McAfee Labs Threat Advisory

Ransom-Everbe

September 7, 2018

McAfee Labs periodically publishes Threat Advisories to provide customers with a detailed analysis of prevalent malware. This Threat Advisory contains behavioral information, characteristics, and symptoms that might be used to mitigate or discover this threat, and suggestions for mitigation in addition to the coverage provided by the DATs.

To receive a notification when a Threat Advisory is published by McAfee Labs, select to receive "Malware and Threat Reports" at the following URL: https://sns.secure.mcafee.com/signup_login.

Summary

Ransom-Everbe is a family of ransomware that, on execution, encrypts files present on the user's system. The compromised user must pay the attacker with a ransom to get the files decrypted.
Ransom-Everbe appears to be using the same distribution method used by traditional ransomware, which is known to be distributed via Exploit Kits (EK) and malicious email campaigns. However, it is also suspected that this variant is being distributed via targeted attacks. Attackers might already have access to an organization's network via prior successful hacking or infection attempts.

Detailed information about the threat, its propagation, characteristics, and mitigation are in the following sections:

- Infection and Propagation Vectors
- Mitigation
- Characteristics and Symptoms
- Restart Mechanism
- McAfee Foundstone Services

The minimum DAT versions required for detection are:

Detection Name	MD5 of samples	DAT Version	Date
Ransom-Divine	52C183E8875E08B19DD7DC3F4BD42E47	V2: 9010 V2: 3461	Sept 8, 2018
Real Protect-EC!52C183E8875E	52C183E8875E08B19DD7DC3F4BD42E47		Sept 8, 2018

Table 1: Minimum DAT versions for coverage.

The Threat Intelligence Library contains the date that the above signatures were most recently updated. Review the Threat Intelligence Library for the most up-to-date coverage information.

Infection and Propagation Vectors

- Currently, the infection vector of Ransom-Everbe is unknown.
- Most ransomware campaigns typically spread via Exploit Kits and malspam campaigns instrumented via various botnets.
- However, Ransom-Everbe is suspected to be distributed using highly targeted attacks, such as brute forcing of RDP connections on unprotected systems in an organization's network.
- When the attackers have access to the organization's network, Ransom-Everbe might be deployed to business-critical systems to cause maximum disruption of services, and in-turn warrant a considerable ransom.

Mitigation

Mitigating the threat at multiple levels such as file, registry, and URL can be achieved at various layers of McAfee products. Browse the product guidelines available here to mitigate the threats based on the behavior described below in the Characteristics and symptoms section.

Never open unsolicited emails and their attachments. Also, be wary of suspicious looking advertisements. Customers are advised to regularly update their infrastructure, both operating system and application software, with the latest updates to ensure full coverage in addition to updated McAfee Anti-Virus software.

Endpoint Security 10.x

- Mitigation methods for assorted malware are available in the following product guide. Any specific mitigation steps, if necessary, will be described later in this Threat Advisory: http://b2b-download.mcafee.com/products/evaluation/Endpoint_Security/Evaluation/ens_1000_help_0-00_en-us.pdf
- Refer to article KB86577 to create an Endpoint Security Threat Prevention user-defined Access Protection Rule for a file or folder registry.

ePolicy Orchestrator (ePO)

- To block the access to USB drives through the ePO DLP policy, refer to this tutorial.

VirusScan Enterprise

- Refer to article KB53346 to use Access Protection policies in VirusScan Enterprise to protect against viruses that can disable regedit.
- Refer to article KB53355 to use Access Protection policies in VirusScan Enterprise to protect against viruses that can disable Task Manager.
- Refer to article KB53356 to use Access Protection policies in VirusScan Enterprise to prevent malware from changing folder options.

Host Intrusion Prevention

- To blacklist applications using a Host Intrusion Prevention custom signature, refer to article KB71329.
- To create application blocking rules policies to prevent the binary from running, or to prevent a specific executable from hooking any other executable, refer to article KB71794.

Others

- To disable the Autorun feature on Windows remotely using Windows Group Policies, refer to this article from Microsoft.

Characteristics and Symptoms

System Backup Deletion

When executed in the target system, Ransom-Everbe begins its malicious actions by launching the following command to delete backup shadow copies:

- `vssadmin delete shadows /all /quiet`

Target Folder/File Scanning for Encryption

After the previous step is executed, the malware starts scanning the system for all the targeted drives that are connected and searches for predefined files types that could be encrypted.

