



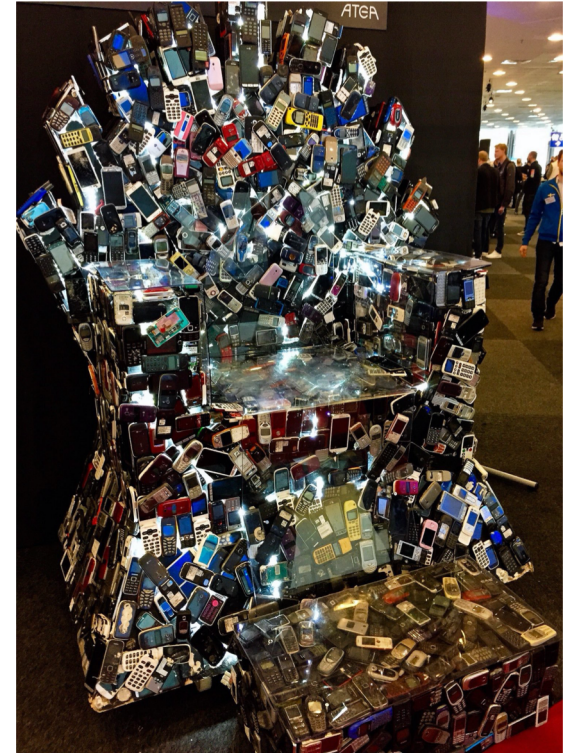
Prioritizing ATT&CK Informed Defenses

The CIS Way

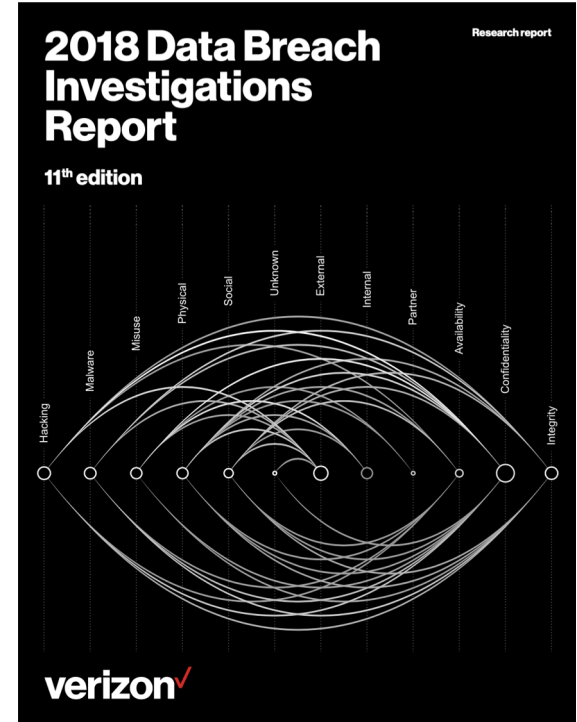
Philippe Langlois
Senior Risk Analyst
Verizon DBIR

Joshua M Franklin
Senior Cybersecurity Engineer
Center for Internet Security

- Product owner of CIS Controls v7.1
- 10 years in the US government
 - NIST
 - Election Assistance Commission
- Telecommunications security, mobile security, mobile app vetting
 - Contributor to Mobile ATT&CK
- Election security
- Cybersecurity standards (e.g., NIST, CIS, IEEE, OASIS, 3GPP)



- Current:
 - Verizon DBIR Co-Author
- Former
 - Product Owner @ CIS
 - CIS Controls
 - Nationwide Cyber Security Review
 - Integrated Product Team Lead
- Focus on risk management and cyber security
- Can maybe code himself out of a paper bag



Defender's Dilemma

- What's the right thing to do, and how much do I need to do?
- How do I actually do it?
- And how can I demonstrate to others that I have done the right thing?

