مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

BERT Ransomware Campaign

Tracking #:432317474

Date:10-07-2025

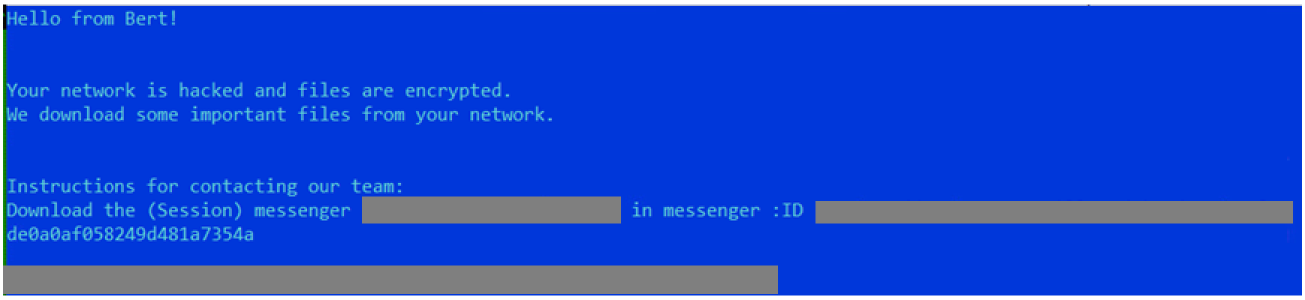
THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a newly emerged ransomware group, BERT (tracked by Trend Micro as Water Pombero), has launched widespread, cross-platform attacks targeting healthcare and IT services organizations worldwide.

TECHNICAL DETAILS:

A newly emerged ransomware group, BERT (tracked by Trend Micro as Water Pombero), has launched widespread, cross-platform attacks targeting healthcare and IT services organizations worldwide.
The group employs simple but effective tooling, focusing on PowerShell loaders, privilege escalation, and high-speed encryption, with observed impacts on critical sectors such as healthcare and IT services.
Notably, BERT's Windows and Linux variants differ in their tactics but both aim to disable defenses and encrypt files rapidly, even targeting ESXi hosts for maximum impact. The use of Russian-registered infrastructure, PowerShell-based delivery mechanisms, and the resemblance to REvil and Babuk code indicate the reuse of code from former prominent ransomware families.



```
Hello from Bert!


Your network is hacked and files are encrypted.
We download some important files from your network.


Instructions for contacting our team:
Download the (Session) messenger [redacted] in messenger :ID [redacted]
de0a0af058249d481a7354a

[redacted]
```

BERT ransom note

Observed Tactics, Techniques, and Procedures (TTPs):

Tactic	Technique	MITRE ID	Platform	Description
Execution	PowerShell Execution	T1059.001	Windows	Uses start.ps1 to load payload
Defense Evasion	Disable or Modify Tools	T1562.001	Windows	Disables Defender, UAC, Firewall
Defense Evasion	Disable System Firewall	T1562.004	Windows	Disables domain, public, and private profiles
Privilege Escalation	Bypass UAC	T1548.002	Windows	Elevates via PowerShell with -Verb RunAs
Discovery	File and Directory Discovery	T1083	Windows / Linux	Enumerates target paths

Discovery	Virtual Machine Discovery	T1673	Linux	Uses esxcli vm process list
Discovery	Process Discovery	T1057	Windows	Terminates key services
Impact	Data Encryption	T1486	Windows / Linux	Encrypts data using AES
Impact	Data Destruction	T1485	Windows / Linux	Deletes or overwrites backups/snapshots
Impact	Inhibit System Recovery	T1490	Windows / Linux	Targets ESXi VM snapshots

Indicators of Compromise (IoC):

SHA256	Description
1ef6c1a4dfdc39b63bfe650ca81ab89510de6c0d3d7c608ac5be80033e559326	Defender Disabling Tool (DefenderControl)
70211a3f90376bbc61f49c22a63075d1d4ddd53f0aefa976216c46e6ba39a9f4	Process Hacker Binary
75fa5b506d095015046248cf6d2ec1c48111931b4584a040ceca57447e9b9d71	BERT Ransomware (Windows - New Variant)
8478d5f5a33850457abc89a99718fc871b80a8fb0f5b509ac1102f441189a311	BERT Ransomware (Windows - Older Variant)
b2f601ca68551c0669631fd5427e6992926ce164f8b3a25ae969c7f6c6ce8e4f	PowerShell Loader (start.ps1)
bd2c2cf0631d881ed382817afcce2b093f4e412ffb170a719e2762f250abfea4	Alternate Process Hacker Variant
c7efe9b84b8f48b71248d40143e759e6fc9c6b7177224eb69e0816cc2db393db	BERT Ransomware (Linux Variant)
hxxp://185[.]100[.]157[.]74/payload[.]exe	Malware payload download site

RECOMMENDATIONS:

- IOC Review and Threat Hunting: Conduct immediate IOC sweeps using the provided file hashes, IP addresses, and domains.
- Limit PowerShell access to admin accounts only.
- Enable PowerShell logging (ModuleLogging, ScriptBlockLogging) for monitoring.
- Audit and minimize local administrator privileges.
- Prevent bypass of UAC by enforcing Always Notify for User Account Control.
- Isolate ESXi/vCenter management interfaces from the internet and production LAN.
- Disable unused management protocols and restrict access via ACLs/VPN.
- Maintain offline, encrypted, and immutable backups.
- Regularly test restoration of virtual machines, snapshots, and databases.
- Block execution of unauthorized admin tools (e.g., Process Hacker, DefenderControl).
- Train employees to recognize phishing, fake download links, and macro-laced documents.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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