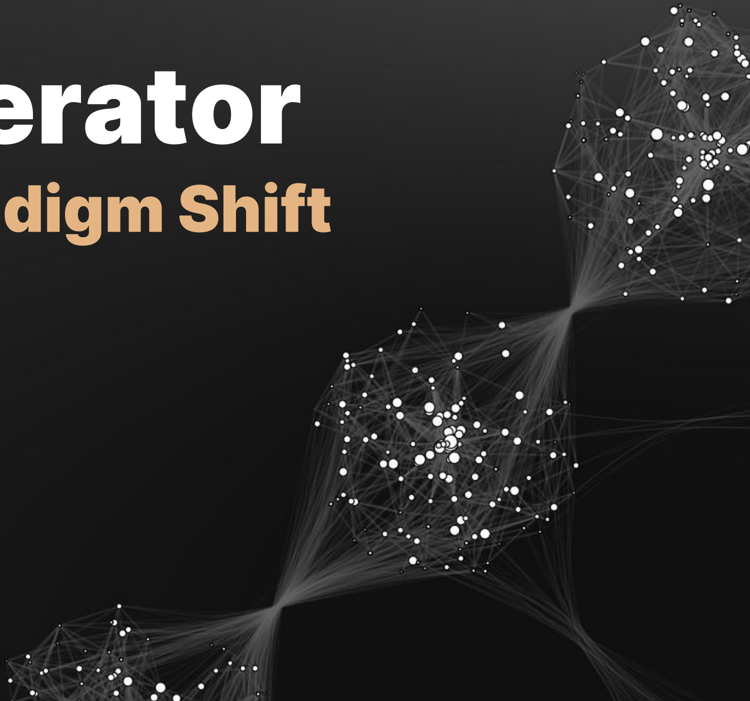
ATT&CKing The Operator

Disrupting The Ransomware Paradigm Shift



Nick Lowe

Sr. Director, Intelligence Services

Recorded Future

- 17+ years cyber security industry experience
- Former Director, Falcon OverWatch at CrowdStrike
- Extensive experience serving as both a practitioner and senior leader specializing in threat hunting, security operations, threat intelligence, managed security services and incident response
- Regular speaker, frequently presenting at global cyber security conferences and briefing executive audiences across private and public sector entities on the threat landscape and various cyber security topics
- Based in Sydney, Australia

in www.linkedin.com/in/nick-cti

X @nick_cti

Agenda

- The State Of The Threat Landscape
- Outpacing The Adversary
- Looking Beyond The CVE
- Know The Enemy, Hunt The Enemy
- Call To Action
- **Q&A**

The State Of The Threat Landscape

Evolving Adversary Operations in 2023

- Zero Day Acquisition An Increasing Operational Priority
- Continued Prolific Exploitation of Known Historic Vulnerabilities
- Rapid Adoption of New Vulnerabilities Narrowing Time-To-Exploitation
- Evolving Criminal Ecosystem Continues to Lower Barriers to Entry
- Ransomware Paradigm Shift From Encryption To Extortion
- Nation State and Criminal Adversaries Highly Adaptable & Increasingly Fast Moving
- Initial Access Preferences Shifting
- Growth in IAB Activity Negating Initial Access Challenges
- Identity Under Siege

Hiding In Plain Sight

- Diminishing reliance on malware enabling lateral movement without obstruction

- Adversaries having increasing success in progressing their actions on objectives without the need to deploy malware

- Proliferation of LOTL techniques combined with use of compromised privileged credentials poses challenges for defenders reliant on technology alone

