ATTIVO NETWORKS

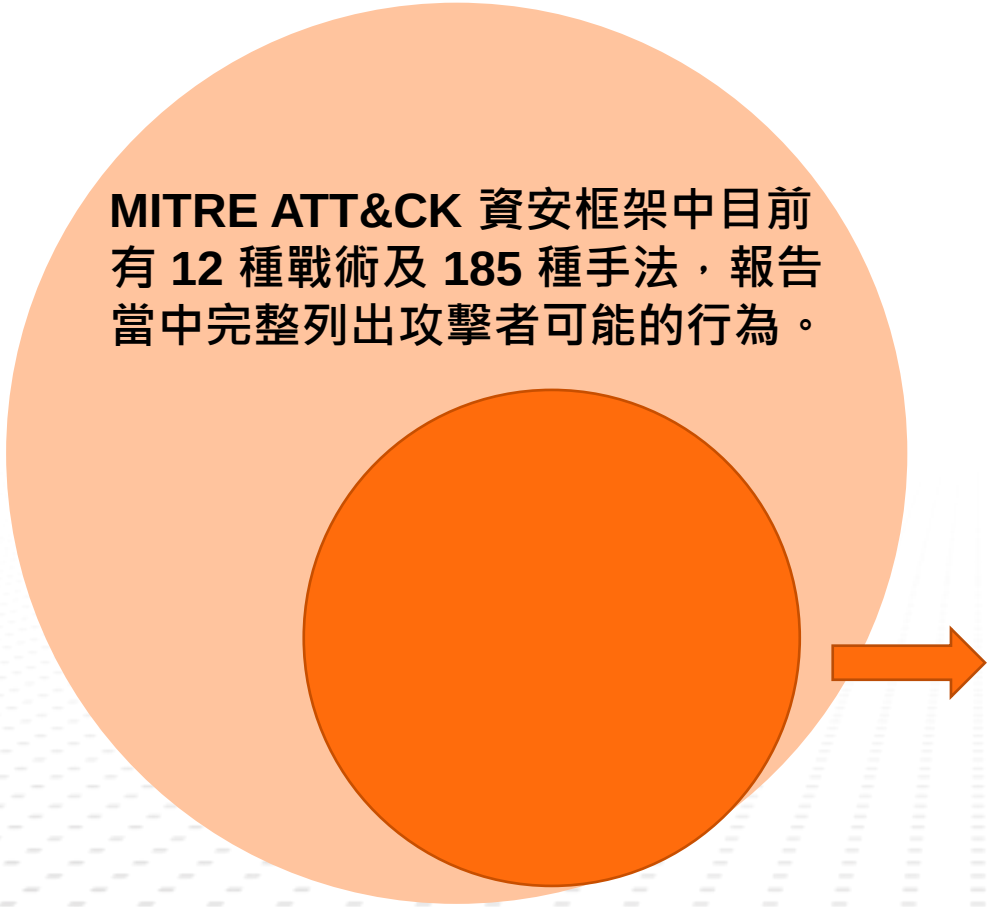
MITRE ATT&CK®

2020.12 版

© 2020 Attivo Networks. All rights reserved.

MITRE ATT&CK

MITRE ATT&CK® 是全球皆可取用的知識庫，其中包含根據實際案例觀察的駭客攻擊戰術和手法



Attivo Networks 涵蓋其中 72 種手法以及廣泛的憑證存取、探索、橫向移動和蒐集戰術資訊，藉以強化偵測效能。

© 2020 Attivo Networks. All rights reserved.

Attivo Networks 全方位威脅偵測

EDR Core Strength ← | **Attivo Networks Core Strength** | → **DLP Core Strength**