Some of the targeted file extensions are listed below:

```
ASP, AVI, BMP, CAB, CHM, DB, DIVINE, DLL, DOC, DOCM, DOCX, DOT, DOTM, DOTX, EXE,
FLV, GIF, HTM, HTT, JPG, JS, MID, MP3, MP4, MPG, OGG, PHP, PNG, POT, POTX, PPS, PPT,
PPTM, PPTX, RAR, SCR, SWF, TIF, TXT, VBS, WAV, WMA, WMV, XLS, XLSB, XLSM, XLSX, XLT,
ZIP
```

Ransom-Everbe also has the capability to encrypt files on network shares. This done by enumerating files on each available network resource and performing subsequent encryption of files.

Encryption Scheme

Encryption procedures:

- Create a pair of RSA keys before encrypting any file.
- Create a random Salsa20 key and a random initial vector for each file and encrypt the file with it.
- Encrypt the Salsa20 key and initial vector with the RSA public key.
- After encryption, append the random initial vector and encrypted Salsa20 key to the content of file, increasing the original file size.

Ransom Notes

Ransom notes are generated in each directory that has been encrypted by the ransomware. These files are usually named:

- `!=How_to_decrypt_files=!.txt`

The Ransom note displays the message in the snapshot below:

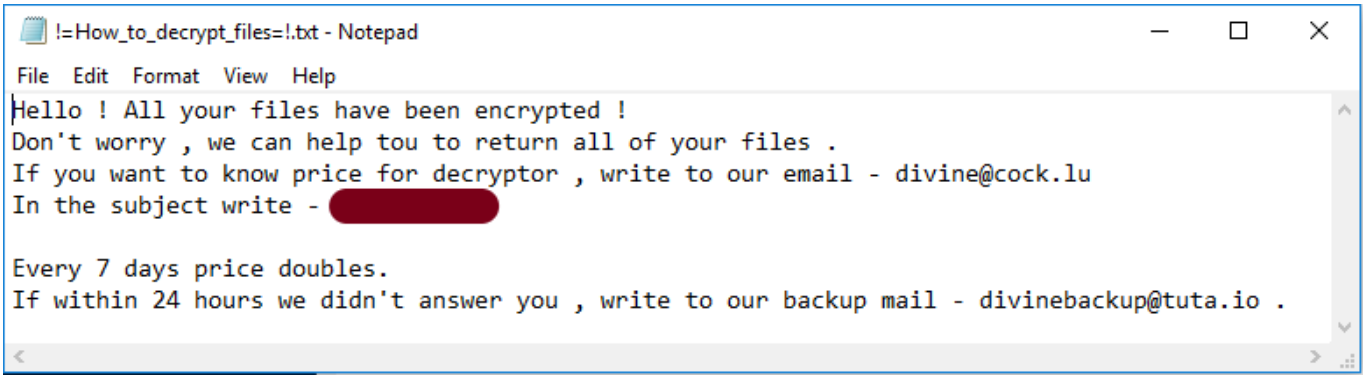

Figure: Ransom-Everbe Ransom Note

Network Connection / Command and Control (C&C) Server Communication

No network connections have been observed while executing this malware.

File Extension for Encrypted files

The targeted files will have the following file extension after being encrypted:

- `<filename>.[divine@cock.lu].divine`

The following file extensions have been observed in previous campaigns:

- `<filename>.[Evil@cock.lu].EVIL`
- `<filename>.[eV3rbe@rape.lol].eV3rbe`

Restart Mechanism

No restart mechanism has been observed for this malware.

Getting Help from the McAfee Foundstone Services team

This document is intended to provide a summary of current intelligence and best practices to ensure the highest level of protection from your McAfee security solution. The McAfee Foundstone Services team offers a full range of strategic and technical consulting services that can further help to ensure you identify security risk and build effective solutions to remediate security vulnerabilities.

You can reach them here: https://secure.mcafee.com/apps/services/services-contact.aspx

This Advisory is for the education and convenience of McAfee customers. We try to ensure the accuracy, relevance, and timeliness of the information and events described; they are subject to change without notice.