NioGuard Security Lab

Corporate Backup Solutions Self-Defense Test

/ MARCH 2018

01

Introduction

In the light of the growing number of ransomware attacks in which cryptolockers terminate database processes to unlock the database files for encryption (Cerber, GlobeImposter, Rapid, Serpent) and can encrypt local and network backups to demand a ransom (Rapid, Spora), we decided to test self-defense capabilities of the top backup solutions used in business environments available for trial.

The test aims at testing sustainability of product's processes and services against typical attacks to security software described below, as well as self-protection of local backup and product's files. Ransomware can encrypt local backup files and configuration files that belong a backup program thereby disabling recovery of the files. Moreover, once access to agent's or server's processes is gained, an attacker can delete backup copies of the files not only locally, but also in the cloud on behalf of a backup solution.

This document is a summary of the corporate backup solutions test report and includes the description of the test environment, list of tested 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.

02

Test environment

The tests were conducted on the virtual machines of:

- Windows 8.1 SP1 32-bit build 9600
- Windows 10 64-bit Enterprise Build 16299
- Windows Server 2012 R2 Standard 64-bit v. 6.3.9600 Build 9600

We tested backup solutions on 32-bit and 64-bit platforms because the process injection techniques used in the test scenarios differ on these platforms. Moreover, 32-bit and 64-bit product builds may contain a different set of features including self-defense ones and their implementation may depend on the OS architecture.

03

Tested products

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

Product name	Components	Version
Acronis Backup	Management Server	12.5 9010
	Agent	12.5 9010
Arcserve	Unified Data Protection Server	6.5.4175 Update 2 Build 667
	Unified Data Protection Client	6.5.4175.791 v.r6.5
Veeam	Backup & Replication	9.5 Update 3
	Agent Windows	2.1.0.423
Veritas Backup Exec	Server	16.0 Rev. 1142
	Agent Utility for Windows	16.0 ver. 1142.1632

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

04

Test scenarios

The test suite consists of 31 tests simulating attacks to local backup files, product's files, processes, services, and a cloud storage that aim at disruption of backup and recovery service. The 'Protection of the product's files' test category contains simple tests aimed at destroying backup and application files making recovery of the encrypted by ransomware data impossible.

The second group of tests 'Protection of the product's processes and services' is crucial for self-defense because malware can inject its malicious code into a backup agent and act on behalf of a backup solution gaining all necessary privileges to control backup files. At the wish of an attacker, a malicious process can terminate processes and services that may lead to crashing the backup and recovery application or deletion of backup files on behalf of a backup solution. The last test set is 'Protection of cloud backup and recovery' and targets communication interfaces with cloud storage. The DNS poisoning attack or improper use of CLI may result in disruption of cloud backup service.

№	Test Category	Test Scenario
	Protection of the product's files	
1	Protection of local backup files	Rename, delete, or encrypt local backup files
2	Protection of the backup product's own files	Delete program files
3		MBR modification and MFT encryption (NotPetya and Petya ransomware)
	Protection of the product's processes and services	
4	Terminating processes and services	End task in Task Manager
5		Stop services and terminate processes using PowerShell
6		Using TerminateProcess()
7		Using TerminateThread()
8		Using TerminateJobObject()
9		Using DebugActiveProcess()
10		Using WinStationTerminateProcess()
11		Send WM_CLOSE event
12		Send WM_QUIT event
13		Send WM_SYSCOMMAND (SC_CLOSE) event
14		Send all possible windows events
15	Code injection	Using CreateRemoteThread()
16		Using NtCreateThreadEx()
17		Using QueueUserAPC()

№	Test Category	Test Scenario
	Protection of the product's processes and services	
18	Code injection	Using SetWindowsHookEx()
19		Using RtlCreateUserThread()
20		Using SetThreadContext()
21		Reflective DLL injection
22	Modification of process memory	Blocking access to the process memory pages setting the PAGE_NOACCESS attribute
23		Trying to free process memory using NtFreeVirtualMemory()
24		Unmap all mapped objects using NtUnmapViewOfSection()
25		Allocate all available memory using NtAllocateVirtualMemory()
26		Allocate all available memory using NtMapViewOfSection()
27		Write in process memory using NtWriteVirtualMemory()
28	Modification of process objects	Duplicate process objects to consume all available resources
29		Duplicate process objects with closing source objects
	Protection of cloud backup and recovery	
30	Modification of cloud backup data	Use product's CLI to delete, modify, or encrypt data in the cloud
31	DNS poisoning	Modify hosts file

