CYBER ADVISORY

04 June 2025

Ivanti EPMM Chained Vulnerabilities

OVERVIEW:

CVE-2025-4427 and CVE-2025-4428 are Ivanti Endpoint Manager Mobile (EPMM) vulnerabilities that when chained together, allow for successful exploitation that leads to unauthenticated remote code execution.[1] These CVE'S are confirmed to be exploited in the wild and are currently assessed to be utilized by the Chinese Threat Actor, UNC5221.[1]

Product	Affected Version(s)	Affected Common Platform Enumeration(CPEs)	Resolved Version(s)
Ivanti Endpoint Manager Mobile (EPMM)	≤ 11.12.0.4	11.12.0.0	11.12.0.5
	≤ 12.3.0.1	11.12.0.1	12.3.0.2
	≤ 12.4.0.4	11.12.0.2	12.4.0.2
	≤ 12.5.0.0	11.12.0.3	12.5.0.1
		12.3.0.0	

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for TLP:CLEAR, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TECHNICAL SUMMARY:

On 13 MAY 2025, Ivanti disclosed two vulnerabilities impacting their EPMM product. CVE-2025-4427, with a CVSS 3.1 base score of 5.3, is an authentication bypass flaw that allows an unauthenticated remote user to gain access to the server's application programming interface (API), a privilege typically reserved for authenticated users.[2,3] CVE-2025-4428, with a CVSS base score of 7.2, is a remote code execution vulnerability that allows an authenticated user to execute arbitrary code on a vulnerable device. [2,3] By chaining these vulnerabilities together, an unauthenticated user can use CVE-2025-4427 to inject malicious remote commands and then exploit CVE-2025-4428, allowing for unauthenticated remote execution.[1,3] Successful exploitation of these vulnerabilities allows threat actors to remotely access, manipulate, or compromise managed devices within an organization.[1]

The California Cybersecurity Integration Center (Cal-CSIC) assesses that organizations operating EPMM are highly likely to remain at significant risk of continued chain exploitation via CVE-2025-4427 and CVE-2025-4428. In addition, the Cal-CSIC also assesses that UNC5221 has a roughly even chance to be associated with exploitation activity relating to these CVE's.

Recommendations:

The Cal-CSIC recommends installing the most up to date versions of the affected software, found here Security Advisory Ivanti Endpoint Manager Mobile (EPMM) May 2025.

Additionally, Ivanti released the following workarounds:

- While this is an effective mitigation, it could impact on the functionality of your solution depending on your specific configurations. Integrations where Internet Protocols (IP) are difficult to determine or change often will be impacted, such as:
    - Windows Device Registrations using Autopilot
    - Microsoft Device Compliance and Graph API integrations

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for TLP:CLEAR, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

- Additionally, a Red Hat Package Manager (RPM) file can be provided if customers need an alternative option. Customers will need to open a Support Case to receive the RPM file. Here's a step-by-step guide to install the RPM file:
- Use Secure Shell (SSH) to connect to the instance and log in to the system Command Line Interface (CLI) as the admin user. The admin account is created during system installation.
- Type *enable* and provide the corresponding system password (set during the system installation) to enter EXEC PRIVILEGED mode. You'll notice the command line prompt changes from > to #.
- Run the command *install rpm* URL https://hostname/pathtorpm to download and install the RPM file.
- Once the RPM installation is complete, type *reload* to restart the system. This will apply the update effectively.

Current MITRE ATT&CK details of UNC5221 exploiting EPMM include:

Tactic: Initial Access (TA0001):
Threat actors utilize CVE-2025-4427 to gain unauthenticated access on vulnerable Ivanti EPMM systems

Tactic: Execution (TA0002): Technique: Command and Scripting Interpreter: Python (T1059.006):
UNC5221 observed to use SOCKS5 proxy to help provide persistent access to the internal network.

Additional Execution techniques utilized:
Tactic: Execution (TA0002): Technique: Exploitation for Client Execution (T1203):

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for TLP:CLEAR, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

Tactic: Persistence (TA0003): Technique: Account Manipulation: Additional Cloud Credentials (T1098.001):

Threat Actors observed utilizing a bash script to dump Office 365 integration tokens and credentials, which could be used by actors to gain unauthorized access to Microsoft Azure Entra ID services.

