NioGuard Security Lab

Soluzioni Corporate di backup

Test di auto-protezione

MARZO 2018

01

Introduzione

Alla luce del crescente numero di attacchi ransomware in cui i cryptolocker interrompono i processi di database per sbloccare i file di database per la crittografia (Cerber, GlobeImposter, Rapid, Serpent) e possono crittografare backup locali e di rete per richiedere il pagamento di un riscatto (Rapid, Spora), abbiamo deciso di testare le capacità di auto-protezione delle migliori soluzioni di backup utilizzate negli ambienti aziendali disponibili per la prova.

Il test mira a controllare la sostenibilità dei processi e dei servizi dei prodotti contro gli attacchi tipici al software di sicurezza descritti di seguito, nonché l'auto-protezione del backup locale e dei file dei prodotti. Il ransomware può crittografare i file di configurazione e i file di backup locali che appartengono a un programma di backup disabilitando il ripristino dei file. Inoltre, una volta ottenuto l'accesso ai processi dell'agente o del server, l'utente autore dell'attacco può eliminare le copie di backup dei file non solo a livello locale, ma anche nel cloud per conto di una soluzione di backup.

Questo documento è un riepilogo del report di test delle soluzioni di backup aziendali e include la descrizione dell'ambiente di test, l'elenco delle soluzioni testate e delle relative versioni, la panoramica degli scenari di test, nonché i risultati e le conclusioni basati su questi risultati. Non classifichiamo le soluzioni testate e non assegniamo alcun premio, ma forniamo i risultati "così come sono" a solo scopo informativo.

02

Ambiente di test

I test sono stati condotti sulle macchine virtuali di:

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

Abbiamo testato soluzioni di backup su piattaforme a 32 e 64 bit perché le tecniche di iniezione di processo utilizzate negli scenari di test differiscono su queste piattaforme. Inoltre, le build di prodotto a 32 e 64 bit possono contenere una diversa serie di funzionalità, tra cui quelle di auto-protezione, e la loro implementazione può dipendere dall'architettura del sistema operativo.

03

Prodotti testati

Sono state testate le versioni più recenti dei seguenti prodotti disponibili al momento del test:

Nome prodotto	Componenti	Versione
Acronis Backup	Management Server	12.5 9010
	Agent	12.5 9010
Arcserve	Unified Data Protection Server	6.5.4175 Aggiornamento 2 Build 667
	Unified Data Protection Client	6.5.4175.791 v.r6.5
Veeam	Backup & Replication	9.5 Aggiornamento 3
	Agent for Microsoft Windows	2.1.0.423
Veritas Backup Exec	Server	16.0 Rev. 1142
	Agent Utility pour Windows	16.0 ver. 1142.1632

Ogni prodotto è stato installato con le impostazioni predefinite e aggiornato prima dell'esecuzione del test.

04

Scenari dei test

La suite di test comprende 31 test che simulano attacchi a file di backup locali, file dei prodotti, processi, servizi e un cloud storage che mirano al blocco del servizio di backup e ripristino. La categoria di test "Protezione dei file dei prodotti" contiene semplici test volti a distruggere i file di backup e di applicazione rendendo impossibile il recupero dei dati crittografati da ransomware.

Il secondo gruppo di test "Protezione dei processi e dei servizi dei prodotti" è essenziale per l'auto-protezione poiché il malware può iniettare il codice dannoso in un agente di backup e agire per conto di una soluzione di backup ottenendo tutti i privilegi necessari per controllare i file di backup. Per volere di un aggressore, un processo dannoso può interrompere processi e servizi con conseguente blocco dell'applicazione di backup e ripristino o eliminazione di file di backup per conto di una soluzione di backup. L'ultima serie di test è "Protezione del backup e del ripristino del cloud" ed è indirizzata alle interfacce di comunicazione con lo storage cloud. L'attacco di poisoning del DNS o l'uso improprio della CLI possono causare l'interruzione del servizio di backup del cloud.