05

Results

Product name	Platform 32-bit / 64-bit	The number of passed tests	The number of failed tests	Not applicable (N/A)	Pass rate
Acronis Backup	32	26	4	1	87%
	64	25	6	0	81%
Arcserve	32	5	24	2	17%
	64	4	26	1	13%
Veeam	32	4	26	1	13%
	64	4	27	0	13%
Veritas Backup Exec	32	5	22	4	19%
	64	4	27	0	13%

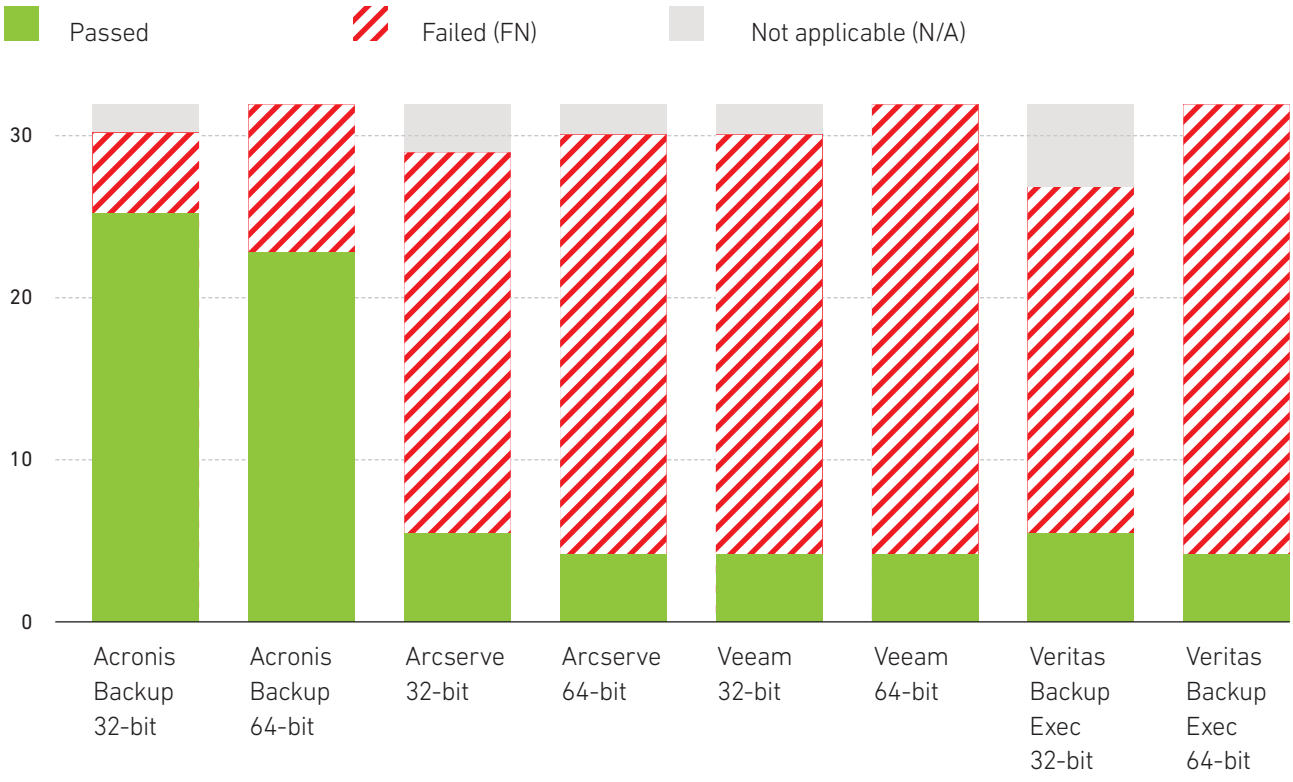
The number of passed tests - the product withstanded the attack preserving workability of the recovery service.

The number of failed tests - the product crashed after the attack losing workability of the recovery service.

Not applicable - the test uses a Windows API function that is not supported by the current version of Windows or the tested feature is not available in the product. For instance, a solution has no CLI tool to manage backups or cloud storage is not available among locations where to store backups.

Pass rate is calculated as The number of passed tests / (Total number of tests - N/A).

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 products.*



06 Conclusion

The aim of the test was to verify the self-defense capabilities of the backup software to protect their files, processes, service, and cloud storage against scenarios that can be potentially executed by ransomware.

The results have shown that the majority of the tested products are not ready in most cases to counteract the ransomware-like attacks allowing a potential attacker to lock user's backups and disable backup and recovery services. Only Acronis Backup showed good results with 87% and 81% pass rate for 32-bit and 64-bit products correspondingly providing comprehensive self-defense capabilities as well as service sustainability.

07 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 accuracy and completeness of the content provided in this report.

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