Additional Persistence techniques utilized:

Tactic: Persistence (TA0003): Technique: Server Software Component: SQL Stored Procedures (T1505.001)

Tactic: Defense Evasion (TA0005): Technique: Deobfuscate/Decode Files or Information (T1140):

Threat Actors utilizing KrustyLoader decrypt an AES-128-CFB encrypted version of Sliver backdoor to allow threat actors to establish remote access on the compromised system.

Additional Defense Evasion techniques utilized:

Tactic: Defense Evasion (TA0005): Technique: Impair Defenses: Disable or Modify Linux Audit System (T1562.012):
Tactic: Defense Evasion (TA0005): Technique: Indicator Removal: Clear Linux or Mac System Logs (T1070.002)
Tactic: Defense Evasion (TA0005): Technique: Indicator Removal: Clear Command History (T1070.003)
Tactic: Defense Evasion (TA0005): Technique: Indirect Command Execution (T1202)
Tactic: Defense Evasion (TA0005): Technique: Obfuscated Files or Information: Command Obfuscation (T1027.010)

Tactic: Credential Access (TA0006): Technique: Unsecured Credentials: Credentials In Files (T1552.001):

Threat actors leverage hardcoded MySQL database credentials to access the backend mifs (MobileIron File Service) database in Ivanti EPMM systems.

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for TLP:CLEAR, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

Additional Credential Access techniques utilized:

Tactic: Credential Access (TA0006): Technique: Credentials from Password Stores (T1555)
Tactic: Credential Access (TA0006): Technique: OS Credential Dumping: Cached Domain Credentials (T1003.005)
Tactic: Credential Access (TA0006): Technique: Unsecured Credentials: Credentials In Files (T1552.001)

Tactic: Discovery (TA0007):

Threat actors obtain access to the mifs (MobileIron File Service) database to obtain visibility into managed mobile devices, Lightweight Directory Access Protocol (LDAP) users and Office 365 access tokens.

Additional Discovery techniques utilized:

Tactic: Discovery (TA0007): Technique: Account Discovery (T1087)
Tactic: Discovery (TA0007): Technique: Cloud Service Discovery (T1526)
Tactic: Discovery (TA0007): Technique: Domain Trust Discovery (T1482)
Tactic: Discovery (TA0007): Technique: File and Directory Discovery (T1083)
Tactic: Discovery (TA0007): Technique: Group Policy Discovery (T1615)
Tactic: Discovery (TA0007): Technique: Network Service Discovery (T1046)
Tactic: Discovery (TA0007): Technique: Network Share Discovery (T1135)
Tactic: Discovery (TA0007): Technique: Permission Groups Discovery (T1069)
Tactic: Discovery (TA0007): Technique: Process Discovery (T1057)
Tactic: Discovery (TA0007): Technique: Remote System Discovery (T1018)
Tactic: Discovery (TA0007): Technique: Software Discovery (T1518)
Tactic: Discovery (TA0007): Technique: System Network Connections Discovery (T1049)
Tactic: Discovery (TA0007): Technique: System Service Discovery (T1007)

Tactic: Exfiltration (TA0010): Technique: Automated Exfiltration (T1020)

Threat Actors were found to issue scripted SQL queries to automate exfiltration of metadata.

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for TLP:CLEAR, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

Additional Exfiltration techniques utilized:

Tactic: Exfiltration (TA0010): Technique: Exfiltration Over C2 Channel (T1041)
Tactic: Exfiltration (TA0010): Technique: Exfiltration Over Web Service (T1567)
Tactic: Exfiltration (TA0010): Technique: Transfer Data to Cloud Account (T1537)

Tactic: Command and Control (TA0011): Technique: Ingress Tool Transfer (T1105):
Threat actors utilizing KrustyLoader embed an encrypted URL pointing to the Sliver C2 implant.

Tactic: Resource Development (TA0042): Technique: Stage Capabilities: Upload Tool (T1608.002):
Threat actors observed to install FRP (Fast Reverse Proxy), to establish a reverse SOCKS5 proxy.

