Single Product Test

Superna Ransomware Test

Language: English
June 2017

Last Revision: 4th July 2017

www.av-comparatives.org

Commissioned by Superna

1 Introduction

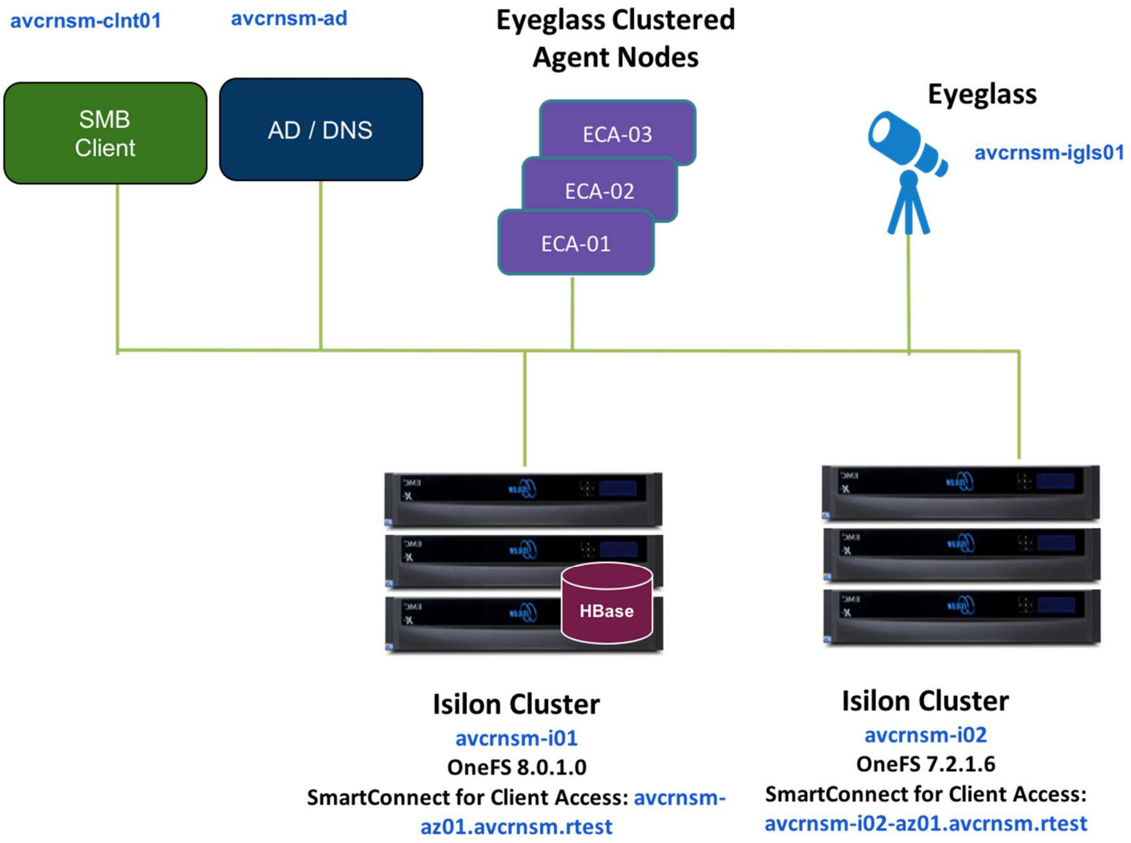
This report has been commissioned by Superna.

The product Superna Eyeglass 1.9.2 has been tested in June 2017.

Superna Eyeglass Ransomware Defender prevents ransomware from encrypting user data on storage clusters. It does not replace endpoint protection software on client or server computers, but is designed to be used in conjunction with this. Ransomware Defender works by monitoring user data on storage clusters in real time, and checking for file-write operations typically conducted by ransomware programs, i.e. encryption of the files. As soon as such activity is detected, access from the infected user's computer to the storage cluster is blocked. The product can manage multiple clusters, each with multiple shares, and when ransomware activity is detected on one share on one cluster, the user's access to all managed shares and clusters will be removed. A notification is immediately sent to the administrator when ransomware activity is spotted and a user is blocked.

Superna Eyeglass was provided in the form of preconfigured virtual hard disks for the VMware vSphere platform. A web-based interface was provided to manage the product.

2 Test Configuration



3 Test scenario

The ransomware was executed manually on a client with connected shares. Ransomware Defender was in “Blocking Mode”.

3.1 Shares

Four shares were mapped to 2 clusters as network drives to the client before the sample was executed. The shares’ content was provided by Superna containing different types of documents.