- US-based forward-thinking, non-profit entity that harnesses the power of a global IT community
- Goal of safeguarding private and public organizations against cyber threats
- CIS Vision: Leading the global community to secure our connected world
- CIS Mission:
 - Identify, develop, validate, promote, and sustain best practice solutions for cyber defense
 - Build and lead communities to enable an environment of trust in cyberspace



Multi-State Information Sharing and Analysis Center



The MS-ISAC has been designated by DHS as the key resource for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal, and territorial governments

<https://www.cisecurity.org/ms-isac/>

TLP: WHITE

Security Best Practices

- CIS Benchmarks
 - Community developed security configuration guidance
 - Covers major applications and OS
 - Recognized by FISMA, FedRAMP, and PCI
 - Freely available in PDF Format
- CIS Controls
 - Internationally utilized standard
 - Making best practice, common practice

140+ benchmarks available

- RHEL 8,
- Microsoft Windows Server 2019, Kubernetes,
- Cloud Foundations for AWS,
- Azure,
- GCP,
- Ubuntu,
- CentOS



NSA/DoD Project

The Consensus Audit Guidelines (CSIS)

“The SANS Top 20” (the SANS Institute)

The Critical Security Controls (CCS/CIS)





V7.1

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

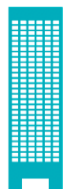
- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises



Implementation Groups



Implementation Group 3

A mature organization with significant resources and cybersecurity experience to allocate to Sub-Controls



Implementation Group 2

An organization with moderate resources and cybersecurity expertise to implement Sub-Controls



Implementation Group 1

An organization with limited resources and cybersecurity expertise available to implement Sub-Controls

Definitions

Implementation Group 1

CIS Sub-Controls for small, commercial off-the-shelf or home office software environments where sensitivity of the data is low will typically fall under IG1. Remember, any IG1 steps should also be followed by organizations in IG2 and IG3.

Implementation Group 2

CIS Sub-Controls focused on helping security teams manage sensitive client or company information fall under IG2. IG2 steps should also be followed by organizations in IG3.

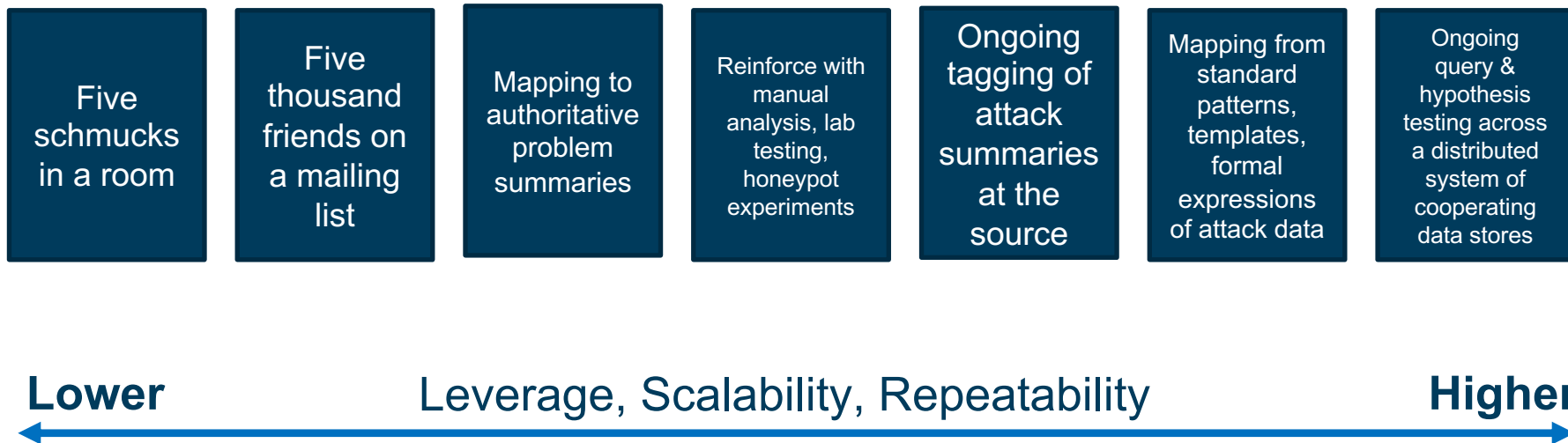
Implementation Group 3

CIS Sub-Controls that reduce the impact of zero-day attacks and targeted attacks from sophisticated adversaries typically fall into IG3. IG1 and IG2 organizations may be unable to implement all IG3 Sub-Controls.