Tactic: Reconnaissance (TA0043):
Threat actor leverages compromised Ivanti EPMM systems to export LDAP server details and to enumerate active directories

ATT&CK MITIGATIONS based off Tactics Techniques Procedures identified:[4]

1. **M1015: Active Directory Configuration:** Implement robust Active Directory (AD) configurations using group policies to secure user accounts, control access, and minimize the attack surface.
2. **M1017: User Training:** Educating employees and contractors on recognizing, reporting, and preventing cyber threats that rely on human interaction, such as phishing, social engineering, and other manipulative techniques.
3. **M1018: User Account Management:** Implementing and enforcing policies for the lifecycle of user accounts, including creation, modification, and deactivation. Proper account management reduces the attack surface by limiting unauthorized access, managing account privileges, and ensuring accounts are used according to organizational policies.
4. **M1021: Restrict Web-Based Content:** Restricting web-based content involves enforcing policies and technologies that limit access to potentially malicious websites, unsafe downloads, and unauthorized browser behaviors.

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for TLP:CLEAR, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

5. **M1022: Restrict File and Directory Permissions:** Restricting file and directory permissions involves setting access controls at the file system level to limit which users, groups, or processes can read, write, or execute files. By configuring permissions appropriately, organizations can reduce the attack surface for adversaries seeking to access sensitive data, plant malicious code, or tamper with system files.
6. **M1026: Privileged Account Management:** Implementing policies, controls, and tools to securely manage privileged accounts (e.g., SYSTEM, root, or administrative accounts).
7. **M1027: Password Policies:** Set and enforce secure password policies for accounts to reduce the likelihood of unauthorized access. Strong password policies include enforcing password complexity, requiring regular password changes, and preventing password reuse.
8. **M1028: Operating System Configuration:** Adjusting system settings and hardening the default configurations of an operating system (OS) to mitigate adversary exploitation and prevent abuse of system functionality.
9. **M1029: Remote Data Storage:** Moving critical data, such as security logs and sensitive files, to secure, off-host locations to minimize unauthorized access, tampering, or destruction by adversaries.
10. **M1030: Network Segmentation:** Network segmentation involves dividing a network into smaller, isolated segments to control and limit the flow of traffic between devices, systems, and applications.
11. **M1031: Network Intrusion Prevention:** Use intrusion detection signatures to block traffic at network boundaries.
12. **M1032: Multi-factor Authentication:** Use two or more pieces of evidence to authenticate to a system, such as username and password in addition to a token from a physical smart card or token generator.
13. **M1033: Limit Software Installation:** Prevent users or groups from installing unauthorized or unapproved software to reduce the risk of introducing malicious or vulnerable applications.
14. **M1037: Filter Network Traffic:** Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic.
15. **M1038: Execution Prevention:** Block execution of code on a system through application control, and/or script blocking.

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for TLP:CLEAR, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

16. **M1039: Environment Variable Permissions:** Restrict the modification of environment variables to authorized users and processes by enforcing strict permissions and policies.
17. **M1040: Behavior Prevention on Endpoint:** Use of technologies and strategies to detect and block potentially malicious activities by analyzing the behavior of processes, files, API calls, and other endpoint events.
18. **M1041: Encrypt Sensitive Information:** Protect sensitive data-at-rest with strong encryption.
19. **M1042: Disable or Remove Feature or Program:** Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.
20. **M1045: Code Signing:** Enforce binary and application integrity with digital signature verification to prevent untrusted code from executing.
21. **M1047: Audit**: Process of recording activity and systematically reviewing and analyzing the activity and system configurations. The primary purpose of auditing is to detect anomalies and identify potential threats or weaknesses in the environment.
22. **M1048: Application Isolation and Sandboxing:** Restrict the execution of code to a virtual environment on or in-transit to an endpoint system.
23. **M1049: Antivirus/Antimalware:** Utilize signatures, heuristics, and behavioral analysis to detect, block, and remediate malicious software, including viruses, trojans, ransomware, and spyware.
24. **M1050: Exploit Protection:** Deploy capabilities that detect, block, and mitigate conditions indicative of software exploits.
25. **M1051: Update Software:** Perform regular software updates to mitigate exploitation risk.
26. **M1054: Software Configuration:** Making security-focused adjustments to the settings of applications, middleware, databases, or other software to mitigate potential threats.
27. **M1056: Pre-compromise:** Proactive measures and defenses implemented to prevent adversaries from successfully identifying and exploiting weaknesses during the Reconnaissance and Resource Development phases of an attack.
28. **M1057: Data Loss Prevention:** Implementing strategies and technologies to identify, categorize, monitor, and control the movement of sensitive data within an organization.