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Access Token
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	BITS Jobs
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Bypass User Account Control
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Clear Command History
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	CMSTP
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Code Signing
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compile After Delivery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Compiled HTML File
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Firmware
	InstallUtil	Component Firmware	Extra Window Memory Injection	Component Object Model Hijacking
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Connection Proxy
	Local Job Scheduling	Create Account	Hooking	Control Panel Items
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	DCShadow
	Mshta	Dylib Hijacking	Launch Daemon	Deobfuscate/Decode Files or Information
	PowerShell	Emond	New Service	Disabling Security Tools
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	DLL Search Order Hijacking
	Regsvr32	File System Permissions Weakness	Path Interception	DLL Side-Loading
	Rundll32	Hidden Files and Directories	Plist Modification	Execution Guardrails
	Scheduled Task	Hooking	Port Monitors	Exploitation for Defense Evasion
	Scripting	Hypervisor	PowerShell Profile	Extra Window Memory Injection
	Service Execution	Image File Execution Options Injection	Process Injection	File and Directory Permissions Modification
	Signed Binary Proxy Execution	Implant Container Image	Scheduled Task	File Deletion
	Signed Script Proxy Execution	Kernel Modules and Extensions	Service Registry Permissions Weakness	File System Logical Offsets
	Source	Launch Agent	Setuid and Setgid	Gatekeeper Bypass
	Space after Filename	Launch Daemon	SID-History Injection	Group Policy Modification
	Third-party Software	Launchctl	Startup Items	Hidden Files and Directories
	Trap	LC_LOAD_DYLIB Addition	Sudo	Hidden Users
	Trusted Developer Utilities	Local Job Scheduling	Sudo Caching	Hidden Window
	User Execution	Login Item	Valid Accounts	HISTCONTROL
	Windows Management Instrumentation	Logon Scripts	Web Shell	Image File Execution Options Injection
	Windows Remote Management	LSASS Driver		Indicator Blocking
	XSL Script Processing	Modify Existing Service		Indicator Removal from Tools
		Netsh Helper DLL		Indicator Removal on Host
		New Service		Indicator Removal on Host
		Office Application Startup		Indirect Command Execution
		Path Interception		Install Root Certificate
		Plist Modification		InstallUtil
		Port Knocking		Launchctl
		Port Monitors		LC_MAIN Hijacking
		PowerShell Profile		Masquerading
		Rc.common		Modify Registry
		Re-opened Applications		Mshta
		Redundant Access		Network Share Connection Removal
		Registry Run Keys / Startup Folder		NTFS File Attributes
		Scheduled Task		Obfuscated Files or Information
		Screensaver		Parent PID Spoofing
		Security Support Provider		Plist Modification
		Server Software Component		Port Knocking
		Service Registry Permissions Weakness		Process Doppelgänging
		Setuid and Setgid		Process Hollowing
		Shortcut Modification		Process Injection
		SIP and Trust Provider Hijacking		Redundant Access
		Startup Items		Regsvcs/Regasm
		System Firmware		Regsvr32
		Systemd Service		Revert Cloud Instance
		Time Providers		Rootkit
		Trap		Rundll32
		Valid Accounts		Scripting
		Web Shell		Signed Binary Proxy Execution
		Windows Management Instrumentation		Signed Script Proxy Execution
		Event Subscription		SIP and Trust Provider Hijacking
		Winlogon Helper DLL		Software Packing
				Space after Filename
				Template Injection
				Timestomp
				Trusted Developer Utilities
				Unused/Unsupported Cloud Regions
				Valid Accounts
				Virtualization/Sandbox Evasion
				Web Service
				Web Session Cookie
				XSL Script Processing

Credential Access	Discovery	Lateral Movement	Collection
Account Manipulation	Account Discovery	AppleScript	Audio Capture
Bash History	Application Window Discovery	Application Access Token	Automated Collection
Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data
Cloud Instance Metadata API	Cloud Service Dashboard	Component Object Model and Distributed COM	Data from Cloud Storage Object
Credential Dumping	Cloud Service Discovery	Exploitation of Remote Services	Data from Information Repositories
Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	Data from Local System
Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Network Shared Drive
Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Removable Media
Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data Staged
Forced Authentication	Network Sniffing	Remote Desktop Protocol	Email Collection
Hooking	Password Policy Discovery	Remote File Copy	Input Capture
Input Capture	Peripheral Device Discovery	Remote Services	Man in the Browser
Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Screen Capture
Kerberoasting	Process Discovery	Shared Webroot	Video Capture
Keychain	Query Registry	SSH Hijacking	
LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content	
Network Sniffing	Security Software Discovery	Third-party Software	
Password Filter DLL	Software Discovery	Web Session Cookie	
Private Keys	System Information Discovery	Windows Admin Shares	
Securityd Memory	System Network Configuration Discovery	Windows Remote Management	
Steal Application Access Token	System Network Connections Discovery		
Steal Web Session Cookie	System Owner/User Discovery		
Two-Factor Authentication Interception	System Service Discovery		
	System Time Discovery		
	Virtualization/Sandbox Evasion		