	1	2	3
Implementation Group 1	●		
Implementation Group 2	●	●	
Implementation Group 3	●	●	●

CIS defines Implementation Group 1 as Basic Cyber Hygiene

Evolving the CIS Controls Selection Process





“Pre” ATT&CK

Community Attack Model v1.0

- CIS effort to analyze pertinent information relating to real-world attacks in the wild
- **Goal:** help enterprises make good choices about the most effective defensive actions they can take
- Released via Blackhat in 2016
- Leverages additional frameworks such as NIST CSF and Lockheed Martin Cyber Kill Chain

Why a Community Attack Model?

- Ensure offense informs defense
- Able to better prioritize defensive controls based on real-world techniques
- Communicate trade-offs
 - What techniques are likely to be successful if I don't put a control in place?
- Most enterprises can't go on their own
 - Or do it more than once



		Attack Stages								
	CIS Controls (V6.0)	Initial Recon	Acquire/Develop Tools	Delivery	Initial Compromise	Misuse/Escalate Privilege	Internal Recon	Lateral Movement	Establish Persistence	Execute Mission Objectives
	Identify		CSC 4		CSC 1, 2	CSC 5				
	Protect	CSC 7, 9		CSC 7	CSC 3, 7, 8, 11, 15, 18	CSC 5, 14, 16	CSC 5	CSC 3, 5, 8, 14	CSC 8	CSC 13
	Detect			CSC 17	CSC 4, 6, 8	CSC 16, 17	CSC 6	CSC 4, 8, 16	CSC 8	
	Respond				CSC 4	CSC 6		CSC 4, 6		CSC 19
	Recover									CSC 10

- Verizon Data Breach Investigations Report
- FireEye M-Trends Report
- ESET Cybersecurity Trends
- Symantec Internet Security Threat Report
- Arbor Networks Worldwide Security Report
- IBM X-Force Threat Intelligence Index
- Microsoft Security Intelligence Report
- Akamai [State of the internet]
- ...

Before
READ ALL THE
THINGS!



After



- If you want data, it's available
- But...
 - Reviewing is time intensive
 - Inconsistent language
 - Vendor biases
 - Sometimes Marketing focused
 - Often difficult to get underlying data and check their work

More concisely:

1. *How do we compare reports?*
2. *How can we use them?*



50ccs of ATT&CK

Towards Standardization

- We can engineer a solution to some of these problems
 - Specifically, the use of standard language
- MITRE ATT&CK can be used as a *lingua franca*
- Mitigations were added as an object (huzzah!)
- Working to map the CIS Controls to MITRE ATT&CK

