AusCERT 2019

Flipping the Cyberdefense Equation to Tip the Scales Back in Our Favor

Rick McElroy – Principal Security Strategist
@infosecrick

Carbon Black.

Key Takeaways

1

The Modern Threatscape

2

The Defender's Advantages

3

Tipping the Scales

Threatscape

The new APT, dubbed White Company, is likely Middle Eastern, but shows fingerprints of U.S.-trained personnel.

'Darkhotel' hack targets executives using hotel Internet

Using hotel Wi-Fi networks, the hackers are able to infect corporate executives' computers with malicious software, according to security research firm Kaspersky Lab.

A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.

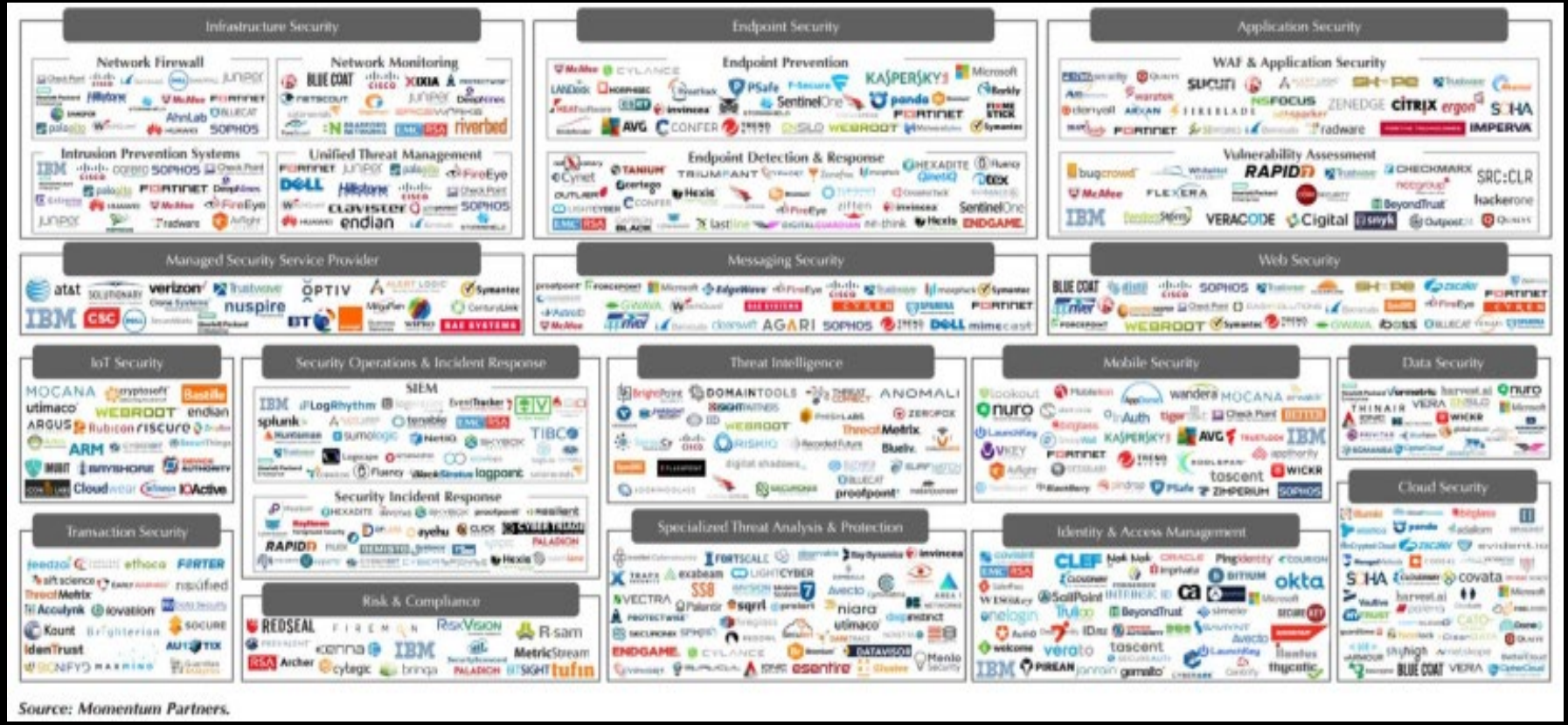
Carbon Black.

