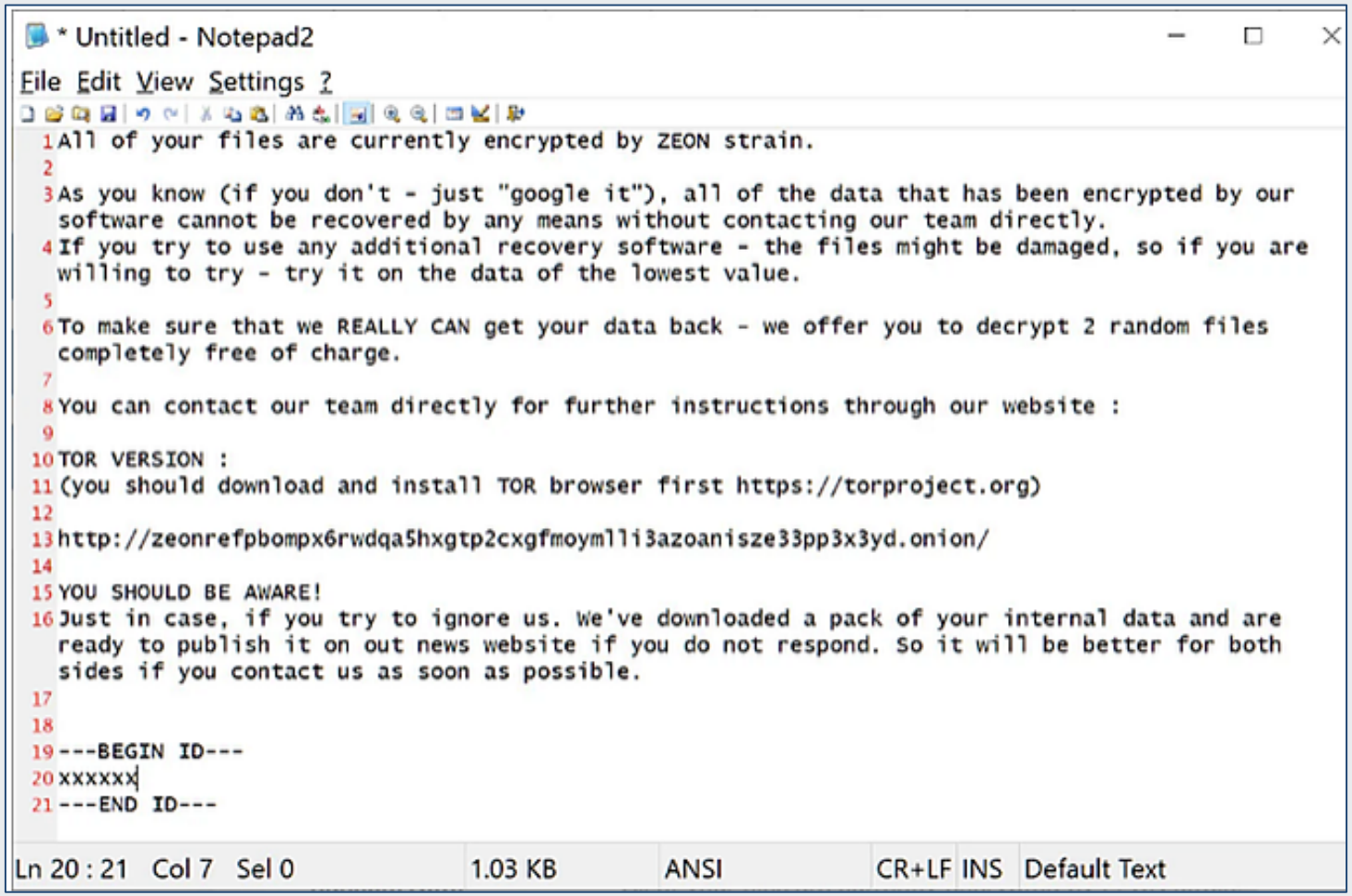
Royal ransomware was first observed in September 2022. Once infected, the requested demand for payment has been seen to range anywhere from $250,000 U.S. Dollars (USD) to over $2 million USD. Royal is an operation that appears to consist of experienced actors from other groups, as there have been observed elements from previous ransomware operations. While most of the known ransomware operators have performed Ransomware-as-a-Service, Royal appears to be a private group without any affiliates while maintaining financial motivation as their goal. The group does claim to steal data for double-extortion attacks, where they will also exfiltrate sensitive data.

Once a network has been compromised, they will perform activities commonly seen from other operations, including deploying Cobalt Strike for persistence, harvesting credentials, and moving laterally through a system until they ultimately encrypt the files. Originally, the ransomware operation used BlackCat's encryptor, but eventually started using Zeon, which generated a ransomware note that was identified as being similar to Conti's. The ransom notes appear in a **README.TXT**, which also contains a link to the victim's private negotiation page. This note was later changed to Royal in September 2022.

https://t.me/learningnets

Impact on Healthcare, Part 2

- Originally used BlackCat's encryptor, then transitioned to their own Zeon encryptor that generates a ransomware note similar to the Conti group (known to target the health sector).
- October 2022: Threat actors behind Zeon encryptor impersonate healthcare patient data software.
- Stolen data is used for double-extortion attacks, where the group will also exfiltrate sensitive data.
- The ransomware deletes all Volume Shadow Copies that provide point-in-time copy of a file.



A Zeon ransomware note.
Source: Bleeping Computer

https://t.me/learningnets

Key Findings

- Unique approach to evade anti-ransomware defenses
- Multi-threaded ransomware
- Global ransomware operation
- Different methods of deployment

README.TXT - Notepad2

File Edit View Settings ?

```
Hello!

  If you are reading this, it means that your system were hit by Royal ransomware.
  Please contact us via :
  http://royal2xthig3ou5hd7zsliqagy6yygk2cdelaxtni2fyad6dpmpxedid.onion/xxx

In the meantime, let us explain this case.It may seem complicated, but it is not!
Most likely what happened was that you decided to save some money on your security infrastructure.
Alas, as a result your critical data was not only encrypted but also copied from your systems on a
secure server.
From there it can be published online.Then anyone on the internet from darknet criminals, ACLU
journalists, Chinese government(different names for the same thing),
and even your employees will be able to see your internal documentation: personal data, HR reviews,
internal lawsuitsand complains, financial reports, accounting, intellectual property, and more!

  Fortunately we got you covered!

Royal offers you a unique deal.For a modest royalty(got it; got it ? ) for our pentesting services we
will not only provide you with an amazing risk mitigation service,
covering you from reputational, legal, financial, regulatory, and insurance risks, but will also
provide you with a security review for your systems.
To put it simply, your files will be decrypted, your data restoredand kept confidential, and your
systems will remain secure.

  Try Royal today and enter the new era of data security!
  We are looking to hearing from you soon!
```

Ln 20 : 20 Col 43 Sel 0 | 1.41 KB | ANSI | CR+LF | INS | Default Text

Royal's newly-branded ransomware note.
Source: Bleeping Computer

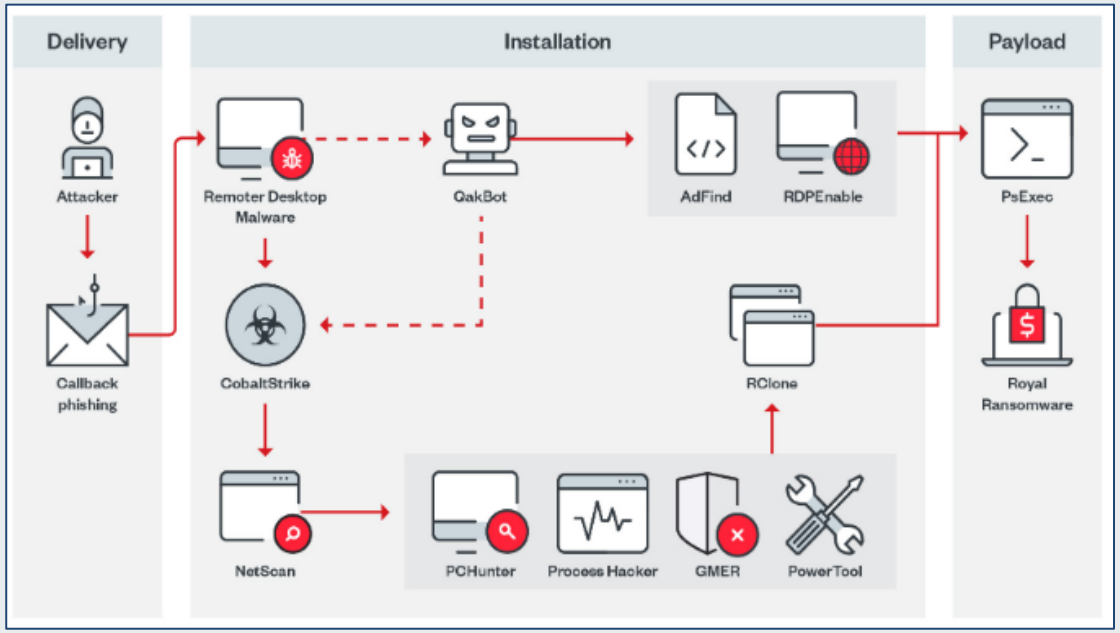
https://t.me/learningnets

Tactics & Techniques

Initially attributed to Dev-0569, Royal Ransomware is distributed by seasoned threat actors, and attacks that use it indicate a pattern of continuous innovation.

Delivery methods include:

- Using Google Ads in a campaign to blend in with normal ad traffic.
- Making malicious downloads appear authentic by hosting fake installer files on legitimate-looking software download sites.
- Using contact forms located on an organization's website to distribute phishing links.

