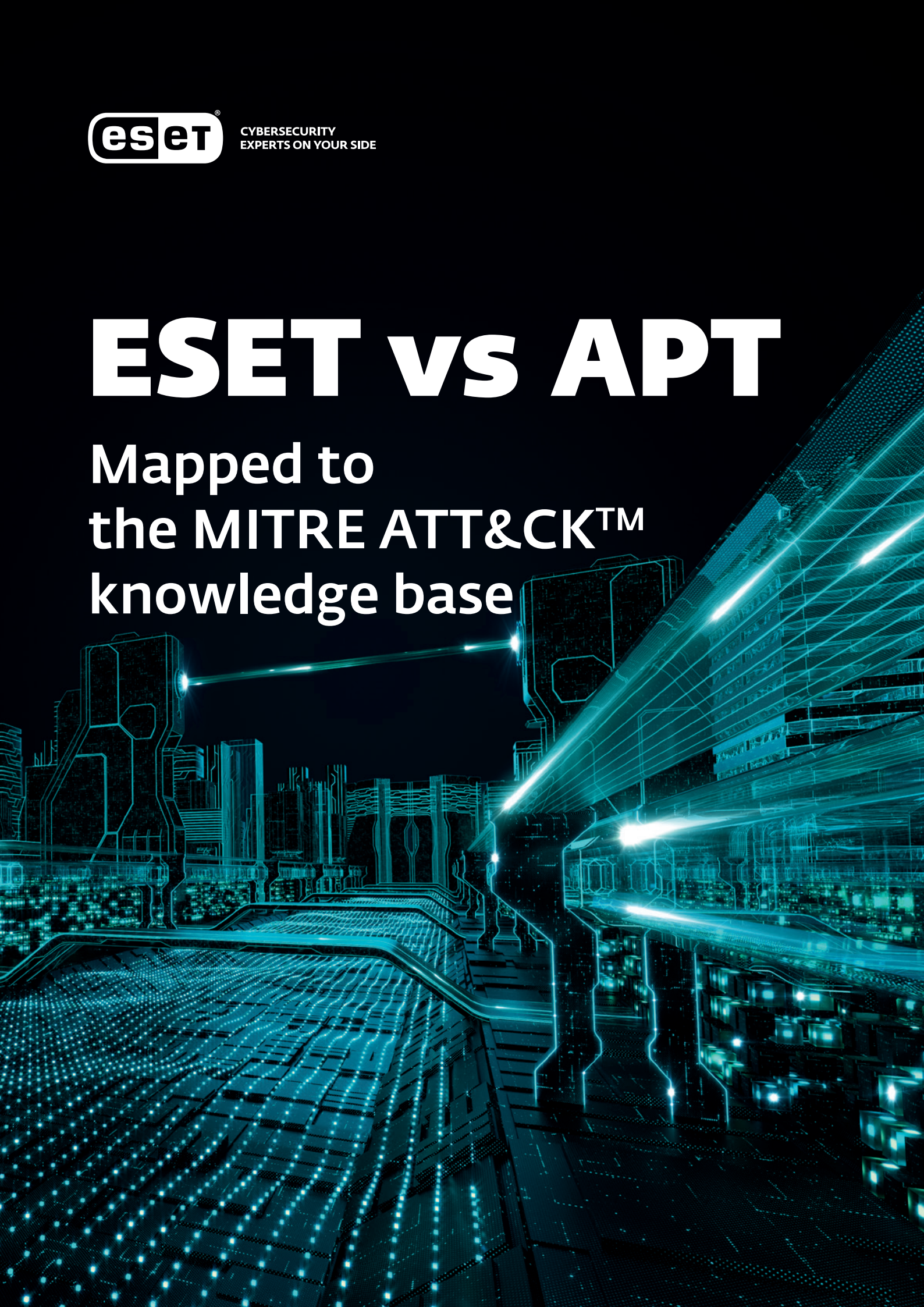
CYBERSECURITY
EXPERTS ON YOUR SIDE

ESET vs APT

Mapped to the MITRE ATT&CK™ knowledge base



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command & Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command & Control Protocol
1 Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command & Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-hop Proxy
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Launchctl	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	Shared Webroot	Screen Capture		Multiband Communication
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Keychain	Remote System Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content			Port Knocking
	Mshta	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking	Network Sniffing	System Information Discovery	Third-party Software			Remote Access Tools
	PowerShell	Dylib Hijacking	Path Interception	DLL Side-Loading	Password Filter DLL	System Network Configuration Discovery	Windows Admin Shares			Remote File Copy
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	System Network Connections Discovery	Windows Remote Management			Standard Application Layer Protocol
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection	Securityd Memory	System Owner/User Discovery				Standard Cryptographic Protocol
	Rundll32	Hidden Files and Directories	Process Injection	File Deletion	Two-Factor Authentication Interception	System Service Discovery				Standard Non-Application Layer Protocol
	Scheduled Task	Hooking	Scheduled Task	File Permissions Modification		System Time Discovery				Uncommonly Used Port
	Scripting	Hypervisor	Service Registry Permissions Weakness	File System Logical Offsets						Web Service
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	Gatekeeper Bypass						
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	Hidden Files and Directories						
	Signed Script Proxy Execution	Launch Agent	Startup Items	Hidden Users						
	Source	Launch Daemon	Sudo	Hidden Window						
