Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

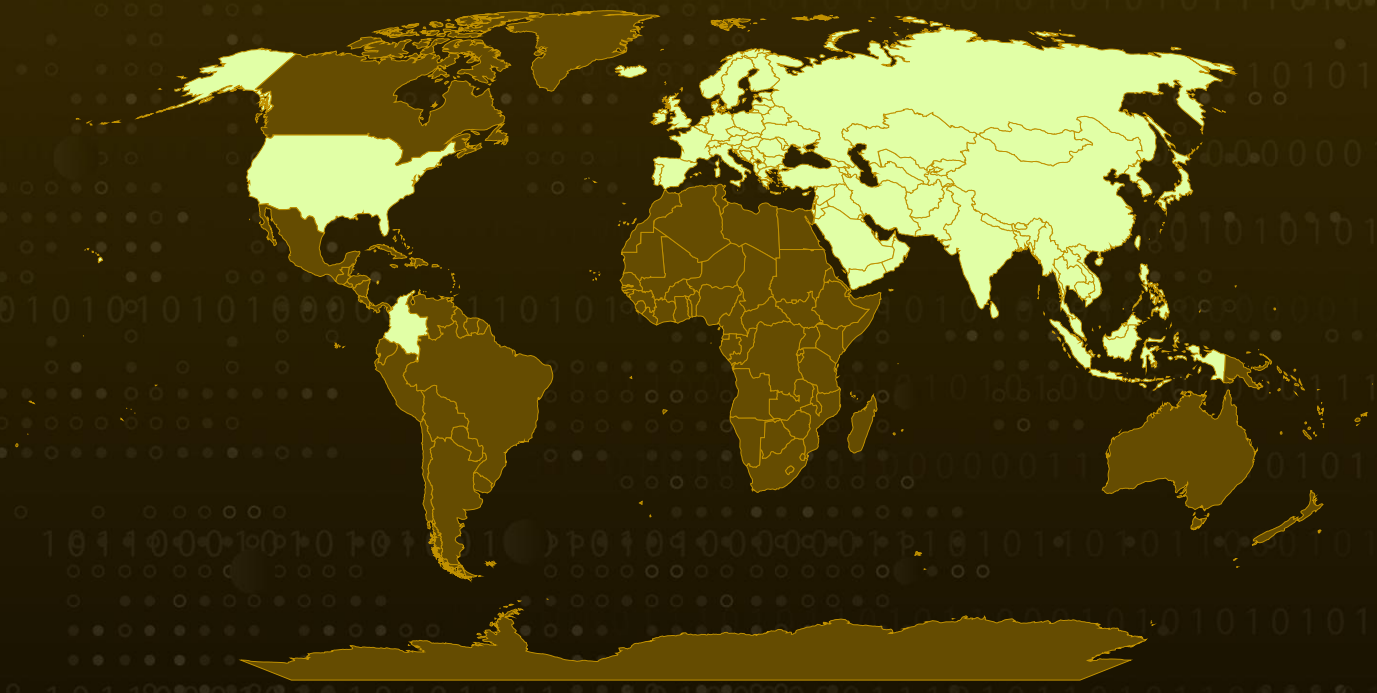
BERT Ransomware Quietly Gains Global Ground

Date of Publication	Last Update Date	Admiralty Code	TA Number
June 23, 2025	July 30, 2025	A1	TA2025197

Summary

Active Since: March 2025
Malware: Bert Ransomware (aka Water Pombero)
Targeted Regions: United States, Colombia, Asia, Europe
Targeted Industries: Transportation, Technology, Healthcare, Business Services, Manufacturing
Targeted Platforms: Windows and Linux
Ransom: 1.5 BTC (approximately $152,000)
Attack: BERT ransomware, active since March 2025, has rapidly evolved into a multi-platform threat targeting systems across critical sectors. Leveraging REvil's code and demanding Bitcoin via the Session messenger, the campaign's growing operational footprint and double-extortion tactics signal a persistent and escalating threat landscape for global enterprises.

Attack Regions



Attack Details

#1 In mid-March 2025, a new ransomware strain known as BERT, also known as Water Pombero, emerged in the wild. It allegedly claimed multiple victims across the Healthcare, Technology, and Transportation sectors in Türkiye, the United States, and the United Kingdom. The strain follows a typical double-extortion format.

#2 The ransomware initially targeted Windows environments, leveraging phishing emails containing malicious attachments or links as its primary infection vector. These emails typically deliver PowerShell-based loaders designed to evade security measures, escalate privileges, and deploy the ransomware payload.

#3 By May 2025, the threat actors behind BERT had expanded their operations to include Linux systems, employing custom ELF binaries while retaining the same phishing-based delivery approach. Notably, BERT's Linux variant shares approximately 80% of its codebase with REvil (Sodinokibi), one of the most notorious ransomware families to date.