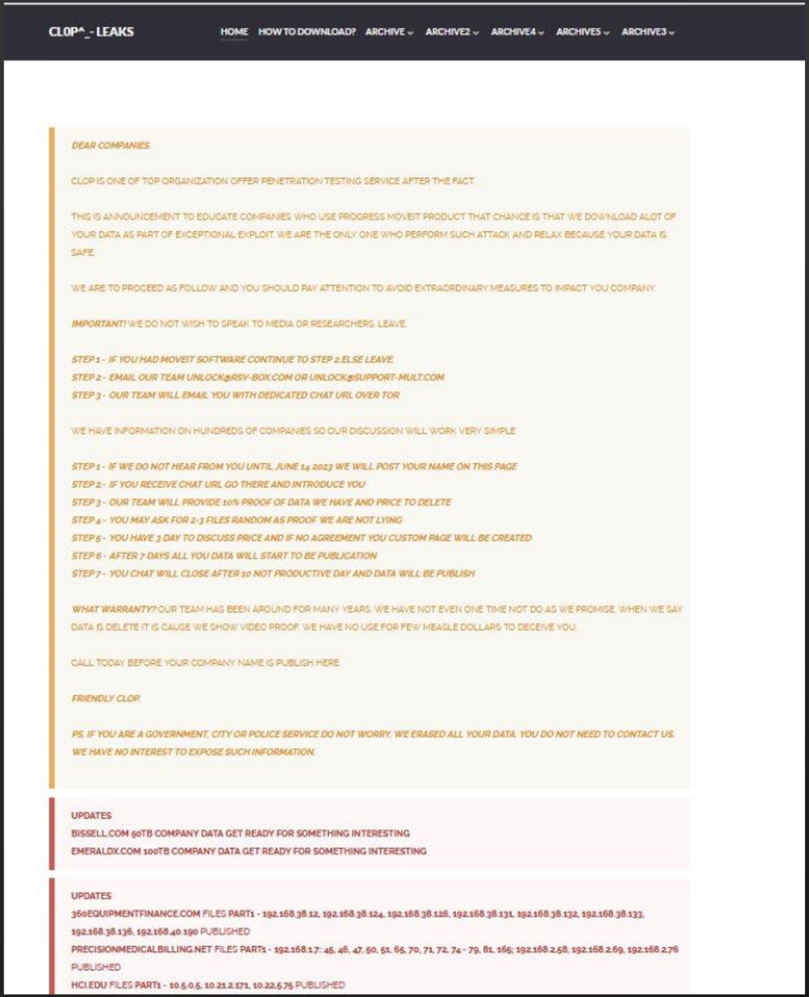
Why You Need To Care

- Speed of Detection Is Critical As Adversary Tempo Accelerates
- Basic Security Hygiene Remains a Challenge, And Adversaries Know It
- Surging IAB Activity Exposing Organisations To Veritable Army of Threat Actors
- Reactive Defences Powerless Against Increasingly Capable Adversaries
- The Time-To-Mass-Exploitation Delta Continues To Narrow as Public Disclosure of Vulnerabilities Rapidly Followed by Same Day In The Wild Exploitation

Outpacing The Adversary

Learning From The MOVEit MFT Compromise

- Large scale supply chain compromise
- Targeted, rather than opportunistic attack initially exploiting zero-day SQL injection vulnerability
- Carefully considered, multiple stage exploitation process
- Extensive collection of tactics, techniques and procedures utilized to support actor objectives
- Focus on access maintenance to enable ongoing interactive command execution on compromised systems



DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.
STEP 2 - EMAIL OUR TEAM UNLOCK@RSV-BOX.COM OR UNLOCK@SUPPORT-MULT.COM
STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE

STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE
STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU
STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE
STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING
STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED
STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION
STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH

WHAT WARRANTY? OUR TEAM HAS BEEN AROUND FOR MANY YEARS. WE HAVE NOT EVEN ONE TIME NOT DO AS WE PROMISE. WHEN WE SAY DATA IS DELETE IT IS CAUSE WE SHOW VIDEO PROOF. WE HAVE NO USE FOR FEW MEASLE DOLLARS TO DECEIVE YOU.

CALL TODAY BEFORE YOUR COMPANY NAME IS PUBLISH HERE.

FRIENDLY CLOP.

PS. IF YOU ARE A GOVERNMENT, CITY OR POLICE SERVICE DO NOT WORRY, WE ERASED ALL YOUR DATA. YOU DO NOT NEED TO CONTACT US. WE HAVE NO INTEREST TO EXPOSE SUCH INFORMATION.

UPDATES
BISSELL.COM 50TB COMPANY DATA GET READY FOR SOMETHING INTERESTING
EMERALDX.COM 100TB COMPANY DATA GET READY FOR SOMETHING INTERESTING

UPDATES
360EQUIPMENTFINANCE.COM FILES PART1 - 192.168.38.12, 192.168.38.124, 192.168.38.126, 192.168.38.131, 192.168.38.132, 192.168.38.133, 192.168.38.136, 192.168.40.190 PUBLISHED
PRECISIONMEDICALBILLING.NET FILES PART1 - 192.168.1.7: 45, 46, 47, 50, 51, 65, 70, 71, 72, 74 - 79, 81, 165; 192.168.2.58, 192.168.2.69, 192.168.2.76 PUBLISHED
HCI.EDU FILES PART1 - 10.5.0.5, 10.21.2.171, 10.22.5.75 PUBLISHED

Cl0p: (LEMUR) Looting And Extortion

- Successful exploitation led to unauthorized access to underlying MOVEit DB's
- Deployment of `LEMURLOOT` webshell to persist operator access and support pursuit of hands-on actions on objectives
- Deletion of default MOVEit user account with 'LoginName' and 'RealName' values set to '`Health Check Services`'
- Creation of new actor controlled, privileged account with matching values
- Enumeration of Azure data and SQL DB contents
- Collection and `.gzip` compression of data followed by exfiltration

Profiling The Adversary

Adversary **Aliases**	**Cl0p** FANCY CAT, TA505, FIN11, Lace Tempest	
Classification **Origin**	Criminal Russia	
Targeting	All Sectors	
Methods	Affinity for targeting and exploiting MFT platforms including Accellion FTA, SolarWinds Serv-U, GoAnyWhere & MOVEit Extorts victims with threats of publishing exfiltrated confidential data	
Tooling	LEMURLOOT DEWMODE SDBot	Cobalt Strike Trubot FlawedAmmyy
MITRE **ATT&CK TTPs**	**T1190:** Exploit Public Facing Application **T1059.001:** PowerShell **T1505.003:** Webshell **T1105:** Ingress Tool Transfer **T1041**: Exfiltration Over C2 Channel **T1021.002:** SMB/Windows Admin Shares **T1068:** Exploitation For Privilege Escalation	

MOVEit Exploitation.
By The Numbers.

