NioGuard Security Lab

Ransomware

Protection Test

April 2017

Introduction

This paper is a summary of the ransomware protection test report and includes the description of the test environment, list of tested security solutions and their versions, overview of the test scenarios, as well as the results and conclusions based on these results. We do not rank the tested solutions and do not give any awards but provide the results “as is” for information purposes only.

Test environment

The tests were conducted on Windows 8.1 SP1 32-bit build 9600 except the test of AhnLab V3 Internet Security 8.0.7.5, which was conducted on a machine running Windows 7 SP1 32-bit operating system. The “System Protection” option was turned on to test operations with shadow copies.

Tested products

The latest versions of the following products available at the time of testing were tested:

Product name	Version
Acronis True Image	2017.6182
Antivirus A	
Antivirus B	
Antivirus C	
Antivirus D	
Antivirus E	
Antivirus F	
Antivirus G	
Antivirus H	
Antivirus I	
Antivirus J	
Antivirus K	
Antivirus L	
Antivirus N	
Antivirus O	
Antivirus P	
Antivirus Q	
Antivirus R	
Antivirus S	
Antivirus T	

Antivirus U	
Antivirus V	
Antivirus W	

Every product was installed with the default settings and updated before testing.

Test scenarios

The Ransomware Protection Test designed to verify the capabilities of the current security solutions to detect ransomware activity on a user's computer running the Windows operating system. The test includes scenarios that are similar but not equal to the RanSim scenarios by KnowBe4, plus additional test cases to reflect the behavior of the real-world ransomware.

The tests are run within the NioCryptoSim testing framework. Every test scenario is executed with the help of a Python script, the latest version of which is available at Github. The framework uses the following crypto interfaces, tools, and packages: PyCrypto, MS CryptoAPI, GPG, OpenSSL, and gzip.

The test suite consists of 18 tests: three false positive tests: ARCHIVE, MOVE, REMOVE, that should pass undetected, and 15 ransomware simulations, behavior of which should be detected and blocked.

No	NioCryptoSim Scenario	Description	Behavior
1	ENCRYPT_AND_REPLACE	InsideCryptor*	Encrypts files using AES-256-CBC and overwrites the content of the original files with the encrypted data.
2	ENCRYPT_TO_NEW_FILE	StrongCryptorFast*	Encrypts files to new files using AES-256-CBC and deletes original files.
3	ENCRYPT_SAFE_DELETE	StrongCryptor*	Encrypts files using AES-256-CBC and safely deletes the original files with CIPHER /W
4	ENCRYPT_HTTP	StrongCryptorNet*	Encrypts files using AES-256-CBC and deletes the original files. Simulates sending the encryption key to a server using an HTTP connection.

5	ENCRYPT_TO_STREAM	Streamer*	Writes files data into a single file and encrypts this file
6	ARCHIVE (FP test)	Archiver*	Archives files using gzip. This scenario should not be blocked.
7	REMOVE (FP test)	Remover*	Deletes files in a folder. This scenario should not be blocked.
8	REPLACE	Replacer*	Replaces the content of the files.
9	MOVE (FP test)	Mover* (modified)	Moves files to a different folder. This scenario should not be blocked.
10	ENCRYPT_XOR	WeakCryptor*	Encrypts files using XOR and deletes the original files.
11	LOCKY	Locky simulator	Simulates the behavior of the Locky ransomware: -Encrypts files using random AES-128 keys using MS CryptoAPI. -AES-128 keys are encrypted by RSA-2048 using WinCryptoAPI. -Removes shadow copies of the files. -Adds registry keys. -Connects to a C&C via HTTP.
12	THOR	Thor simulator	Simulates the behavior of the Thor ransomware.
13	NEMUCOD	Nemucod simulator	Simulates the behavior of the Nemucod ransomware. Encrypts first 2048 bytes of the file with the XOR 255 byte key.
14	VAULTCRYPT	Vaultcrypt simulator	Simulates the behavior of the VaultCrypt ransomware.

			-Encrypts files with RSA-1024 using the GPG tool. -Then encrypts the session RSA private key with the encoded master RSA public key. -Runs ‘cipher /w’ to wipe data from the hard disk.
15	DELETE_SHADOWS	Atomic function used by ransomware	Deletes shadow copies of the files: ‘vssadmin.exe Delete Shadows /All /Quiet’
16	ENCRYPT_CRYPTOAPI	Atomic function used by ransomware	Encrypts files in a folder to new files using MS CryptoAPI and deletes original files.
17	ENCRYPT_GPG	Atomic function used by ransomware	Encrypts files to new files with AES-256 using GnuPG tool. Deletes original files.
18	ENCRYPT_OPENSSL	Atomic function used by ransomware	Encrypts files using the OpenSSL library.