	Space after Filename	Launchctl	Sudo Caching	HISTCONTROL						
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Image File Execution Options Injection						
	Trap	Local Job Scheduling	Web Shell	Indicator Blocking						
	Trusted Developer Utilities	Login Item		Indicator Removal from Tools						
	User Execution	Logon Scripts		Indicator Removal on Host						
	Windows Management Instrumentation	LSASS Driver		Indirect Command Execution						
	Windows Remote Management	Modify Existing Service		Install Root Certificate						
	XSL Script Processing	Netsh Helper DLL		InstallUtil						
		New Service		Launchctl						
		Office Application Startup		LC_MAIN Hijacking						
		Path Interception		Masquerading						
		Plist Modification		Modify Registry						
		Port Knocking		Mshta						
		Port Monitors		Network Share Connection Removal						
		Rc.common		NTFS File Attributes						
		Re-opened Applications		Obfuscated Files or Information						
		Redundant Access		Plist Modification						
		Registry Run Keys / Startup Folder		Port Knocking						
		Scheduled Task		Process Doppelgänging						
		Screensaver		Process Hollowing						
		Security Support Provider		Process Injection						
		Service Registry Permissions Weakness		Redundant Access						
		Setuid and Setgid		Regsvcs/Regasm						
		Shortcut Modification		Regsvr32						
		SIP and Trust Provider Hijacking		Rootkit						
		Startup Items		Rundll32						
		System Firmware		Scripting						
		Time Providers		Signed Binary Proxy Execution						
		Trap		Signed Script Proxy Execution						
		Valid Accounts		SIP and Trust Provider Hijacking						
		Web Shell		Software Packing						
		Windows Management Instrumentation Event Subscription		Space after Filename						
		Winlogon Helper DLL		Template Injection						
				Timestomp						
				Trusted Developer Utilities						
				Valid Accounts						
				Web Service						
				XSL Script Processing						

1 Spearphishing Attachment

ID: T1193
Tactic: Initial Access
Platform: Windows, macOS, Linux

Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry.

