Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

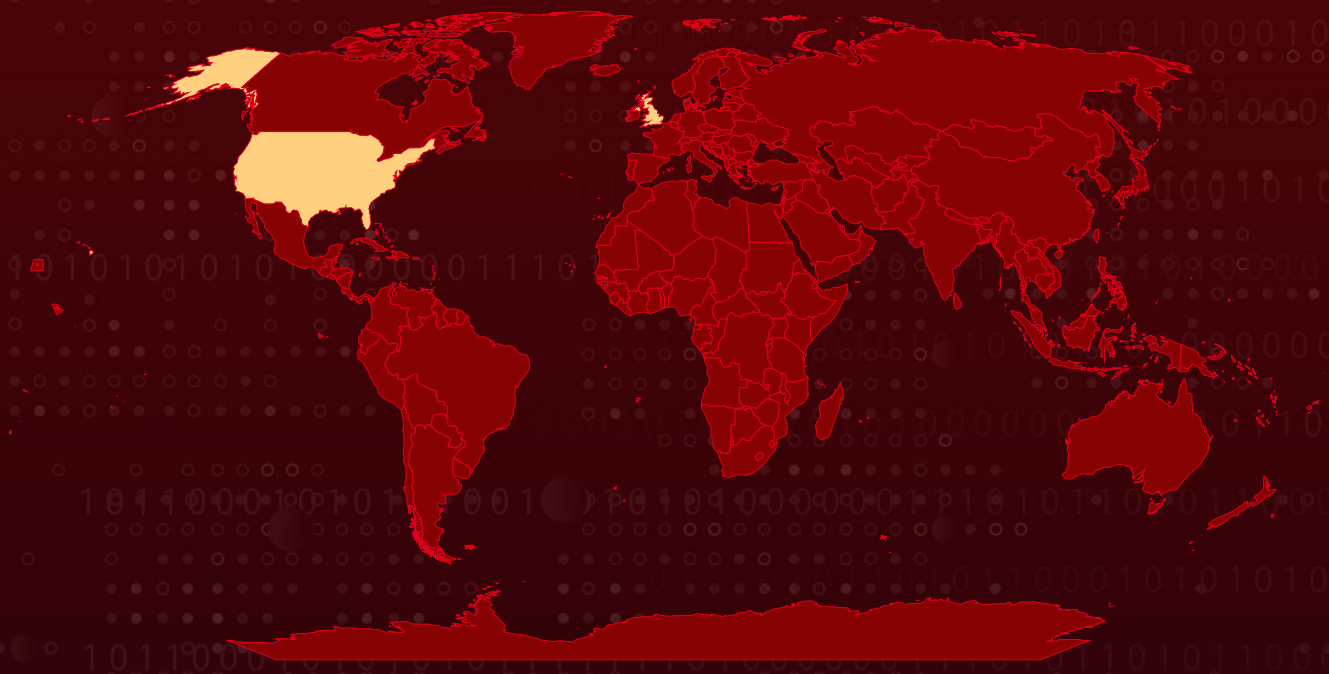
Interlock Ransomware Blurs Line Between Cybercrime and Espionage

Date of Publication	Admiralty Code	TA Number
May 21, 2025	A1	TA2025158

Summary

First Seen: 2025
Targeted Countries: United States, United Kingdom
Malware: Interlock ransomware
Targeted Industries: Defense, Government, Finance
Attack: Interlock Ransomware is a growing cyber threat targeting critical sectors, including defense, government, and finance. It uses advanced evasion techniques and psychological tactics to pressure victims. Recent breaches exposed sensitive military data and disrupted trusted institutions. The group's expanding reach underscores the urgent need for cross-sector cybersecurity vigilance.