Controls to Mitigations to Techniques v0.1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	33 items	59 items	28 items	67 items	19 items	22 items	17 items	13 items	22 items	9 items	14 items
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	Binary Padding	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	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppCert DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Inhibit System Recovery	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Alternative Protocol	Endpoint Denial of Service
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 Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Network Denial of Service
Spearphishing via Service	Execution through Module Load	BITS Jobs	Compiled HTML File	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting Algorithms	Exfiltration Over Physical Medium	Resource Hijacking
Supply Chain Compromise	Graphical User Interface	Bootkit	DLL Search Order Hijacking	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Fallback Channels	Scheduled Transfer	Runtime Data Manipulation
Trusted Relationship	InstallUtil	Change Default File Association	Dylib Hijacking	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy	Multi-Stage Channels	Service Stop
Valid Accounts	Launchctl	Component Firmware	Exploitation for Privilege Escalation	Control Panel Items	Kerberoasting	Process Discovery	Replication Through Removable Media	Screen Capture	Multiband Communication	Multilayer Encryption	Stored Data Manipulation
	Local Job Scheduling	Component Object Model Hijacking	Extra Window Memory Injection	DCShadow	Keychain	Query Registry	Shared Webroot	Video Capture	Port Knocking	Remote Access Tools	Transmitted Data Manipulation
	LSASS Driver	Create Account	File System Permissions Weakness	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	SSH Hijacking				
	Mshta	DLL Search Order Hijacking	Hooking	Disabling Security Tools	Network Sniffing	System Information Discovery	Taint Shared Content				
	PowerShell	DLL Search Order Hijacking	Image File Execution Options Injection	DLL Search Order Hijacking	Password Filter DLL	System Network Configuration Discovery	Third-party Software				
	Regsvcs/Regasm	Dylib Hijacking	Launch Daemon	DLL Side-Loading	Private Keys	System Network Connections Discovery	Windows Admin Shares				
	Regsvr32	External Remote Services	Launch Daemon	Execution Guardrails	Securityd Memory	System Owner/User Discovery	Windows Remote Management				
	Rundll32	File System Permissions Weakness	New Service	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Service Discovery					
	Scheduled Task	Path Interception	Path Interception	Extra Window Memory Injection		System Time Discovery					
	Scripting	Hidden Files and Directories	Plist Modification	File Deletion		Virtualization/Sandbox Evasion					
	Service Execution	Hooking	Port Monitors	File Permissions Modification							
	Signed Binary Proxy Execution	Hypervisor	Process Injection	File System Logical Offsets							
	Signed Script Proxy Execution	Image File Execution Options Injection	Scheduled Task	Gatekeeper Bypass							
	Source	Kernel Modules and Extensions	Service Registry Permissions Weakness	Group Policy Modification							
	Space after Filename	Launch Agent	Setuid and Setgid	Hidden Files and Directories							
	Third-party Software	Launch Daemon	SID-History Injection	Hidden Users							
	Trap	Launch Daemon	HISTCONTROL	Hidden Window							
	Trusted Developer Utilities	Launchctl	Sudo	Image File Execution Options Injection							
	Unsafe Execution	LC_LOAD_DYLIB									