ABOUT MITRE ATT&CK™

MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

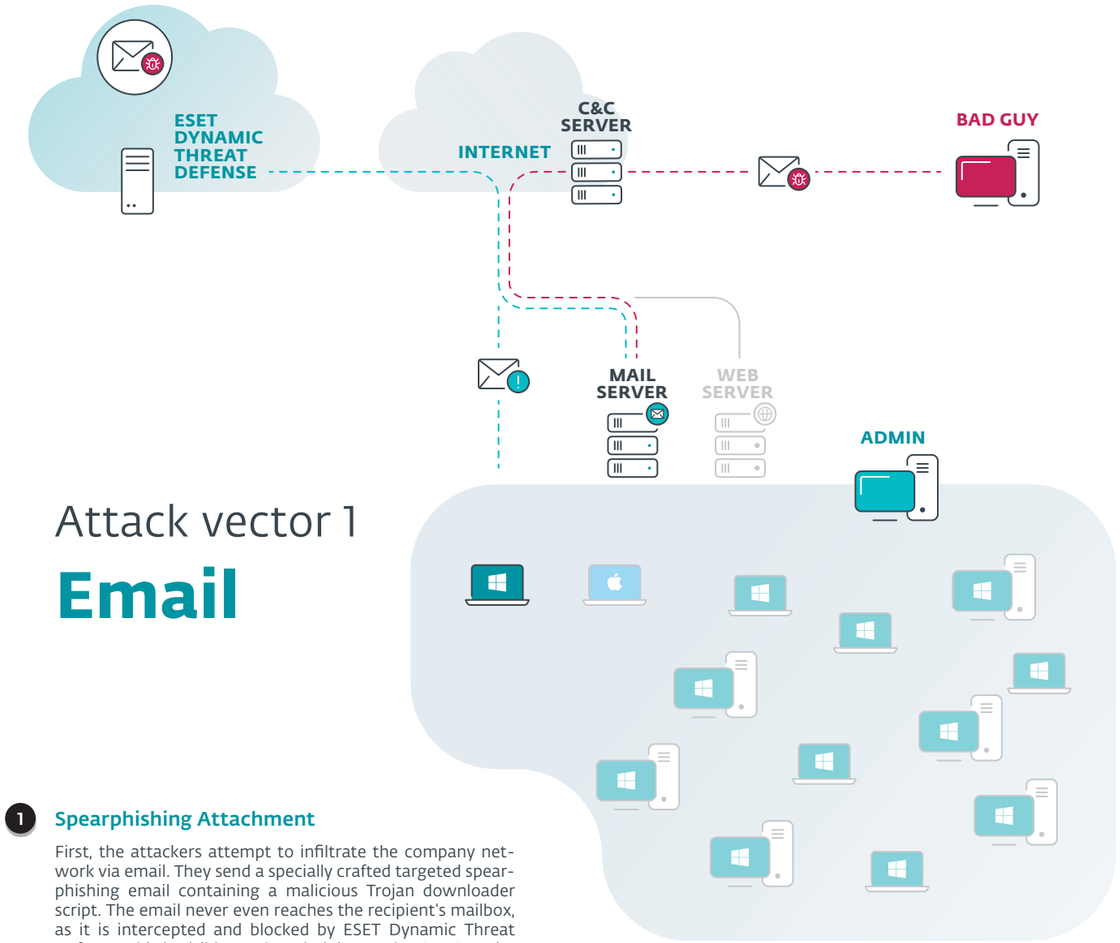
With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

Source: https://attack.mitre.org

INTRODUCTION

ESET security experts have prepared a demonstration of how ESET technologies counter an Advanced Persistent Threat (APT). In this scenario, inspired by a real case, the attackers attempt to infiltrate the target network using three different attack vectors with several stages.

This document illustrates how different layers of ESET's multi-layered security solutions would block the threat in its various stages. Tactics and techniques used in each stage of the attack are mapped to the MITRE ATT&CK knowledge base and enumerated for better orientation in the document.



Attack vector 1

Email

1 Spearphishing Attachment

First, the attackers attempt to infiltrate the company network via email. They send a specially crafted targeted spearphishing email containing a malicious Trojan downloader script. The email never even reaches the recipient's mailbox, as it is intercepted and blocked by ESET Dynamic Threat Defense. This is visible on the administrator's ESET Security Management Center console and the recipients only receive a notification email about the blocking.

MITRE | ATT&CK™

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command & Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	**Credential Dumping**	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command & Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	**Network Service Scanning**	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	**Bypass User Account Control**	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	**Exfiltration Over Command & Control Channel**	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	**Exploitation for Client Execution**	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-hop Proxy
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		**Multi-Stage Channels**
	Launchctl	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	Shared Webroot	Screen Capture		Multiband Communication
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Keychain	Remote System Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content			Port Knocking
	Mshta	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking	Network Sniffing	System Information Discovery	Third-party Software			Remote Access Tools
	PowerShell	Dylib Hijacking	Path Interception	DLL Side-Loading	Password Filter DLL	**System Network Configuration Discovery**	Windows Admin Shares			Remote File Copy
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	System Network Connections Discovery	Windows Remote Management			Standard Application Layer Protocol
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection	Securityd Memory	System Owner/User Discovery				Standard Cryptographic Protocol

2 Replication Through Removable Media

ID: T1091
Tactic: Lateral Movement, Initial Access
Platform: Windows

Adversaries may move onto systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes.