#4 Once deployed, the ransomware encrypts files across the compromised network, appending extensions such as .encryptedbybert, .encryptedbybert3, or .hellofrombert to the affected files. It also drops a ransom note named note.txt into each directory containing encrypted data.

#5 Victims are instructed to contact the attackers via the privacy-centric Session messenger to negotiate a ransom payment, which is demanded exclusively in Bitcoin. BERT's activity has resulted in several high-profile incidents. In April 2025, SIMCO Electronics (USA) suffered a significant breach that disrupted manufacturing processes and exposed confidential internal data.

#6 The following month, All Ring Tech (Taiwan) was targeted by a ransomware attack that crippled logistics systems and halted shipment tracking. Most recently, in June 2025, the group claimed responsibility for stealing nearly 140 GB of sensitive information from S5 Agency World, a UK-based maritime logistics firm operating in over 360 ports worldwide.

Recommendations

Strengthen Email Security and Phishing Defenses: Enhance email gateway controls to detect and quarantine phishing emails carrying malicious attachments or links. Leverage advanced threat protection, sandboxing, and dynamic analysis tools to inspect attachments and URLs before delivery.

Implement the 3-2-1 Backup Rule: Maintain three total copies of your data, with two backups stored on different devices and one backup kept offsite or in the cloud. This ensures redundancy and protects against data loss from ransomware attacks.

Backup & Recovery Preparedness: Maintain offline, immutable, and regularly tested backups. Ensure recovery time objectives (RTOs) and recovery point objectives (RPOs) meet business continuity requirements in the event of ransomware deployment.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
TA0010 Exfiltration	**TA0040** Impact	**T1566** Phishing	**T1204** User Execution
T1204.002 Malicious File	**T1059.001** PowerShell	**T1059** Command and Scripting Interpreter	**T1547** Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	**T1543** Create or Modify System Process	**T1543.003** Windows Service	**T1548** Abuse Elevation Control Mechanism
T1548.002 Bypass User Account Control	**T1068** Exploitation for Privilege Escalation	**T1562** Impair Defenses	**T1562.001** Disable or Modify Tools
T1027 Obfuscated Files or Information	**T1070.004** File Deletion	**T1070** Indicator Removal	**T1083** File and Directory Discovery
T1049 System Network Connections Discovery	**T1005** Data from Local System	**T1573** Encrypted Channel	**T1041** Exfiltration Over C2 Channel

T1106 Native API	T1053.005 Scheduled Task	T1053 Scheduled Task/Job	T1574 Hijack Execution Flow
T1574.001 DLL	T1140 Deobfuscate/Decode Files or Information	T1070.006 Timestomp	T1497 Virtualization/Sandbox Evasion
T1564.001 Hidden Files and Directories	T1564 Hide Artifacts	T1055 Process Injection	T1082 System Information Discovery
T1071 Application Layer Protocol	T1056 Input Capture	T1518 Software Discovery	T1518.001 Security Software Discovery
T1012 Query Registry	T1057 Process Discovery	T1087 Account Discovery	T1489 Service Stop
T1486 Data Encrypted for Impact	T1490 Inhibit System Recovery	T1491 Defacement	T1657 Financial Theft
T1562.004 Disable or Modify System Firewall	T1673 Virtual Machine Discovery	T1485 Data Destruction	

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxp[:]//185[.]100[.]157[.]74/payload[.]exe, hxxp[:]//169[.]254[.]169[.]254/latest/meta-data/ami-id, hxxp[:]//185[.]100[.]157[.]74/start[.]ps1
IPv4	169[.]254[.]169[.]254, 185[.]100[.]157[.]74
MD5	71dc9540eb03f2ed4d1b6496b13fe839, 00fdc504be1788231aa7b7d2d1335893, d1013bbaa2f151195d563b2b65126fa3, 3e581aad42a2a9e080a4a676de42f015, edec051ce461d62fbbd3abf09534b731, 5cab4fabffeb5903f684c936a90e0b46,