#31a354

Control 1: Inventory of Hard

✕

#3182bd

Control 2: Inventory of Softw

✕

#fc3b3b

Control 3: Vulnerability Mani

✕

#fce93b

Control 4: Control of Admin

✕

#756bb1

Control 5: Secure Configura

✕

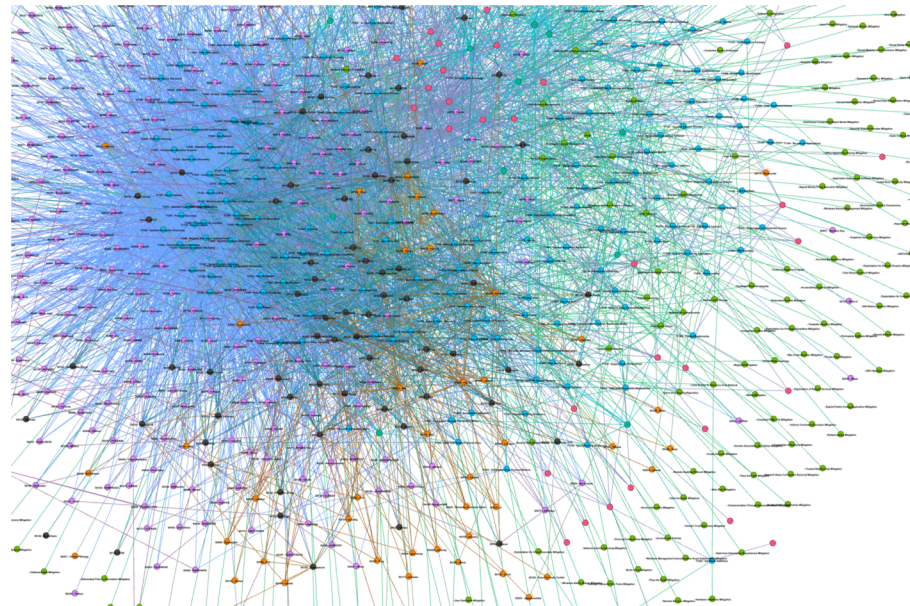
Add Item

Clear

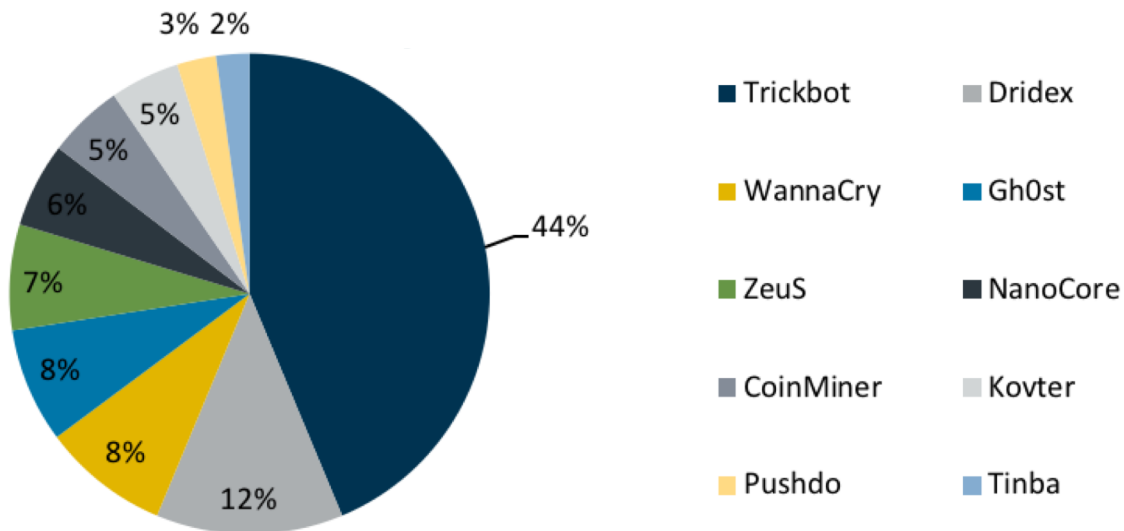
Community Attack Model v2

- Revamp of the Model
- Tie to a standard method of expression
- General methodology:
 - Analyze data sources
 - Identify key attack paths
 - Identify mitigations for key attacks
 - Map mitigations to CIS Controls
- Output:
 - Mapping of the CIS Controls to MITRE ATT&CK
 - Mapping of the CIS Controls to MITRE ATT&CK Mitigations
 - Data-backed attack patterns that the CIS Controls defend against

- ...let's make a network
 - What are central points for Adversaries
 - What are the central points for Software
- Caveats
 - This just tells us what is commonly found in ATT&CK, NOT what is found out there in the wild
 - Focused largely on APT



- MS-ISAC + EI-ISAC to the rescue
- 100+ network sensors,
- 100+ forensic reports a year