Attack Regions



Attack Details

#1

Interlock Ransomware has emerged as a significant threat to the defense industrial base, with recent attacks targeting major U.S. defense contractors such as National Defense Corporation (NDC) and its subsidiary AMTEC. These breaches resulted in the theft and public exposure of highly sensitive documents, including logistics data, supplier information, and contract details involving key defense entities. Beyond financial extortion, Interlock's actions risk undermining national security by exposing critical military supply chains to adversaries.

#2

Technically, Interlock employs a range of evasion and persistence techniques, including obfuscated payloads, living-off-the-land binaries, credential theft, and lateral movement via remote access tools like AnyDesk and PuTTY. The group's ransom notes have become more psychologically manipulative, emphasizing legal and regulatory consequences to increase pressure on victims. Interlock's infrastructure is tightly controlled, and its malware is frequently updated to evade detection, with recent variants incorporating advanced info-stealers and modular payloads for greater flexibility and stealth.

#3

While Interlock appears financially motivated, its focus on high-value, strategic targets and the nature of stolen data raise concerns about possible nation-state links. These attacks illustrate how ransomware can serve both criminal and espionage purposes—an especially alarming amid ongoing global tensions.

#4

The implications of these attacks are far-reaching. Exposed data can reveal the structure and vulnerabilities of defense logistics networks, including warehouse locations, shipment schedules, and personnel identities. Such intelligence is highly valuable to foreign state actors and could be exploited to disrupt operations, intercept shipments, or replicate export-controlled technologies. The theft of intellectual property also presents a long-term strategic threat to U.S. military competitiveness.

#5

Importantly, Interlock's campaign is not limited to the defense sector. The group has a known history of targeting critical infrastructure, including healthcare, education, and government entities. Most recently, on May 21, 2025, Interlock claimed responsibility for compromising West Lothian Council, a local government authority in the UK, and Semple, Marchal & Cooper, LLP, a prominent U.S.-based accounting firm. These incidents underscore the group's broad operational reach and highlight the urgent need for enhanced cybersecurity vigilance across all sectors.

Recommendations

Strengthen Supply Chain Cybersecurity: Defense contractors and their suppliers, especially small and medium-sized businesses, must enhance cybersecurity measures. This includes implementing strict access controls, network segmentation, and regular security audits to reduce the risk of lateral movement and limit exposure in case of compromise.

Deploy Advanced Threat Detection and Response: Organizations should invest in real-time monitoring solutions and endpoint detection and response (EDR) tools that can identify obfuscated payloads, living-off-the-land tactics, and credential theft. Regular threat hunting and penetration testing can help detect early indicators of compromise.

Strengthen Email and Web Security: Deploy advanced email gateways and web filters to block phishing attempts, malicious links, and attachments that may deliver initial payloads. Educate employees to recognize social engineering tactics, such as fake software updates and deceptive IT support prompts

Conduct Regular Data Backups and Test Restoration: Regularly backup critical data and systems, store them securely offline. Test restoration processes to ensure backup integrity and availability. In case of an Agenda ransomware attack, up-to-date backups enable recovery without paying the ransom.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection
TA0011 Command and Control	TA0010 Exfiltration	TA0040 Impact	T1566 Phishing

T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1203 Exploitation for Client Execution	T1053 Scheduled Task/Job
T1053.005 Scheduled Task	T1543 Create or Modify System Process	T1037 Boot or Logon Initialization Scripts	T1070 Indicator Removal
T1070.004 File Deletion	T1027 Obfuscated Files or Information	T1036 Masquerading	T1036.005 Match Legitimate Name or Location
T1555 Credentials from Password Stores	T1083 File and Directory Discovery	T1049 System Network Connections Discovery	T1082 System Information Discovery
T1115 Clipboard Data	T1021 Remote Services	T1105 Ingress Tool Transfer	T1005 Data from Local System
T1041 Exfiltration Over C2 Channel	T1486 Data Encrypted for Impact	T1491 Defacement	T1195 Supply Chain Compromise