2+

Years Testing
The Exploit

6

Distinct
Vulnerabilities

2000

Victim
Organisations

+

6 Distinct CVE’s

CVE-2023-34362

SQL injection vulnerability enabling unauthenticated attacker to gain unauthorised access to SQL DB, query, execute statements and modify DB contents

CVE-2023-35036

SQL injection vulnerability enabling unauthenticated attacker to access DB and submit crafted payloads to MOVEit application resulting in possible modification or disclosure of MOVEit DB content

CVE-2023-35708

SQL injection vulnerability enabling unauthenticated attacker to access DB and submit crafted payloads to MOVEit application resulting in possible modification or disclosure of MOVEit DB content

CVE-2023-36932

SQL injection vulnerability enabling unauthenticated attacker to access DB and submit crafted payloads to MOVEit application resulting in possible modification or disclosure of MOVEit DB content

CVE-2023-36933

Allows attacker to invoke a method resulting in unhandled exception, potentially causing the MOVEit application to unexpectedly terminate

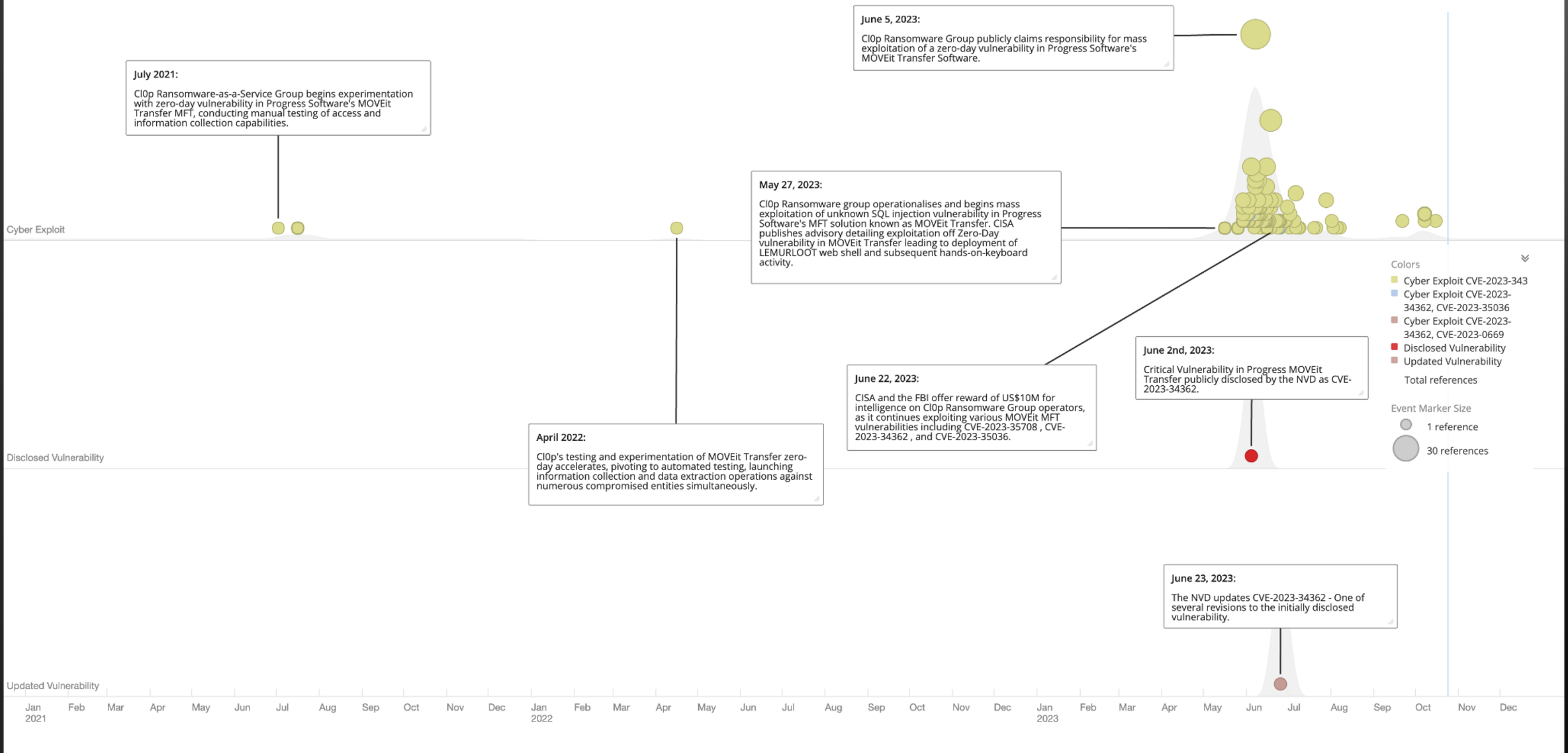
CVE-2023-36934

SQL injection vulnerability enabling unauthenticated attacker to access DB and submit crafted payloads to MOVEit application resulting in possible modification or disclosure of MOVEit DB content

```
rule M_Webshell_LEMURLOOT_DLL_1 {
    meta:
        disclaimer = "This rule is meant for hunting and is not tested
to run in a production environment"
        description = "Detects the compiled DLLs generated from
human2.aspx LEMURLOOT payloads."
        sample =
"c58c2c2ea608c83fad9326055a8271d47d8246dc9cb401e420c0971c67e19cbf"
        date = "2023/06/01"
        version = "1"
    strings:
        $net = "ASP.NET"
        $human = "Create_ASP_human2_aspx"
        $s1 = "X-siLock-Comment" wide
        $s2 = "X-siLock-Step3" wide
        $s3 = "X-siLock-Step2" wide
        $s4 = "Health Check Service" wide
        $s5 = "attachment; filename={0}" wide
    condition:
        uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and
        filesize < 15KB and
        $net and
        (
            ($human and 2 of ($s*)) or
            (3 of ($s*))
        )
}
```

“Speed. Both Your **Greatest Adversary,** And Biggest Advantage.”

CVE-2023-34362: Cl0p MOVEit MFT Initial Exploitation and Disclosure Timeline



July 2021:
Cl0p Ransomware-as-a-Service Group begins experimentation with zero-day vulnerability in Progress Software's MOVEit Transfer MFT, conducting manual testing of access and information collection capabilities.

April 2022:
Cl0p's testing and experimentation of MOVEit Transfer zero-day accelerates, pivoting to automated testing, launching information collection and data extraction operations against numerous compromised entities simultaneously.

May 27, 2023:
Cl0p Ransomware group operationalises and begins mass exploitation of unknown SQL injection vulnerability in Progress Software's MFT solution known as MOVEit Transfer. CISA publishes advisory detailing exploitation off Zero-Day vulnerability in MOVEit Transfer leading to deployment of LEMURLOOT web shell and subsequent hands-on-keyboard activity.

June 2nd, 2023:
Critical Vulnerability in Progress MOVEit Transfer publicly disclosed by the NVD as CVE-2023-34362.

June 5, 2023:
Cl0p Ransomware Group publicly claims responsibility for mass exploitation of a zero-day vulnerability in Progress Software's MOVEit Transfer Software.

June 22, 2023:
CISA and the FBI offer reward of US$10M for intelligence on Cl0p Ransomware Group operators, as it continues exploiting various MOVEit MFT vulnerabilities including CVE-2023-35708 , CVE-2023-34362 , and CVE-2023-35036.

June 23, 2023:
The NVD updates CVE-2023-34362 - One of several revisions to the initially disclosed vulnerability.

Recorded Future

Criminal Adversaries Picking Up The Pace

- Actors increasingly operationalizing exploits same day
- Proof-of-Concept code readily available on Dark Web forums
- Delta between disclosure and mass exploitation represents the very narrow window of opportunity for defenders to stop adversaries in their tracks

Proactive Effects. Powered By ATT&CK.

- Helps to close the detection gap and enable critical early warning
- Empowers defenders with a superior vantage point
- Accelerates analysis and decision outcomes and lightens the cognitive burden on analysts
- Informs proactive operations including threat hunting missions

Looking Beyond The CVE

New CVE.
Same Old Tricks.

- Number of disclosed vulnerabilities continues to accelerate year-on-year, with **25,000+** in the last 12 months

- Reactively focusing defensive efforts on mitigation of individual CVE's does little to thwart determined adversaries who will simply pivot if one exploit is unsuccessful.

- Focus on post-exploitation behaviors rather than individual CVE's.

