Using Threat Intelligence to Focus ATT&CK Activities

October 29, 2019

Nationwide®
is on your side

The Nationwide MITRE ATT&CK Team

- **Andy Kettell**
  - 20+ years IT security experience
  - 4+ years at Nationwide in Cyber Security Operations Center
  - CISSP, CCSP

- **David Westin**
  - 20+ years of Intelligence in U.S. Marine Corps
  - 4 years at U.S. Cyber Command
  - 1 year at Nationwide

Others:

- *Risk Leaders*
- *Business Area Leaders*
- *Infrastructure Personnel*
- *Columbus Collaboratory*

In the beginning…

This ATT&CK thing is cool! I want it!

Okay…how do we do this?

Our First Attempt (February 2017)

“Project Squishee…”

- What we did
  - Tried to analyze 240+ techniques, one technique at a time
  - Techniques chosen based on group consensus

- Six months to get three mitigations
- No real movement towards operationalizing the framework within the company

Our First Attempt (February 2017)

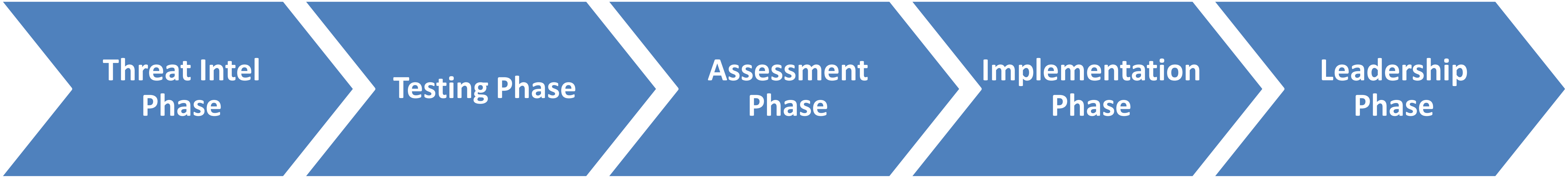
- **Why it didn’t work:**
  - Tried to do everything (no focus)
  - Unfocused choosing of technique for deep dive analysis (what is cool…)
  - Tried to work technique from analysis to completing remediation issues
  - Bogged down in minutiae (took too long…)
  - No differentiation between basic and advanced techniques
  - No idea what we will get from this
  - Participation fatigue
  - No Intel personnel

Bright Idea: Focus on the Threat!!

Who is targeting us?

What techniques do they use?