3 Exploitation for Client Execution

ID: T1203
Tactic: Execution
Platform: Linux, Windows, macOS

Vulnerabilities can exist in software due to unsecure coding practices that can lead to unanticipated behavior. Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution.

4 Multi-Stage Channels

ID: T1104
Tactic: Command & Control
Platform: Linux, macOS, Windows

Adversaries may create multiple stages for Command & Control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the Command & Control channel to make detection more difficult.

5 Bypass User Account Control

ID: T1088
Tactic: Defense Evasion, Privilege Escalation
Platform: Windows

Windows User Account Control (UAC) allows a program to elevate its privileges to perform a task under administrator-level permissions by prompting the user for confirmation. The impact for the user ranges from denying the operation under high enforcement, to allowing the user to perform the action if they are in the local administrators group and click through the prompt, or allowing them to enter an administrator password to complete the action.

6 Exfiltration Over Command & Control Channel

ID: T1041
Tactic: Exfiltration
Platform: Linux, macOS, Windows

Data exfiltration is performed over the Command & Control channel. Data is encoded into the normal communications channel using the same protocol as Command & Control communications.

7 System Network Configuration Discovery

ID: T1016
Tactic: Discovery
Platform: Linux, macOS, Windows

Adversaries will likely look for details about the network configuration and settings of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information.

8 Network Service Scanning

ID: T1046
Tactic: Discovery
Platform: Linux, Windows, macOS

Adversaries may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation. Methods to acquire this information include port scans and vulnerability scans using tools that are brought onto a system.

9 Credential Dumping

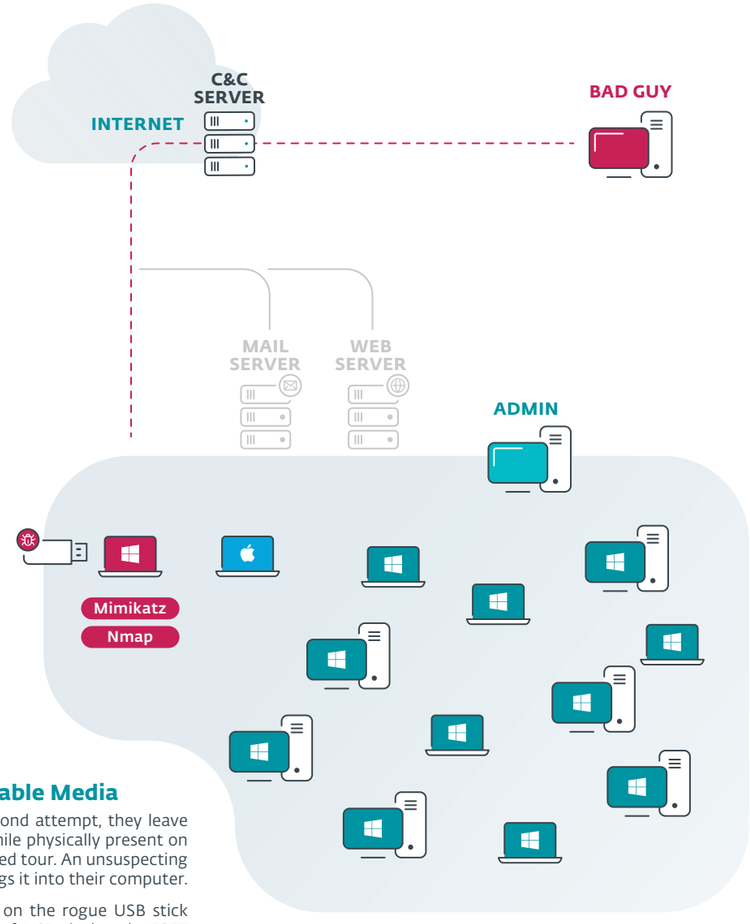
ID: T1003
Tactic: Credential Access
Platform: Windows, Linux, macOS

Credential dumping is the process of obtaining account login and password information, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information.