Constantly Evolving Environment

Carbon Black.

Time is not on our side

Complexity..Complexity…Complexity



Carbon Black.

Home Field Advantage

Carbon Black.

Home Field Advantage

Carbon Black.

Prevent what you can

Carbon Black.

Detect and respond where you can't

Carbon Black.

The attackers are going to look just like insider's

Carbon Black.

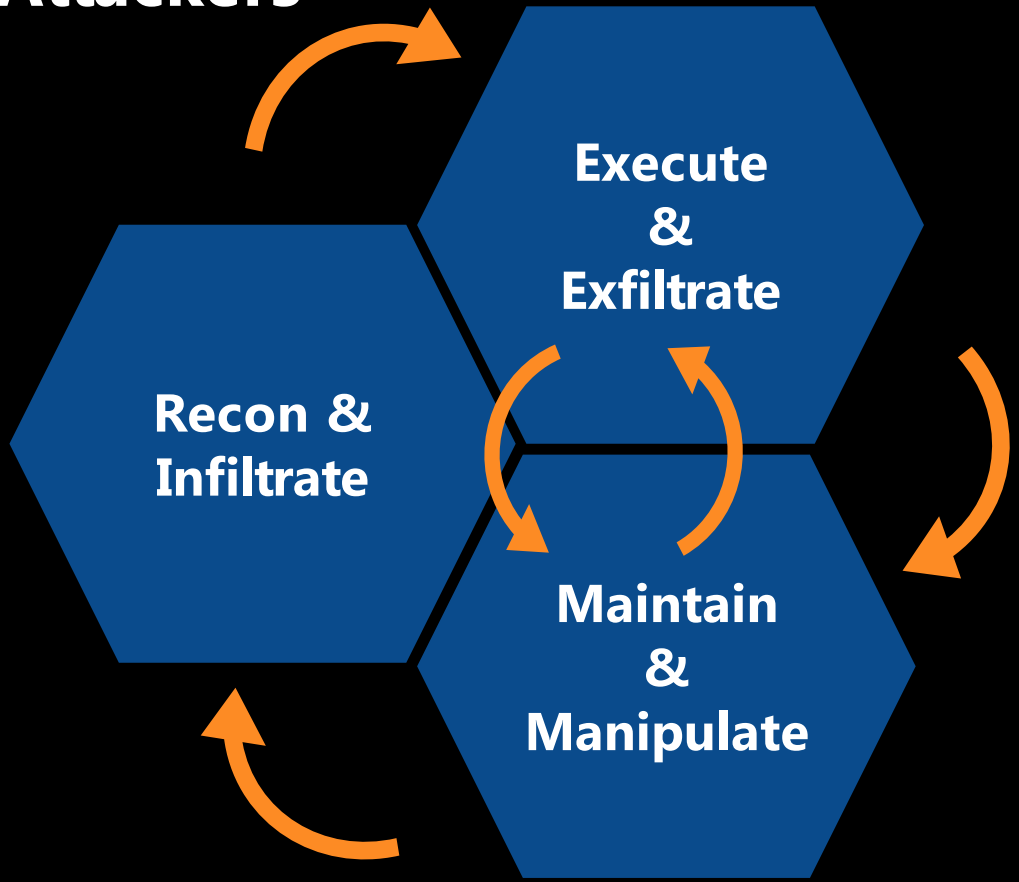
Kill Chains

Lockheed Martin KillChain 2011

MITRE ATT&CK 2018

Carbon Black.