Nationwide MITRE ATT&CK Process Was Born



Threat Intel Phase

Testing Phase

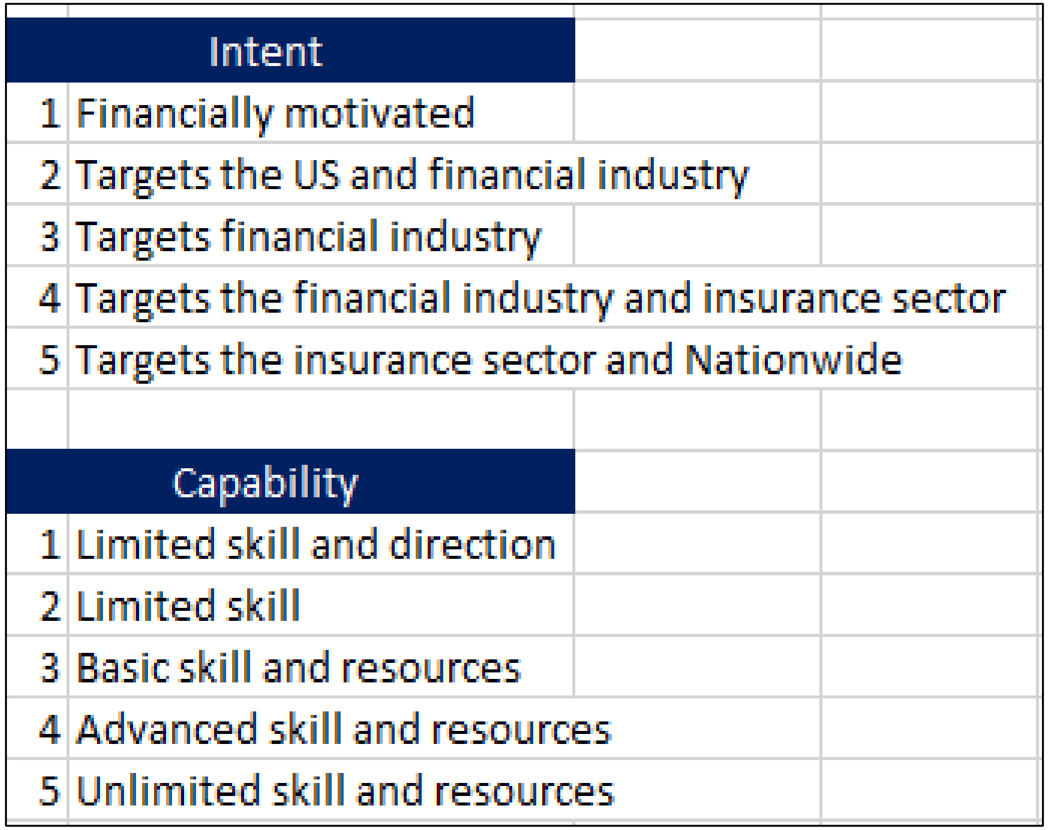
Assessment Phase

Implementation Phase

Leadership Phase

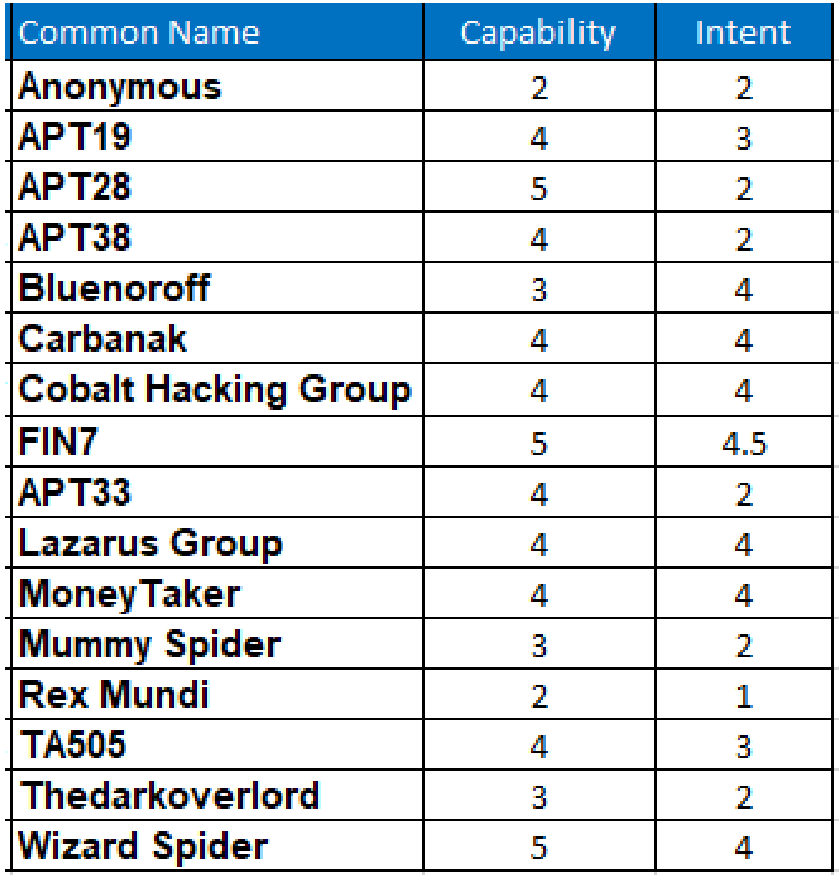
Threat Intel provided the compass and map…

Should I Care About Everything?



	Intent
1	Financially motivated
2	Targets the US and financial industry
3	Targets financial industry
4	Targets the financial industry and insurance sector
5	Targets the insurance sector and Nationwide

	Capability
1	Limited skill and direction
2	Limited skill
3	Basic skill and resources
4	Advanced skill and resources
5	Unlimited skill and resources