TYPE	VALUE
MD5	003291d904b89142bada57a9db732ae7, 29a2cc59a9ebd334103ce146bca38522, 38ce06bf89b28ccebf5a78404eb3818e
SHA256	8478d5f5a33850457abc89a99718fc871b80a8fb0f5b509ac1102f441189a311, 6182df9c60f9069094fb353c4b3294d13130a71f3e677566267d4419f281ef02, ced4ed5e5ef7505dd008ed7dd28b8aff38df7febe073d990d6d74837408ea4be, f2dc218ea8e2caa8668e54bae6561afd9fbf035a40b80ce9e847664ff0809799, 25c693808095f45d297171eba5196e9a5176281a2d248cb1a8cfa07a68bbe332, 78eb838238dad971dcbc46b86491d95e297f3d47dc770de5c43af3163990d31c, 5bba035c4cb3c2e09a355d9356b3397184af4bf1ac1ff1df99ae9c15edee9f2b, c7efe9b84b8f48b71248d40143e759e6fc9c6b7177224eb69e0816cc2db393db, b2f601ca68551c0669631fd5427e6992926ce164f8b3a25ae969c7f6c6ce8e4f, 1ef6c1a4dfdc39b63bfe650ca81ab89510de6c0d3d7c608ac5be80033e559326, 70211a3f90376bbc61f49c22a63075d1d4ddd53f0aefa976216c46e6ba39a9f4, 75fa5b506d095015046248cf6d2ec1c48111931b4584a040ceca57447e9b9d71, bd2c2cf0631d881ed382817afcce2b093f4e412ffb170a719e2762f250abfea4
Filename	note.txt
TOR Address	bertblogsoqmm4ow7nqyh5ik7etsmefdbf25stauecytvwy7tkgizhad[.]onion, wtwdv3ss4d637dka7iafl7737ucykei7pluzc7is3mgo2vl5nmq7eeid[.]onion

Recent Breaches

https://s5agencyworld.com/
https://columbiati.com.br/
https://www.wawasandengkil.com/
https://allring-tech.com.tw/
https://www.simco.com/
https://yozgatsehir.saglik.gov.tr/
https://nationalticket.com/

References

https://theravenfile.com/2025/06/16/bert-ransomware/

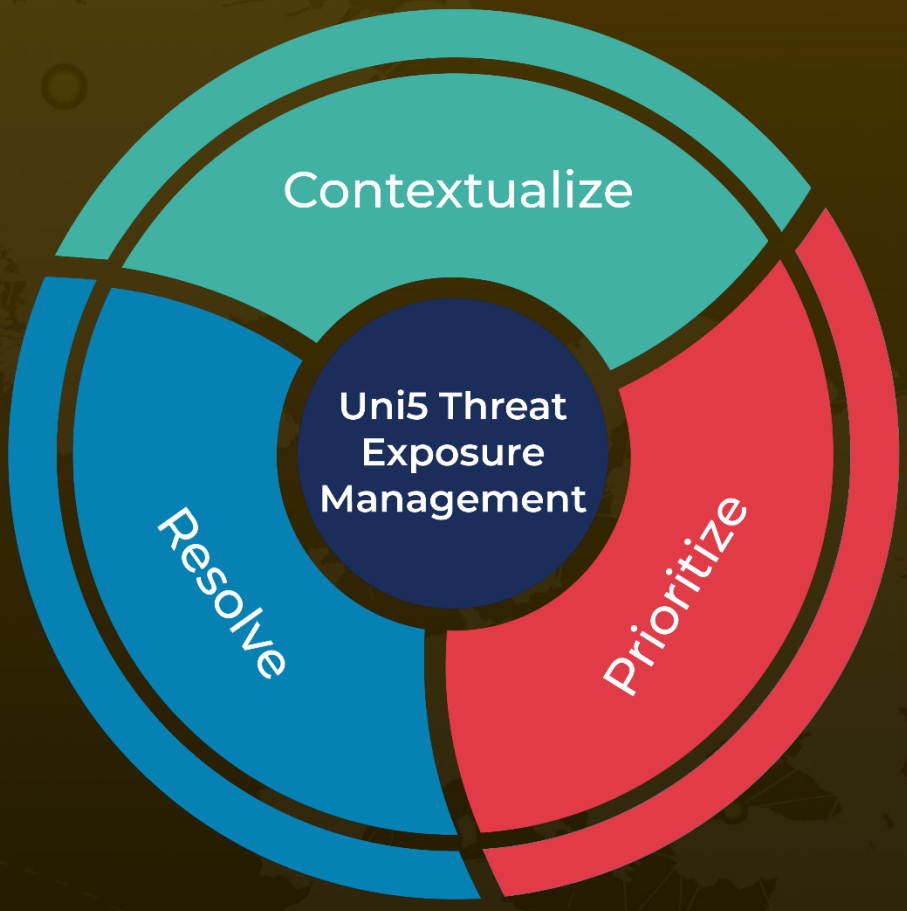
https://www.broadcom.com/support/security-center/protection-bulletin/bert-ransomware

https://www.trendmicro.com/en_us/research/25/g/bert-ransomware-group-targets-asia-and-europe-on-multiple-platforms.html

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

June 23, 2025 • 10:30 PM

More at www.hivepro.com