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for TLP:CLEAR, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

DETECTION STRATEGIES:

1. **Review Ivanti EPMM Logs:** HTTP request logs can be found in /mi/tomcat/logs/access-logs*. These are Tomcat access logs that record all HTTP traffic processed by the EPMM server and are critical for detecting web-based attacks, including remote code execution (RCE) attempts.
2. **Utilize Regex-Based Detection for Remote Code Execution:** Identify suspicious Java-based remote command execution attempts via the format parameter, use format=.*exec(?:%28|\()([‘”}|%27)(.+?)\1 to search within access logs. This pattern will match with any attempts to invoke Java’s Runtime.exec() using reflection techniques commonly seen in RCE payloads.
3. **File System Monitoring for Suspicious File Activity**
4. **Monitor high-risk directories:** Look for unauthorized file uploads, executable drops or unusual script activity
    a. **/tmp/**
    b. **/var/tmp/**
    c. **/mi/tomcat/webapps/mifs/images/**
5. **Ingest and parse logs:** Access logs and process creations logs via SIEM/XDR platforms
6. **Create alerts:**
    a. For suspicious parameters within HTTP requests (?format= followed by encoded commands)
    b. For the execution of binaries in the high-risk directories

Indicator of Compromise (IoCs)

1. **KrustyLoader Samples**
    a. 44c4a0d1826369993d1a2c4fcc00a86bf45723342cfd9f3a8b44b673eee6733a
    b. 7a4e0eb5fbab9709c8f42beb322a5dfefbc4ec5f914938a8862f8e26a31d30a5
    c. f34db4ea8ec3c2cbe53fde3d73229ccaa2a9e7168cd96d9a49bf89adef5ab47c
    d. 150ccd3b24a1b40630e46300100a3f810aa7a6badeb6806b59ed6ba7bafb7b21

2. **Sliver C2 Sample**
    a. 29ae4fa86329bf6d0955020319b618d4c183d433830187b80979d392bf159768
3. **Linux Bash Script that was used to dump MySQL Database**
    a. 64764ffe4b1e4fc5b9fe27b513e02f0392f659c4e033d23a4ba7a3b7f20c6d30
    b. b422645db18e95aa0b4daaf5277417b73322bed306f42385ecfd6d49be26bfab
4. **Malicious domains used to deliver KrustyLoader payloads**
    a. openrbf.s3.amazonaws[.]com
    b. tnegadge.s3.amazonaws[.]com
    c. fconnect.s3.amazonaws[.]com
    d. trkbucket.s3.amazonaws[.]com
    e. the-mentor.s3.amazonaws[.]com
    f. tkshopqd.s3.amazonaws[.]com
5. **Staging URL for Sliver**
    a. http://abbeglasses.s3.amazonaws[.]com/dSn9tM
6. **Malicious Script hosting Site**
    a. https://dpaste[.]com/9MQEJ6VYR.txt
7. **Verify RCE via DNS Callback**
    a. ns1.cybertunnel[.]run

