Bert Ransomware – Malware Trends Tracker by ANY.RUN

By Stanislav Gayvoronsky

Archived: 2026-04-05 20:54:47 UTC

Bert Ransomware: The Silent Storm Sweeping Critical Sectors

Key Takeaways

- Bert is a **fast-evolving ransomware family** that encrypts files and demands cryptocurrency payments.
- **High-value targets** include SMBs, healthcare, financial institutions, and government agencies.
- Once inside, Bert can **encrypt data, disable backups, kill security tools, and spread laterally** across networks.

Observe Bert's killchain, network connections, and processes in ANY.RUN's Interactive Sandbox:

 Bert Ransomware detonated in Interactive Sandbox *Bert Ransomware Windows variant detonated in Interactive Sandbox*

- **Double extortion** tactics – data theft plus encryption – raise both financial and reputational risks.
- Bert infections usually start with **phishing, weak RDP credentials, or unpatched vulnerabilities**
- Detection relies on behavioral monitoring, IOCs, and **real-time threat intelligence** to flag suspicious activity early.

Use ANY.RUN's Threat Intelligence Lookup to gather and explore Bert's IOCs and TTPs:

threatName:"bert"

 Bert samples found via TI Lookup *Bert samples found via TI Lookup: watch behavior, gather indicators*

- **Prevention** requires MFA, patching, backups, phishing awareness training, and threat intelligence-driven defenses.

What is Bert Ransomware?

BERT ransomware distinguishes itself through its multi-platform capabilities and streamlined attack execution. Bert has been observed targeting organizations since April 2025, with confirmed victims in sectors including healthcare, technology and event services. The ransomware group operates with a sophisticated approach that belies its relatively simple code structure, demonstrating how modern cybercriminals can achieve maximum impact with efficient tools.

An analysis of an infection of a Windows system found that the variant used a straightforward code structure, with specific strings to match and terminate certain processes. Files were encrypted using the standard AES algorithm.

The public key, file extension, and ransom note were easily accessible. This approach allows for rapid deployment while maintaining strong encryption capabilities that make data recovery without payment extremely difficult.

The ransomware is cross-platform, with Windows variants using PowerShell loaders for initial execution and Linux variants optimized for server environments like VMware ESXi. Bert's operations blend traditional encryption with advanced evasion techniques, such as multi-threaded processing for speed and targeted shutdowns of virtual machines.

By July 2025, multiple iterations have been observed, including updates to encryption libraries and command-line flags, highlighting the group's adaptability. Unlike more sophisticated actors, Bert prioritizes speed over stealth — encrypting files as they are discovered rather than pre-scanning — making it a growing concern for hybrid IT environments.

Bert has a modular structure: it can integrate with other malware loaders and is often distributed through phishing emails, malicious attachments, and compromised remote desktop protocol (RDP) access. This adaptability makes it dangerous for businesses across different sectors.

Multiple infection vectors include:

- Malicious email attachments and links.
- Exploited RDP services.
- Unpatched software vulnerabilities.
- Trojanized software installers.
- Lateral movement across corporate networks after initial compromise.

Bert Ransomware Victimology

The group's victim selection appears strategic, focusing on organizations that are likely to pay ransoms quickly due to the critical nature of their operations.

Primary target sectors include:

- **Healthcare organizations**, where downtime can directly impact patient care and lives.
- **Technology companies**, which often possess valuable intellectual property and customer data.
- **Event services**, where timing is crucial and disruption can cause significant financial losses.
- **Manufacturing facilities**, where operational disruption can halt production lines.

Geographically, Bert ransomware has demonstrated global reach with confirmed attacks across Asia, Europe, and the United States. The group shows no preference for organization size, targeting both large enterprises and smaller businesses that may have fewer cybersecurity resources to defend against sophisticated attacks.

How Bert Malware Functions

Bert ransomware operates through a sophisticated multi-stage attack process that maximizes efficiency while minimizing detection opportunities. The group's tactics include PowerShell-based loaders, privilege escalation,

and concurrent file encryption, allowing them streamlined attack execution and evasion despite their reliance on relatively simple underlying code.

The ransomware's operational process follows these key stages:

- **Initial Deployment**: Bert typically begins with PowerShell-based loaders that are designed to evade initial security screenings. These loaders are responsible for establishing the initial foothold and preparing the system for the main ransomware payload.
- **Privilege Escalation**: Once active, Bert systematically escalates privileges to gain administrative access to the target system. This step is crucial for the ransomware's ability to disable security controls and access protected files and systems.
- **Defense Evasion**: The ransomware specifically targets and disables security software, including Windows Defender, firewall services, and other protective mechanisms. This creates an environment where the encryption process can proceed without interference.
- **Encryption Process**: Bert uses standard AES encryption to systematically encrypt files across the infected system. The process is designed to be both thorough and fast, using multiple threads to accelerate the encryption while making detection more difficult.
- **Communication**: The group downloads and executes ransomware from a remote IP address associated with ASN 39134. This suggests the ransomware maintains communication with command and control servers throughout the attack process.
- **Ransom Delivery**: Following successful encryption, Bert deploys ransom notes that provide instructions for payment and recovery. The ransomware uses easily accessible formats for these communications, ensuring victims can understand the demands and payment process.

Bert Ransomware Attack Example and Technical Analysis

ANY.RUN’s Interactive Sandbox allows to analyze both Windows and Linux Bert variants and contains a number of samples targeting both systems, analyzed by the Sandbox community of over 15K SOC teams.

Bert runs in 64-bit Windows 10/11 environments and server versions. It tracks and terminates/destroys database, web server, and virtualization processes (e.g., MSSQL, Apache, VMware) to accelerate encryption and complicate recovery.

