

This documentation contains confidential material and is intended solely for ACME personnel. Any unauthorized use or dissemination of this confidential material, either in full or in part, is strictly prohibited.

|  |  |
| --- | --- |
| **CISA Alert Code** | **aa25-203a** |
| **Date** | **July 30, 2025** |
| **Priority** | **Critical** |
| **Source and Information Reliability** | **A1** |
| **Sensitivity** | **Red** |

**Threat Intelligence Summary and Suggested Mitigation Techniques for Interlock Ransomware**

The ransomware variant known as Interlock first appeared in September 2024. Threat actors utilizing Interlock are known to target “business, critical infrastructure, and other organizations in North America and Europe [1].” The FBI has concluded that these threat actors are using this variant of ransomware to exploit system vulnerabilities for financial gain. Interlock gains unauthorized access to systems by way of drive-by downloads and/or social engineering. From this initial access, threat actors then move into the discovery, credential access, and lateral movement phases of the MITRE ATT&CK Matrix. This report is especially troubling due to ACME’s direct exposure to this threat. CISA lists several aspects of our internal network utilized by our essential business critical systems as being used to leverage Interlock ransomware against other organizations. The Windows and Linux operating systems we use at ACME along with tools such as “AnyDesk, Cobalt Strike, and ScreenConnect [1]” are all vulnerable to the threat from Interlock. These OS’ and tools are not directly to blame for the Interlock ransomware attacks, but their usage on business-critical systems does open the door to this threat. Due to Interlocks damage potential, broad range of attack vectors, and the currently vulnerable attack surface of our ICS environment, this threat must be our top priority at the moment.

Luckily, CISA has also outlined mitigation techniques and other recommended defensive strategies to combat this threat to our business continuity. CISA suggests that teams implement “DNS filtering, web access firewalls, [1]” as well as employee education regarding social engineering. Other mitigation techniques include thorough and consistent patch management programs and fine-tuned network segmentation. Lastly, CISA suggests using Implement identity, credential, and access management (ICAM) policies and multifactor authentication (MFA) for all services whenever possible.

**ACME Action Plan for Interlock Ransomware**

The action plan that I am suggesting ACME carries out to lessen our risk of falling prey to the threat from Interlock is multipronged and follows guidelines laid out by both CISA and NIST regarding this threat and other potential threats to ACME business continuity.

1. Relevant teams should collectively meet and begin a deep investigative process to determine if ACME systems have already been exploited by this threat or others. A full and comprehensive risk assessment and vulnerability analysis should be performed annually, and records indicate that the last instance was over three years ago. Even though we do not currently have visible indicators of compromise, this does not mean threat actors are not already at work in our sensitive systems full of confidential data.
2. After a full analysis and inventory of all internal ACME systems and assets is complete, suggested mitigation techniques can begin. CISA and NIST both suggest:
   1. DNS filtering, web access firewalls, routine patching policies, granular network segmentation, traffic filtering, disabling of unused ports, and the implementation of a zero-trust framework.
   2. Implementation of a comprehensive incident response plan and recovery plan.
   3. More robust password policies, MFA, ICAM, time-based account access policies, and new policies regarding which accounts can open a command line or execute scripts.
   4. Improvements to our SIEM for better threat detection and prevention.
   5. Periodic review of all domain controllers, servers, assets, and ACME’s active directory environment for unauthorized access or accounts, as well as an audit of all current user accounts.
   6. All system backups should be regularly performed, maintained offline, held in a separate secure geographical location, and encrypted.
   7. Regularly performed and proactive threat hunting and cyber threat intelligence (CTI) knowledge and awareness building.
3. While mitigation techniques are being performed, a cybersecurity awareness training program must begin. This should include current threats that face ACME such as social engineering, ransomware, etc. These meetings should be conducted with refreshed information every quarter with a more intensive and in-depth training session for all members of management as well.
4. Once ACME systems have been declared as clear of the Interlock ransomware threat, mitigation techniques performed, and first training session conducted, a third-party assessment to review if we are protected against the threat from Interlock should be performed.

**Industry and Media Coverage of Interlock Ransomware**

As expected, the cybersecurity industry was much earlier to report on this threat than the media at large. Cisco and Fortinet both published documentation regarding Interlock in November of 2024 with most media outlets publishing articles 8 months later in July 2025. Had ACME security teams performed more regular CTI knowledge sharing and building, we could have been made aware of this threat last November. However, this team is still highly capable, experienced, and driven to protect ACME and its ability to continue as an organization. We must collectively use this oversight as a learning opportunity to prepare for the next threat that comes our way.

References:

[1] Cybersecurity and Infrastructure Security Agency. “#StopRansomware: Interlock.” CISA. [Online] Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-203a>. Accessed: 7/30/25

[2] Biasiotto, E; Johnson, A; Raghuprasad, C; Szeliga, M. “Unwrapping the emerging Interlock ransomware attack.” Cisco. [Online] Available: <https://blog.talosintelligence.com/emerging-interlock-ransomware/>. Accessed: 7/30/25

[3] Imano, S; Gutierrez, F. “Ransomware Roundup - Interlock.” Fortinet. [Online] Available: <https://www.fortinet.com/blog/threat-research/ransomware-roundup-interlock>. Accessed: 7/30/25