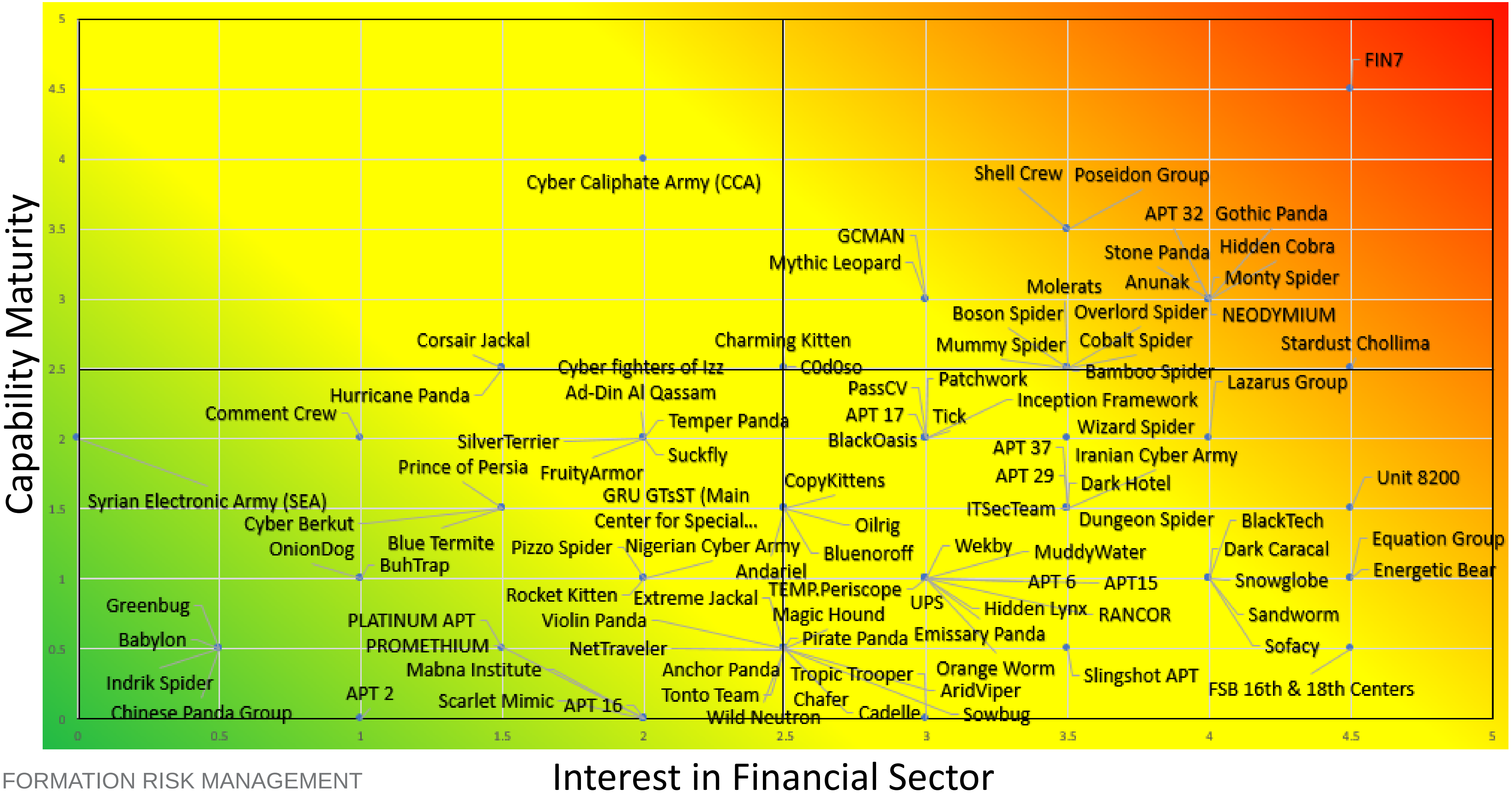
Common Name	Capability	Intent
Anonymous	2	2
APT19	4	3
APT28	5	2
APT38	4	2
Bluenoroff	3	4
Carbanak	4	4
Cobalt Hacking Group	4	4
FIN7	5	4.5
APT33	4	2
Lazarus Group	4	4
MoneyTaker	4	4
Mummy Spider	3	2
Rex Mundi	2	1
TA505	4	3
Thedarkoverlord	3	2
Wizard Spider	5	4

- *Started with Excel spreadsheet created by Florian Roth (@cyb3rops)*
- *Added capability/intent; simplified based on Nationwide needs*
- *Used simple aging out criteria based on last known reports*

