

- [Trend Micro](#)
- [About TrendLabs Security Intelligence Blog](#)



Search:

- [Home](#)
- [Categories](#)

[Home](#) » [Ransomware](#) » Erebus Resurfaces as Linux Ransomware

Erebus Resurfaces as Linux Ransomware

- Posted on: [June 19, 2017](#) at 5:08 am
- Posted in: [Ransomware](#)
- Author: [Trend Micro](#)

0

by Ziv Chang, Gilbert Sison, and Jeanne Jocson

On June 10, South Korean web hosting company [NAYANA was hit by Erebus ransomware](#) (detected by Trend Micro as [RANSOM_ELFEREBUS.A](#)), infecting 153 Linux servers and over 3,400 business websites the company hosts.

In a [notice](#) posted on NAYANA's website last June 12, the company shared that the attackers demanded an unprecedented ransom of 550 Bitcoins (BTC), or US\$1.62 million, in order to decrypt the affected files from all its servers. In an [update](#) on June 14, NAYANA negotiated a payment of 397.6 BTC (around \$1.01 million as of June 19, 2017) to be paid in installments. In a [statement](#) posted on NAYANA's website on June 17, the second of three payments was already made. On [June 18](#), NAYANA started the process of recovering the servers in batches. Some of the servers in the second batch are currently experiencing database (DB) errors. A third payment installment is also expected to be paid after the first and second batches of servers have been successfully recovered.

While not comparable in terms of the ransom amount, this is reminiscent of what happened to [Kansas Hospital](#), which didn't get full access to the encrypted files after paying the ransom, but was instead extorted a second time.

Erebus was [first seen on September 2016 via malvertisements](#) and reemerged on February 2017 and used [a method that bypasses Windows' User Account Control](#). Here are some of the notable technical details we've uncovered so far about Erebus' Linux version:



Figure 1: Erebus has a multilingual ransom note (English shown above)

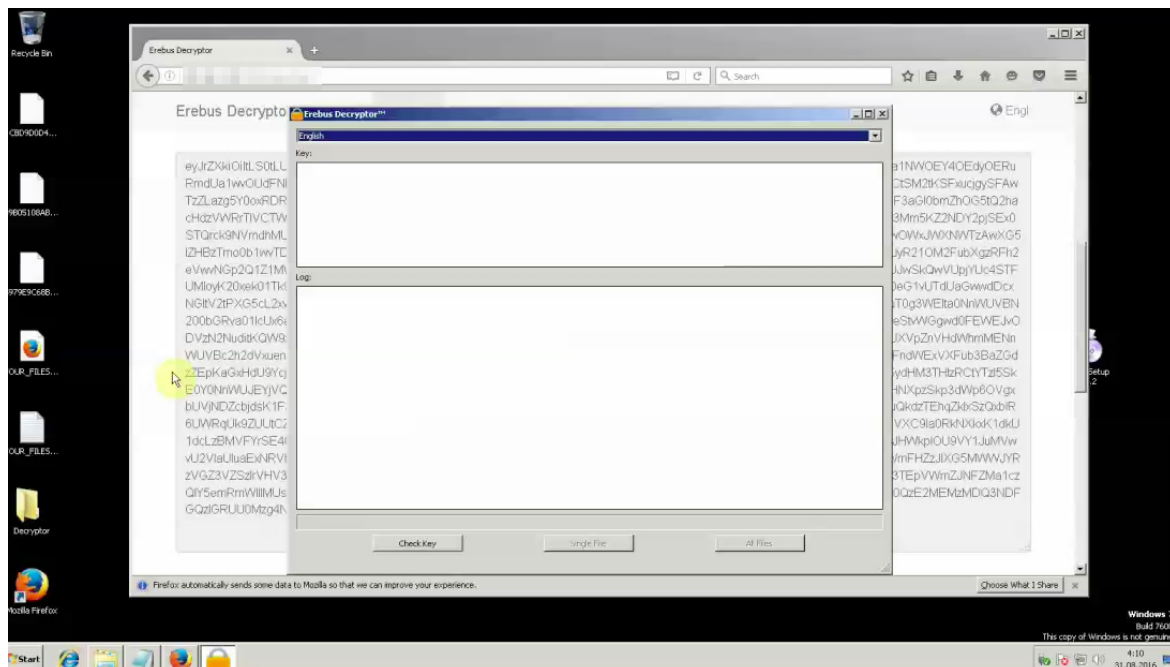


Figure 2: Screenshot of a demo video from the attackers showing how to decrypt the encrypted files

Possible Arrival Vector

As for how this Linux ransomware arrives, we can only infer that Erebus may have possibly leveraged vulnerabilities or a local Linux exploit. For instance, based on open-source intelligence, NAYANA's [website](#) runs on Linux kernel 2.6.24.2, which was compiled back in 2008. Security flaws like [DIRTY COW](#) that can provide attackers root access to vulnerable Linux systems are just some of the threats it may have been exposed to.