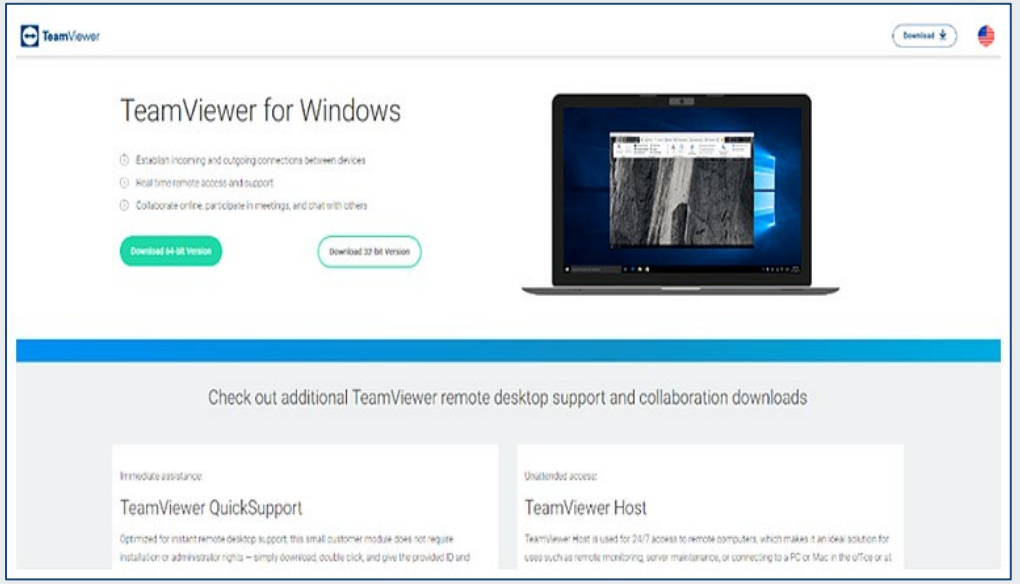


Royal Ransomware's attack flow.
Source: Trend Micro

https://t.me/learningnets

Tactics & Techniques, Part 2

- Per Microsoft, Royal uses signed binaries and delivers encrypted malware payloads – relying heavily on defense evasion techniques.
- Leverages open-source tool, *Nsudo*, to disable antivirus solutions.
- Sends malicious links to victim to gain initial access; victims are directed to malicious files signed by Royal using a legitimate certificate.
- Malicious files appear as installers or updates for legitimate applications, such as Microsoft Teams or Zoom.
- Once applications are launched, BATLOADER uses MSI Custom Actions to launch malicious PowerShell activity and to run batch scripts attempting to disable security solutions, delivering encrypted malware payloads.
- Hosts BATLOADER on attacker-created domains disguised as software download sites such as anydeskos[.]com, GitHub and One Drive.



BATLOADER Masquerading as Teamviewer Installer.
Source: Microsoft

https://t.me/learningnets

Technical Analysis: Setting Up The Ransomware

Royal Ransomware can take three arguments in its command line:

- -path [optional]: The path to be encrypted
- -ep [optional]: The number that represents the percentage of the file that will be encrypted
- -id: A 32-digit array

```
pNumArgs = 0;
v4 = GetCommandLineW();
v5 = CommandLineToArgvW(v4, &pNumArgs);
v6 = 50;
v7 = 0i64;
v8 = 0;
v21 = 0;
*MultiByteStr = 0i64;
for ( i = 0i64; v8 < pNumArgs; ++v5 )
{
  if ( lstrcmpW(*v5, L"-path") )
  {
    if ( lstrcmpW(*v5, L"-id") )
    {
      if ( !lstrcmpW(*v5, L"-ep") )
      {
        v11 = v5[1];
        ++v5;
        ++v8;
        v6 = unknown_libname_21(v11);
        if ( (v6 - 1) > 0x63 )
          v6 = 50;
      }
    }
    else
```

Arguments accepted by Royal Ransomware binary.
Source: TrendMicro

https://t.me/learningnets

Technical Analysis: Setting Up The Ransomware, Part 2

After the command line is validated, Royal attempts to delete shadow copy backups using the process Vssadmin.exe, with the command line “delete shadows /all /quiet.”

```
wsprintfW(CommandLine, L" delete shadows /all /quiet");
StartupInfo.cb = 104;
memset(&StartupInfo.cb + 1, 0, 100);
memset(&ProcessInformation, 0, sizeof(ProcessInformation));
if ( CreateProcessW(
        L"C:\\Windows\\System32\\vssadmin.exe",
        CommandLine,
        0i64,
        0i64,
        0,
        0,
        0i64,
        0i64,
        &StartupInfo,
        &ProcessInformation) )
```

Royal ransomware deleting shadow copies.
Source: Cybereason

https://t.me/learningnets

Technical Analysis: Setting Up The Ransomware, Part 3

Royal Ransomware will set its exclusion paths to indicate files or directories that will be excluded from encryption.

```
sub_14007CD00(&v47, 8ui64, v30, L"perflogs");
v37 = a1[87];
if ( v37 == a1[88] )
{
  e_add_to_array_sub_14007E260(a1 + 86, v37, &v47);// add perflogs



e_exclude_directories_sub_14007C9F0(&v47, L"tor browser", v41);
sub_14007E050(a1 + 86, &v47);
unknown_libname_4(&v47);
e_exclude_directories_sub_14007C9F0(&v47, L"boot", v42);
sub_14007E050(a1 + 86, &v47);
unknown_libname_4(&v47);
e_exclude_directories_sub_14007C9F0(&v47, L"$windows.~ws", v43);
sub_14007E050(a1 + 86, &v47);
unknown_libname_4(&v47);
e_exclude_directories_sub_14007C9F0(&v47, L"$windows.~bt", v44);
sub_14007E050(a1 + 86, &v47);
unknown_libname_4(&v47);
e_exclude_directories_sub_14007C9F0(&v47, L"windows.old", v45);
```

Royal ransomware setting the directories exclusion list.
Source: Cybereason

Technical Analysis: Network Scanner

The following steps occur, if no path is given in command line arguments:

- Royal will scan network interfaces, searching for and retrieving for the target machine(s), using the API call GetIpAddrTable.
- Royal will establish a socket using the API WSASocketW, associating it with a completion port using CreateIoCompletionPort, use API call htons to set the port to SMB, and attempt connection to the instructed IP addresses via the LPFN_CONNECTEX callback function:

```
if ( !GetIpAddrTable(var_pIpAddrTable, &pdwSize, 0) )// retrieves the interface-to-IPv4 address mapping table
{
  v4 = 0;
  v18 = 0;
  if ( var_pIpAddrTable->dwNumEntries )
  {
    p_dwAddr = &var_pIpAddrTable->table[0].dwAddr;
    do
    {
      p_dwMask = p_dwAddr[2];
      v7 = p_dwMask & *p_dwAddr;
      v8 = *p_dwAddr | ~p_dwMask;          // search for IP addresses that starts with "192. \ 10. \ 100. \ 172."
      if ( v7 == 192 && (v7 & 0xFF00) == 0xA800 || v7 == 10 || v7 == 100 || v7 == 172 )
```

Network Scanning
Source: Cybereason

https://t.me/learningnets

Technical Analysis: Network Scanner, Part 2

- Ransomware will use API call NetShareEnum to enumerate shared resources of given IP addresses; if “\\<IP_Address>\ADMIN$” or “\\<IP_Address>\IPC$” will not be encrypted.

```
WSAAddressToStringW(&saAddress, 0x10u, 0i64, szAddressString, &dwAddressStringLength);
do
{
  entriesread = 0;
  totalentries = 0;
  resume_handle = 0;
  var_shared_bufptr = 0i64;
  v4 = NetShareEnum(                    // retrieve information about its shared resources
         szAddressString,
         1u,
         &var_shared_bufptr,
         0xFFFFFFFF,
         &entriesread,
         &totalentries,
         &resume_handle);
  v5 = v4;
  if ( v4 && v4 != 0xEA )
    break;
  tmp_ShareInfoBuffer = var_shared_bufptr;
  v7 = 1;
  if ( entriesread )
  {
    do
    {
      if ( lstrcmpiW(L"ADMIN$", *tmp_ShareInfoBuffer) && lstrcmpiW(L"IPC$", *tmp_ShareInfoBuffer) )
      {
        wsprintfW(&var_remote_share_path, L"\\\\%s\\%s", szAddressString, *tmp_ShareInfoBuffer);
```

Enumerating network resources and avoiding ADMIN$ and IPC$ file shares.
Source: Cybereason

https://t.me/learningnets

Technical Analysis: Encryption Thread

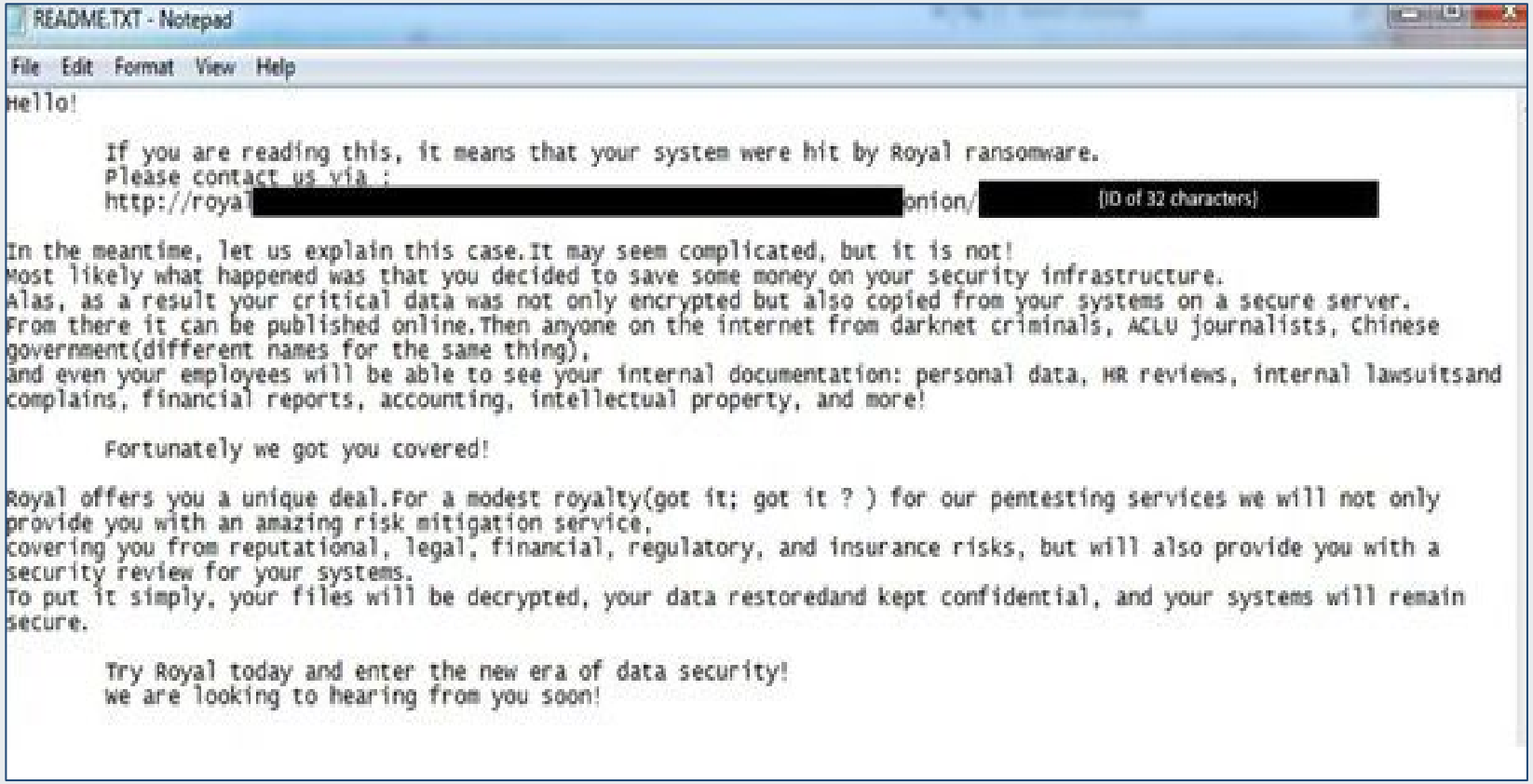
Royal Ransomware's encryption process is multi-threaded. The number of running threads is selected by using API call GetNativeSystemInfo to collect the number of processors in a machine. The result is multiplied by two and the number of threads is created.

```
  ProcessId = GetProcessId(CurrentProcess);
  Toolhelp32Snapshot = CreateToolhelp32Snapshot(2u, 0);
  v10 = Toolhelp32Snapshot;
  if ( Toolhelp32Snapshot == -1i64 )
    goto LABEL_16;
  pe.dwSize = 568;
  if ( !Process32FirstW(Toolhelp32Snapshot, &pe) || !Process32NextW(v10, &pe) )
  {
LABEL_15:
    CloseHandle(v10);
LABEL_16:
    th32ProcessID = 0;
    goto LABEL_17;
  }
  while ( lstrcmpiW(pe.szExeFile, L"explorer.exe") )// check if explorer.exe
  {
    if ( !Process32NextW(v10, &pe) )
      goto LABEL_15;
  }
  CloseHandle(v10);
  th32ProcessID = pe.th32ProcessID;
LABEL_17:
  v12 = 0;
  if ( pnProcInfo )
  {
    v13 = v6;
    while ( v13->Process.dwProcessId != ProcessId && v13->Process.dwProcessId != th32ProcessID )
    {
      ++v12;
      ++v13;
      if ( v12 >= pnProcInfo )
        goto LABEL_22;
    }
    goto LABEL_29;
  }
LABEL_22:
  v14 = RmShutdown(pSessionHandle, 1u, 0i64);   // killing the process
```

