



# Laying a Minefield for Attackers

Rob Collins  
Director of Sales Engineering - APAC

# Agenda

- Attack lifecycle and MITRE ATT&CK Framework
- CylancePROTECT strategies
- CylanceOPTICS strategies
- Bringing it all together to lay the minefield – live demo
- Q&A

## Notes:

- This will be recorded
- The slides will be made available
- The webinar is eligible for 1 CPE credit in the (ISC)2 Program



# Safe Harbor

---

The information in this presentation is confidential and proprietary to Cylance® and may not be disclosed without the permission of Cylance. This presentation is not subject to your license agreement or any other service or subscription agreement with Cylance. Cylance has no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein.

This document, or any related presentation and Cylance's strategy and possible future development, product, and/or platform direction and functionality are all subject to change and may be changed by Cylance at any time for any reason without notice. The information on this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. This document is for informational purposes and may not be incorporated into a contract. Cylance assumes no responsibility for errors or omissions in this document.

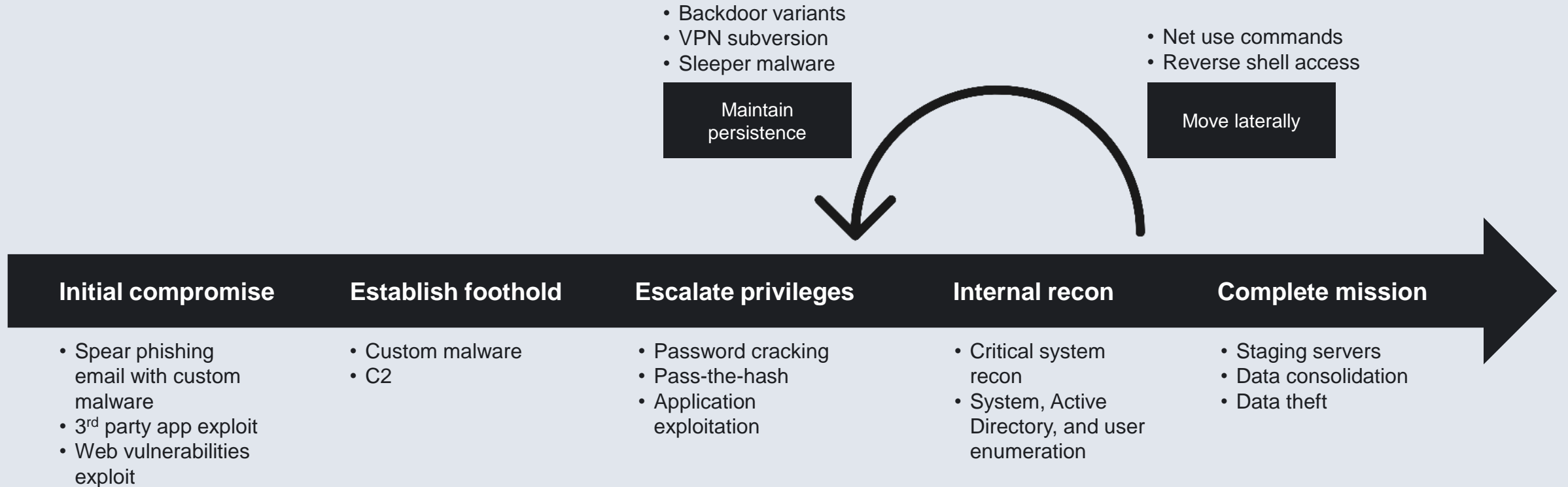
---

**“Perfect is the enemy of good”**

---

-Voltaire

# Attack Lifecycle



## ATT&amp;CK Matrix for Enterprise

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



	1	2	1	1						1	1	2	1	2	1	2	1			1	1	1			1	1	2	1
	1	1	3	2	1	1	1	2	1	2	1	2	1	2	1			1	2	3	3	2	2	1	3	3	4	1
	1	1	2	2	2	2	2	2	2	1	2	1	2	2	2	1		1	1	1	1	2	2	2	2	1	3	
		1	2	2	2	3	3	1	1				1	1			1	2	2	2	2	3	2	2	3	1	3	
		2	3	2	2	1	1	1	1				2	3	4	2	1		1	1	1	1		1	2	1		
		2	1	2	2	1	1	1	1			1	3	1	1	2		1	1	2	2	3	2	1	1	2	2	
		1	2	3	3	3	2	2	1	1			1	1	5	2			1	2	2	2	1	2	2	1		
1	1	1	1	2	2	1	1	2					1	2	2	2	1	2	2	3	2	2	1	2	2	2	2	
1	1	2	2	1	2	4	3	1	1				1	1	1	1	3	1	1	2		1	3	3	2	1	1	
2	2	3	2			1	1	3	2				1	1	1	1	1	1	8	4	1	1	1	1	1	1	1	
1	1	2	2	2	1			3	3	1	1	2	1	1	1	3	1	1	1	1	1	1	2	2	2	1	1	
2	2	1	2	3	1			2	3	3	2	1	2	2	2	3	1	1	5	2	1	1	1	1	1	2		
1	1		2	1	2	2	2	2	2	3	2	1	1	1	2	2	4	1	1	1	1	1	1	1	2	1		
1	1		1	2	2	3	1	1	2	2	4	3	4	3	4	3	4	3	3	3	2	1	1	1	1	2	2	
						2	3	1	1	3	1	1	1	2	5	4	2	1			1	3	1	2				
						1	1	1		1	1	3	4	2	2	2	1	1	3	2	1			1	1	1	2	