Adversary Tactics And Techniques

Cl0p

VOLT TYPHOON

ALPHV

LAZARUS

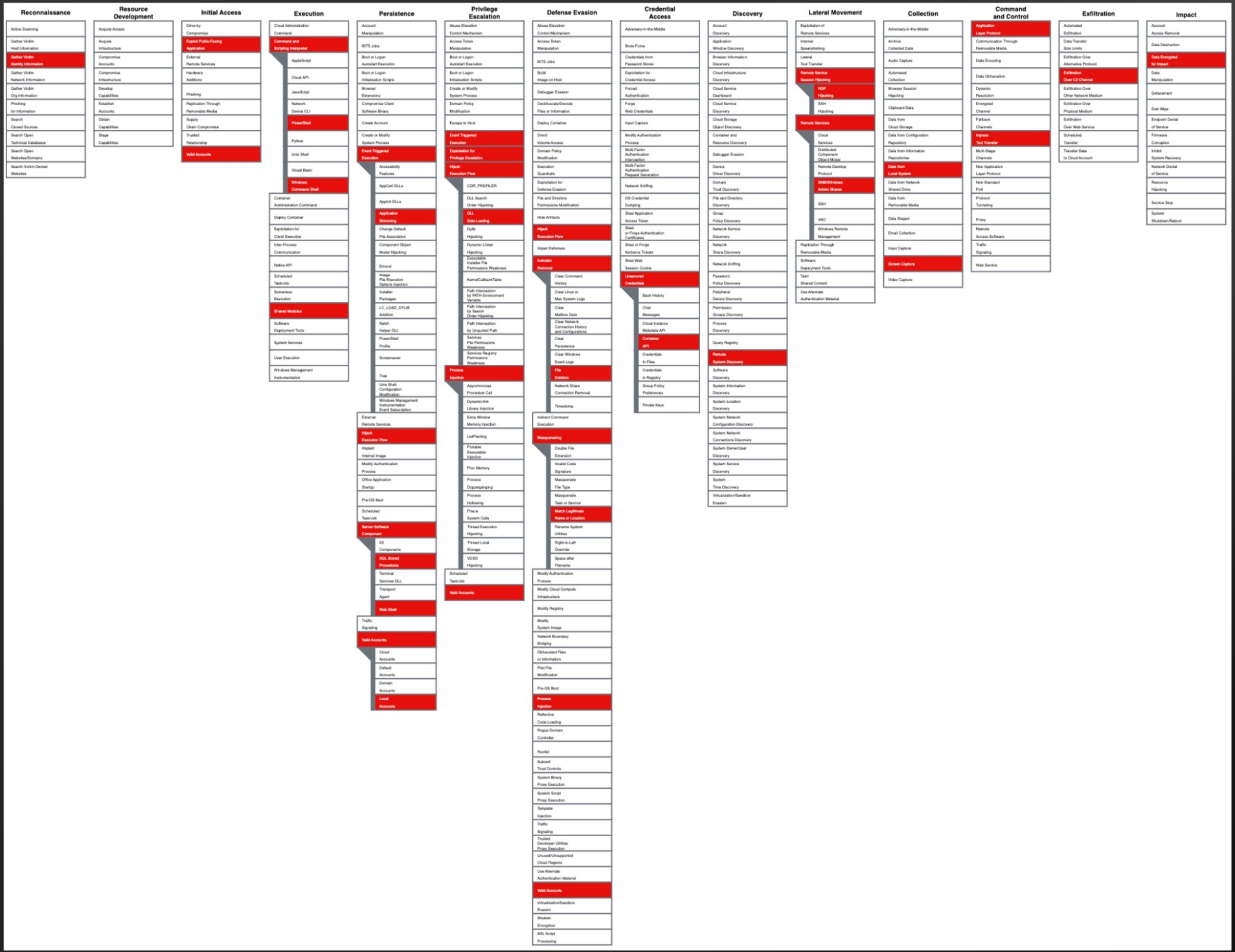
Four Adversaries. One Thing In Common.

Ransomware.
Without Ransomware.

- Ransomware continues to undergo paradigm shift as operators increasingly favor extortion over encryption

- The evolution of ransomware into double and triple extortion negates the need to deploy or execute an encryption binary

- Defenders must look beyond the existence of known ransomware



Reconnaissance

- Active Scanning
- Gather Victim Host Information
- **Gather Victim Identity Information**
- Gather Victim Network Information
- Gather Victim Org Information
- Phishing for Information
- Search Closed Sources
- Search Open Technical Databases
- Search Open Websites/Domains
- Search Victim-Owned Websites

Resource Development

- Acquire Access
- Acquire Infrastructure
- Compromise Accounts
- Compromise Infrastructure
- Develop Capabilities
- Establish Accounts
- Obtain Capabilities
- Stage Capabilities

Initial Access

- Drive-by Compromise
- **Exploit Public-Facing Application**
- External Remote Services
- Hardware Additions
- Phishing
- Replication Through Removable Media
- Supply Chain Compromise
- Trusted Relationship
- **Valid Accounts**

Execution

- Cloud Administration Command
- **Command and Scripting Interpreter**
  - AppleScript
  - Cloud API
  - JavaScript
  - Network Device CLI
  - **PowerShell**
  - Python
  - Unix Shell
  - Visual Basic
  - **Windows Command Shell**
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication
- Native API
- Scheduled Task/Job
- Serverless Execution
- **Shared Modules**
- Software Deployment Tools
- System Services
- User Execution
- Windows Management Instrumentation