ESET

Attack vector 2

USB stick



2 Replication Through Removable Media

The attackers are persistent, so in a second attempt, they leave a malware-laden USB stick on a desk while physically present on the company premises during an organized tour. An unsuspecting and curious employee picks it up and plugs it into their computer.

The user is not able to access the files on the rogue USB stick because of company-wide blacklisting of USB devices in ESET Device Control.

3 Exploitation for Client Execution

If these rules were not set, the user would see that the USB stick contains a malicious document exploiting a RTF vulnerability. When the user opens it, Microsoft Word attempts to execute the malicious payload. It is, however, detected proactively by DNA detection CVE-2014-1761.

If it hadn't been detected by its DNA, it would be blocked by ESET Exploit Blocker technology.

4 Multi-Stage Channels

If it hadn't been for Exploit Blocker, the payload would attempt to download the second stage malware from the attacker's remote server. This Trojan would be caught by an ESET DNA detection.

5 Bypass User Account Control
6 Exfiltration Over Command & Control Channel

If the malware was allowed to run, it would try to elevate its privileges using a UAC bypass technique. This action, along with many others, would be visible in the ESET Enterprise Inspector console.

Afterwards, the Trojan would initiate communication with its Command & Control (C&C) server in order to download further post-exploitation tools and afterwards siphon off data from the victim network. The attempt to establish C&C network communication would be detected by ESET's Botnet Protection.

7 System Network Configuration Discovery
8 Network Service Scanning

The first tool the Trojan would try to download is nmap, in order to discover other computers in the network, and start the lateral movement stage of the attack. As nmap is not malware but a legitimate network tool, it would not trigger a DNA detection under normal circumstances. Its execution would, however, be visible in ESET Enterprise Inspector.

Using nmap, the attackers have discovered other computers of interest, including the company web server and the CEO's Macbook.

9 Credential Dumping

The second tool the Trojan attempts to download and run is the infamous mimikatz, in order to harvest administrator credentials for later use. It would be detected by a DNA detection either right away as the downloaded file was being saved to the hard drive, or just after execution by ESET's Advanced Memory Scanner (detected as Win32/SharpS).

MITRE | ATT&CK™

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command & Control
10 Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command & Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command & Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	12 Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
13 **Valid Accounts**	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	**Remote Services**	Input Capture		Multi-hop Proxy
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Launchctl	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	Shared Webroot	Screen Capture		Multiband Communication
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Keychain	Remote System Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content			Port Knocking
	Mshta	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking	Network Sniffing	System Information Discovery	Third-party Software			Remote Access Tools
	11 **PowerShell**	Dylib Hijacking	Path Interception	DLL Side-Loading	Password Filter DLL	System Network Configuration Discovery	14 **Windows Admin Shares**			Remote File Copy
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	System Network Connections Discovery	Windows Remote Management			Standard Application Layer Protocol
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection	Securityd Memory	System Owner/User Discovery				Standard Cryptographic Protocol
	Rundll32	Hidden Files and Directories	Process Injection	File Deletion	Two-Factor Authentication Interception	System Service Discovery				Standard Non-Application Layer Protocol
	Scheduled Task	Hooking	Scheduled Task	File Permissions Modification		System Time Discovery				Uncommonly Used Port
	Scripting	Hypervisor	Service Registry Permissions Weakness	File System Logical Offsets						Web Service
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	Gatekeeper Bypass						
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	Hidden Files and Directories						
	Signed Script Proxy Execution	Launch Agent	Startup Items	Hidden Users						
	Source	Launch Daemon	Sudo	Hidden Window						
	Space after Filename	Launchctl	Sudo Caching	HISTCONTROL						
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Image File Execution Options Injection						
	Trap	Local Job Scheduling	Web Shell	Indicator Blocking						
	Trusted Developer Utilities	Login Item		Indicator Removal from Tools						
	User Execution	Logon Scripts		Indicator Removal on Host						
	Windows Management Instrumentation	LSASS Driver		Indirect Command Execution						
	Windows Remote Management	Modify Existing Service		Install Root Certificate						
	XSL Script Processing	Netsh Helper DLL		InstallUtil						
		New Service		Launchctl						
		Office Application Startup		LC_MAIN Hijacking						

10 Exploit Public-Facing Application

ID: T1190
Tactic: Initial Access
Platform: Linux, Windows, macOS

The use of software, data, or commands to take advantage of a weakness in an internet-facing computer system or program in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability.