Prioritize…

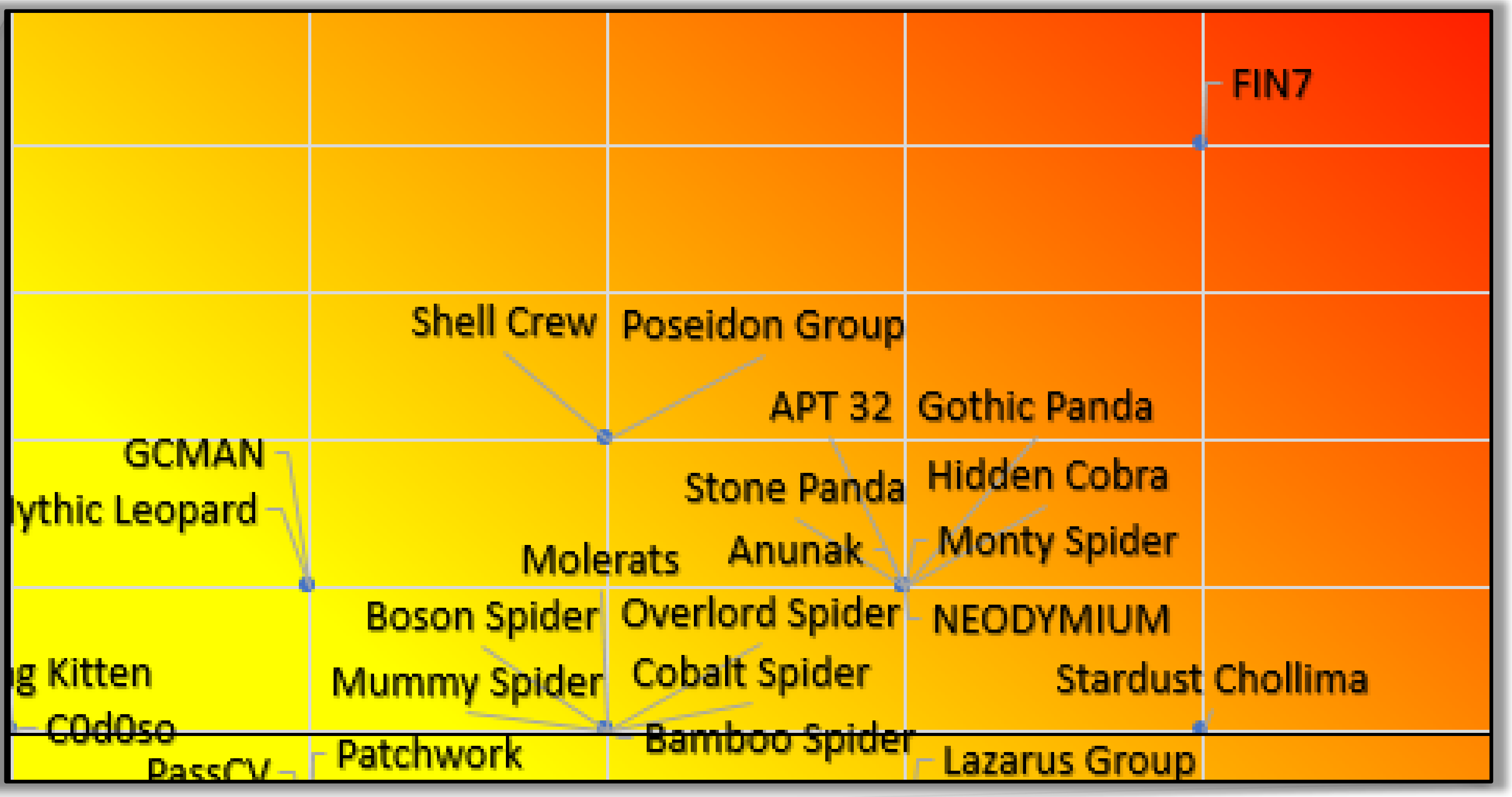
Put It In a Pretty Chart

Adversaries to the Financial Sector

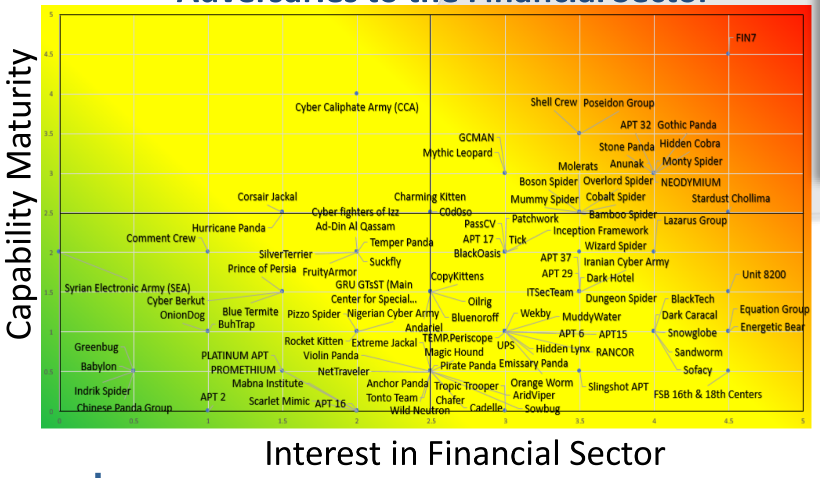


Focus on What Matters

- *100+ threat actors down to 27*
- *Focus is on those threat actors with capability and intent to go after finance/insurance industry*