Royal Ransomware killing processes.
Source: Cybereason

Technical Analysis: Writing Ransom Note

During the entire Royal Ransomware process, the ransomware creates an additional thread using the API call GetLogicalDrives to retrieve the logical drives, “README.TXT” ransom note in every directory that is not in the exclusion list.


README.TXT - Notepad

File Edit Format View Help

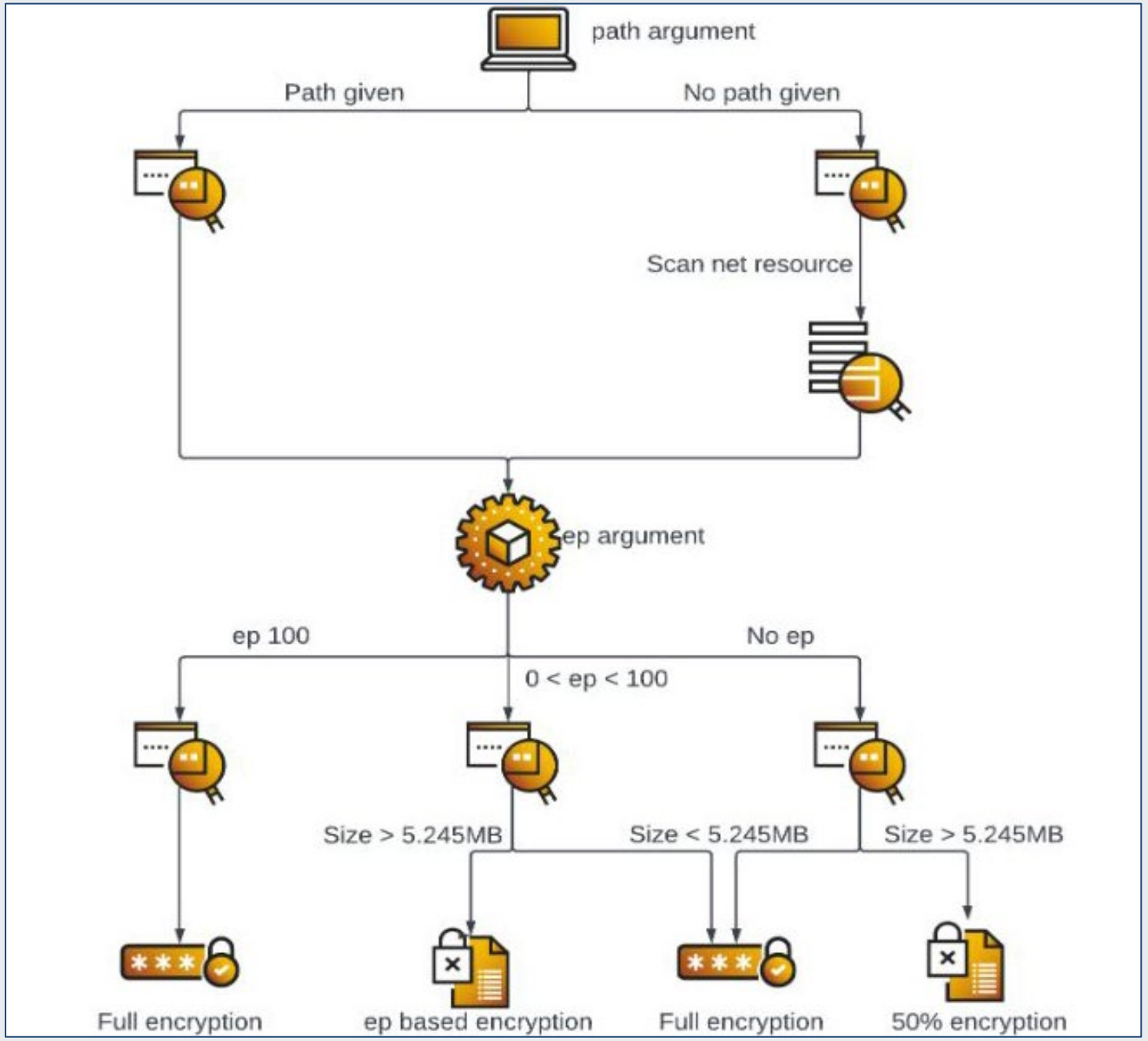
```
Hello!

        If you are reading this, it means that your system were hit by Royal ransomware.
        Please contact us via :
        http://royal[redacted]onion/[redacted (ID of 32 characters)]

In the meantime, let us explain this case.It may seem complicated, but it is not!
Most likely what happened was that you decided to save some money on your security infrastructure.
Alas, as a result your critical data was not only encrypted but also copied from your systems on a secure server.
From there it can be published online.Then anyone on the internet from darknet criminals, ACLU journalists, Chinese
government(different names for the same thing),
and even your employees will be able to see your internal documentation: personal data, HR reviews, internal lawsuitsand
complains, financial reports, accounting, intellectual property, and more!

        Fortunately we got you covered!

Royal offers you a unique deal.For a modest royalty(got it; got it ? ) for our pentesting services we will not only
provide you with an amazing risk mitigation service,
covering you from reputational, legal, financial, regulatory, and insurance risks, but will also provide you with a
security review for your systems.
To put it simply, your files will be decrypted, your data restoredand kept confidential, and your systems will remain
secure.

        Try Royal today and enter the new era of data security!
        We are looking to hearing from you soon!
```

Contents of “README.TXT” with sample ID researchers used appended on TOR link.
Source: Trend Micro

https://t.me/learningnets

Encryption Process

Royal Ransomware's encryption process shown in this image from the beginning to the end.



Royal ransomware encryption process decision tree.
Source: Cybereason

https://t.me/learningnets

BlackCat Ransomware

A relatively new but highly-capable ransomware threat to the health sector

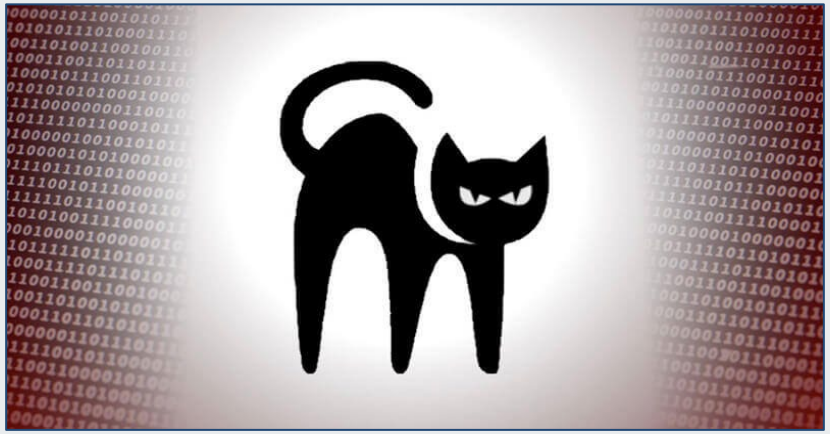
https://t.me/learningnets

Who is BlackCat?