Command and Control	Exfiltration	Impact
Commonly Used Port	Automated Exfiltration	Account Access Removal
Communication Through Removable Media	Data Compressed	Data Destruction
Connection Proxy	Data Encrypted	Data Encrypted for Impact
Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Fallback Channels	Transfer Data to Cloud Account	Network Denial of Service
Multi-hop Proxy		Resource Hijacking
Multi-Stage Channels		Runtime Data Manipulation
Multiband Communication		Service Stop
Multilayer Encryption		Stored Data Manipulation
Port Knocking		System Shutdown/Reboot
Remote Access Tools		Transmitted Data Manipulation
Remote File Copy		
Standard Application Layer Protocol		
Standard Cryptographic Protocol		
Standard Non-Application Layer Protocol		
Uncommonly Used Port		
Web Service		

經 MITRE ATT&ACK 測試
使用 Attivo 欺敵平台可提升EDR

42%

的威脅偵測效能

© 2020 Attivo Networks. All rights reserved.

Attivo Networks 全方位威脅偵測

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Trusted Relationship EDN (ADSecure)	PowerShell EDN (ADSecure)	Account Manipulation EDN (ADSecure)	File System Permissions Weakness EDN (ThreatPath)	DCShadow EDN (ADSecure)	Account Manipulation EDN (ADSecure)	Account Discovery EDN (ThreatStrike & ThreatPath & ADSecure)	AppleScript EDN (ThreatStrike)	Data from Information Repositories BOTsink		Automated Exfiltration BOTsink	Account Access Removal EDN (ThreatStrike & ADSecure)
Valid Accounts EDN (ADSecure)		Create Account EDN (ADSecure)	Path Interception EDN (ThreatPath)	Group Policy Modification EDN (ThreatStrike & ADSecure)	Bash History EDN (ThreatStrike)	Browser Bookmark Discovery EDN (ThreatStrike)	Application Deployment Software BOTsink	Data from Local System BOTsink & EDN (ThreatStrike & Ransomware)			Data Destruction BOTsink & EDN (Ransomware)
		Port Knocking BOTsink	PowerShell Profile EDN (ADSecure)	Valid Accounts EDN (ADSecure)	Brute Force BOTsink & EDN (ADSecure)	Cloud Service Discovery EDN (ThreatStrike & ThreatPath)	Component Object Model and Distributed COM BOTsink	Data from Network Shared Drive BOTsink & EDN (ThreatStrike & Ransomware)			Data Encrypted for Impact BOTsink & EDN (Ransomware)
		PowerShell Profile EDN (ADSecure)	Service Registry Permissions Weakness EDN (ThreatPath)		Credential Dumping EDN (ThreatStrike & Ransomware)	Domain Trust Discovery EDN (ADSecure)	Exploitation of Remote Services BOTsink & EDN (ThreatStrike & ADSecure)				Resource Hijacking BOTsink
		Valid Accounts EDN (ADSecure & ThreatStrike)	Valid Accounts EDN (ADSecure)		Credentials from Web Browsers EDN(ThreatStrike & Ransomware)	File and Directory Discovery EDN (ThreatStrike & Ransomware)	Logon Scripts BOTsink				
					Credentials in Files EDN(ThreatStrike & Ransomware)	Network Service Scanning BOTsink & EDN (Deflect)	Pass the Hash BOTsink & EDN (ADSecure & ThreatStrike)				
					Credentials in Registry EDN (ThreatStrike)	Network Share Discovery EDN (ThreatStrike & Ransomware)	Pass the Ticket EDN (ThreatStrike & ADSecure)				
					Forced Authentication EDN (ThreatPath)	Network Sniffing BOTsiink	Remote Desktop Protocol BOTsink & EDN (ThreatStrike & ThreatPath & ADSecure)				
					Kerberoasting EDN (ThreatStrike & ADSecure)	Permission Groups Discovery EDN (ADSecure)	Remote File Copy BOTsink & EDN (ThreatStrike)				
					Keychain EDN (ThreatStrike)	Remote System Discovery EDN (ADSecure & BOTsink)	Remote Services BOTsink & EDN (ThreatStrike)				
					LLMNR/NBT-NS Poisoning and Relay BOTsink	System Network Configuration Discovery BOTsink & EDN (Deflect & ADSecure)	Shared Webroot EDN (ThreatPath)				
					Network Sniffing BOTsink	System Network Connections Discovery EDN (ADSecure & ThreatStrike)	Taint Shared Content EDN (ThreatStrike & Ransomware)				
					Private Keys EDN (ThreatStrike & Ransomware)	System Owner/User Discovery EDN (ThreatStrike & ADSecure & ThreatPath)	Third-party Software BOTsink				
					Steal Web Session Cookie EDN (ThreatStrike)	System Time Discovery BOTsink	Web Session Cookie EDN (ThreatStrike)				
							Windows Admin Shares EDN (ThreatStrike & Ransomware)				
							Windows Remote Management EDN (ThreatStrike & BOTsink)				

根據 Attivo 現有的覆蓋範圍...