Persistence

- Account Manipulation
- BITS Jobs
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Browser Extensions
- Compromise Client Software Binary
- Create Account
- Create or Modify System Process
- **Event Triggered Execution**
  - Accessibility Features
  - AppCert DLLs
  - AppInit DLLs
  - **Application Shimming**
  - Change Default File Association
  - Component Object Model Hijacking
  - Emond
  - Image File Execution Options Injection
  - Installer Packages
  - LC_LOAD_DYLIB Addition
  - Netsh Helper DLL
  - PowerShell Profile
  - Screensaver
  - Trap
  - Unix Shell Configuration Modification
  - Windows Management Instrumentation Event Subscription
- External Remote Services
- **Hijack Execution Flow**
- Implant Internal Image
- Modify Authentication Process
- Office Application Startup
- Pre-OS Boot
- Scheduled Task/Job
- **Server Software Component**
  - IIS Components
  - **SQL Stored Procedures**
  - Terminal Services DLL
  - Transport Agent
  - **Web Shell**
- Traffic Signaling
- **Valid Accounts**
  - Cloud Accounts
  - Default Accounts
  - Domain Accounts
  - **Local Accounts**

Privilege Escalation

- Abuse Elevation Control Mechanism
- Access Token Manipulation
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Create or Modify System Process
- Domain Policy Modification
- Escape to Host
- **Event Triggered Execution**
- **Exploitation for Privilege Escalation**
- **Hijack Execution Flow**
  - COR_PROFILER
  - DLL Search Order Hijacking
  - **DLL Side-Loading**
  - Dylib Hijacking
  - Dynamic Linker Hijacking
  - Executable Installer File Permissions Weakness
  - KernelCallbackTable
  - Path Interception by PATH Environment Variable
  - Path Interception by Search Order Hijacking
  - Path Interception by Unquoted Path
  - Services File Permissions Weakness
  - Services Registry Permissions Weakness
- **Process Injection**
  - Asynchronous Procedure Call
  - Dynamic-link Library Injection
  - Extra Window Memory Injection
  - ListPlanting
  - Portable Executable Injection
  - Proc Memory
  - Process Doppelgänging
  - Process Hollowing
  - Ptrace System Calls
  - Thread Execution Hijacking
  - Thread Local Storage
  - VDSO Hijacking
- Scheduled Task/Job
- **Valid Accounts**

Defense Evasion

- Abuse Elevation Control Mechanism
- Access Token Manipulation
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification
- Execution Guardrails
- Exploitation for Defense Evasion
- File and Directory Permissions Modification
- Hide Artifacts
- **Hijack Execution Flow**
- Impair Defenses
- **Indicator Removal**
  - Clear Command History
  - Clear Linux or Mac System Logs
  - Clear Mailbox Data
  - Clear Network Connection History and Configurations
  - Clear Persistence
  - Clear Windows Event Logs
  - **File Deletion**
  - Network Share Connection Removal
  - Timestomp
- Indirect Command Execution
- **Masquerading**
  - Double File Extension
  - Invalid Code Signature
  - Masquerade File Type
  - Masquerade Task or Service
  - **Match Legitimate Name or Location**
  - Rename System Utilities
  - Right-to-Left Override
  - Space after Filename
- Modify Authentication Process
- Modify Cloud Compute Infrastructure
- Modify Registry
- Modify System Image
- Network Boundary Bridging
- Obfuscated Files or Information
- Plist File Modification
- Pre-OS Boot
- **Process Injection**
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit
- Subvert Trust Controls
- System Binary Proxy Execution
- System Script Proxy Execution
- Template Injection
- Traffic Signaling
- Trusted Developer Utilities Proxy Execution
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material
- **Valid Accounts**
- Virtualization/Sandbox Evasion
- Weaken Encryption
- XSL Script Processing

Credential Access

- Adversary-in-the-Middle
- Brute Force
- Credentials from Password Stores
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials
- Input Capture
- Modify Authentication Process
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets
- Steal Web Session Cookie
- **Unsecured Credentials**
  - Bash History
  - Chat Messages
  - Cloud Instance Metadata API
  - **Container API**
  - Credentials In Files
  - Credentials in Registry
  - Group Policy Preferences
  - Private Keys

Discovery

- Account Discovery
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- **Remote System Discovery**
- Software Discovery
- System Information Discovery
- System Location Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

Lateral Movement

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- **Remote Service Session Hijacking**
  - **RDP Hijacking**
  - SSH Hijacking
- **Remote Services**
  - Cloud Services
  - Distributed Component Object Model
  - Remote Desktop Protocol
  - **SMB/Windows Admin Shares**
  - SSH
  - VNC
  - Windows Remote Management
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material