Adversaries to the Financial Sector



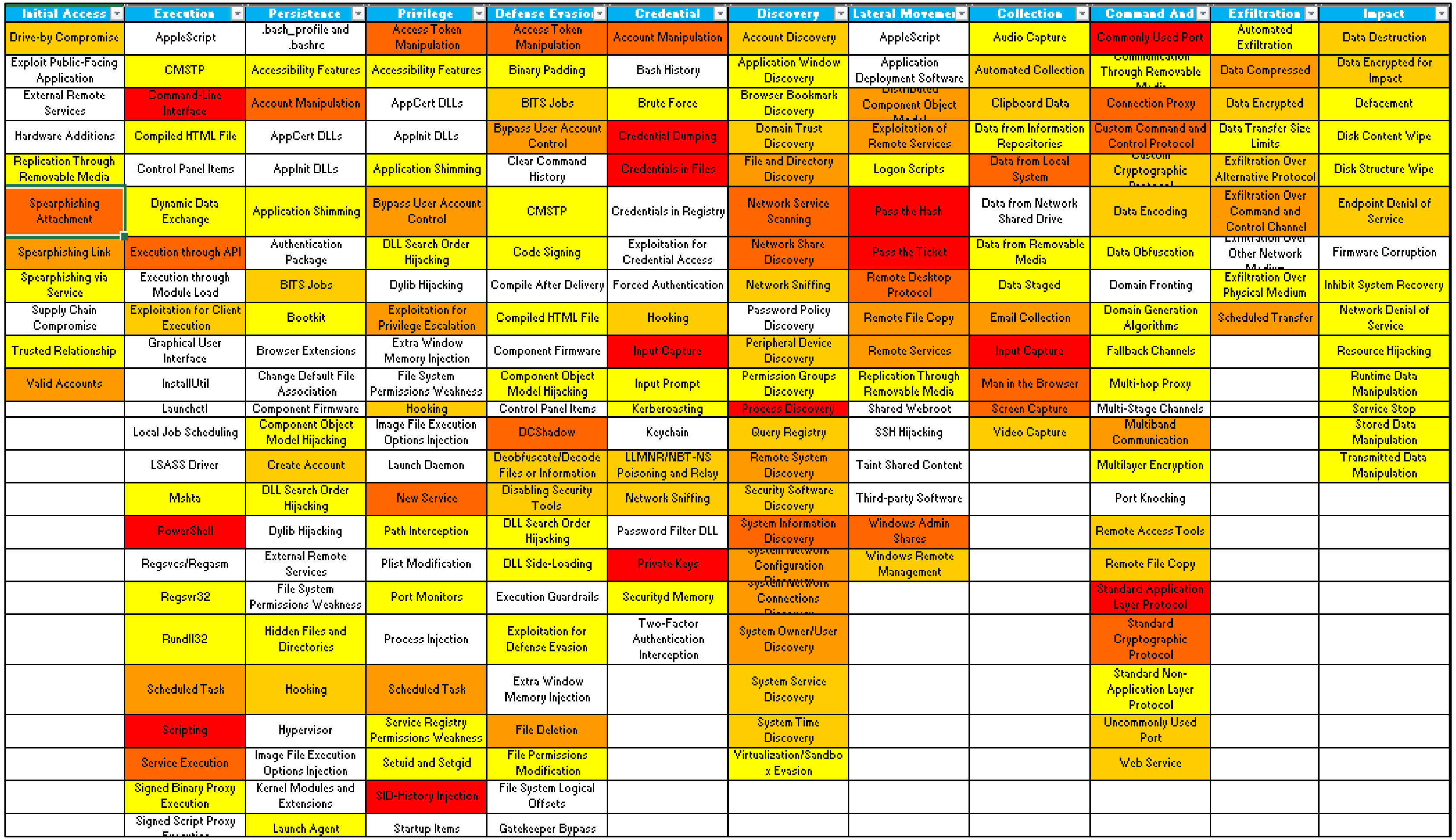
I Know 'Who', But Not 'What'…

Researching Threat Actor Techniques

- Intelligence collection tool of choice
- MITRE ATT&CK Site (of course…)
- ISAC/ISAO
- Security Researchers
- Twitter
- Top Techniques Reported
- Many others…

Collect All The Things…

Tying Research to ATT&CK Matrix



Initial Access	Execution	Persistence	Privilege	Defense Evasio	Credential	Discovery	Lateral Movemei	Collection	Command And	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	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	AppInit 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	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	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 Removable Media	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 Staged	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-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		System Time Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service		
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Startup Items	Gatekeeper Bypass							

- If used by threat actor, add to chart
- More red = more threat actors using that technique
- Simple Excel spreadsheet math…

Still Messy…

Focusing Only On Identified Techniques…

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	Command-Line Interface	Accessibility Features	Access Token Manipulation	Code Signing	Account Manipulation	Account Discovery	Application Deployment Software	Data Staged	Data Compressed	Commonly Used Port
Spearphishing Attachment	Mshta	Application Shimming	Accessibility Features	Disabling Security Tools	Brute Force	Application Window Discovery	Exploitation of Remote Services	Data from Local System	Data Encrypted	Connection Proxy
Spearphishing Link	PowerShell	Create Account	Application Shimming	File Deletion	Credential Dumping	File and Directory Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Data Encoding
Trusted Relationship	Regsvr32	DLL Search Order Hijacking	DLL Search Order Hijacking	Hidden Files and Directories	Credentials in Files	Network Service Scanning	Remote Desktop Protocol	Email Collection	Exfiltration Over Command and Control Channel	Data Obfuscation
Valid Accounts	Rundll32	Hidden Files and Directories	Exploitation for Privilege Escalation	Indicator Removal from Tools	Input Capture	Permission Groups Discovery	Remote File Copy			Fallback Channels
	Scheduled Task	New Service	New Service	Indicator Removal on Host		Process Discovery	Remote Services			Multi-Stage Channels
	Scripting	Registry Run Keys / Start Folder	Process Injection	Masquerading		Query Registry	Windows Admin Shares			Standard Application Layer Protocol
	User Execution	Scheduled Task	Scheduled Task	Mshta		Remote System Discovery				Standard Cyrptographic Protocol
	Windows Management Instrumentation	Shortcut Modification	Valid Accounts	Obfuscated Files or Information		System Information Discovery				Standard Non-Application Protocol
			Web Shell	Process Injection		System Network Configuration Discovery				Uncommonly Used Port
				Regsvr32		System Network Connections Discovery				
				Rundll32		System Owner/User Discovery				
				Software Packing						
				Timestomp						
				Valid Accounts						
				Web Service						

- *91 techniques across 11 tactics*
- *Initial data necessary for prioritization*

Manageable Project…

Winning Quotes

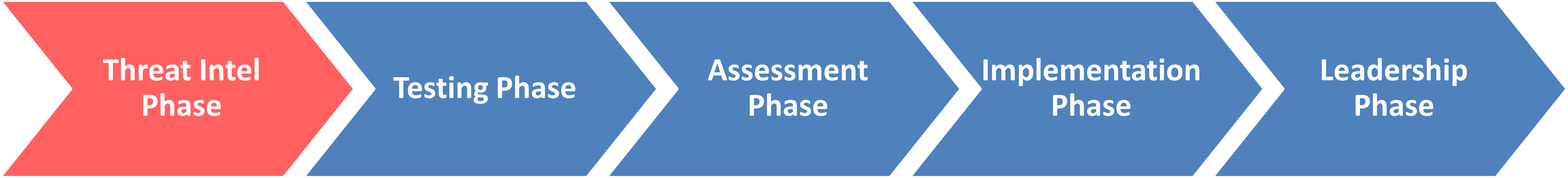
“Knowing Is Half The Battle”