- BlackCat ransomware, AKA ALPHV, AlphaVM, Noberus, Coreid, FIN7, Carbon Spider
- First detected in November 2021; per the FBI, they compromised at least 60 victims in four months
- Written in Rust; highly adaptable; Ransomware-as-a-service
- Conducts triple extortion (ransomware, threats to leak stolen data and distributed denial of service attacks)
- Suspected to be a successor group of Darkside/BlackMatter; recruiting from REvil
  - BlackCat admin is former REvil member
- Searchable data posted to open web to increase leak pressure
- Their targeting is focused on the U.S. and includes healthcare:
  - According to the group, “We do not attack state medical institutions, ambulances, hospitals. This rule does not apply to pharmaceutical companies, private clinics.”
  - Many cybercriminal gangs have broken promises not to attack healthcare targets in the past

Who is BlackCat? (Continued)

- Encryption algorithms: AES and ChaCha20
- Multiple encryption modes
- They have demanded ransoms as high as $1.5M; affiliates keep 80-90% of the ransom fee
- They use bulletproof hosting for their websites and a Bitcoin mixer to anonymize transactions



https://t.me/learningnets

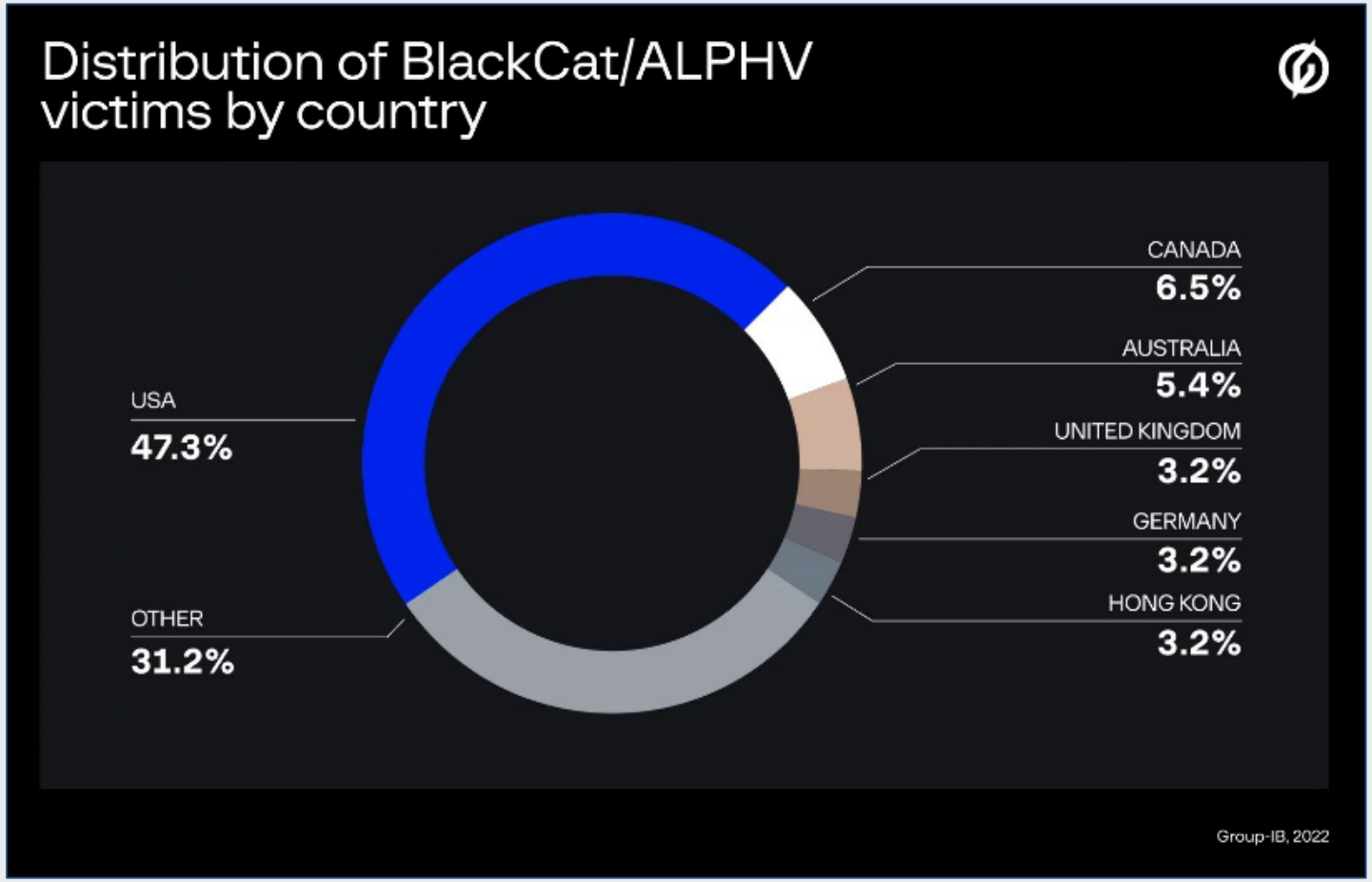
BlackCat: Targeting

Strategic and tactical

https://t.me/learningnets

BlackCat Favors U.S. Targets

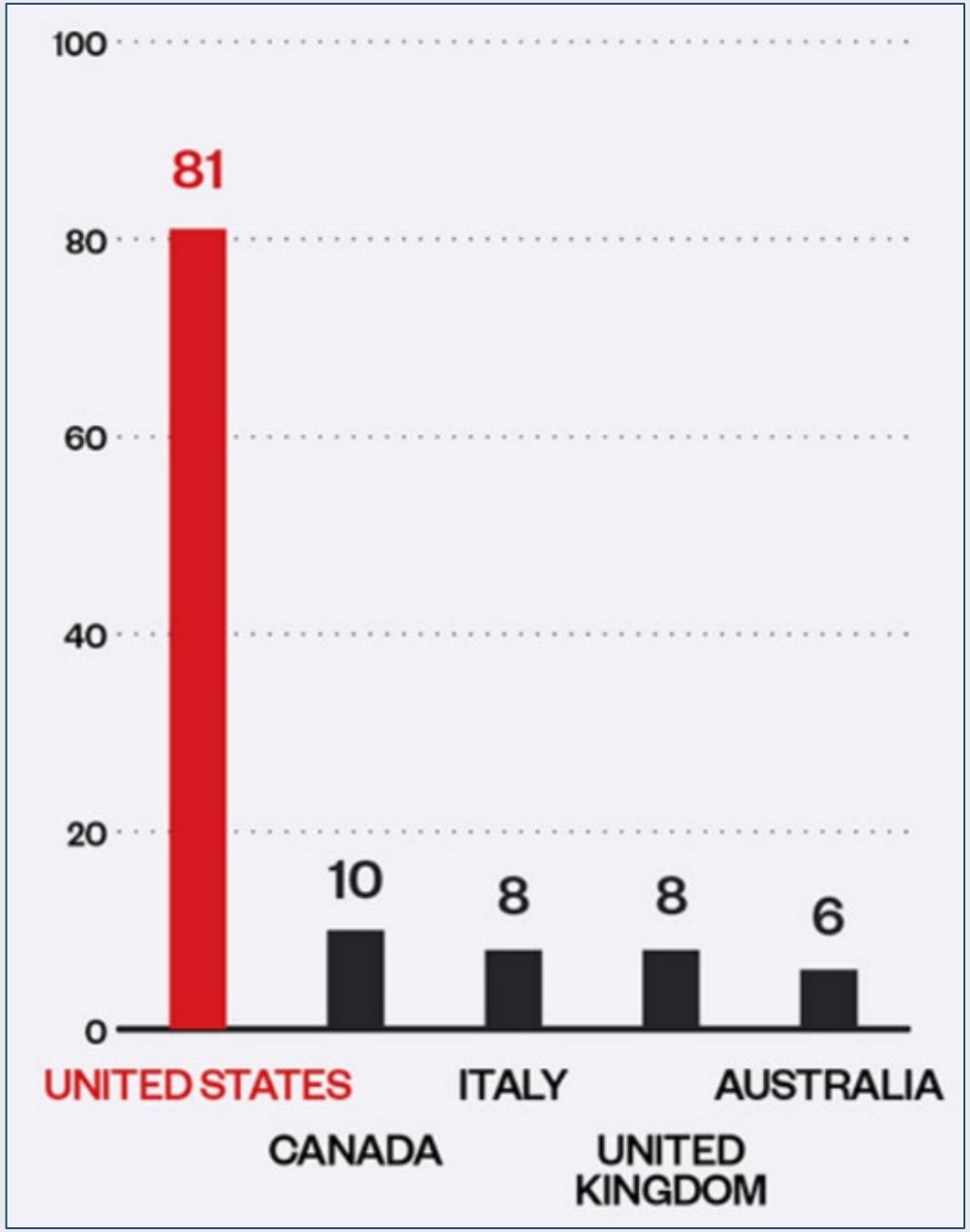
This chart, provided by Group-IB, provides the distribution by country of BlackCat victims.



https://t.me/learningnets

BlackCat Favors U.S. Targets (Part 2)

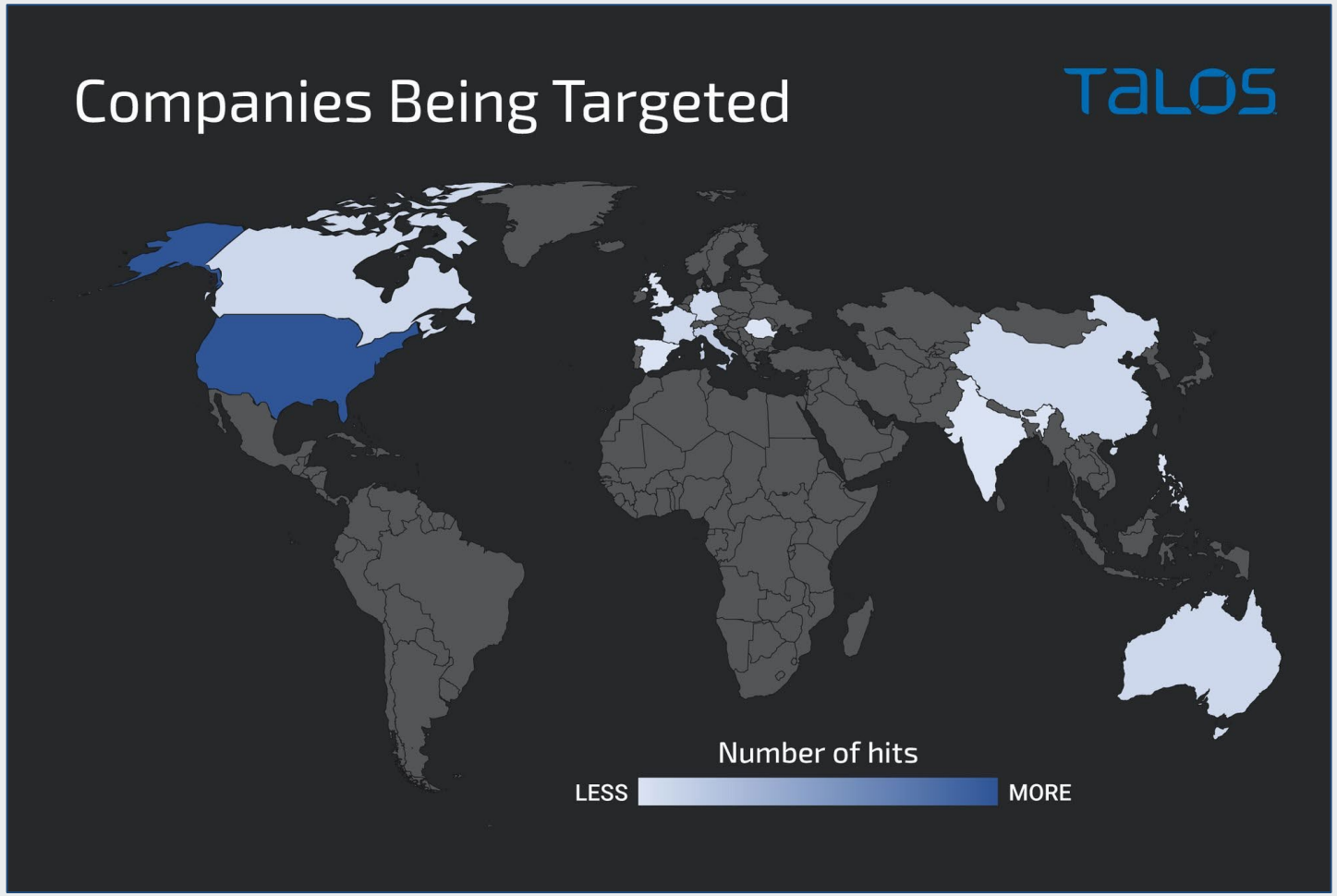
This chart, provided by Trend Micro, provides the distribution by country of BlackCat victims from December 1, 2021 to September 30, 2022.



https://t.me/learningnets

BlackCat Favors U.S. Targets (Part 3)

This chart, provided by Cisco Talos, provides the distribution by country of BlackCat victims.



https://t.me/learningnets

Targeting Versatility

BlackCat is capable of targeting a number of operating systems.