攻擊者極不可能在內網中橫向移動，而不被 Attivo 偵測到

© 2020 Attivo Networks. All rights reserved.

勒贖程式的攻擊絞殺鏈

抵禦橫向移動的能力

Ransomware
勒贖程式

Infection
病毒感染

1st Step:

外部到內部

- 網路釣魚 (Phishing)
- 網站漏洞
- RDP 暴力攻擊 (Brute Force)
- USB 隨身碟

網路釣魚電子郵件

Persistence
持久性

2nd Step:

存在於本機

- 權限提升
- 憑證獲取
- 登錄
- Powershell

加密指令與控制

Exploitation
剝削攻擊

3rd Step:

加密

- 檔案加密
- 新變種

惡意程式碼變種

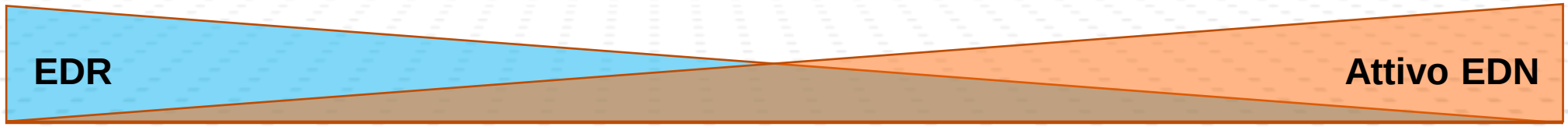
Lateral Movement
橫向移動

4th Step:

水平式散播

- SMB共享
- RDP暴力攻擊
- 系統漏洞
- 不當的設定 (Misconfiguation)