- G.I. Joe

“Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win”

- Sun Tzu

Intel Driving Operations



Threat Intel Phase

Testing Phase

Assessment Phase

Implementation Phase

Leadership Phase

Objective: Focus project on most likely adversary techniques

Objective: Determine susceptibility to prioritized techniques

Objective: Determine recommended detection & mitigation strategies

Objective: Develop & implement detection and mitigation actions

Objective: Determine risk associated with non-implemented strategies

Teams Involved: Threat Intelligence, Attack & Penetration, Infrastructure Operations, Security Tool administrators, Incident Response, Security Architecture, 2nd Line of Defense consultants, executive leadership

Everyone Involved…

Where Did We End Up?

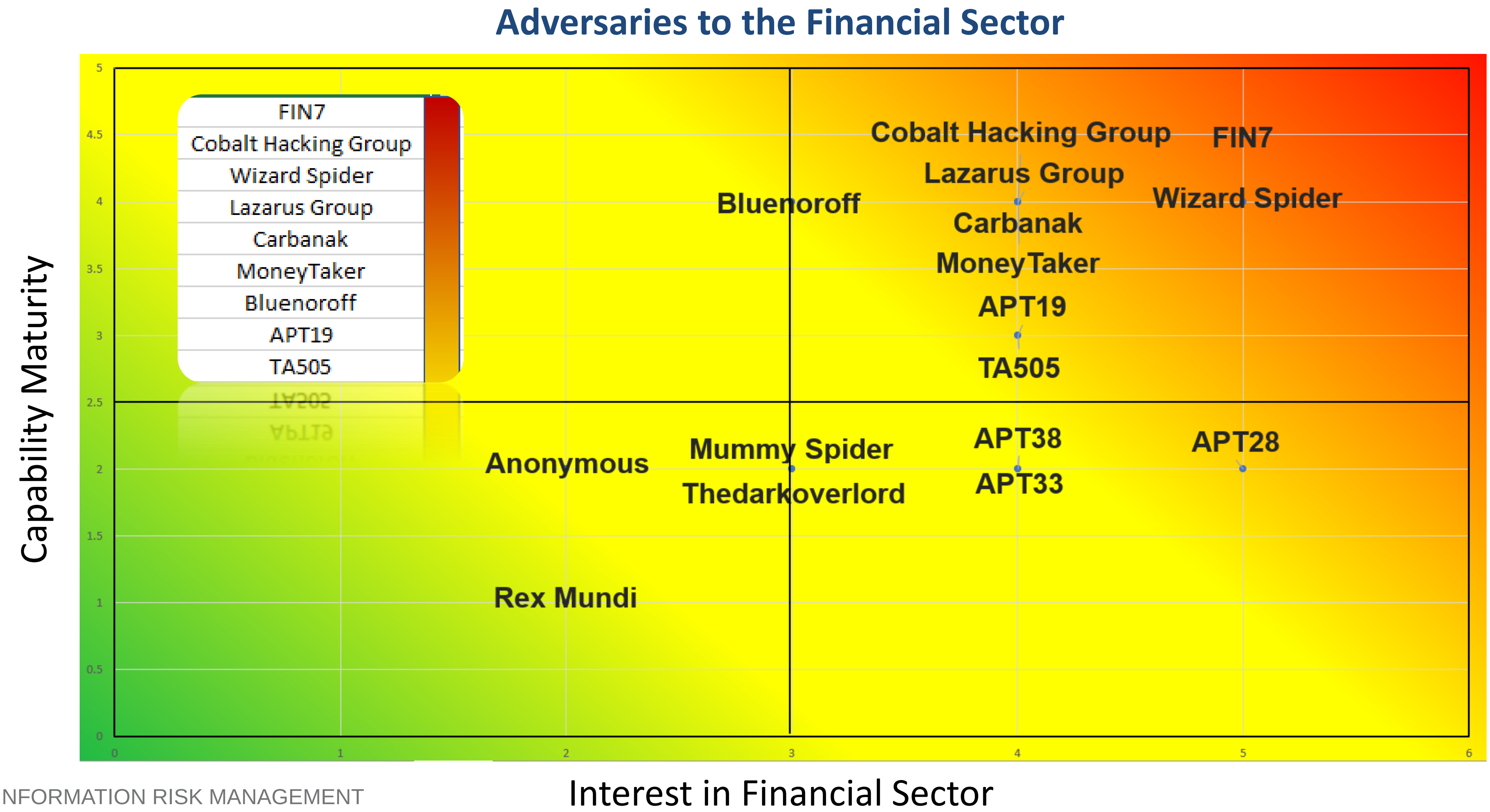
- Reduced tested techniques from 240+ to 91
- Clear understanding of our security posture related to MITRE ATT&CK techniques associated with threat actors targeting the finance/insurance industry
- Security focused recommendations vs. IT audit driven
- Enabled MITRE ATT&CK to gain a foothold in the organization
- Framework built to enable follow-on actions

Keep The Momentum Going

Are we done yet?