It's believed that BlackCat can support (and is capable of targeting) the following operating systems:

- Windows, 7 to 11, as well as Server 2008r2, 2012, 2016, 2019, 2022 (XP and 2003 can be encrypted over Server Message Block
- ESXI (at least versions 5.5, 6.5, 7.0.2u)
- Debian (at least versions 7,8 and 9)
- Ubuntu (at least versions 18.04 and 20.04)
- ReadyNAS
- Synology

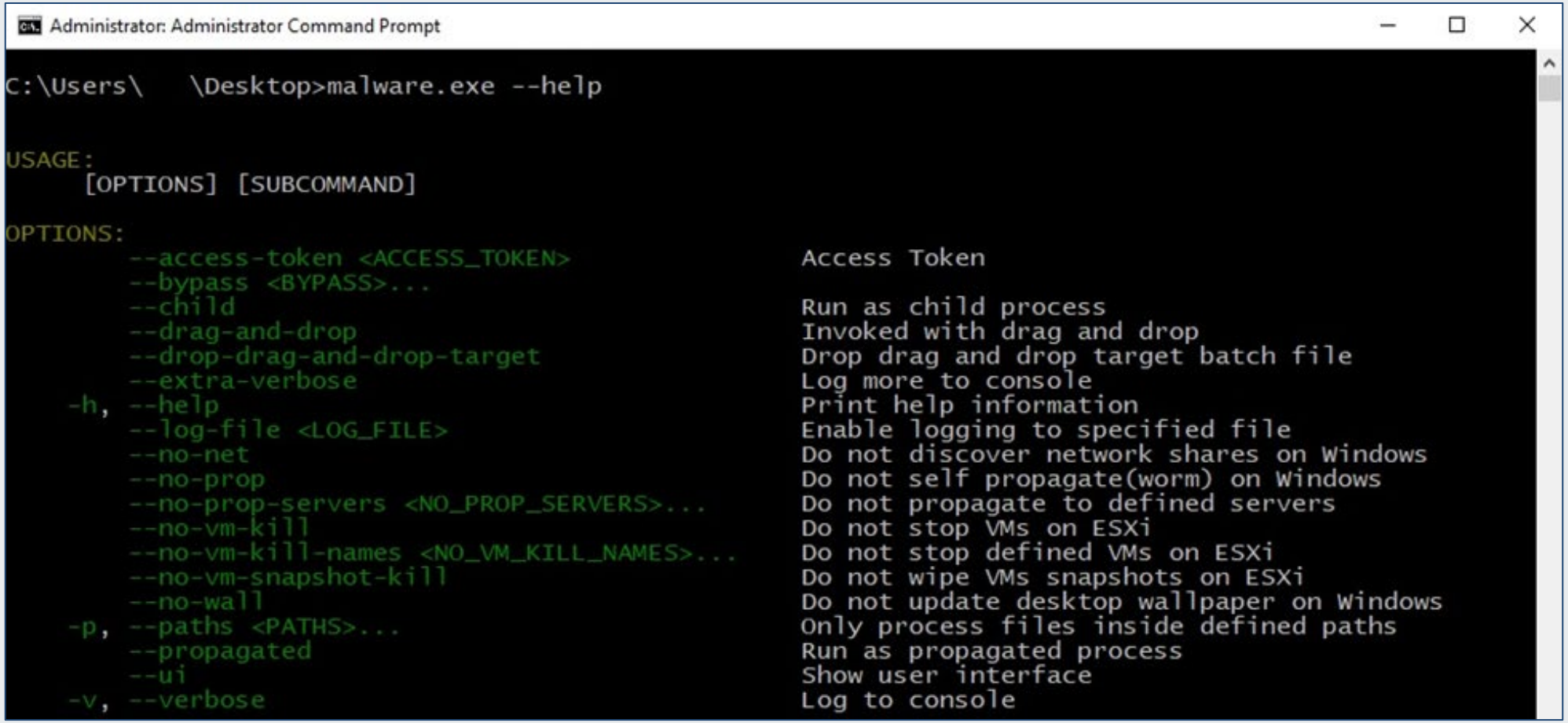
https://t.me/learningnets

BlackCat: Technical Operations

How BlackCat operates – tactics, techniques and procedures

https://t.me/learningnets

Command Prompt View/Capabilities



https://t.me/learningnets

BlackCat: Tooling

BlackCat attacks are known to leverage:

Direct use

- ADRecon
- Cobalt Strike
- PsExec
- Mimikatz
- Nirsoft
- Emotet
- ExMatter

Indirect use (affiliates/partners)

- Bloodhound tool
- Softperfect Netscan
- CrackMapExec
- Inveigh/InveighZero
- MegaSync
- Rclone
- Adfind
- Rubeus
- Stealbit

Please note: BlackCat tooling is constantly changing as they cycle through testing/usage, updating their arsenal frequently.

https://t.me/learningnets

BlackCat: Evading Detection and Defense

As part of its evasion capabilities, BlackCat attempts to terminate several processes and services to hinder detection and mitigation efforts. (Source of lists: PaloAlto Unit 42)

Process list:

agntsvc, dbeng50, dbsnmp, encsvc, excel, firefox, infopath, isqlplussvc, msaccess, mspub, mydesktopqos, mydesktopservice, notepad, ocautoupds, ocomm, ocssd, onenote, oracle, outlook, powerpnt, sqbcoreservice, sql, steam, synctime, tbirdconfig, thebat, thunderbird, visio, winword, wordpad, xfssvccon, *sql*, bedbh, vxmon, benetns, bengien, pvlsvr, beserver, raw_agent_svc, vsnapvss, CagService, QBIDPService, QBDBMgrN, QBCFMonitorService, SAP, TeamViewer_Service, TeamViewer, tv_w32, tv_x64, CVMountd, cvd, cvfwd, CVODS, saphostexec, saposcol, sapstartsrv, avagent, avscc, DellSystemDetect, EnterpriseClient, VeeamNFSSvc, VeeamTransportSvc, VeeamDeploymentSvc

Service List:

mepocs, memtas, veeam, svc$, backup, sql, vss, msexchange, sql$, mysql, mysql$, sophos, MSExchange, MSExchange$, WSBExchange, PDVFSService, BackupExecVSSProvider, BackupExecAgentAccelerator, BackupExecAgentBrowser, BackupExecDiveciMediaService, BackupExecJobEngine, BackupExecManagementService, BackupExecRPCService, GxBlr, GxVss, GxCIMgrS, GxCVD, GxCIMgr, GXMMM, GxVssHWProv, GxFWD, SAPService, SAP, SAP$, SAPD$, SAPHostControl, SAPHostExec, QBCFMonitorService, QBDBMgrN, QBIDPService, AcronisAgent, VeeamNFSSvc, VeeamDeploymentService, VeeamTransportSvc, MVArmor, MVarmor64, VSNAPVSS, AcrSch2Svc

https://t.me/learningnets

Data Exfiltration: ExMatter, Part 1

ExMatter

- BlackCat's primary data exfiltration tool, customized and developed from Fendr
  - Originally utilized by BlackMatter, also used by Conti
- Leverages a targeted approach to file discovery and exfiltration
- Uses native API to acquire OS version, and Windows APIs for some advanced NTFS features
- ExMatter can delete itself with the following PowerShell script:

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"  -WindowStyle
Hidden -C $path = 'C:\Users\user\Desktop\sender2.exe';Get-Process | Where-
Object {$_.Path -like $path} | Stop-Process -Force;[byte[]]$arr = new-
object byte[] 65536;Set-Content -Path $path -Value $arr;Remove-Item -Path
$path;
```


https://t.me/learningnets

Data Exfiltration: ExMatter, Part 2

Exmatter is known to be versatile and effective as compared to other data exfil tools.

	ExMatter
File Type	Win32 EXE (.NET).
Operating System	Windows XP and later versions.
Targeting Approach	Targets specific sets of files based on defined criteria. Avoids common system files and programs.
Obfuscation	Code is Protected by ConfuserEx, with some less-prevalent variants utilizing other options.
Usage Flexibility	Accepts specific command-line parameters.
Network	Uses secure file transfer protocol (SFTP), SOCKS5, or WebDAV for exfiltration. C2 infrastructure identified during analysis is hosted across two (2) unique hosting services / ASNs, with over 85% hosted by one (1) provider / ASN.

ExMatter Capabilities chart courtesy of Accenture

https://t.me/learningnets

Data Exfiltration: ExMatter, Part 3

File extensions marked for exfiltration

Extension			
.pdf	.doc	.docx	.xls
.xlsx	.png	.jpg	.jpeg
.txt	.sql	.bmp	.rdp
.msg	.pst	.zip	.rtf
.ipt	.dwg		

Excluded file extension chart courtesy of Stairwell

https://t.me/learningnets

Data Exfiltration: ExMatter, Part 4

Directory locations excluded from file exfiltration

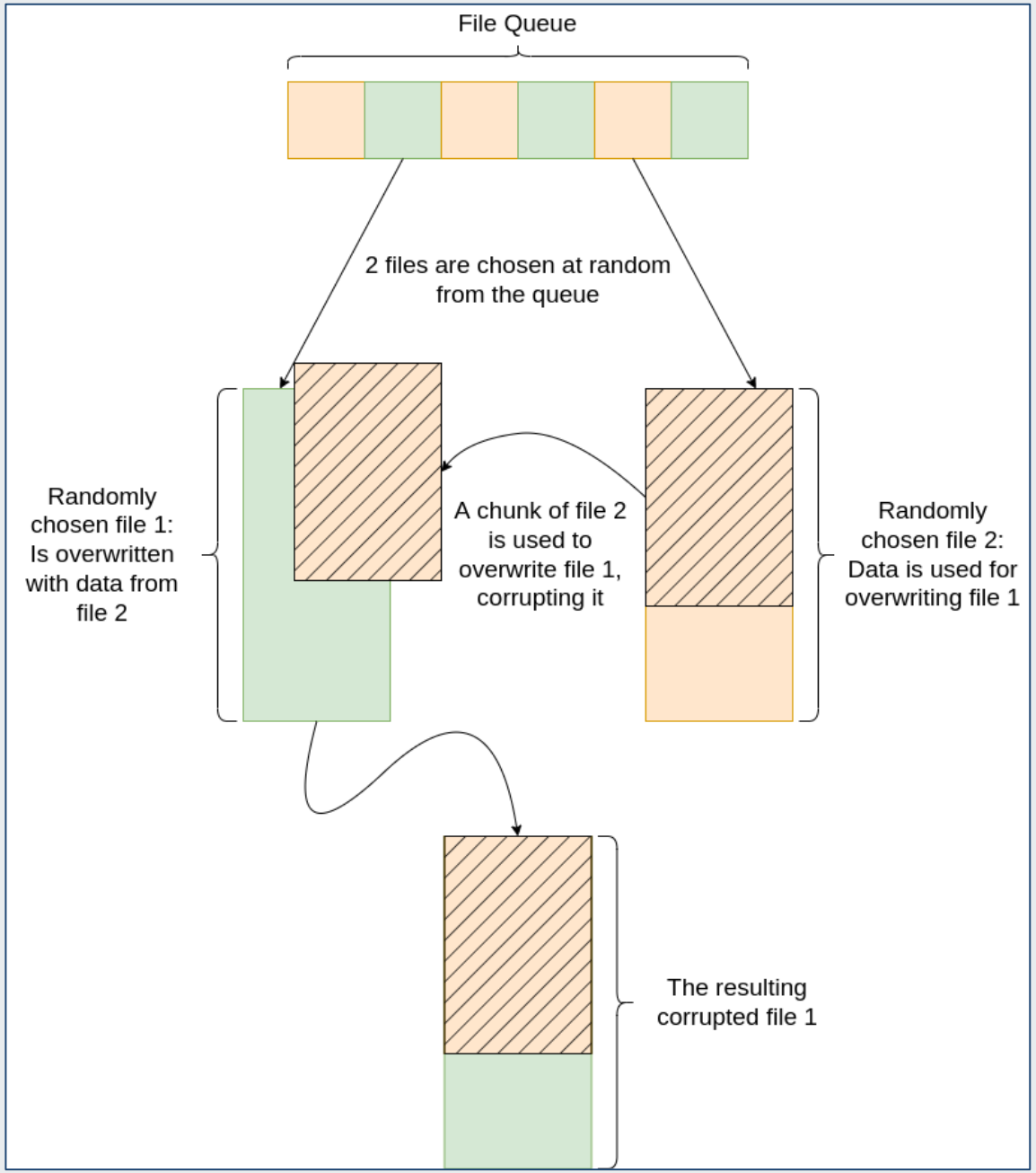
Excluded directories	
C:\Users\All Users\Microsoft	C:\ProgramData
C:\Windows	C:\$Recycle.Bin
C:\Documents and Settings	C:\PerfLogs
AppData\Roaming\Microsoft	AppData\Local\Microsoft
AppData\Local\Packages	C:\Program Files
C:\Program Files (x86)	

Excluded directories chart courtesy of Stairwell

https://t.me/learningnets

Data Exfiltration: ExMatter, Part 5

ExMatter is also developing data destruction capabilities.



ExMatter file corruption diagram courtesy of Stairwell

https://t.me/learningnets

BlackCat Encryption: Overview

BlackCat encryption:

- Two encryption algorithms: ChaCha20 and AES
- Six encryption modes
  - Full
  - HeadOnly
  - DotPattern
  - SmartPattern
  - AdvancedSmartPattern
  - Auto
- Several of these implement intermittent encryption

https://t.me/learningnets

BlackCat: Encryption Modes

BlackCat supports the six encryption modes on this chart.

Encryption mode	Description
Full	Encrypt all file content.
HeadOnly [N]	Encrypt the first N bytes of the file.
DotPattern [N,Y]	Encrypt every N bytes of the file with a step of Y bytes.
SmartPattern [N,P]	Encrypt the first N bytes of the file. BlackCat divides the rest of the file into equal-sized blocks, such that each block is 10% of the rest of the file in size. BlackCat encrypts P% of the bytes of each block.
AdvancedSmartPattern [N,P,B]	Encrypt the first N bytes of the file. BlackCat divides the rest of the file into B equal-sized blocks. BlackCat encrypts P% of the bytes of each block.
Auto	Combinatory file encryption mode. Encrypt the content of the file according to one of the file encryption modes `Full`, `DotPattern` [N,Y], and `AdvancedSmartPattern` [N,P,B]. BlackCat selects and parametrizes a file encryption mode based on the filename extension and the size of the file.

https://t.me/learningnets

ExMatter file corruption diagram courtesy of Stairwell

BlackCat: Encryption Algorithms

Advanced Encryption Standard (AES)

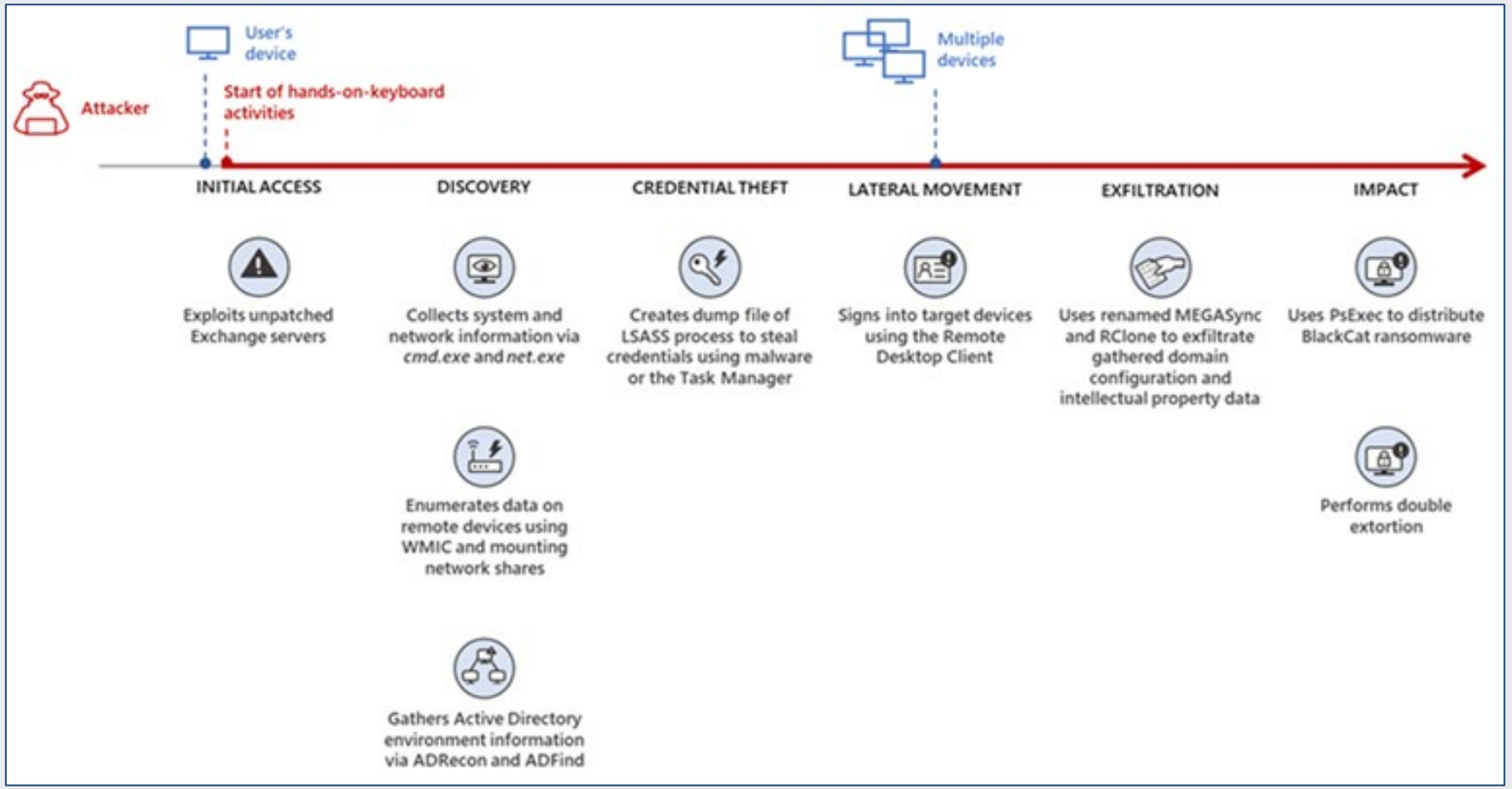
- Variation of Rijndael block cypher
  - Block/chunk size of 128 bits
- Designed based on a principle known as a substitution–permutation network
- 256-bit AES is standard for ransomware
  - Same strength as is approved for U.S. Intelligence Community
- Symmetric keys
  - Key is encrypted with RSA public key embedded in ransomware, which means that a private key is needed to decrypt

ChaCha20

- 256-bit, 20-round stream cipher
- Significantly faster than AES
- Based on a variant of 8-round Salsa20
- Symmetric keys
  - Key is encrypted with RSA public key embedded in ransomware, which means that a private key is needed to decrypt

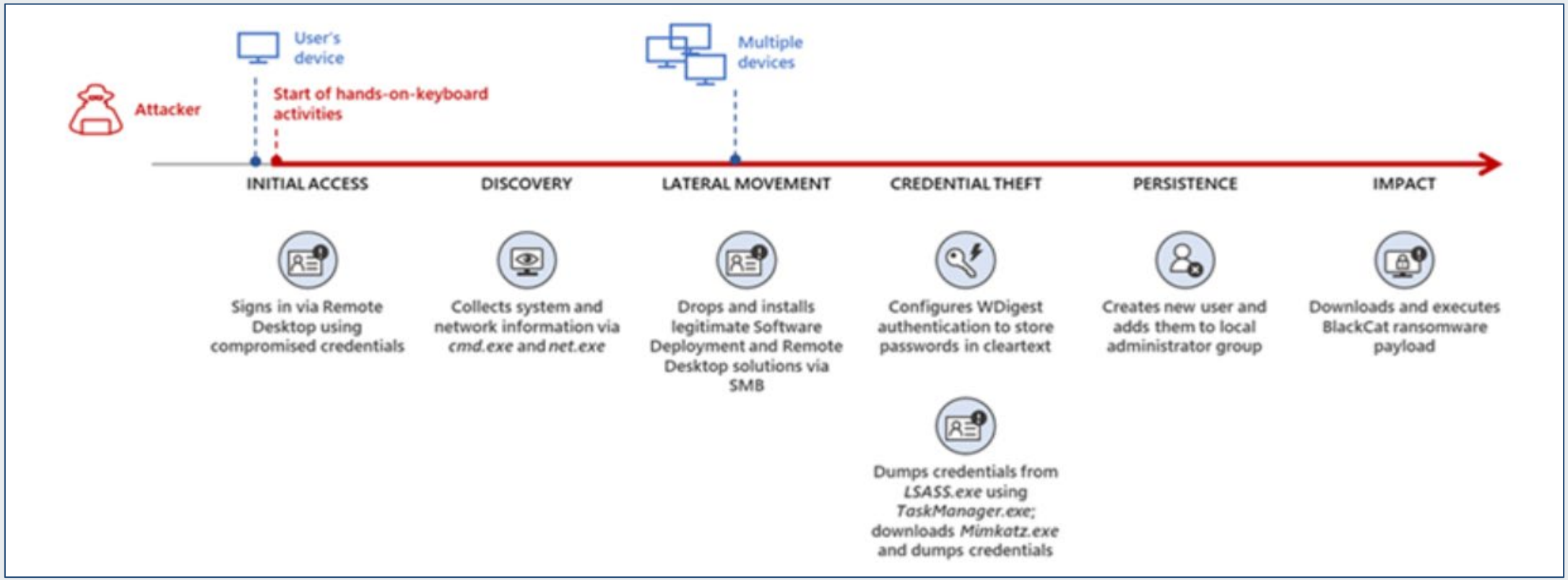
https://t.me/learningnets

BlackCat Attack: Exchange Server Entry Point



https://t.me/learningnets

BlackCat Attack: Compromised Credential Entry

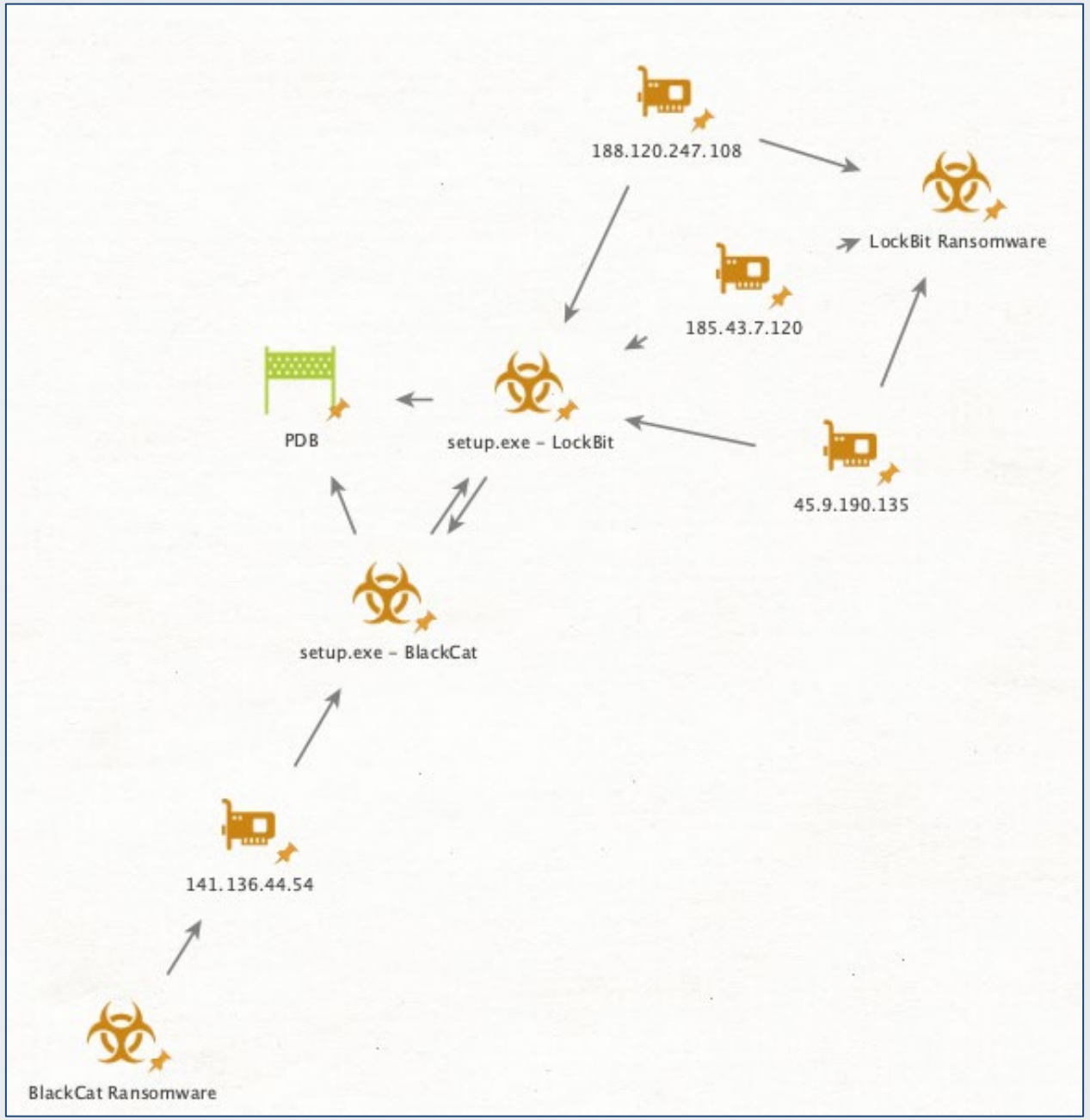


https://t.me/learningnets

BlackCat and LockBit

Overlap between BlackCat and LockBit? Maybe.

This might indicate cooperation on a personnel or technical level.



https://t.me/learningnets

Similarities between BlackCat and BlackMatter

Additional indications of technical similarities between the two groups.

Source: Cisco Talos

Commonalities & Differences in the MITRE ATT&CK® Framework

TALOS

MITRE ATT&CK®	BlackCat	BlackMatter
Initial access		Microsoft Exchange Vulnerability
Persistence	Reverse SSH tunnel Scheduled tasks image file execution option	Reverse SSH tunnel Scheduled tasks
Defense evasion	Disabling system logs Disabling endpoint protection Gmer	
Credential access	Dump lsass Browser password stealer	Dump lsass
Discovery	ADRecon softperfect network scanner	
Lateral movement	Impacket Powershell RDP psexec	Impacket RDP psexec
Command and control	Reverse SSH tunnel Impacket	Reverse SSH tunnel Impacket
Impact	Group policy Netlogon share BlackCat Ransomware	Group policy Netlogon share BlackMatter Ransomware

Same C2 domain

TALOS

Attack	Domain	IP	Port
BlackCat	windows[.]menu	52.149.228[.]45	8443
BlackMatter		52.149.228[.]45	443
BlackMatter		20.46.245[.]56	443

https://t.me/learningnets

Mitigations and Defense

How to protect your organization against Royal, BlackCat, and other ransomware variants

https://t.me/learningnets

Mitigations and Defense

Royal

- Indicators of Compromise (sample):
  - https://www.cybereason.com/blog/royal-ransomware-analysis
  - https://yoroi.company/research/reconstructing-the-last-activities-of-royal-ransomware/
  - https://www.avertium.com/resources/threat-reports/everything-you-need-to-know-about-royal-ransomware
  - https://www.trendmicro.com/en_us/research/22/l/conti-team-one-splinter-group-resurfaces-as-royal-ransomware-wit.html
- Yara rule:
  - https://yoroi.company/research/reconstructing-the-last-activities-of-royal-ransomware/
  - https://malpedia.caad.fkie.fraunhofer.de/yara/win.royal_ransom