N.	Categoria test	Scenario test
	Protezione dei file dei prodotti	
1	Protezione dei file di backup locali	Ridenominazione, eliminazione o crittografia dei file di backup locali
2	Protezione di propri file dei prodotti di backup	Eliminazione dei file di programma
3		Modifica dell'MBR e crittografia dell'MFT (ransomware NotPetya e Petya)
	Protezione dei processi e dei servizi dei prodotti	
4	Interruzione di processi e servizi	Termine attività nella Gestione attività
5		Arresto dei servizi e termine dei processi tramite PowerShell
6		Uso di TerminateProcess()
7		Uso di TerminateThread()
8		Uso di TerminateJobObject()
9		Uso di DebugActiveProcess()
10		Uso di WinStationTerminateProcess()
11		Invio dell'evento WM_CLOSE
12		Invio dell'evento WM_QUIT
13		Invio dell'evento WM_SYSCOMMAND (SC_CLOSE)
14		Invio di tutti gli eventi di Windows possibili
15	Iniezione codice	Uso di CreateRemoteThread()
16		Uso di NtCreateThreadEx()
17		Uso di QueueUserAPC()

N.	Categoria test	Scenario test
	Protezione dei processi e dei servizi dei prodotti	
18	Iniezione codice	Uso di SetWindowsHookEx()
19		Uso di RtlCreateUserThread()
20		Uso di SetThreadContext()
21		Iniezione DLL riflettente
22	Modifica della memoria di processo	Blocco dell'accesso alle pagine della memoria di processo impostando l'attributo PAGE_NOACCESS
23		Tentativo di liberare la memoria di processo mediante NtFreeVirtualMemory()
24		Annullamento del mapping di tutti gli oggetti mappati mediante NtUnmapViewOfSection()
25		Allocazione di tutta la memoria disponibile mediante NtAllocateVirtualMemory()
26		Allocazione di tutta la memoria disponibile mediante NtMapViewOfSection()
27		Scrittura nella memoria di processo mediante NtWriteVirtualMemory()
28	Modifica di oggetti di processo	Duplicazione di oggetti di processo per consumare tutte le risorse disponibili
29		Duplicazione di oggetti di processo con oggetti di origine di chiusura
	Protezione del backup e del ripristino del cloud	
30	Modifica dei dati di backup del cloud	Uso della CLI del prodotto per eliminare, modificare o crittografare i dati nel cloud
31	Poisoning del DNS	Modifica dei file host

05

Risultati

Nome prodotto	Piattaforma a 32 bit / 64 bit	Numero di test superati	Numero di test non riusciti	Non pertinente (N/A)	Tasso di efficacia
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%