1. Corp
2. Engineering
3. Finance
4. Marketing

3.2 Client

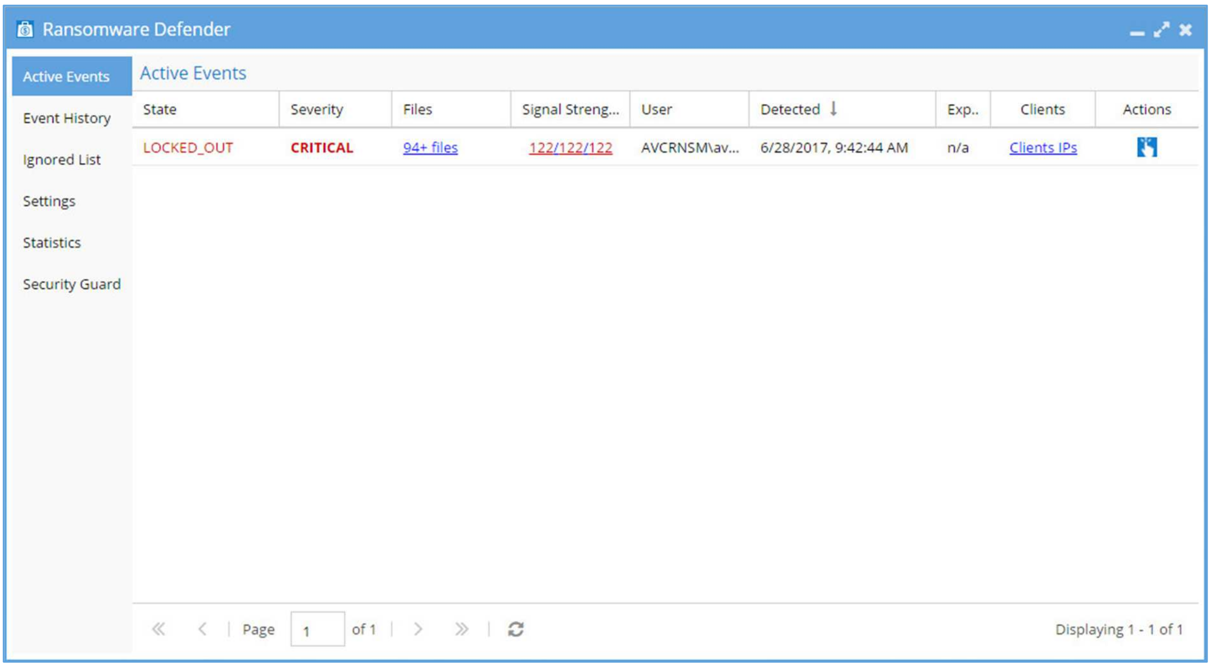
Windows 7 64bit English

3.3 Sample Selection

One ransomware sample family, Locky, was used. This ransomware family was chosen by Superna as a known variant that attacks network attached drives.

4 How it works

Superna Eyeglass Ransomware Defender prevents ransomware from encrypting user data on storage clusters by monitoring file operations. As soon as a blacklisted activity is detected and a given threshold is reached, access from the infected user's computer to the storage cluster is blocked by locking the user out.



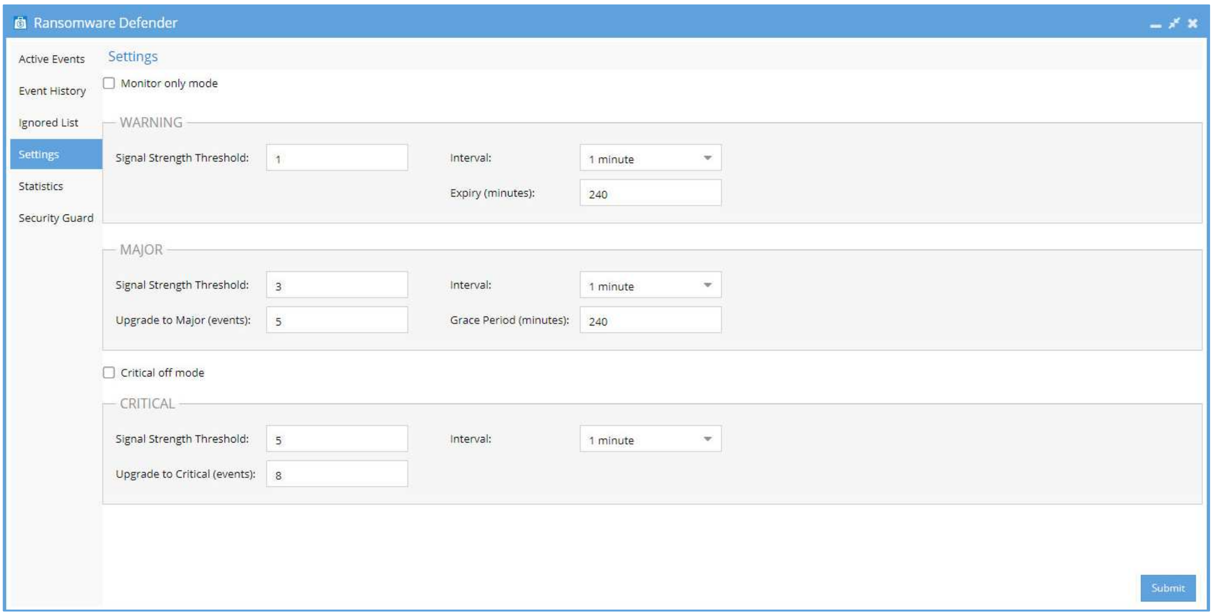
Active Events

State	Severity	Files	Signal Streng...	User	Detected ↓	Exp..	Clients	Actions
LOCKED_OUT	CRITICAL	94+ files	122/122/122	AVCRNSM\av...	6/28/2017, 9:42:44 AM	n/a	Clients IPs	