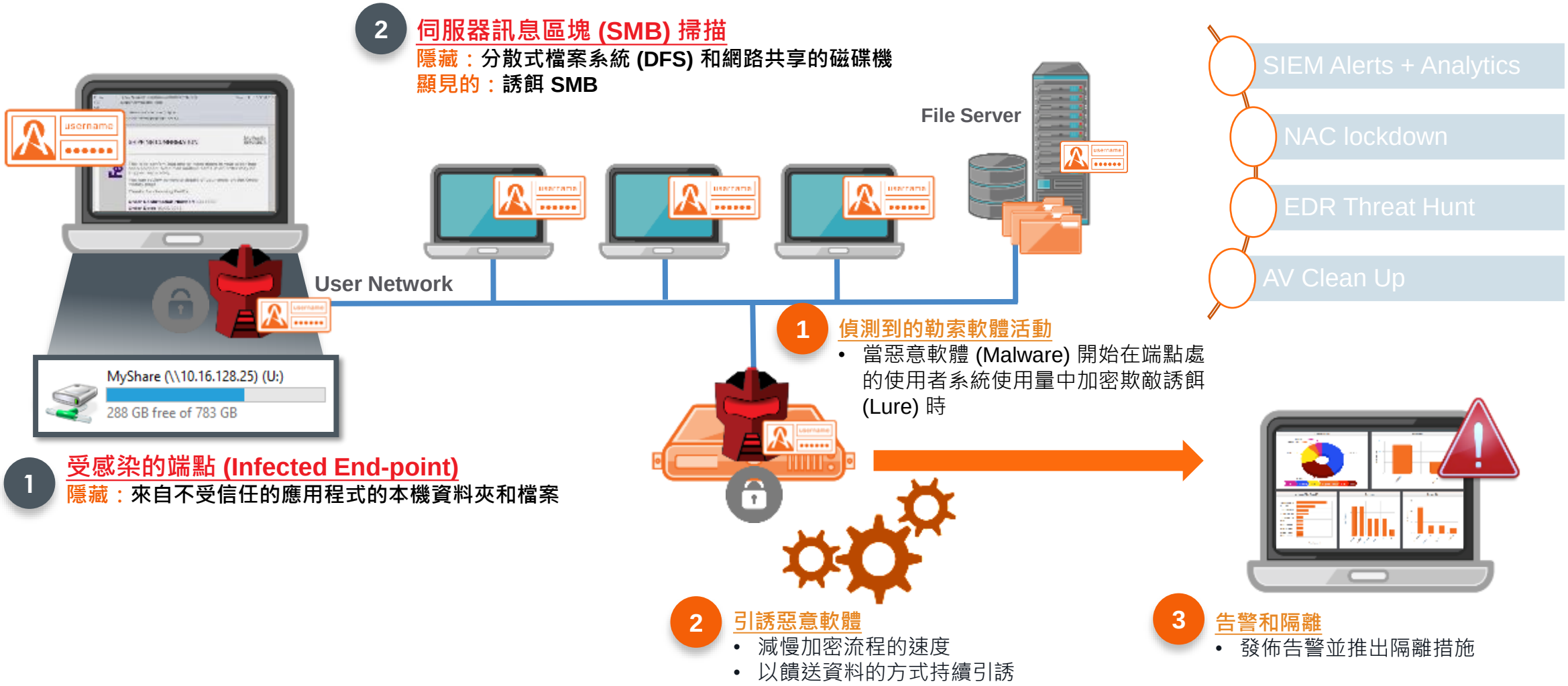
無法被偵測的慢速掃描



***單點防禦：**一旦勒索軟體進入內網，就會迅速地以水平方式進行多方向的散播，單靠防火牆或防毒軟體並無法抵禦。被勒索軟體 WannaCry 感染的企業組織全都有防火牆和防毒軟體。

© 2020 Attivo Networks. All rights reserved.

Attivo勒贖程式偵測及端點保護



© 2020 Attivo Networks. All rights reserved.

Attivo 端點偵測網(EDN) 的高度整合力

Attivo EDN + Crowdstrike EDR

Attivo Networks 是什麼樣的公司？

- ✓ **技術創新者：**偵測威脅和防止攻擊者在內網從事探索、橫向移動和權限提升。
- ✓ **欺敵平台：**在攻擊者已破壞端點，且以傳統 EDR 無法偵測出的方法進行攻擊時，該平台能偵測出攻擊活動，並將攻擊者引離攻擊目標。

為什麼選擇 Attivo Networks？

- ✓ **有效阻擋橫向移動：**
  在傳統 EDR 系統專注在抵制攻擊者攻擊端點的同時，Attivo 則能防止攻擊者在端點內網做橫向的移動。

為什麼上述的功能如此重要？

- ✓ **攻擊進化：**現今先進的攻擊者靠橫向移動和其它手法打敗防禦技術。
- ✓ **第三方認證：**MITRE ATT&CK 矩陣模型(MITRE ATT&CK Matrix)展現出 CrowdStrike 端點上 Attivo 技術可量化的價值。

© 2020 Attivo Networks. All rights reserved.

Attivo 端點偵測網(EDN) 的高度整合力

Attivo 為 CrowdStrike 整合協力廠商，並整合 Falcon Platform

Attivo EDN 解決方案關鍵要素

1. **ADSecure**
   防止攻擊者提取 AD 資訊 (當他們從端點查詢 AD 時)
2. **高仿真誘餌(Lure)**
   偵測憑證竊取和權限提升的攻擊
3. **使攻擊者轉向**
   偵測並拒絕攻擊者進行橫向移動
4. **勒索軟體**
   隱藏資料和儲存裝置，並拒絕攻擊者取用，同時以高度互動的方式延緩攻擊
5. **縮小攻擊面**
   識別並修正暴露的憑證和不當的設定，讓攻擊者無法用來作橫向移動

廠商	加權計分			原始計分		
	原始表現	加上 Attivo	提升率	原始表現	加上 Attivo	提升率
Crowdstrike	280	442	58%	151	191	26%

© 2020 Attivo Networks. All rights reserved.

EDN Boosts APT29 測試結果

在結合原始和加權計分 (Flat and Weighted Scoring) 表現平均提升 42%

廠商	加權計分			原始計分		
	原始表現	加上 Attivo	提升率	原始表現	加上 Attivo	提升率
A	280	442	58%	151	191	26%
B	214	413	93%	91	176	93%
C	637	743	17%	288	298	3%
D	407	526	29%	192	225	17%
Average			**49%**			**35%**

© 2020 Attivo Networks. All rights reserved.

Attivo NETWORKS

Deceptively Simple Threat Detection

© 2020 Attivo Networks. All rights reserved.