Ransomware Test of Padvish AntiCrypto

Date of the Report: October 16th 2017, last update December 15th, 2017

Introduction

Padvish commissioned AV-TEST to perform a dedicated Ransomware test of the product Padvish AntiCrypto.

The tested categories are as follows:

- PROTECTION
  - Detection of Real-World Ransomware
  - Detection of simulated Ransomware attacks
- FALSE POSITIVE TESTING
  - False Detection of typical user-behavior, like
    - Copying files
    - Packing/unpacking files

The tests have been carried out in September 2017 on Windows 10 RS2 (English) 64-Bit. The version of Padvish AntiCrypto was 1.5.108.619.

Methodology

Platforms

All tests were performed on actual physical machines. No Virtual Machines were used. All tests for a defined operating system were carried out on devices with identical hardware configurations as described below. The operating system used was Windows 10 RS2 (English), 64-bit.

Testing Approach

There are a few generic principles that were followed:

(1) **Physical devices**. The test devices used were physical devices. No Virtual Machines were used.
(2) **Product cloud/Internet connection**. The Internet was available to all tested products.
(3) **Product configuration**. All products were run with their default, out-of-the-box configuration.
(4) **Clean device for the start of the test**. The test devices were restored to a clean state before testing the malware samples.
(5) **Sample cloud/Internet accessibility.** If the malware used the internet connection to reach other sites in order to download other files and infect the system, care was taken to make sure that the cloud access was available to the malware sample in a **safe** way such that the testing network was not under the threat of getting infected.

Protection Test

The detection test measured the protection against real-world ransomware and simulated attacks by using typical ransomware behavior.

The test aims to determine if the user's data is protected without any impairments.

Padvish AntiCrypto was installed on the system and the ransomware samples were executed with an active internet connection. The system is monitored to verify whether the infection is stopped. The possibly affected files will be validated to ensure that no data is encrypted.

The simulated test cases followed the same methodology.

False positive Test

The test contains two scenarios: A test set of files with commonly used file extensions was copied from a local and a network source into the "User\Documents" folder. The second scenario was to pack and unpack files in the "User\Documents" folder as well on a second partition.

Results

PROTECTION

The protection test has been carried out with 23 ransomware attacks (real-world and simulated). Table 1 displays the detection rates.

Test Category	Number of Test Cases	Successful Detection	Completely Blocked	Detection Rate
Real-World attacks	15	15	15	100%
Simulated attacks	8	8	4	50%

Table 1 PROTECTION Test Results

In case of real-world ransomware attacks all were detected and successfully blocked. The detection rate of 100% is perfect. For the simulated attacks half of them were detected and completely blocked. The second half were detected but at least one file was encrypted before the malware could be stopped. We assume this happened because the simulated attacks did not start to encrypt files in the "Documents" folder, rather they start in a random folder on the primary partition.

The encrypted files of the 4 not completely blocked test cases are successfully recovered by Padvish's Data Cop Protection. Here Padvish use the Windows History (Volume Shadow Storage) functionality to recover different versions of files.

USABILITY

This test has been carried out against typical user behavior on a Windows PC like copying a set of files from a local and network path and packing/unpacking these files. In both scenarios Padvish AntiCrypto did not alert on the behavior or generate any false warnings.

Summary

Padvish AntiCrypto demonstrated the ability to protect the user's data without any measurable user restrictions. The widely distributed ransomware samples were completely detected and blocked.

However, we found that the protection approach can be bypassed if Ransomware changes its behavior. Currently Padvish creates a folder "!!AntiCrypto!!" containing fake files with lots of different file extension. The default behavior of the ransomware at the present time follows the sequence A-Z. Therefore, the ransomware tries to encrypt the files in the fake folder first. This enables Padvish AntiCrypto to detect the behavior and block the malware without causing any damage to the actually relevant user data.