Top 6 Malware Techniques to Controls

Combined	Trickbot	Zeus	Dridex	Gh0st	NanoCore	WannaCry	+	selection controls	layer controls	technique controls	
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	33 items	59 items	28 items	67 items	19 items	22 items	17 items	13 items	22 items	9 items	14 items
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	Accessability Features	Accessability Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
	Command-Line Interface	Account Manipulation	AppCert DLLs	Bypass User Account Control	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	Clear Command History	Credential Dumping	Domain Trust Discovery	Data from Information Repositories	Custom Command and Control Protocol		Data Transfer Size Limits	Disk Content Wipe
Hardware Additions	Control Panel Items	Appinit DLLs	Appinit DLLs	CMSTP	Credentials in Files	File and Directory Discovery	Exploitation of Remote Services	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	Application Shimming	Code Signing	Credentials in Registry	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Attachment	Execution through API	Authentication Package	Bypass User Account Control	Compile After Delivery	Exploitation for Credential Access	Network Share Discovery	Pass the Hash	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Spearphishing Link	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Compiled HTML File	Forced Authentication	Network Sniffing	Pass the Ticket	Data from Removable Media	Domain Generation Algorithms	Exfiltration Over Scheduled Transfer	Inhibit System Recovery
Spearphishing via Service	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Domain Generation Algorithms	Exfiltration Over Physical Medium	Network Denial of Service
Supply Chain Compromise	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Control Panel Items	Input Capture	Process Discovery	Remote File Copy	Email Collection	Fallback Channels	Exfiltration Over Physical Medium	Resource Hijacking
Trusted Relationship	InstallUtil	Component Firmware	Extra Window Memory Injection	DCShadow	Input Prompt	Query Registry	Remote Services	Input Capture	Fallback Channels	Exfiltration Over Physical Medium	Resource Hijacking
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Deobfuscate/Decode Files or Information	Kerberoasting	Remote System Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy	Scheduled Transfer	Runtime Data Manipulation
Valid Accounts	Local Job Scheduling	Create Account	Hooking	Disabling Security Tools	Keychain	Security Software Discovery	System Information Discovery	Screen Capture	Multi-Stage Channels		Service Stop
	LSASS Driver	DLL Search Order Hijacking	Hooking	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	System Information Discovery	Shared Webroot	Video Capture	Multi-Stage Channels		Service Stop
	Mshta	DLL Search Order Hijacking	Hooking	DLL Side-Loading	Network Sniffing	System Network Configuration Discovery	SSH Hijacking	Video Capture	Multi-Stage Channels		Service Stop
	PowerShell	Dylib Hijacking	Image File Execution Options Injection	Execution Guardrails	Password Filter DLL	System Network Connections Discovery	Taint Shared Content	Video Capture	Multi-Stage Channels		Service Stop
	Regsvcs/Regasm	External Remote Services	Launch Daemon	Exploitation for Defense Evasion	Private Keys	System Network Connections Discovery	Third-party Software	Video Capture	Multi-Stage Channels		Service Stop
	Regsvr32	File System Permissions Weakness	New Service	Extra Window Memory Injection	Securityd Memory	System Owner/User Discovery	Windows Admin Shares	Video Capture	Multi-Stage Channels		Service Stop
	Rundll32	Path Interception	Path Interception	File Deletion	Two-Factor Authentication Interception	System Service Discovery	Windows Remote Management	Video Capture	Multi-Stage Channels		Service Stop
	Scheduled Task	Plist Modification	Plist Modification	File Permissions Modification		System Time Discovery	Windows Remote Management	Video Capture	Multi-Stage Channels		Service Stop
	Scripting	Port Monitors	Port Monitors	File System Logical Offsets		Virtualization/Sandbox Evasion		Video Capture	Multi-Stage Channels		Service Stop
	Service Execution	Hooking	Hooking	Gatekeeper Bypass				Video Capture	Multi-Stage Channels		Service Stop
	Signed Binary Proxy Execution	Hypervisor	Hypervisor	Group Policy Modification				Video Capture	Multi-Stage Channels		Service Stop
	Signed Script Proxy Execution	Image File Execution Options Injection	Image File Execution Options Injection	Hidden Files and Directories				Video Capture	Multi-Stage Channels		Service Stop
	Source	Kernel Modules and Extensions	Service Registry Permissions Weakness	Hidden Users				Video Capture	Multi-Stage Channels		Service Stop
	Space after Filename	Launch Agent	Setuid and Setgid	Hidden Window				Video Capture	Multi-Stage Channels		Service Stop
	Third-party Software	Launch Daemon	SID-History Injection	HISTCONTROL				Video Capture	Multi-Stage Channels		Service Stop
	Trap	Launchctl	Startup Name	Image File Execution Options				Video Capture	Multi-Stage Channels		Service Stop

Attack Paths

- Logical ordering of events and techniques that occur
 - Conditions have to be right for the attack to be successful
- We “control” the environment and circumstances that they have to operate in
- What are the conditions and preconditions required for certain techniques?
 - Are certain techniques more commonly used with conditions that we can more easily influence