https://t.me/learningnets

Mitigations and Defense

BlackCat

- Courses of Action:
  - https://unit42.paloaltonetworks.com/blackcat-ransomware/
- Indicators of Compromise (sample):
  - https://www.ic3.gov/Media/News/2022/220420.pdf
  - https://resecurity.com/blog/article/blackcat-aka-alphv-ransomware-is-increasing-stakes-up-to-25m-in-demands
  - https://securityscorecard.com/research/deep-dive-into-alphv-blackcat-ransomware
  - https://otx.alienvault.com/pulse/62960d2bab11f2124cb4962e
- Yara rule:
  - https://www.advintel.io/post/blackcat-in-a-shifting-threat-landscape-it-helps-to-land-on-your-feet-tech-dive

https://t.me/learningnets

Mitigations and Defense (Source: FBI)

- 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 the 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.

https://t.me/learningnets

Recommendations

In addition to following the mitigations, HC3 recommends organizations review and utilize CISA's Free Cybersecurity Services and Tools, which can be accessed by visiting https://www.cisa.gov/free-cybersecurity-services-and-tools .

https://t.me/learningnets

Reference Materials

https://t.me/learningnets

References

Royal (.royal) ransomware virus - removal and decryption options
https://www.pcrisk.com/removal-guides/24971-royal-ransomware

Free Cybersecurity Services and Tools
https://www.cisa.gov/free-cybersecurity-services-and-tools

Everything You Need to Know About Royal Ransomware
https://www.avertium.com/resources/threat-reports/everything-you-need-to-know-about-royal-ransomware

US Health Dept warns of Royal Ransomware targeting healthcare
https://www.bleepingcomputer.com/news/security/us-health-dept-warns-of-royal-ransomware-targeting-healthcare/

19th December – Threat Intelligence Report
https://research.checkpoint.com/2022/19th-december-threat-intelligence-report/

https://t.me/learningnets

References

Microsoft Warns of Cybercrime Group Delivering Royal Ransomware, Other Malware
https://www.securityweek.com/microsoft-warns-cybercrime-group-delivering-royal-ransomware-other-malware

New Royal Ransomware emerges in multi-million dollar attacks
https://www.bleepingcomputer.com/news/security/new-royal-ransomware-emerges-in-multi-million-dollar-attacks/

Royal Ransomware Threat Takes Aim at U.S. Healthcare System
https://thehackernews.com/2022/12/royal-ransomware-threat-takes-aim-at-us.html

This sneaky ransomware gang keeps changing tactics to spread its malware
https://www.zdnet.com/article/this-sneaky-ransomware-gang-keeps-changing-tactics-to-spread-its-malware/

DEV-0569 Ransomware Group Remarkably Innovative, Microsoft Cautions
https://www.darkreading.com/endpoint/dev-0569-ransomware-group-remarkably-innovative-microsoft-cautions

https://t.me/learningnets

References

HHS warns Royal ransomware threat targeting healthcare providers
https://www.scmagazine.com/analysis/ransomware/hhs-warns-royal-ransomware-threat-targeting-healthcare-providers

Health Industry Cybersecurity Practices (HICP) - Small Healthcare Organization
https://405d.hhs.gov/Documents/405d-Quick-Start-Guides-for-Small-Practices-Official-Document-R.pdf

DEV-0569 finds new ways to deliver Royal ransomware, various payloads
https://www.microsoft.com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/

Health Industry Cybersecurity Practices (HICP) – Medium & Large Healthcare Organizations
https://405d.hhs.gov/Documents/405d-Quick-Start-Guides-for-Medium-to-Large-Organizations-Official-Document-R.pdf

Royal Ransomware," HC3 Analyst Note
https://www.hhs.gov/sites/default/files/royal-ransomware-analyst-note.pdf

https://t.me/learningnets

References

Conti Team One Splinter Group Resurfaces as Royal Ransomware with Callback Phishing Attacks
https://www.trendmicro.com/en_us/research/22/l/conti-team-one-splinter-group-resurfaces-as-royal-ransomware-wit.html

Novel Royal ransomware operation ramps up attacks
https://www.scmagazine.com/brief/ransomware/novel-royal-ransomware-operation-ramps-up-attacks

Healthcare Organizations Warned of Royal Ransomware Attacks
https://www.securityweek.com/healthcare-organizations-warned-royal-ransomware-attacks

Royal ransomware tied to Conti gang
https://www.scmagazine.com/brief/ransomware/royal-ransomware-tied-to-conti-gang

DEV-0569 finds new ways to deliver Royal ransomware, various payloads
https://www.microsoft.com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/

https://t.me/learningnets

References

BlackCat — In a Shifting Threat Landscape, It Helps to Land on Your Feet: Tech Dive
https://www.advintel.io/post/blackcat-in-a-shifting-threat-landscape-it-helps-to-land-on-your-feet-tech-dive

Ransomware Group Debuts Searchable Victim Data
https://krebsonsecurity.com/2022/06/ransomware-group-debuts-searchable-victim-data/

Fat Cats - An analysis of the BlackCat ransomware affiliate program
https://blog.group-ib.com/blackcat

BlackCat ransomware's data exfiltration tool gets an upgrade
https://www.bleepingcomputer.com/news/security/blackcat-ransomware-s-data-exfiltration-tool-gets-an-upgrade/

BlackCat, LockBit 3.0 ransomware target healthcare with customizable tactics, triple extortion
https://www.scmagazine.com/analysis/ransomware/blackcat-lockbit-3-0-ransomware-target-healthcare-with-customizable-tactics-triple-extortion

https://t.me/learningnets

References

A Deep Dive Into ALPHV/BlackCat Ransomware
https://securityscorecard.com/research/deep-dive-into-alphv-blackcat-ransomware

BlackCat ransomware's data exfiltration tool gets an upgrade
https://www.bleepingcomputer.com/news/security/blackcat-ransomware-s-data-exfiltration-tool-gets-an-upgrade/

Leading Ransomware Variants Q3 2022
https://intel471.com/resources/whitepapers/leading-ransomware-variants-q3-2022

Noberus Ransomware: Darkside and BlackMatter Successor Continues to Evolve its Tactics
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-ransomware-ttps

Analyzing Exmatter: A Ransomware Data Exfiltration Tool
https://www.kroll.com/en/insights/publications/cyber/analyzing-exmatter-ransomware-data-exfiltration-tool

https://t.me/learningnets

References

Emotet botnet now pushes Quantum and BlackCat ransomware
https://www.bleepingcomputer.com/news/security/emotet-botnet-now-pushes-quantum-and-blackcat-ransomware/

BlackCat ransomware claims attack on European gas pipeline