11 PowerShell

ID: T1086
Tactic: Execution
Platform: Windows

PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code.

12 Remote Services

ID: T1021
Tactic: Lateral Movement
Platform: Linux, macOS, Windows

An adversary may use valid accounts to log into a service specifically designed to accept remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user.

13 Valid Accounts

ID: T1078
Tactic: Defense Evasion, Persistence, Privilege Escalation, Initial Access
Platform: Linux, macOS, Windows

Adversaries may steal the credentials of a specific user or service account using credential access techniques or capture credentials earlier in their reconnaissance process through social engineering for means of gaining initial access.

14 Windows Admin Shares

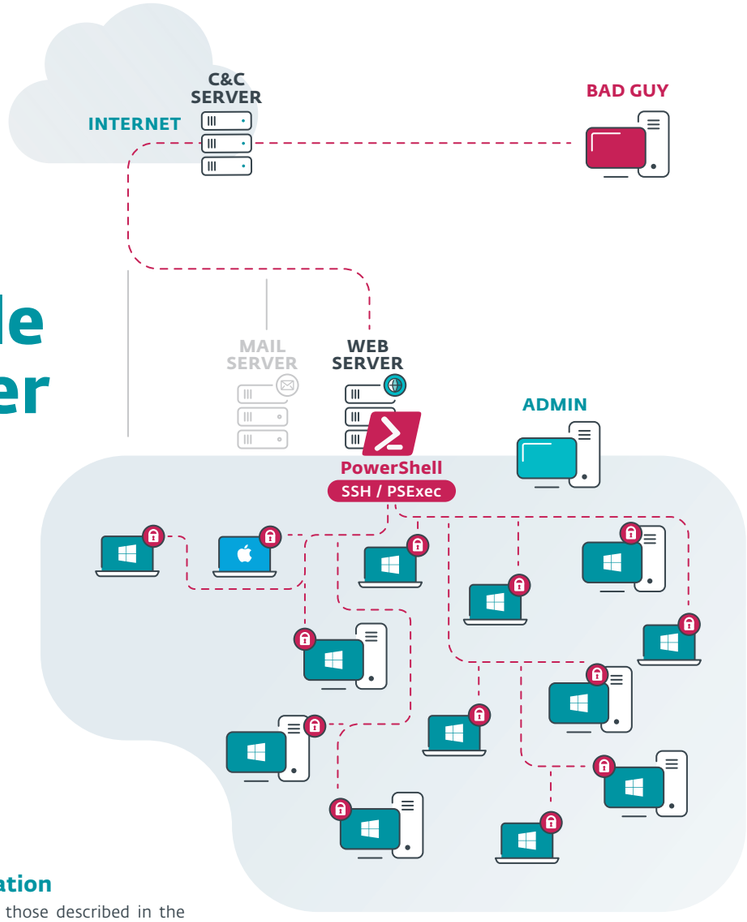
ID: T1077
Tactic: Lateral Movement
Platform: Windows

Windows systems have hidden network shares that are accessible only to administrators and provide the ability for remote file copy and other administrative functions. Examples of network shares include C$, ADMIN$, and IPC$.

ESET

Attack vector 3

Vulnerable web server



10 Exploit Public-Facing Application

Even when ESET technologies (such as those described in the previous steps) detect and prevent attacks and malware infections, oftentimes during targeted APT attacks, the attackers make multiple attempts to compromise their target.

In this scenario, the attacker attempts to regain access to the company network using the previously discovered vulnerability on the web server.