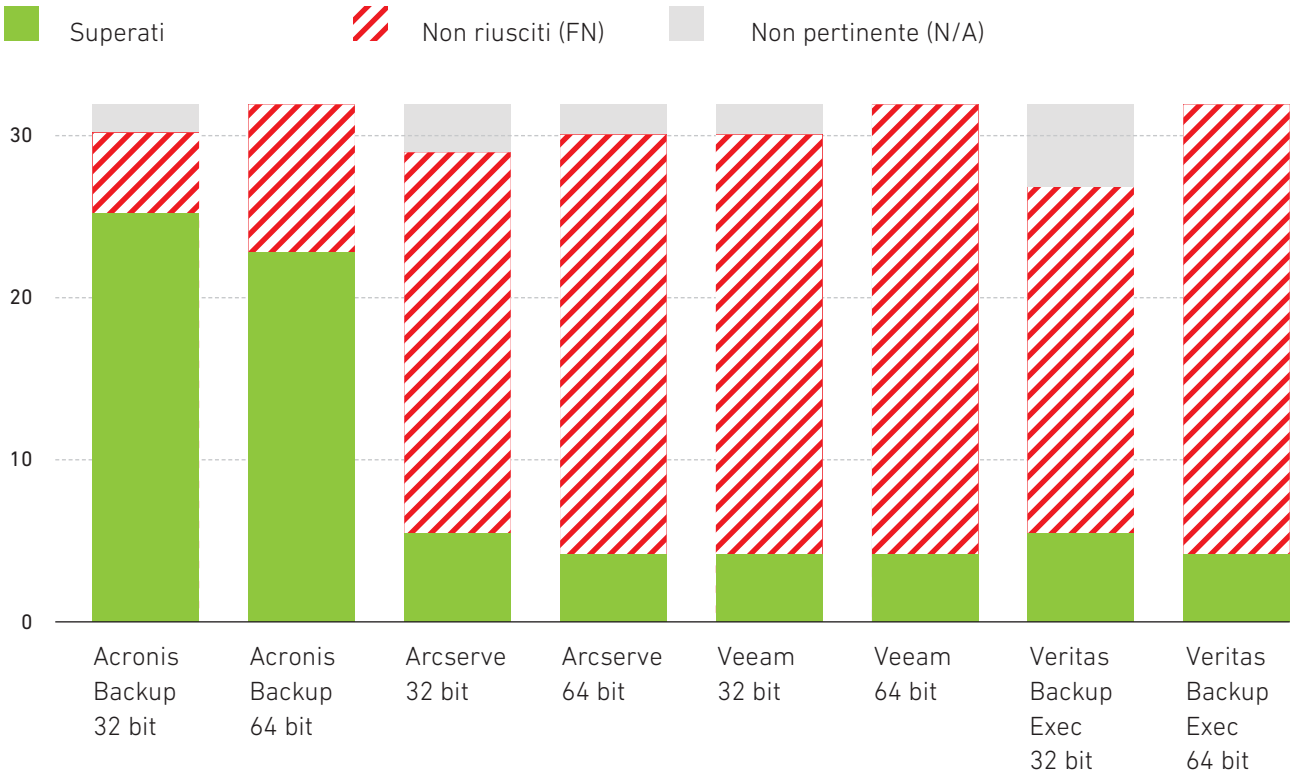
Numero di test superati - il prodotto ha resistito all'attacco mantenendo la lavorabilità del servizio di recupero.

Numero di test non riusciti - il prodotto si è bloccato dopo l'attacco perdendo la lavorabilità del servizio di recupero.

Non pertinente - il test utilizza una funzione API di Windows che non è supportata dalla versione corrente di Windows o la funzionalità testata non è disponibile nel prodotto. Ad esempio, una soluzione non presenta alcuno strumento CLI per gestire i backup o il cloud storage non è disponibile tra le posizioni in cui archiviare i backup.

Tasso di efficacia - viene calcolato come Numero di test superati / (Numero totale di test - N/A).

Nota: *i risultati mostrano unicamente il numero totale di test non riusciti senza specificare quali test specifici sono falliti. Ciò viene fatto intenzionalmente per impedire ai criminali di ottenere informazioni sui punti deboli dei prodotti testati.*



06

Conclusioni

Lo scopo del test consisteva nel verificare le capacità di auto-protezione del software di backup per proteggere i relativi file, processi, servizi e cloud storage dagli scenari che possono essere potenzialmente eseguiti dal ransomware.

I risultati hanno mostrato che la maggior parte dei prodotti testati non è pronta in molti casi a contrastare gli attacchi di tipo ransomware consentendo a un potenziale aggressore di bloccare i backup dell'utente e disabilitare i servizi di backup e ripristino. Soltanto Acronis Backup ha mostrato buoni risultati con un tasso di efficacia dell'87% e dell'81% per prodotti a 32 bit e 64 bit, fornendo in modo analogo funzionalità complete di auto-protezione e sostenibilità dei servizi.

07 Copyright e limitazione di responsabilità

Qualsiasi utilizzo dei risultati forniti nel presente rapporto è consentito unicamente dopo l'esplicito accordo scritto con NioGuard Security Lab prima di qualsiasi pubblicazione.

Non siamo responsabili per eventuali danni o perdite che potrebbero verificarsi in connessione con l'uso delle informazioni fornite nel presente documento, compreso lo script dei test. Non garantiamo l'esattezza e la completezza dei contenuti forniti in questo rapporto.

Per ulteriori informazioni relative a NioGuard Security Lab e alla metodologia di esecuzione dei test, visita il nostro sito Web www.nioguard.com oppure contattaci via e-mail: ada@nioguard.com.