What’s next?

Constantly Evolving



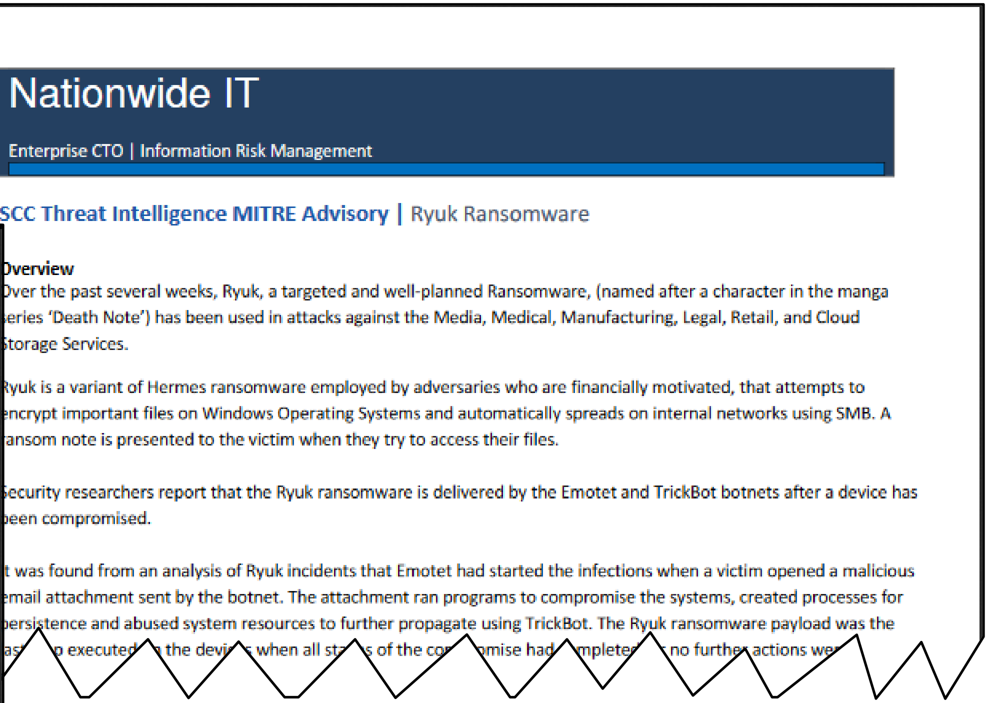
Intelligence Led Prioritization

- **Prioritization of techniques**
  - Third party research (Red Canary’s analysis of top techniques)
  - Attack & Penetration test results
  - Security expert input (FS-ISAC, Columbus Collaboratory, etc…)
  - Analysis of recent breach reports (Ryuk, Emotet, Qakbot, Fin7, etc…)
  - Analysis of Nationwide existing controls and effectiveness

Priority	Tactic	Technique
1	Execution	PowerShell
2	Credential Access	Credential Dumping
3	Execution	Command-Line Interface
4	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Valid Accounts
5	Initial Access	Spearphishing Attachment
6	Initial Access	Spearphishing Link
7	Exfiltration	Data Compressed
8	Execution, Persistence, Privilege Escalation	Scheduled Task
9	Defense Evasion	Masquerading
10	Defense Evasion	Obfuscated Files

