Erebus Linux Ransomware: Impact to Servers and Countermeasures

Archived: 2026-04-05 16:55:31 UTC

On June 10, South Korea-based web hosting company NAYANA became one of the latest high-profile victims of ransomware after 153 of its Linux servers were found infected with an Erebus ransomware (detected by Trend Micro as RANSOM_ELFEREBUS.A) variant. The ransomware attack affected the websites, database and multimedia files of around 3,400 businesses employing NAYANA's service.

In the latest notice posted on the company's website, it appears cybercriminals successfully forced NAYANA into paying the ransom—they paid the first of three payments they plan to make for all the keys needed to decrypt the infected files. However, NAYANA has yet to receive the first decryption key.

[Related: Learn more about SAMSAM, one of the first ransomware to infect servers]

Erebus evolved from using exploit kits to bypassing User Account Control

Erebus ransomware (RANSOM_EREBUS.A) first emerged last September 2016news- cybercrime-and-digital-threats being distributed by malvertisements (malicious advertisements). The malicious ads diverted victims to the Rig exploit kit, which infects the victim's systems with the ransomware. This Erebus variant targets 423 file types, scrambles files with RSA-2048 encryption algorithm, and appends the affected files with the *.ecrypt* extension. This version of Erebus was observed using compromised websites in South Korea as its command and control (C&C) servers.

By February 2017, Erebus was found to have evolved and changed tacticsnews- cybercrime-and-digital-threats, using a technique that bypassesnews article User Account Control (UAC)—a Windows feature that helps prevent unauthorized changes in the system—in order to execute the ransomware with elevated privileges. In its ransom note, Erebus threatens to delete the victim's files within 96 hours unless the ransom is paid, which is 0.085 Bitcoin (US$216 as of June 15, 2017). This version (RANSOM_EREBUS.TOR) also deletes shadow copies to prevent victims from recovering their files.

[Read: A technical overview of the fileless, code-injecting SOREBRECT ransomware that can encrypt network shares]

Erebus Ransomware can now infect servers

The variant that infected NAYANA's servers is Erebus ransomware ported to Linux servers. Trend Micro's ongoing analysis indicates that this version uses RSA algorithm to encrypt AES keys; infected files are encrypted with unique AES keys. Its persistence mechanisms include adding a fake Bluetooth service to ensure that the ransomware is executed even after the system or server is rebooted. It also employs the UNIX cron—a utility in Unix-like operating systems like Linux that schedules jobs via commands or shell scripts—to check hourly if the

ransomware is running. Similar to NAYANA's case, it originally demanded 10 Bitcoins ($24,689), but the ransom has since gone down to 5 BTC ($12,344).

This iteration of Erebus targets 433 file types, some of which include:

- Office documents (.pptx, .docx, .xlsx)
- Databases (.sql, .mdb, .dbf, .odb)
- Archives (.zip, .rar)
- Email files (.eml, .msg)
- Website-related and developer project files (.html, .css, .php, .java)
- Multimedia files (.avi, .mp4)

[READ: How UNIX-like systems like Linux affected the ransomware landscape]

Erebus isn't the first file-encrypting malware to target Linux systems, or even servers. Linux.Encodernews-cybercrime-and-digital-threats, Encryptor RaaS, a version of KillDisknews- cybercrime-and-digital-threats, Rexnews- cybercrime-and-digital-threats, Fairware, and KimcilWarenews- cybercrime-and-digital-threats are all capable of targeting machines running Linux. In fact, Linux ransomware emerged as early as 2014, and were offshootsnews article of open-source projects supposedly designed for educational purposes. SAMSAM, Petya, and Crysis ransomware are just some of the families known to target and breach servers.

While Linux ransomware isn't as established or mature as its Windows counterparts, they can still present significant adverse impact to users and especially enterprises. As exemplified by NAYANA, Linux is an increasingly popular operating system and a ubiquitous element in the business processes of organizations across various industries—from servers and databases to web development and mobile devices. Data centers and hosting/storage service providers also commonly use machines running Linux, for instance.

[READ: Multilayered solutions to server-side ransomware]

Best practices for securing Linux servers and systems

The impact of ransomware such as Erebus to an organization's operations, reputation, and bottom line highlights the importance of securing the servers and systems that power an enterprise's business processes. Additionally, the effect is multiplied if a ransomware also manages to infect not only endpoints but also servers/networks. Here are some best practices that IT/system administrators and information security professionals can adopt to strengthen the security posture of their servers and systems:

- ***Keep the system and server updated.*** A strong patch management policy should be enforced to ensure that the system and server have the latest patches, fixes, and kernel.
- ***Avoid or minimize adding third-party or unknown repositories or packages.*** This limits the vulnerabilities attackers can use as entry points into the server or system. The risks can be further lessened by removing or disabling unnecessary components or services in the server.
- ***Apply the principle of least privilege.*** Linux's privilege separation provides a way to restrict the modifications a program can make to the system. Restricting permissions/privileges also helps mitigate exposure and further damage as well as prevent unauthorized use. IT/system administrators can consider

using extensions that implement mandatory policies that manage the extent of access a program can have to a system file or network resource.

- ***Proactively monitor and validate your network traffic.*** Protecting the network against threats is a must for any enterprise. Deploying intrusion detection and prevention systems as well as firewalls helps identify, filter, and block traffic, which can indicate a malware infection. Event logs provide forensic information that can help IT/system administrators detect incursion attempts and actual attacks.
- ***Back up your files.*** An effective countermeasure against ransomware's fear-mongering tactic and impact is to keep backups of files stored in the system or server—with at least three copies in two different formats, with one stored offsite.
- ***Apply network segmentation and data categorization.*** Network segmentationnews article curbs the spread of infection, while data categorization mitigates the damage that may be incurred from an attack.

An update on the incident and a technical overview of the ransomware can be found in this article.

Trend Micro Solutions

Trend Micro™ Deep Security™ stops ransomware from compromising enterprise servers and workloads– regardless if they're physical, virtual, in the cloud, or in containers. Deep Security™ defends against network threats with intrusion prevention (IPS) and host firewall, shielding vulnerable servers from attack with a virtual patch until a software patch can be applied. Deep Security™ keeps malware, including ransomware, off of servers with sophisticated anti-malware and behavioral analysis, ensuring that malicious actions are stopped immediately. Deep Security™ also has system security, including application control to lock down servers, and integrity monitoring that can detect potential indicators of compromise (IOCs), including ransomware.

HIDE

Like it? Add this infographic to your site:
1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

We Recommend

-
-
-
-

- The Industrialization of Botnets: Automation and Scale as a New Threat Infrastructurenews article
- Complexity and Visibility Gaps in Power Automatenews article
- Cracking the Isolation: Novel Docker Desktop VM Escape Techniques Under WSL2news article
- Azure Control Plane Threat Detection With TrendAI Vision One™news article

- - The AI-fication of Cyberthreats: Trend Micro Security Predictions for 2026predictions
  - Ransomware Spotlight: DragonForcenews article
- - Stay Ahead of AI Threats: Secure LLM Applications With Trend Vision Onenews article
  - The Road to Agentic AI: Navigating Architecture, Threats, and Solutionsnews article

---