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	23[.]95[.]182[.]59, 195[.]201[.]21[.]34, 159[.]223[.]46[.]184, 23[.]227[.]203[.]162, 65[.]109[.]226[.]176, 65[.]38[.]120[.]47, 216[.]245[.]184[.]181, 212[.]237[.]217[.]182, 168[.]119[.]96[.]41, 216[.]245[.]184[.]170, 65[.]108[.]80[.]58,

TYPE	VALUE
IPv4	84[.]200[.]24[.]41, 206[.]206[.]123[.]65, 49[.]12[.]102[.]206, 193[.]149[.]180[.]158, 85[.]239[.]52[.]252, 5[.]252[.]177[.]228, 80[.]87[.]206[.]189, 65[.]108[.]80[.]58, 212[.]104[.]133[.]72, 140[.]82[.]14[.]117, 64[.]94[.]84[.]85, 49[.]12[.]69[.]80, 96[.]62[.]214[.]11, 177[.]136[.]225[.]153, 188[.]34[.]195[.]44, 45[.]61[.]136[.]202

Recent Breaches

https://www.westlothian.gov.uk
https://semplecpa.com
https://bentleyindustriesinc.com
https://fesd.org
https://jancosteel.com
https://www.davita.com
https://www.madisonaz.org

References

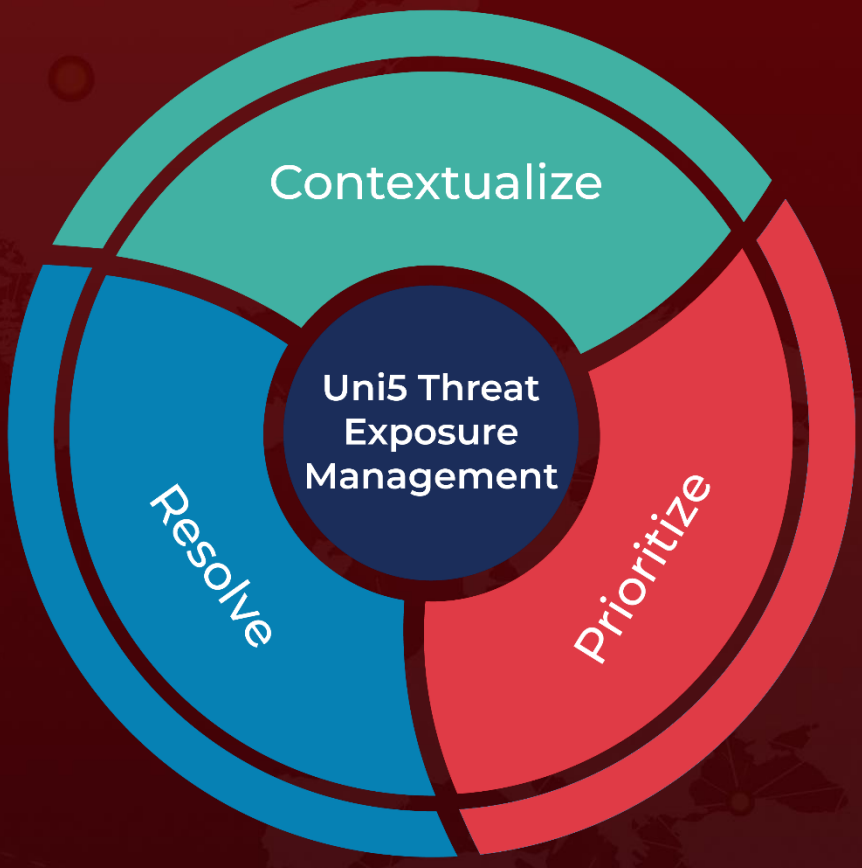
https://www.resecurity.com/blog/article/how-interlock-ransomware-affects-the-defense-industrial-base-supply-chain

https://hivepro.com/threat-advisory/interlock-double-punch-encryption-and-exposure-at-scale/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

May 21, 2025 • 9:00 PM

More at www.hivepro.com