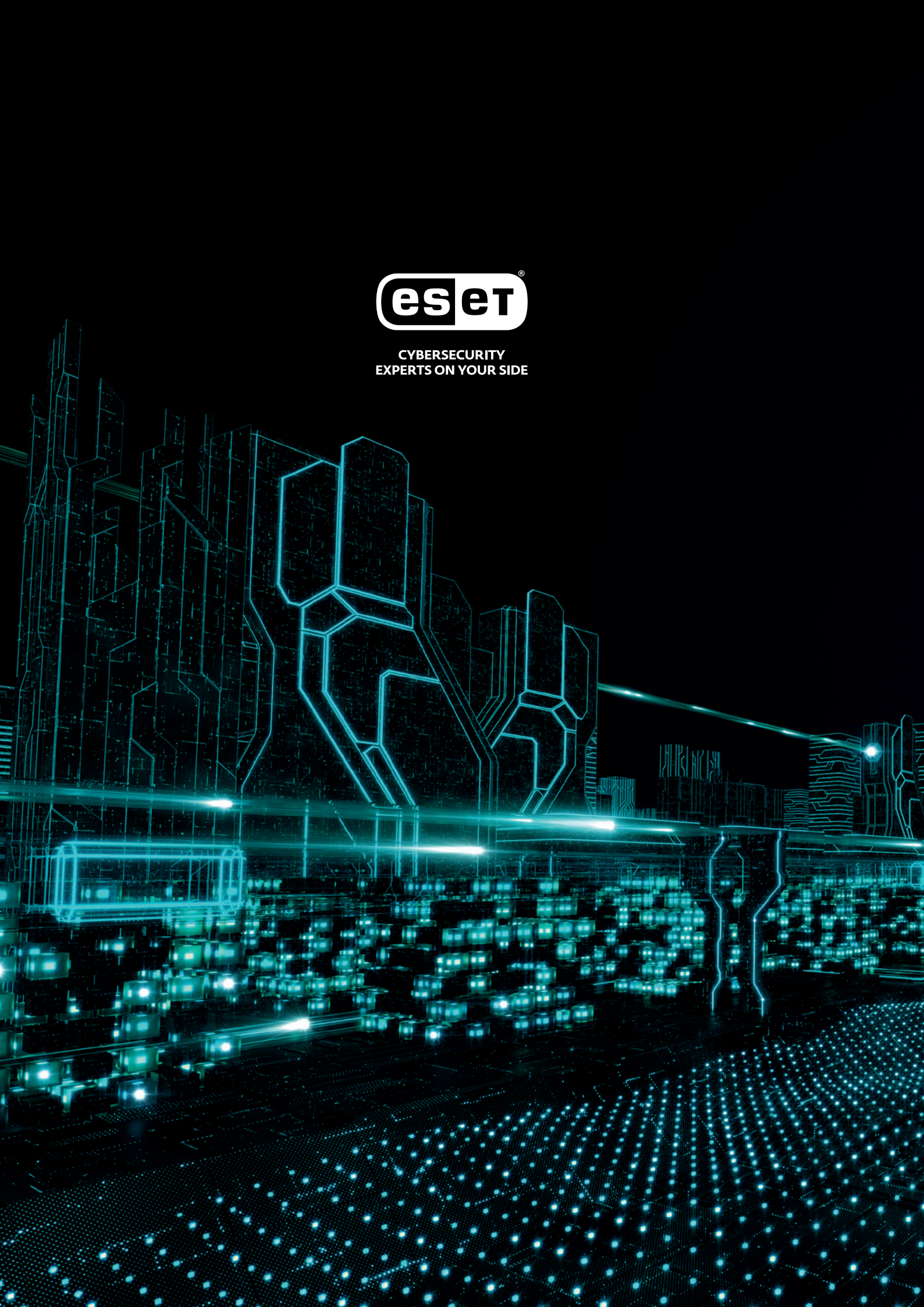
11 PowerShell
12 Remote Services
13 Valid Accounts

If the attack had gone through, a malicious fileless PowerShell script would have been executed by the server's PHP interpreter. This (along with all other actions) would, of course, be visible in ESET Enterprise Inspector.

The functionality of the malicious script is to launch malware on other computers in the company network. First, it would try to install macOS ransomware on the discovered MacBook through SSH (using stolen credentials). This is blocked on the MacBook using a DNA detection.

13 Valid Accounts
14 Windows Admin Shares

Finally, the script attempts to execute ransomware on other Windows computers in the network using PSExec and stolen credentials. Not only would this be detected by ESET Enterprise Inspector, but also by a DNA detection on the individual endpoints or the specialized Ransomware Shield technology.


CYBERSECURITY
EXPERTS ON YOUR SIDE