Additionally, NAYANA's website uses Apache version 1.3.36 and PHP version 5.1.4, both of which were released back in 2006. [Apache vulnerabilities](#) and [PHP exploits](#) are well-known; in fact, there was even [a tool sold in the Chinese underground expressly for exploiting Apache Struts](#). The version of Apache NAYANA used is run as a user of *nobody*(*uid=99*), which indicates that a local exploit may have also been used in the attack.

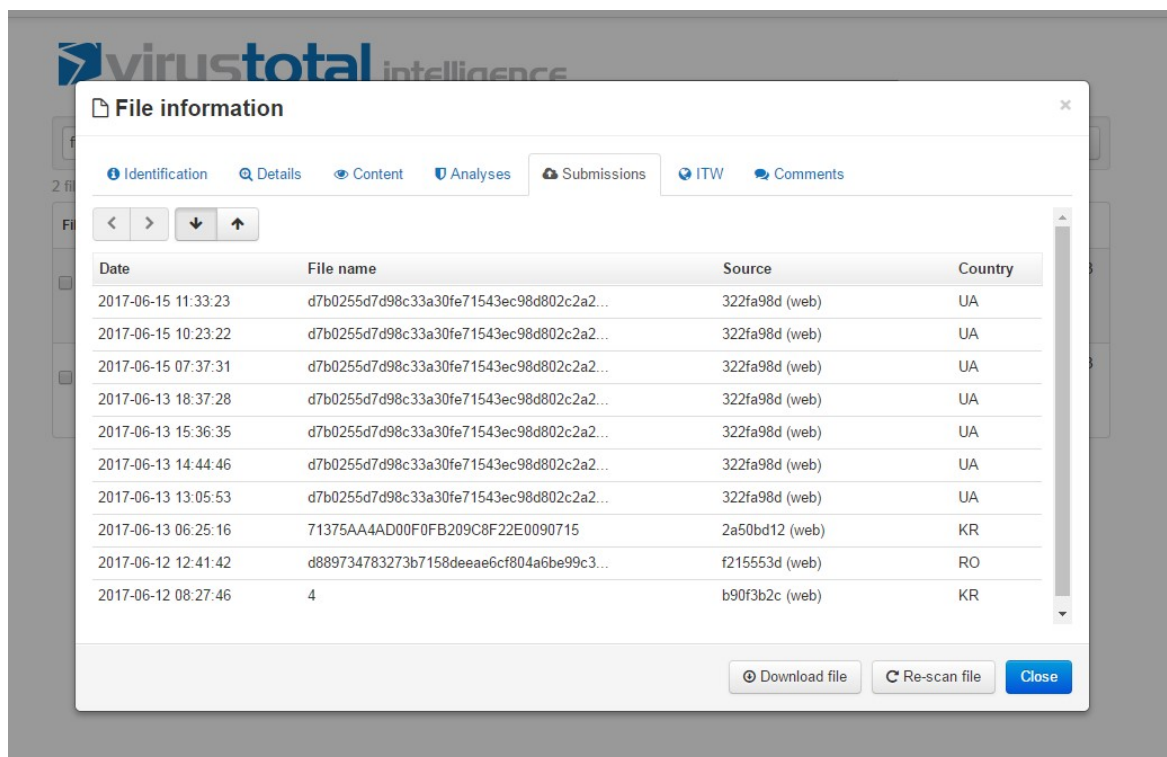


Figure 3: VirusTotal submissions of the Erebus Linux ransomware

It's worth noting that this ransomware is limited in terms of coverage, and is, in fact, heavily concentrated in South Korea. While this may indicate that this ransomware attack is targeted, VirusTotal showed otherwise—several samples were also submitted from Ukraine and Romania. These submissions can also indicate they were from other security researchers.

Encryption Routine

Some ransomware families are known to scramble files in layers of encryption algorithms, such as [UIWIX](#), [later versions of Cerber](#), and [DMA Locker](#). Erebus takes this up a notch; each file encrypted by Erebus will have this format:

Header (0x438 bytes)
 RSA-2048-encrypted original filename
 RSA-2048-encrypted AES key
 RSA-2048-encrypted RC4 key
 RC4-encrypted data

The file is first scrambled with RC4 encryption in 500kB blocks with randomly generated keys. The RC4 key is then encoded with AES encryption algorithm, which is stored in the file. The AES key is again encrypted using RSA-2048 algorithm that is also stored in the file.