https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-attack-on-european-gas-pipeline/

BlackCat ransomware could be about to get a whole lot nastier
https://www.techradar.com/news/blackcat-ransomware-could-be-about-to-get-a-whole-lot-nastier

BlackCat Ransomware Group Deploys Brute Ratel Pen Testing Kit
https://www.infosecurity-magazine.com/news/blackcat-ransomware-group-pen-test/

BlackCat ransomware attacks not merely a byproduct of bad luck
https://news.sophos.com/en-us/2022/07/14/blackcat-ransomware-attacks-not-merely-a-byproduct-of-bad-luck/

https://t.me/learningnets

References

BlackCat (aka ALPHV) Ransomware is Increasing Stakes up to $2.5M in Demands
https://resecurity.com/blog/article/blackcat-aka-alphv-ransomware-is-increasing-stakes-up-to-25m-in-demands

Ransomware gang creates site for employees to search for their stolen data #ALPHV #BlackCat
https://www.bleepingcomputer.com/news/security/ransomware-gang-creates-site-for-employees-to-search-for-their-stolen-data/

Prolific Ransomware Affiliate Groups Deploy BlackCat
https://duo.com/decipher/prolific-affiliate-threat-groups-linked-to-blackcat-ransomware

Microsoft: Exchange servers hacked to deploy BlackCat ransomware
https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-blackcat-ransomware/

The many lives of BlackCat ransomware
https://www.microsoft.com/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/

https://t.me/learningnets

References

BlackCat — In a Shifting Threat Landscape, It Helps to Land on Your Feet: Tech Dive
https://www.advintel.io/post/blackcat-in-a-shifting-threat-landscape-it-helps-to-land-on-your-feet-tech-dive

Novel BlackCat Ransomware Tactic Speeds Up Encryption Process
https://duo.com/decipher/novel-blackcat-ransomware-tactic-speeds-up-encryption-process

FBI: BlackCat ransomware breached at least 60 entities worldwide
https://www.bleepingcomputer.com/news/security/fbi-blackcat-ransomware-breached-at-least-60-entities-worldwide/

FBI: BlackCat/ALPHV Ransomware Indicators of Compromise
https://www.ic3.gov/Media/News/2022/220420.pdf

An Investigation of the BlackCat Ransomware via Trend Micro Vision One
https://www.trendmicro.com/en_us/research/22/d/an-investigation-of-the-blackcat-ransomware.html

https://t.me/learningnets

References

BlackCat Purveyor Shows Ransomware Operators Have 9 Lives
https://www.darkreading.com/attacks-breaches/blackcat-purveyor-shows-ransomware-operators-have-nine-lives

BlackCat Ransomware Targets Industrial Companies
https://www.securityweek.com/blackcat-ransomware-targets-industrial-companies

A Bad Luck BlackCat
https://securelist.com/a-bad-luck-blackcat/106254/

A look at the ransomware threat landscape. BlackMatter affiliate connected to BlackCat. EXOTIC LILY provides initial access for ransomware actors.
https://thecyberwire.com/podcasts/research-briefing/109/notes

From BlackMatter to BlackCat: Analyzing two attacks from one affiliate
http://blog.talosintelligence.com/2022/03/from-blackmatter-to-blackcat-analyzing.html

https://t.me/learningnets

References

Cybereason vs. BlackCat Ransomware
https://www.cybereason.com/blog/cybereason-vs.-blackcat-ransomware

LockBit, BlackCat, Swissport, Oh My! Ransomware Activity Stays Strong
https://threatpost.com/lockbit-blackcat-swissport-ransomware-activity/178261/

BlackCat (ALPHV) ransomware linked to BlackMatter, DarkSide gangs
https://www.bleepingcomputer.com/news/security/blackcat-alphv-ransomware-linked-to-blackmatter-darkside-gangs/

An ALPHV (BlackCat) representative discusses the group's plans for a ransomware 'meta-universe'
https://therecord.media/an-alphv-blackcat-representative-discusses-the-groups-plans-for-a-ransomware-meta-universe/

Threat Assessment: BlackCat Ransomware
https://unit42.paloaltonetworks.com/blackcat-ransomware/

https://t.me/learningnets

References

Who Wrote the ALPHV/BlackCat Ransomware Strain?
https://krebsonsecurity.com/2022/01/who-wrote-the-alphv-blackcat-ransomware-strain/

Actor username01 (aka alphv, ransom) runs ALPHV aka ALPHV-ng, BlackCat ransomware-as-a-service affiliate program
https://titan.intel471.com/report/inforep/aff92438c62c32c3a6a4835d7a62a94c

Noberus: Technical Analysis Shows Sophistication of New Rust-based Ransomware
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-alphv-rust-ransomware

ALPHV BlackCat - This year's most sophisticated ransomware
https://www.bleepingcomputer.com/news/security/alphv-blackcat-this-years-most-sophisticated-ransomware/

ALPHV (BlackCat) is the first professional ransomware gang to use Rust
https://therecord.media/alphv-blackcat-is-the-first-professional-ransomware-gang-to-use-rust/

https://t.me/learningnets

Questions

https://t.me/learningnets

FAQ

Upcoming Briefing

- February 9 – 2022 Healthcare Cybersecurity Year in Review and 2023 Look-Ahead

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are **highly encouraged** to provide feedback. To provide feedback, please complete the HC3 Customer Feedback Survey.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV.

Disclaimer

These recommendations are advisory and are not to be considered as federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. The HHS does not endorse any specific person, entity, product, service, or enterprise.

https://t.me/learningnets

About HC3

The Health Sector Cybersecurity Coordination Center (HC3) works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector. HC3 was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats.

What We Offer

Sector and Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

Alerts and Analyst Notes

Documents that provide in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings

Presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

https://t.me/learningnets

CPE Credits

This 1-hour presentation by HHS HC3 provides you with 1 hour of CPE credits based on your Certification needs.

The areas that qualify for CPE credits are Security and Risk Management, Asset Security, Security Architecture and Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.

Typically, you will earn 1 CPE credit per 1 hour time spent in an activity. You can report CPE credits in 0.25, 0.50 and 0.75 increments.

https://t.me/learningnets

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Contacts

HHS.GOV/HC3

HC3@HHS.GOV

https://t.me/learningnets