Collection

- Adversary-in-the-Middle
- Archive Collected Data
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository
- Data from Information Repositories
- **Data from Local System**
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- **Screen Capture**
- Video Capture

Command and Control

- **Application Layer Protocol**
- Communication Through Removable Media
- Data Encoding
- Data Obfuscation
- Dynamic Resolution
- Encrypted Channel
- Fallback Channels
- **Ingress Tool Transfer**
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy
- Remote Access Software
- Traffic Signaling
- Web Service

Exfiltration

- Automated Exfiltration
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- **Exfiltration Over C2 Channel**
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Exfiltration Over Web Service
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact

- Account Access Removal
- Data Destruction
- **Data Encrypted for Impact**
- Data Manipulation
- Defacement
- Disk Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

- Selection of common Cl0p TTPs at a glance
- 47+ Distinct MITRE ATT&CK techniques & sub-techniques
- Prolific use of LOTL techniques to support actions-on-objectives and maintain access
- Use of custom webshells masquerading as legitimate web service files to enable persistence and RCE

Know Your Enemy.

Hunt Them.

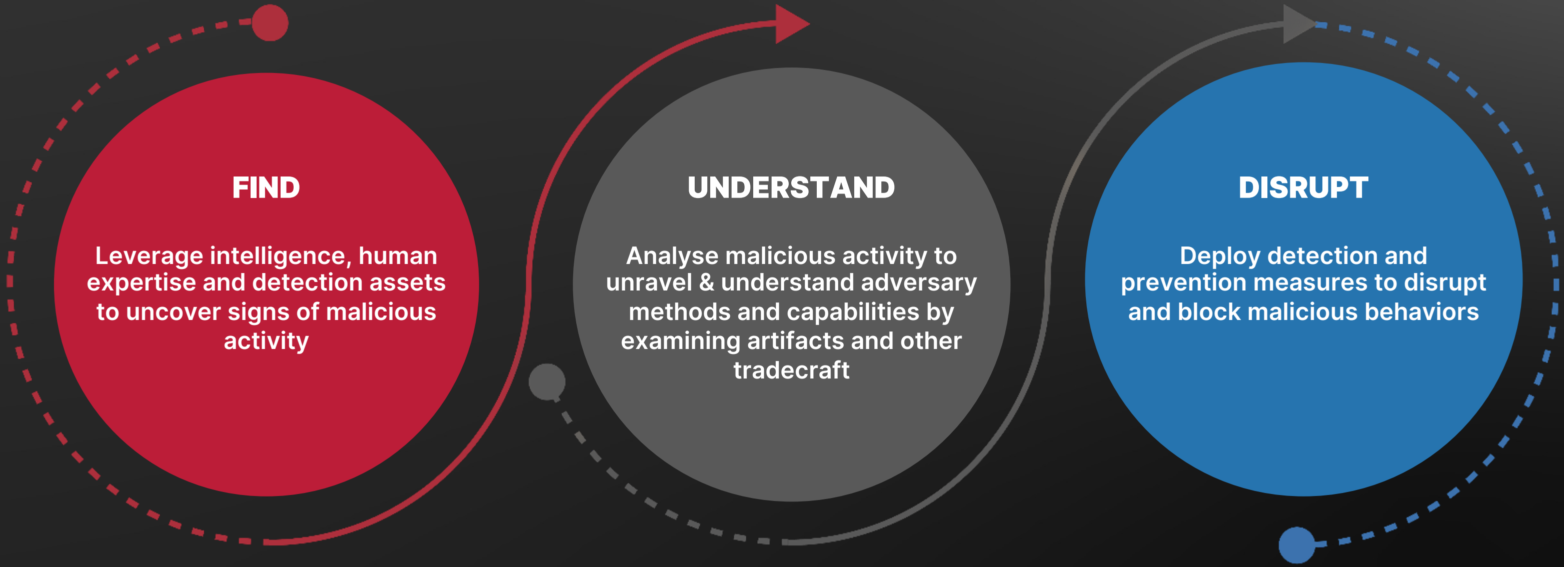
Intelligence Driven Threat Hunting

- The proactive discovery of unknown malicious artifacts and adversary methods not accounted for in passive, automated monitoring.

- Real-time intelligence powers hunting operations with actionable context on adversary targets, capabilities and methods.