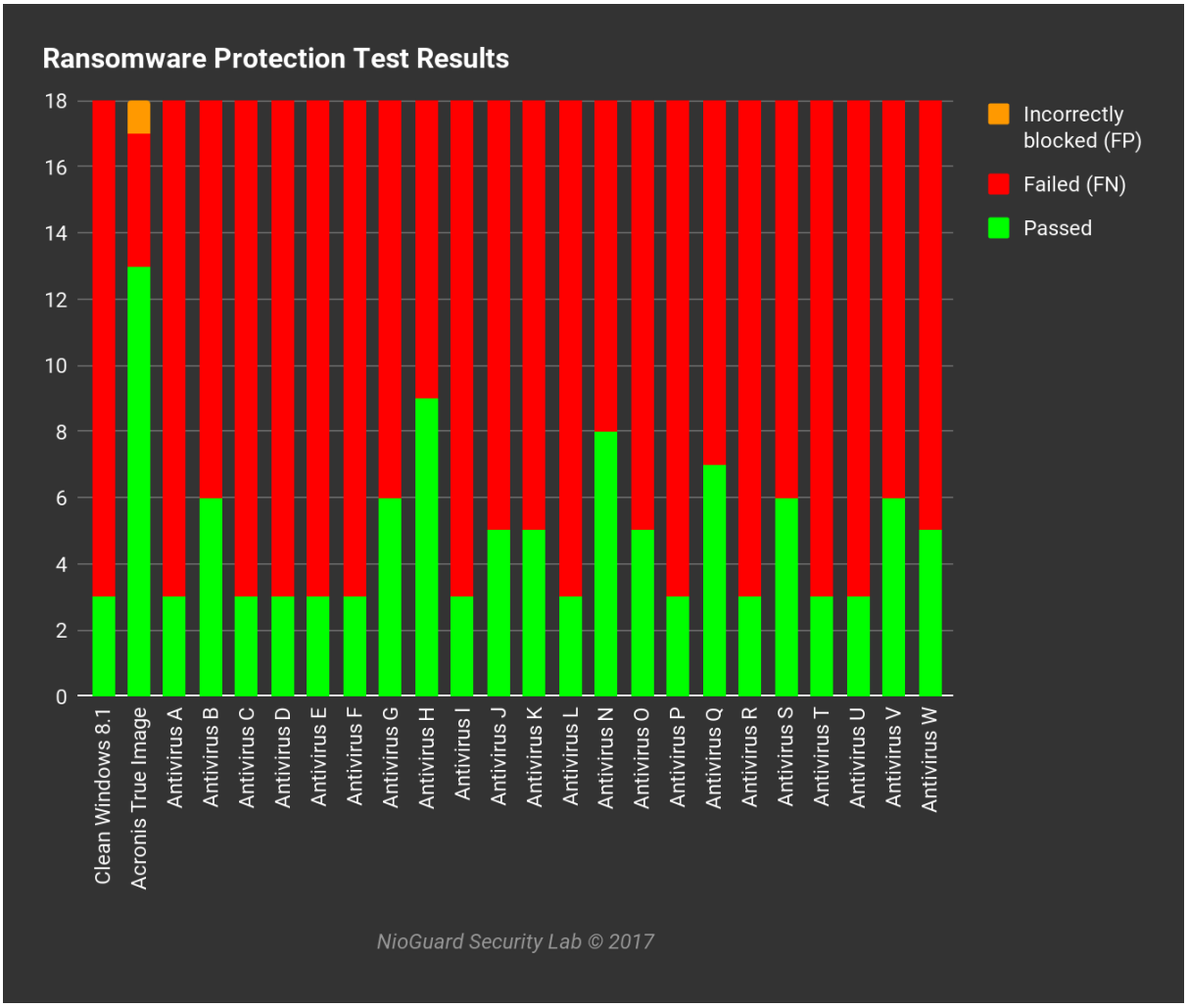
* the test has similar behavior to the RanSim test with the specified name.

Results

Product	Passed	Failed (FN)	Incorrectly blocked (FP)
Clean Windows 8.1 with disabled Defender	3	15	0
Acronis True Image	13	4	1
Antivirus A	3	15	0
Antivirus B	6	12	0
Antivirus C	3	15	0
Antivirus D	3	15	0
Antivirus E	3	15	0
Antivirus F	3	15	0
Antivirus G	6	12	0
Antivirus H	9	9	0
Antivirus I	3	15	0
Antivirus J	5	13	0
Antivirus K	5	13	0
Antivirus L	3	15	0
Antivirus N	8	10	0
Antivirus O	5	13	0
Antivirus P	3	15	0
Antivirus Q	7	11	0
Antivirus R	3	15	0
Antivirus S	6	12	0
Antivirus T	3	15	0
Antivirus U	3	15	0
Antivirus V	6	12	0
Antivirus W	5	13	0

Note:

The results only show the total number of failed tests without specifying which particular tests were failed. This is done intentionally to prevent the criminals from getting information about the weaknesses of the tested security products.



Conclusion

The aim of the Ransomware Protection Test was to verify the anti-ransomware modules and behavior blockers designed to provide real-time protection in addition to the signature-based malware detection capabilities of the software.

The results have shown that despite the “next-generation” anti-ransomware heuristic algorithms implemented in many of the tested products, most of them have severe limitations in detecting the ransomware-like behavior.

We hope that the published results will encourage security vendors to improve their products to protect users against new ransomware (cryptolocker) variants capable of bypassing signature detection with polymorphic encryption and scripting languages.

Copyright and Disclaimer

Any use of the results provided in this report is only permitted after the explicit written agreement with NioGuard Security Lab prior to any publication.

We are not responsible for any damage or loss that might occur in connection with the use of the information provided in this paper including the test script. We do not guarantee the correctness and completeness of the content provided in this report.

For more information regarding NioGuard Security Lab and the testing methodology, please visit our website or contact us via email: ada@nioguard.com.