How to Identify Attack Patterns of Note

- Identifying relevant attack paths is difficult
- How to define relevance:
 - Number of breaches attributed?
 - Criticality of affected assets?
 - Financial impact of breaches?
 - Number of times we're forced to read a security blog about the topic?
- Verizon says 28% of all breaches can be attributed to malware
- Verizon also states that 30% of those incidents can be attributed to ransomware
 - Let's explore the attack path and mapping to CIS Controls

[illegible]

+

technique controls

[illegible]

Xbot (S0298) x +

selection controls layer controls technique controls

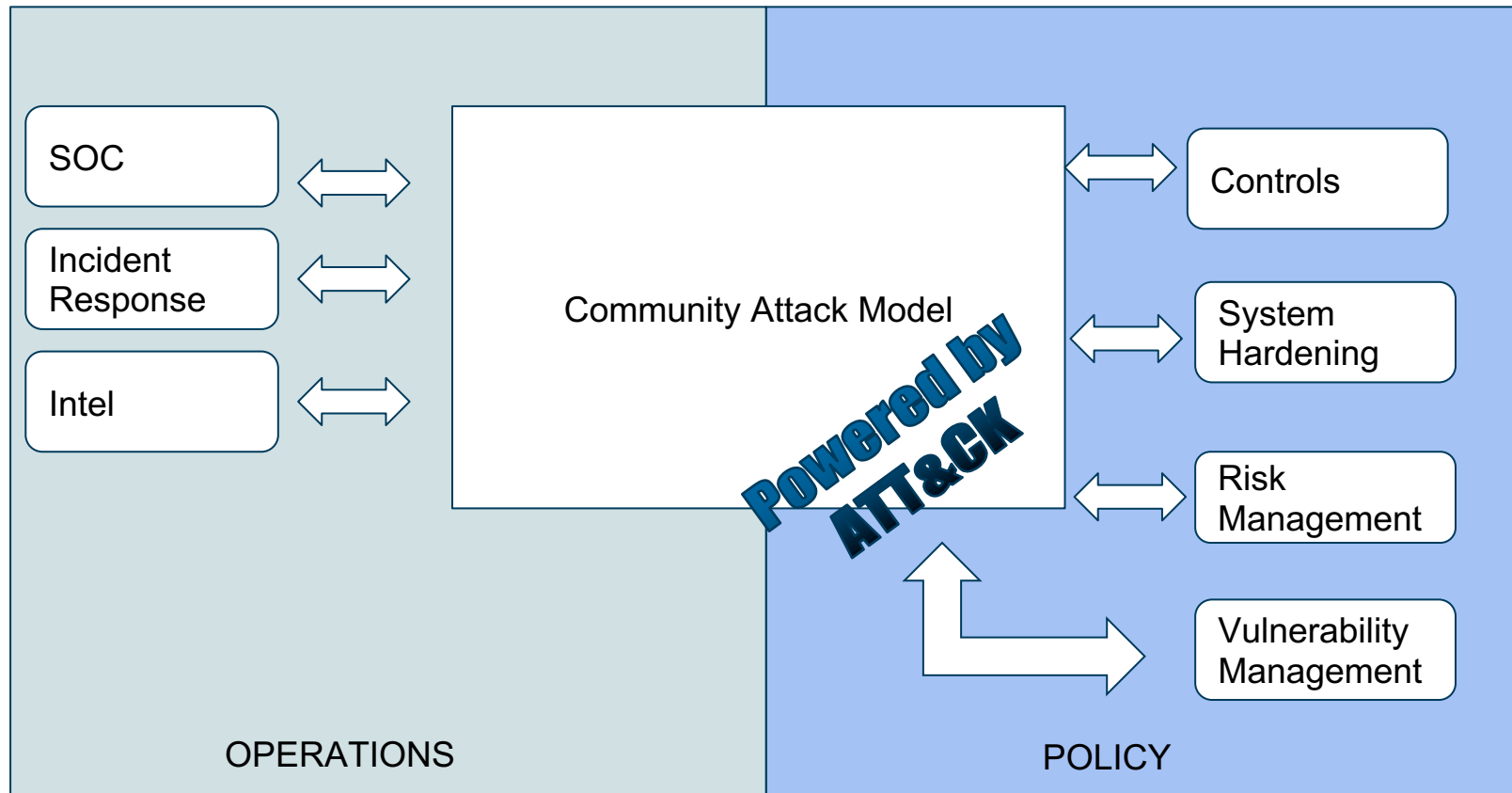
Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact	Collection	Exfiltration	Command And Control	Network Effects	Remote Service Effects
9 items	6 items	2 items	8 items	11 items	8 items	2 items	6 items	12 items	3 items	4 items	9 items	3 items
Deliver Malicious App via Authorized App Store	Abuse Device Administrator Access to Prevent Removal	Exploit OS Vulnerability	Application Discovery	Abuse Accessibility Features	Application Discovery	Attack PC via USB Connection	Encrypt Files	Abuse Accessibility Features	Alternate Network Mediums	Alternate Network Mediums	Downgrade to Insecure Protocols	Obtain Device Cloud Backups
Deliver Malicious App via Other Means	App Auto-Start at Device Boot	Exploit TEE Vulnerability	Disguise Root/Jailbreak Indicators	Access Sensitive Data in Device Logs	Device Type Discovery	Exploit Enterprise Resources	Generate	Access Calendar Entries	Commonly Used Port	Commonly Used Port	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Drive-by Compromise	Modify cached executable code		Download New Code at Runtime	Access Sensitive Data or Credentials in Files	File and Directory Discovery		Lock User Out of Device	Access Call Log	Standard Application Layer Protocol	Standard Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Exploit via Charging Station or PC	Modify OS Kernel or Boot Partition		Install Insecure or Malicious Configuration	Android Intent Hijacking	Network Service Scanning		Manipulate App Store Rankings or Ratings	Access Contact List	Web Service	Web Service	Exploit SS7 to Track Device Location	