Page 1 of 1

Displaying 1 - 1 of 1

Ransomware Defender



Settings

□ Monitor only mode

WARNING

Signal Strength Threshold: 1

Interval: 1 minute

Expiry (minutes): 240

MAJOR

Signal Strength Threshold: 3

Interval: 1 minute

Upgrade to Major (events): 5

Grace Period (minutes): 240

□ Critical off mode

CRITICAL

Signal Strength Threshold: 5

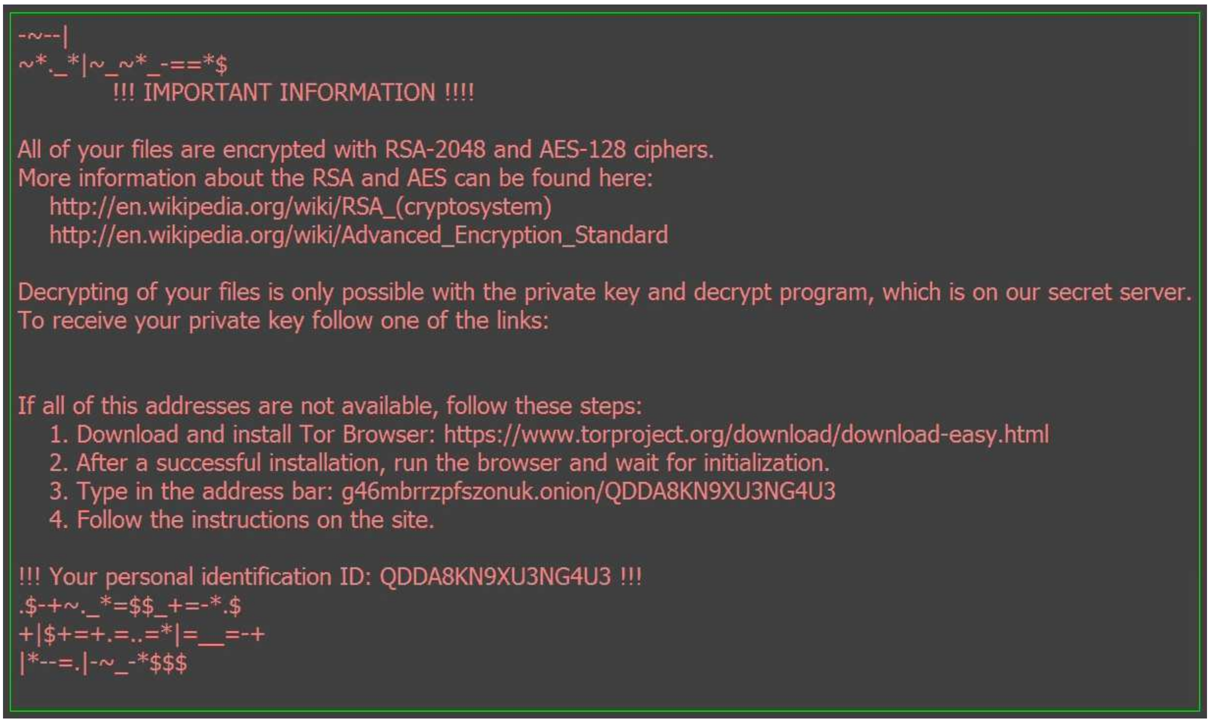
Interval: 1 minute

Upgrade to Critical (events): 8

Ransomware Defender – Threshold Settings

5 Result

The sample encrypted the client and several files on the storage clusters. The number of encrypted files on the clusters before detection and user lockout is dependent on the user behavior threshold settings.



```
-~--|
~*._*|~_~*_-==*$
          !!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
    http://en.wikipedia.org/wiki/RSA_(cryptosystem)
    http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:


If all of this addresses are not available, follow these steps:
    1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
    2. After a successful installation, run the browser and wait for initialization.
    3. Type in the address bar: g46mbrrzpfszonuk.onion/QDDA8KN9XU3NG4U3
    4. Follow the instructions on the site.

!!! Your personal identification ID: QDDA8KN9XU3NG4U3 !!!
.$-+~._*=$$_+=-*.$
+|$+=+.=..=*|=__=-+
|*--=.|-~_-*$$$
```

Superna Eyeglass Ransomware Defender worked as expected and locked out the user from both storage clusters, halting the propagation of file encryptions after reaching the threshold.

The user lockout only affects the compromised user account, allowing other users to access storage cluster data. The product also assists with recovery of affected data by listing the affected files. Once the user workstation has been remediated, the product can return access to all networked attached data by reversing the user lockout and completing the recovery process.

Copyright and Disclaimer

AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives (July 2017)