While each encrypted file has its RC4 and AES keys, the RSA-2048 public key is shared. These RSA-2048 keys are generated locally, but the private key is encrypted using AES encryption and another randomly generated key. Ongoing analysis indicates that decryption is not possible without getting hold of the RSA keys.

Targeted File Types

Office documents, databases, archives, and multimedia files are the usual file types targeted by ransomware. It's the same for this version of Erebus, which encrypts 433 file types. However, the ransomware appears to be coded mainly for targeting and encrypting web servers and data stored in them.

Here is a table that shows the directories and system tablespaces that Erebus searches. Note that *var/www/* is where the files/data of websites are stored, while the *ibdata* files are used in MySQL:

Included directories:	Excluded directories:
var/www/	\$/bin/
Included files:	\$/boot/
ibdata0	\$/dev/
ibdata1	\$/etc/
ibdata2	\$/lib/
ibdata3	\$/lib64/
ibdata4	\$/proc/
ibdata5	\$/run/
ibdata6	\$/sbin/
ibdata7	\$/srv/
ibdata8	\$/sys/
ibdata9	\$/tmp/
ib_logfile0	\$/usr/
ib_logfile1	\$/var/
ib_logfile2	/.gem/
ib_logfile3	/.bundle/
ib_logfile4	/.nvm/
ib_logfile5	/.npm/

Figure 4: System tablespaces Erebus searches

Adopt Best Practices

Despite their market share, [Unix and Unix-like operating systems such as Linux](#) are poised to be lucrative for bad guys as [ransomware continues to diversify and mature in the threat landscape](#). Why? They are a ubiquitous part of the infrastructures that power many enterprises, used by workstations and servers, web and application development frameworks, databases, and mobile devices, among others.

And as we've seen in other families like [WannaCry](#), [SAMSAM](#), [Petya](#), or [HDDCryptor](#), the capability to affect servers and network shares amplifies the impact. A single, vulnerable machine on a network is sometimes all it takes to infect connected systems and servers.

Given the risks to business operations, reputation, and bottom line, enterprises need to be proactive in keeping threats like ransomware at bay. There is no silver bullet to ransomware like Erebus, which is why IT/system administrators should have a defense-in-depth approach to security. [Best practices for mitigating ransomware](#) include:

- [Backing up critical files](#)
- Disabling or minimizing third-party or unverified repositories
- Applying the principle of least privilege
- Ensuring servers and endpoints are updated (or deploying [virtual patching](#))
- [Regularly monitoring the network](#)
- Inspecting event logs to check for signs of intrusions or infection

Some of the security mechanisms that can be considered are:

- IP filtering as well as intrusion prevention and detection systems
- Security extensions in Linux that manage and limit access to files or system/network resources

- [Network segmentation](#) and [data categorization](#) to curtail and mitigate infection and further damage to data
- Enabling privilege separation in Linux

We will update this post as more information from our analysis of this Linux ransomware become available.

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.

Trend Micro [Deep Discovery Inspector™](#) protects customers from this threat via this DDI rule:

- DDI Rule ID 2434 – EREBUS – Ransomware – HTTP (Request)

[TippingPoint](#) customers are protected from this threat via this ThreatDV filter:

- ThreatDV: 28725: HTTP: Erebus Ransomware Check-in

Trend Micro [Deep Security™](#) protects customers from this threat via this DPI rule:

- 1008457 – Ransomware Erebus

Indicators of Compromise:

SHA256 detected as [RANSOM_ELFEREBUS.A](#):

- 0b7996bca486575be15e68dba7cbd802b1e5f90436ba23f802da66292c8a055f
- d889734783273b7158deae6cf804a6be99c3a5353d94225a4dbe92caf3a3d48

Updated on June 20, 2017, 12:10 AM PDT to add solution for [Deep Security™](#).

Related Posts:

- [Large-Scale Petya Ransomware Attack In Progress, Hits Europe Hard](#)
- [Vulnerability in F2FS File System Leads To Memory Corruption on Android, Linux](#)
- [Unix: A Game Changer in the Ransomware Landscape?](#)
- [New Linux Malware Exploits CGI Vulnerability](#)



Say **NO** to ransomware.