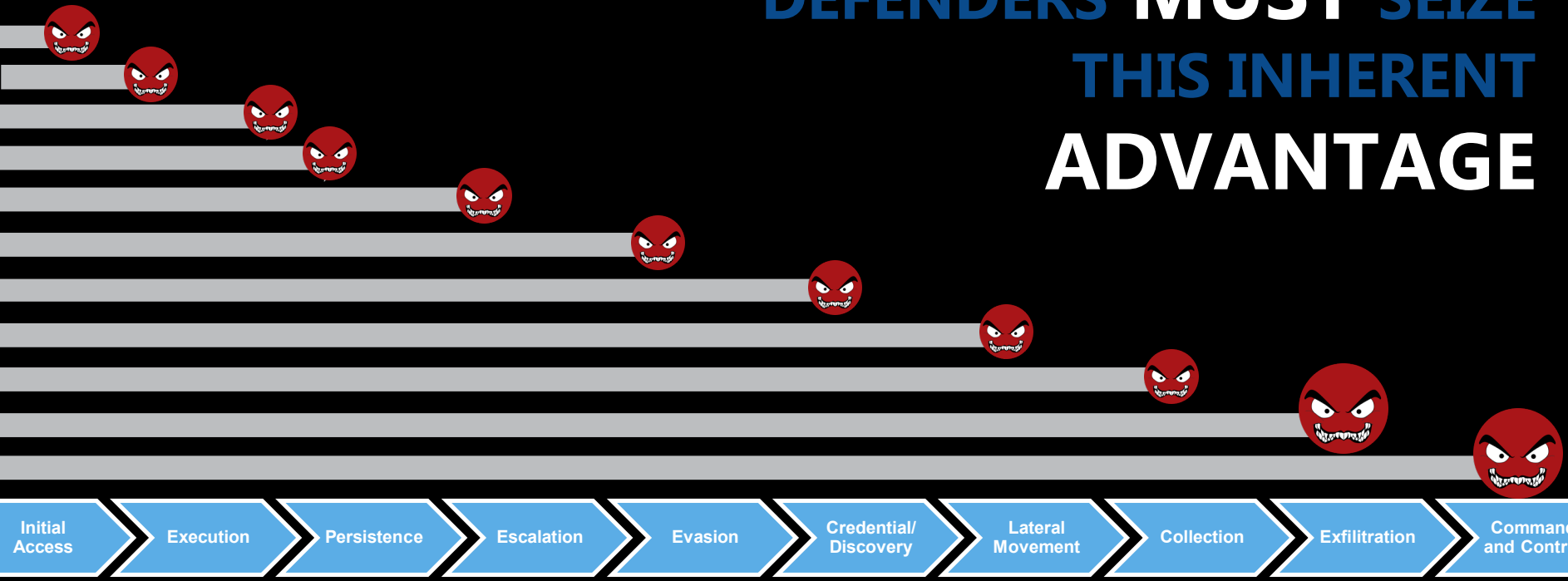
Cognitions of Attackers



Carbon Black.

Just One Mitigation Breaks the Chain

DEFENDERS MUST SEIZE THIS INHERENT ADVANTAGE



MITRE ATT&CK

Carbon Black.

Widows Disruption in Depth

Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Compiled HTML File	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Password Policy Discovery	Remote File Copy	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Kerberoasting	Permission Groups Discovery	Replication Through Removable Media	Input Capture		Multi-hop Proxy
	LSASS Driver	Component Firmware	Hooking	DCShadow	LLMNR/NBT-NS Poisoning	Process Discovery	Shared Webroot	Man in the Browser		Multi-Stage Channels

Initial Access → Execution → Persistence → Escalation → Evasion → Credential/ Discovery → Lateral Movement → Collection → Exfilitration → Command and Control

MITRE ATT&CK

Carbon Black.

You only get one shot?

In this scenario, we didn't have a red flag from the common phishing attachment (MS Office maldoc) where the chain of execution goes `Outlook -> Word -> CMD -> PowerShell`. Thank you, ISO! But we still have multiple ways to raise the activity, and can easily map these to MITRE ATT&CK Techniques if we're so inclined:

- Outlook writing ISO file to disk: T1193 and T1027 (Spearphishing Attachment and Obfuscated Files or Information)
- RegAsm creating an external network connection: T1121 (Regsvcs/Regasm)
- Creation of a scheduled task by an untrusted/unknown binary (in this case, malware):T1053 (Scheduled Task)
- Creation of a scheduled task in an unusual location (in this case, the user profile): T1053

Tipping the Scales

 | |

You only have to be one step faster

 |

Carbon Black.

Carbon Black.

Frustrate Attackers

Carbon Black.

Disrupting the Economy

Carbon Black.

Carbon Black.

Carbon Black.

www.CarbonBlack.com