YARA Rules for Affiliated Malware:

```
rule M_APT_Backdoor_SLIVER_2 {
        meta:
                author = "Mandiant"
                date_created = "2024-03-15"
                date_modified = "2024-03-15"
                md5 = "4f68862d3170abd510acd5c500e43548"
                rev = 1
        strings:
                $str1 = "sliverpb/sliver.proto"
                $str2 = ".sliverpb.Envelope"
                $str3 = ".sliverpb.Register"
                $str4 = ".sliverpb.Register"
                $str5 = ".sliverpb.NetInterface"
                $str6 = ".sliverpb.FileInfo"
                $str7 = ".sliverpb.SockTabEntry.SockAddr"
                $str8 = ".sliverpb.SockTabEntry.SockAddr"
                $str9 = ".sliverpb.SockTabEntry"
                $str10 = ".sliverpb.DNSBlockHeader"
                $str11 = ".sliverpb.ServiceInfoReq"
                $str12 = ".sliverpb.ServiceInfoReq"
                $str13 = ".sliverpb.PivotType"
                $str14 = ".sliverpb.PivotType"
                $str15 = ".sliverpb.NetConnPivot"
                $str16 = ".sliverpb.PivotPeer"
                $str17 = ".sliverpb.PeerFailureType"
                $str18 = ".sliverpb.PivotListener"
                $str19 = ".sliverpb.WGTCPForwarder"
                $str20 = ".sliverpb.WGSocksServer"
                $str21 = ".sliverpb.WGSocksServer"
                $str22 = ".sliverpb.WGTCPForwarder"
                $str23 = ".sliverpb.WindowsPrivilegeEntry"
                $str24 = "sliver/protobuf/sliverpbb"
        condition:
                ((uint16(0) == 0x5a4d and uint32(uint32(0x3C)) == 0x00004550) or uint32(0)
== 0x464c457f or (uint32(0) == 0xBEBAFECA or uint32(0) == 0xFEEDFACE or uint32(0) ==
0xFEEDFACF or uint32(0) == 0xCEFAEDFE)) and 10 of them
}[5]

rule Linux_Downloader_KrustyLoader
{
   meta:
      author = "Theo Letailleur, Synacktiv"
      source = "Synacktiv"
      status = "RELEASED"
      sharing = "TLP:WHITE"
      category = "MALWARE"
      malware = "KrustyLoader"
      description = "Yara rule that detects Linux KrustyLoader"
```

```
strings:
  $tokio_worker = "TOKIO_WORKER_THREADS"
  $tmpdir = "/tmp/"

  // Load "/proc/self/exe" string
  $proc_self_exe = {
    48 B? 73 65 6C 66 2F 65 78 65 // mov     r64, 6578652F666C6573h
    48 8D B4 24 ?? ?? 00 00       // lea     rsi, [rsp+????h]
    48 89 46 0?                   // mov     [rsi+6], r64
    48 B? 2F 70 72 6F 63 2F 73 65 // mov     r64, 65732F636F72702Fh
    48 89 0?                      // mov     [rsi], r64
  }

  $pipe_suffix = "|||||||||||||||||||||||||||"

  // AES key expansion
  $aeskeygenassist = {
    660F3ADF0601 // aeskeygenassist xmm0, xmmword ptr [rsi], 1
    660F7F07     // movdqa  xmmword ptr [rdi], xmm0
    C3           // retn
  }

  // AES InvMixColumns
  $aesinvmixcol = {
    660F38DB06  // aesimc  xmm0, xmmword ptr [rsi]
    660F7F07    // movdqa  xmmword ptr [rdi], xmm0
    C3          // retn
  }

condition:
  uint32(0) == 0x464C457F and
  (
    all of them
  )
```

}[6]

FEEDBACK:

Feedback is critical to ensuring our advisories stay relevant and actionable for you and we'd like to hear from you. Please submit your feedback to CalCSIC@caloes.ca.gov with the CAL-CSIC advisory number in the email subject.

Need Help?	If you need further information about this advisory, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1.						
TIP Tags	CVE-2025-4427, CVE-2025-4428, High, Medium, Exploited						
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.						
Probability Term	**Almost No chance**	**Very Unlikely**	**Unlikely**	**Roughly Even**	**Likely**	**Very Likely**	**Almost Certainly**
Percentage Represented	**01-05%**	**05-20%**	**20-45%**	**45-55%**	**55-80%**	**80-95%**	**95-99%**

Sources

[1] EclecticIQ; "China-Nexus Threat Actor Actively Exploiting Ivanti Endpoint Manager Mobile (CVE-2025-4428) Vulnerability"; https://blog.eclecticiq.com/china-nexus-threat-actor-actively-exploiting-ivanti-endpoint-manager-mobile-cve-2025-4428-vulnerability; accessed 23 May 2025
[2] Ivanti; "Security Advisory Ivanti Endpoint Manager Mobile (EPMM) May 2025 (CVE-2025-4427 and CVE-2025-4428)"; https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM?language=en_US; accessed 27MAY25
[3] Watchtowr; "Expression Payloads Meet Mayhem – Ivanti EPMM Unauth RCE Chain"; https://labs.watchtowr.com/expression-payloads-meet-mayhem-cve-2025-4427-and-cve-2025-4428/; accessed 27MAY25
[4] MITRE; "MITRE ATT&CK"; https://attack.mitre.org/; accessed 27 May 2025
[5] Mandiant Advantage; "Explore Malware and Tools>SLIVER"; https://advantage.mandiant.com/malware/malware--26ab8b42-6258-5723-a57a-5d6bd90afb16#yara; accessed 27 May 2025
[6] GitHub; "krustyloader-analysis"; https://github.com/synacktiv/krustyloader-analysis/blob/main/KrustyLoader.yar; accessed 27 May 2025

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for TLP:CLEAR, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.