- Informs threat hunters as they iteratively cycle through a targeting loop

Mission Objectives



FIND

Leverage intelligence, human expertise and detection assets to uncover signs of malicious activity

UNDERSTAND

Analyse malicious activity to unravel & understand adversary methods and capabilities by examining artifacts and other tradecraft

DISRUPT

Deploy detection and prevention measures to disrupt and block malicious behaviors

The Targeting Loop

Anomaly Based Hunting

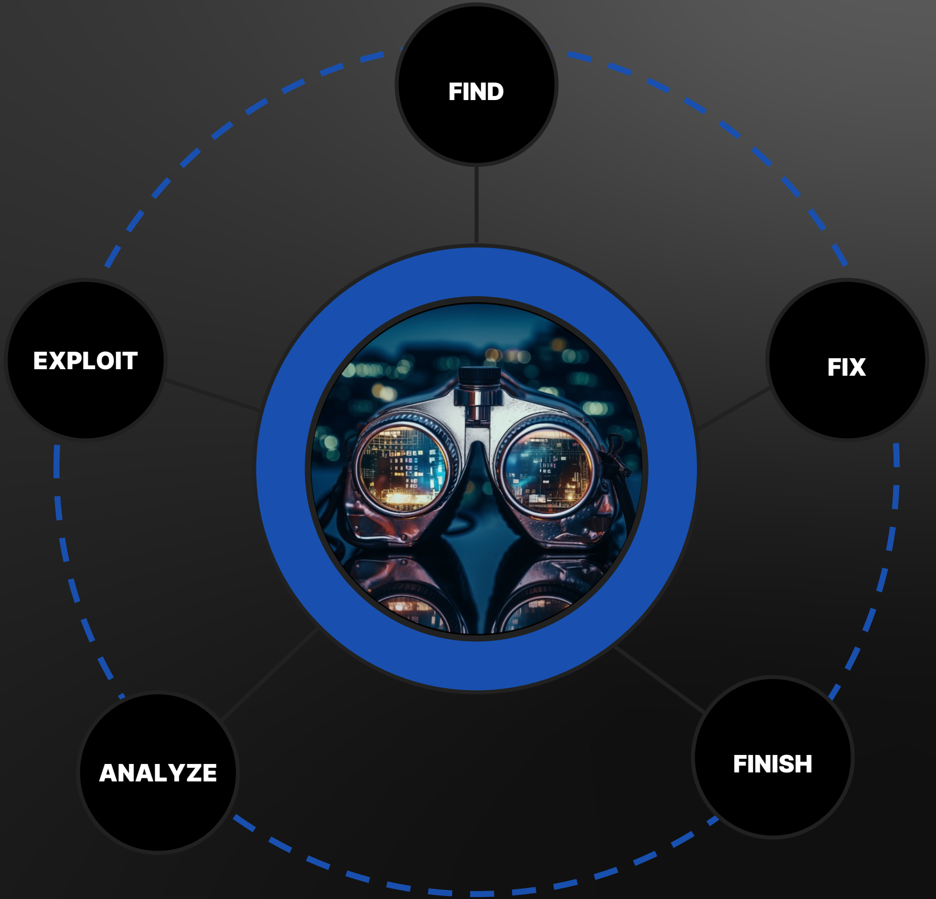
- Determination of statistical anomalies and trends across a broad data set of available telemetry

Hypothesis Based Hunting

- Proactively develop and apply hypothesis around how an adversary is likely to operate based on in depth understanding of their methods, capabilities & targets

Retrospective Hunting

- Intelligence driven approach to hunting leveraging static IOC's and atomic indicators, ie known bads.



Hunting Common Post Exploitation Behaviors

- Post-Exploitation Behaviors Consistent With Web Service Compromise
  - **Example:** Webshells deployed beneath web processes such as the Apache web process `httpd`, or IIS worker process `w3wp.exe`
- Suspicious C2 Communications & Known Actor Tooling
  - **Example:** Webshell communications, use of cloud admin or file sync tools, attempted exfiltration to known actor infrastructure or commonly abused cloud file sharing platforms (ie MEGA, Dropbox)
- Early-Stage Hands-on Ransomware Preparation
  - **Example**: User account creation, lateral movement, network, user and cloud enumeration

Hunting Webshells With Yara

```
rule M_Webshell_LEMURLOOT_DLL_1 {
    meta:
        disclaimer = "This rule is meant for hunting and is not tested to
run in a production environment"
        description = "Detects the compiled DLLs generated from
human2.aspx LEMURLOOT payloads."
        sample =
"c58c2c2ea608c83fad9326055a8271d47d8246dc9cb401e420c0971c67e19cbf"
        date = "2023/06/01"
        version = "1"
    strings:
        $net = "ASP.NET"
        $human = "Create_ASP_human2_aspx"
        $s1 = "X-siLock-Comment" wide
        $s2 = "X-siLock-Step3" wide
        $s3 = "X-siLock-Step2" wide
        $s4 = "Health Check Service" wide
        $s5 = "attachment; filename={0}" wide
    condition:
        uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and
        filesize < 15KB and
        $net and
        (
            ($human and 2 of ($s*)) or
            (3 of ($s*))
        )
}
```

- Looking for payloads associated with the LEMURLOOT webshell deployed by Cl0p during the MOVEit compromise

- Displayed strings show rule focus is identification of `.aspx` webshell activity including tampering with and replacement of MOVEit DB user account

Inform.
Enrich.
Hunt.

Thank you!