# Attack 101



Denial of Service



# CylancePROTECT

## Malware: Auto Quarantine

[Device Policy](#) > Edit Policy Details

### Edit Policy Details

Policy Name: Default

File Actions	Memory Actions	Protection Settings	CylanceOPTICS Settings	Application Control	Agent Settings	Script Control	Device Control
File Type	Unsafe					Abnormal	
		Auto Quarantine with Execution Control				Auto Quarantine with Execution Control	
EXECUTABLE		<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>	

# CylancePROTECT

## Exploits: Memory Protection

File Actions

Memory Actions

Protection Settings

CylanceOPTICS Settings

Application Control

Agent Settings

Script Control

Device Control

Data Privacy

☒ Memory Protection

☒ Exclude Executable Files (relative paths only)

\Windows\System32\WerFault.exe

\Windows\SysWOW64\WerFault.exe

\Windows\System32\sdclt.exe

+ -

+ -

+ -

VIOLATION TYPE	IGNORE	ALERT	BLOCK	TERMINATE
▶ Exploitation	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Stack Pivot	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Stack Protect	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Overwrite Code	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
RAM Scraping	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Malicious Payload	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
▶ Process Injection	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Remote Allocation of Memory	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Remote Mapping of Memory	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Remote Write to Memory	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Remote Write PE to Memory	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Remote Overwrite Code	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Remote Unmap of Memory	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Remote Thread Creation	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Remote APC Scheduled	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
DYLD Injection (macOS and Linux only)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
▶ Escalation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
LSASS Read	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Zero Allocate	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

# CylancePROTECT

## Scripts: Script Control

**Script Control**  
Script Control protects users from malicious scripts running on their devices. Available for **Agent Version 1310** and higher.

☒ Script Control

Agent Version	Active Script <sup>①</sup>	Powershell <sup>①</sup>	Macros <sup>①</sup>
1370 and below	Alert		Not Applicable
1380 and above	Block	Block	Block

☒ Block Powershell console usage<sup>①</sup>  
Available for **Agent Version 1390** and higher.

**Disable Script Control**  
Available for **Agent Version 1430** and higher. Older Agent versions will default to "Alert" if disabled.





















**Disabled** ☐ Active Script ☐ Powershell ☐ Macros

**Folder Exclusions (includes subfolders)<sup>①</sup>**  
Specify a relative path to allow application changes and additions to the below folders while Script Control is enabled.

\\windows\\ccm\\	+ -
\\sysvol\\	+ -
\\netlogon\\	+ -
\\program files\\citrix\\sma\\	+ -
\\scripts\\	+ -















# CylanceOPTICS

## Scripts: Script Intent

SEVERITY		RULE
	High	 jRATscriptlaunch
	High	 Rundll Javascript Invocation
	High	 Fileless Powershell Malware
	High	 Java MSF Payload
	Medium	 Powershell Download
	Medium	 Hidden Powershell Execution
	Medium	 Powershell Encoded Command
	Medium	 Non RFC1918 Connection by script
	Low	 One-Liner ML Module
	High	 Office DDE to Script Interpreter (MITRE)







































# CylanceOPTICS

## Identity: Obtain Credentials

SEVERITY		RULE
	Medium	 Account Discovery (MITRE)
	Low	 Account Discovery macOS (MITRE)
	Low	 Network Share Discovery - Windows (MITRE)
	Low	 Credentials in Registry (MITRE)
	Low	 Credential Dumping (MITRE)
	Low	 Account Discovery - Windows (MITRE)
	Low	 Kerberoast (MITRE)

# CylanceOPTICS

## Admin Tools

SEVERITY	RULE
 Medium	 System Commands hostname, whoami, find, xcopy, nslookup, reg query, net use, net file
 Medium	 AutoIt
 Medium	 AutoIt suspicious filepath
 Info	 PSEXec Usage
 Medium	 BitsAdmin Transfer Execution (MITRE)
 Medium	 RegSvcS RegAsm Bypass (MITRE)
 Medium	 RegSvr32 Remote Install (MITRE)
 Low	 BITS Jobs (MITRE)
 Low	 Control Panel Items (MITRE)
 Low	 Screensaver (MITRE)
 Low	 InstallUtil (MITRE)
 Low	 System Service Discovery (MITRE)
 Low	 System Network Connections Discovery (MITRE)
 Low	 WMIC Reconnaissance (MITRE)
 Low	 Port Monitoring (MITRE)
 Low	 Network Share Connection Removal (MITRE)
 Low	 Modify Service (MITRE)
 Low	 Windows Remote Management (MITRE)
 Low	 System Time Discovery (MITRE)
Low	Scheduled Task Persistence (MITRE)
Info	Create Account (MITRE)

# Demo

# Questions

— + —

# Answers