Trend Micro has **blocked over 100 million** threats and counting

Learn how to protect Enterprises, Small Businesses, and Home Users from ransomware:

[ENTERPRISE](#) »

[SMALL BUSINESS](#) »

[HOME](#) »

Tags: [ErebusLinuxransomware](#)

Featured Stories

- [A Closer Look at North Korea's Internet](#)
- [From Cybercrime to Cyberpropaganda](#)
- [Dnsmasq: A Reality Check and Remediation Practices](#)
- [Business Process Compromise and the Underground's Economy of Coupon Fraud](#)
- [ZNIU: First Android Malware to Exploit Dirty COW Vulnerability](#)

Business Process Compromise

-

Attackers are starting to invest in long-term operations that target specific processes enterprises rely on. They scout for vulnerable practices, susceptible systems and operational loopholes that they can leverage or abuse. To learn more, [read our Security 101: Business Process Compromise](#).

Business Email Compromise

-

How can a sophisticated email scam cause more than \$5.3 billion in damages to businesses around the world?

[See the numbers behind BEC](#)

Latest Ransomware Posts

[Bad Rabbit Ransomware Spreads via Network, Hits Ukraine and Russia](#)

[A Look at Locky Ransomware's Recent Spam Activities](#)

[Magnitude Exploit Kit Now Targeting South Korea With Magniber Ransomware](#)

[WannaCry Ransomware Sold in the Middle Eastern and North African Underground](#)

[Locky Ransomware Pushed Alongside FakeGlobe in Upgraded Spam Campaigns](#)

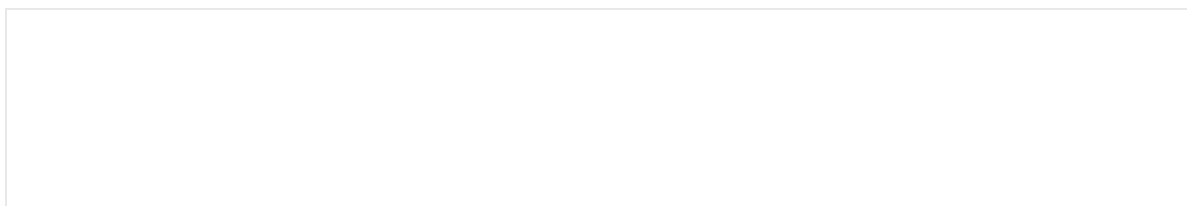
Recent Posts

- [New EMOTET Hijacks a Windows API, Evades Sandbox and Analysis](#)

- [November's Patch Tuesday Includes Defense in Depth Update for Attacks Abusing Dynamic Data Exchange](#)
- [Physical Theft Meets Cybercrime: The Illicit Business of Selling Stolen Apple Devices](#)
- [Toast Overlay Weaponized to Install Several Android Malware](#)
- [REDBALDKNIGHT/BRONZE BUTLER's Daserf Backdoor Now Using Steganography](#)

Ransomware 101

•



This infographic shows how ransomware has evolved, how big the problem has become, and ways to avoid being a ransomware victim.

[Check the infographic](#)

Popular Posts

[Bad Rabbit Ransomware Spreads via Network, Hits Ukraine and Russia](#)
[Coin Miner Mobile Malware Returns, Hits Google Play](#)
[New EMOTET Hijacks a Windows API, Evades Sandbox and Analysis](#)
[Toast Overlay Weaponized to Install Several Android Malware](#)
[REDBALDKNIGHT/BRONZE BUTLER's Daserf Backdoor Now Using Steganography](#)

Latest Tweets

- 500k: the number of installs for a malicious #Android app laden with #TOASTAMIGO, the first to weaponize... twitter.com/i/web/status/9...
[about 6 hours ago](#)
- A new tactic from #ChessMaster involves exploiting the CVE-2017-8759 SOAP WSDL parser vulnerability. bit.ly/2ibWum8
[about 14 hours ago](#)
- Spotted: Kristina, Waffle, and the holiday-themed Christmas #ransomware. Details here: bit.ly/2zIdH0g



[about 20 hours ago](#)

Stay Updated

Email Subscription

Your email here

Subscribe

- [Home and Home Office](#)
- |
- [For Business](#)
- |
- [Security Intelligence](#)
- |
- [About Trend Micro](#)

- Asia Pacific Region (APAC): [Australia](#) / [New Zealand](#), [中国](#), [日本](#), [대한민국](#), [台灣](#)
- Latin America Region (LAR): [Brasil](#), [México](#)
- North America Region (NABU): [United States](#), [Canada](#)
- Europe, Middle East, & Africa Region (EMEA): [France](#), [Deutschland](#) / [Österreich](#) / [Schweiz](#), [Italia](#), [Россия](#), [España](#), [United Kingdom](#) / [Ireland](#)

- [Privacy Statement](#)
- [Legal Policies](#)

- Copyright © 2017 Trend Micro Incorporated. All rights reserved.