The Linux variant, discovered in May 2025, supports up to 50 parallel threads to speed up encryption and accepts command-line parameters --path, --threads, and --silent. In default mode, the malware shuts down all running virtual machines on ESXi hosts using the command "esxcli vm process list" and terminates processes, preventing administrators from creating system snapshots or migrating workloads before encryption begins. After encryption, files receive the extension .encrypted_by_bert, and the note encrypted_by_bert-decrypt.txt shows the number of encrypted files.

Windows Analysis

View Windows variant sandbox detonation


Bert Windows variant *Bert Windows variant in the Interactive Sandbox*

After launching the sample, the ransomware spawns child processes cmd.exe and PowerShell. Through the command line, it gathers system information (systeminfo, wmic), reads the machine GUID from the registry and OS installation date, executes whoami and net config workstation.

In PowerShell, commands are used to disable Windows Defender protection and firewall, as well as to add itself to the startup folder. It also uses processes reg.exe, rundll32.exe, schtasks.exe, and attrib.exe: the first two are used to modify registry and UAC, schtasks creates a task in the scheduler, and attrib hides the payload directory.

Additionally, Bert initiates renaming of user files and adds several extensions such as: *.encryptedbybert, *.encryptedbybert3, *.encryptedbybert11, *.encrypted_bert, *.hellofrombert, and creates the ransom note note.txt.

Linux Analysis

View Linux variant sandbox detonation

 Bert Linux variant *Bert Windows variant in the Interactive Sandbox*

The ransomware executable is launched through the /bin/sh shell. First, it uses a chain of commands to obtain necessary privileges and launch itself:

/bin/sh -c "sudo chown user ... && chmod +x ... && DISPLAY=:0 sudo -i ..." - this is a sequential call of sudo chown to change file ownership to a regular user, chmod +x to grant execution rights, and then sudo -i to run the same file as superuser.

Separate calls to sudo chown user and chmod +x indicate attempts to legitimize and activate the binary file.

After initiation, Bert gathers system information through standard utilities: **uname –a** and **hostname** are called through the chain sh -c "uname -a && echo " | " && hostname" to get kernel architecture and hostname.

This structure lists WorldIDs of virtual machines and closes them, as previously described regarding ESXi VM shutdown behavior.

During encryption, it adds one of the extension variants, in this case *.bert11, and drops the ransom note bert11-decrypt.txt, as well as displays a banner with the number of encrypted files in the console, including directories ~/.config/systemd/ and ~/.config/systemd/user; thus the program leaves ransom notes in each folder.

 Bert ransom note *Bert ransom note on Linux endpoint*

Bert Execution Process in General

After launch, Bert analyzes the platform. On Linux/Linux servers, especially on ESXi hosts, it can identify running virtual machines and, if the --silent parameter is not set, forcibly shuts them down to prevent administrators from creating backups and quickly restoring the system.

On Windows, the loader script checks for administrative rights and restarts itself with elevated privileges, then copies the payload to disk and registers itself in startup through the task scheduler.

For unimpeded execution of malicious actions, the Windows variant of Bert modifies the registry to disable Windows Defender and its real-time protection, stops WinDefend and Sense services, deactivates the firewall, and reduces UAC level to zero. Then it downloads the main ransomware program from a remote IP address and runs it as administrator.

The Linux version embeds configuration in a JSON file and accepts command-line parameters to specify directory and number of encryption threads, providing flexibility and high performance (up to 50 threads).

Before encryption, Bert terminates processes that could interfere with the attack: on Windows - database and virtualization services, on Linux - running ESXi virtual machines. Then parallel encryption begins: on Windows, modern versions use ConcurrentQueue structure and create a separate thread for each volume to immediately process files, while on Linux/ESXi up to 50 threads are used. For encryption, RSA and AES are used on Windows, and a combination of AES, RC4, Salsa20, and ChaCha on Linux.

A ransom note is placed in each folder, and encrypted file names receive characteristic extensions like .encryptedbybert or .encrypted_by_bert, accompanied by data exfiltration to remote servers for double extortion.

Gathering Threat Intelligence on Bert Ransomware

Threat intelligence plays a crucial role in defending against Bert Ransomware. It provides visibility into the tactics, techniques, and procedures (TTPs) of Bert’s operators. Security teams can:

- Detect new campaigns earlier through shared IOCs.
- Understand attacker infrastructure and preemptively block it.
- Prioritize patching based on known vulnerabilities exploited by Bert.
- Enrich SIEM/EDR alerts for faster triage.

Start from querying Threat Intelligence Lookup with a threat name. If you want to select Bert samples targeting only Windows or Linux environment, specify an OS with a search parameter:

threatName:"bert" and os:"22.04.2"


Bert samples found via TI Lookup *Bert samples found via TI Lookup: watch behavior, gather indicators*

Integrate ANY.RUN’s threat intelligence solutions in your company

Contact us

Conclusion

The key to defending against Bert ransomware lies in understanding that this is not merely a technical problem requiring technical solutions, but a comprehensive risk management challenge that affects every aspect of organizational operations. The ransomware's impact extends far beyond encrypted files to encompass business continuity, financial stability, regulatory compliance, and organizational reputation. Organizations must adopt a holistic defense approach that combines technical security controls, employee training, incident response planning, and threat intelligence integration.

The multi-platform nature of BERT ransomware means that defensive strategies must account for both Windows and Linux environments, while the group's sophisticated attack methods require advanced detection and response capabilities.

Start gathering actionable threat intelligence on Bert by sign up for ANY.RUN's TI Lookup: protect your business with timely detection and response.

Source: https://any.run/malware-trends/bert/