*Not real results

Intelligence Driving Security



Nationwide IT

Enterprise CTO | Information Risk Management

SCC Threat Intelligence MITRE Advisory | Ryuk Ransomware

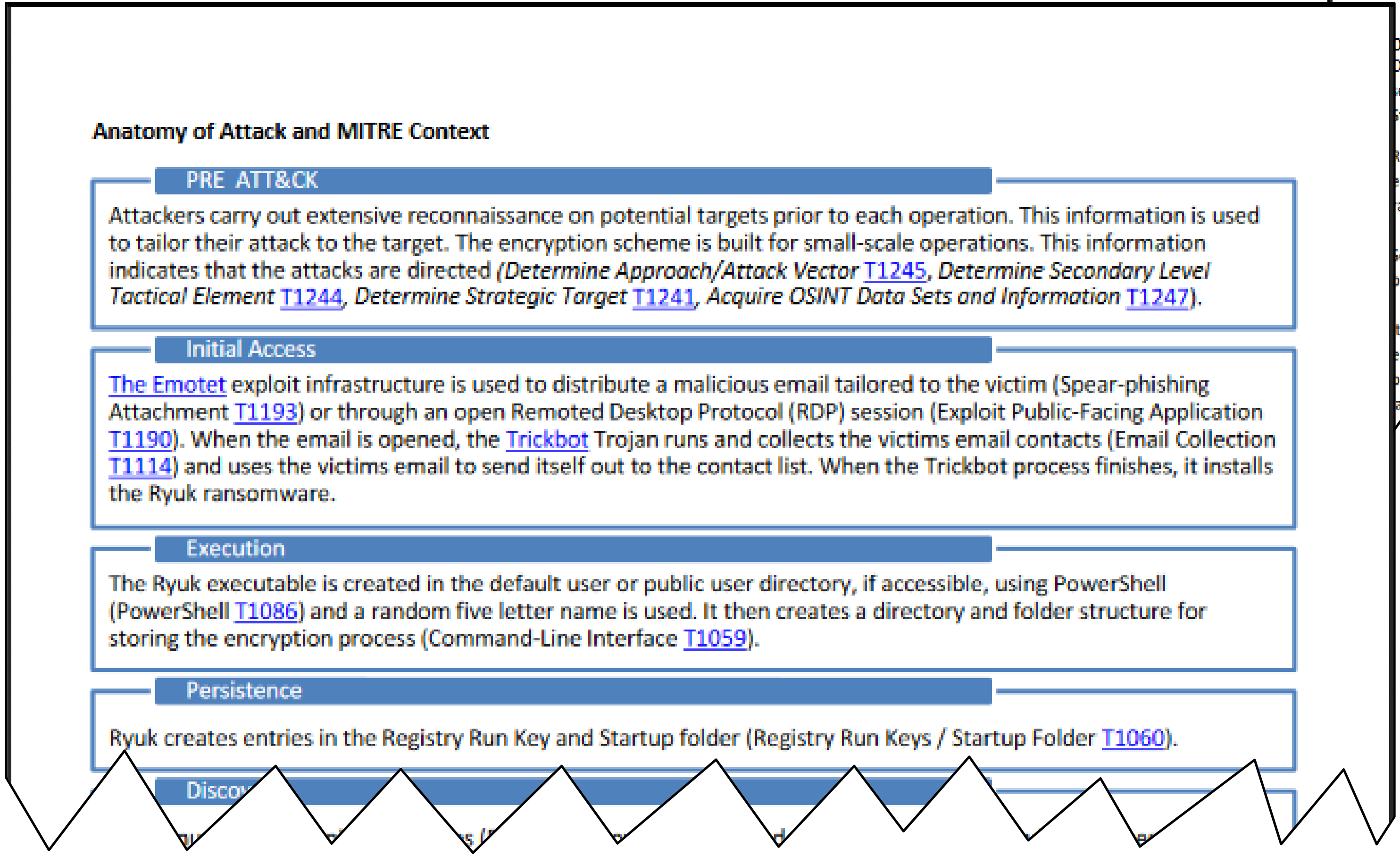
Dverview

Dver the past several weeks, Ryuk, a targeted and well-planned Ransomware, (named after a character in the manga eries 'Death Note') has been used in attacks against the Media, Medical, Manufacturing, Legal, Retail, and Cloud torage Services.

Ryuk is a variant of Hermes ransomware employed by adversaries who are financially motivated, that attempts to ncrypt important files on Windows Operating Systems and automatically spreads on internal networks using SMB. A ansom note is presented to the victim when they try to access their files.

ecurity researchers report that the Ryuk ransomware is delivered by the Emotet and TrickBot botnets after a device has een compromised.

t was found from an analysis of Ryuk incidents that Emotet had started the infections when a victim opened a malicious mail attachment sent by the botnet. The attachment ran programs to compromise the systems, created processes for ersistence and abused system resources to further propagate using TrickBot. The Ryuk ransomware payload was the as p executed the devi s when all st s of the co omise had mpleted no further actions we



Anatomy of Attack and MITRE Context

PRE ATT&CK

Attackers carry out extensive reconnaissance on potential targets prior to each operation. This information is used to tailor their attack to the target. The encryption scheme is built for small-scale operations. This information indicates that the attacks are directed *(Determine Approach/Attack Vector* T1245, *Determine Secondary Level Tactical Element* T1244, *Determine Strategic Target* T1241, *Acquire OSINT Data Sets and Information* T1247).

Initial Access

The Emotet exploit infrastructure is used to distribute a malicious email tailored to the victim (Spear-phishing Attachment T1193) or through an open Remoted Desktop Protocol (RDP) session (Exploit Public-Facing Application T1190). When the email is opened, the Trickbot Trojan runs and collects the victims email contacts (Email Collection T1114) and uses the victims email to send itself out to the contact list. When the Trickbot process finishes, it installs the Ryuk ransomware.

Execution

The Ryuk executable is created in the default user or public user directory, if accessible, using PowerShell (PowerShell T1086) and a random five letter name is used. It then creates a directory and folder structure for storing the encryption process (Command-Line Interface T1059).

Persistence

Ryuk creates entries in the Registry Run Key and Startup folder (Registry Run Keys / Startup Folder T1060).

Discov

- *"Anatomy of ATT&CK" documents*
  - *Use security research and recent external events*
  - *Break down scenario by technique*
  - *Used to confirm security controls are in place*

Key Takeaways

- Intel driven operations ensure clear focus and prioritization
- Focus on threat actors in your sector and techniques they use
- Don’t try to do it all…smaller chunks enable clearer understanding of final objectives
- Constantly evolve and iterate to increase coverage

Questions?

Contact us at:

sccthreatintel@nationwide.com

Andy Kettell

David Westin