Exploit via Radio Interfaces	Modify System Partition		Modify OS Kernel or Boot Partition	Capture Clipboard Data	Process Discovery		Premium SMS Toll Fraud	Access Sensitive Data in Device Logs			Jamming or Denial of Service	
Install Insecure or Malicious Configuration	Modify System Trusted Execution Environment		Modify System Partition	Capture SMS Messages	System Network Configuration Discovery		Wipe Device Data	Access Sensitive Data or Credentials in Files			Manipulate Device Communication	
Lockscreen Bypass			Modify Trusted Execution Environment	Exploit TEE Vulnerability	System Network Connections Discovery			Capture Clipboard Data			Rogue Cellular Base Station	
Repackaged Application			Obfuscated Files or Information	Malicious Third Party Keyboard App	Network Traffic Capture or Redirection			Location Tracking			Rogue Wi-Fi Access Points	
Supply Chain Compromise				URL Scheme Hijacking	URL Scheme Hijacking			Malicious Third Party Keyboard App			SIM Card Swap	
				User Interface Spoofing	User Interface Spoofing			Microphone or Camera Recordings				
								Network Traffic Capture or Redirection				

... of course it's not shared in Mobile ATT&CK!

Attack Paths

- Ransomware contains the *Data Encrypted for Impact* technique
- MITRE maps *Data Encrypted for Impact* to *Data Backup*
- Data Backup can be mapped to CIS Controls 10.1 and 10.5

10	10.1	Ensure Regular Automated BackUps	Ensure that all system data is automatically backed up on a regular basis.
10	10.2	Perform Complete System Backups	Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.
10	10.3	Test Data on Backup Media	Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.
10	10.4	Ensure Protection of Backups	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.
10	10.5	Ensure Backups Have At least One Non-Continuously Addressable Destination	Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.



Next Steps

- Continue developing the CIS Community Attack Model
- Help vet the Controls mapping to MITRE ATT&CK and ATT&CK Mitigations
- Use Community Attack Model to improve Controls v8 and the Implementation Groups
- Reach out to: controlsinfo@cisecurity.org
- Join the Community: <https://workbench.cisecurity.org>



Thank You

Philippe Langlois
philippe.langlois@verizon.com
@langlois925

Joshua M Franklin
josh.franklin@cisecurity.org
@thejoshpit