FORTINET®

VIRTUAL

SECURITY DAY

Lighting it Up Playbook Heat Maps

FortiGuard Labs, Global Threat Intelligence

Derek Manky

Chief of Security Insights, FortiGuard Labs

- Software & reverse engineering (Threat Analysis) background
- 20 years experience in IT
- 15 years experience at Fortinet (FortiGuard)

- Visionary role – threat forecasting and roadmap
- Chief liaison for threat intelligence partnerships & industry
  - Sit on steering committee of Cyber Threat Alliance
  - Pioneered founding efforts, bylaws

- Designed, Created & Lead Cyber SEAL Team (FortiGuard)
  - Seasoned, global threat expertise team
  - Incident response to breaking events
  - Proactive threat research & intelligence
  - Consult to C-Suite worldwide including Fortune 500
  - Train talent & capacity

FortiGuard Labs

Fortinet's Threat Intelligence & Research Organization

FortiGuard Labs Overview

VISIBILITY → INNOVATION → ACTIONABLE THREAT INTELLIGENCE

VISIBILITY

- **Telemetry**
  - Network
  - Web
  - Sandbox
  - Email
  - Endpoint
- **CERTs**
- **Enforcement Partnerships**
- **Zero-Day**
- **OSINT**
- **CTA feeds** (Cyber Threat Alliance)
- **Trusted Partnerships**

INNOVATION

FortiGuard Labs

- AI / Machine Learning
- Fortinet Distribution Network
- Detection and protection in milliseconds
- Federated Machine Learning

ACTIONABLE THREAT INTELLIGENCE

SECURITY FABRIC PROTECTIONS

- IPS
- Application Control
- Web Filtering
- Anti-Virus
- Anti-Spam
- Endpoint Vulnerability
- Indicators of Compromise (IoCs)

PROACTIVE RESEARCH

- Adversary Playbooks
- Security Blogs
- Threat Intel Briefs
- Threat Signals
- Virtual Patches

THREAT INTELLIGENCE SERVICES

- Penetration Testing
- Phishing Service
- Incident Response

Partnerships

Sharing Intelligence / Collaborating on Research & Investigations

Industry – **Collaboration & Innovation**

Enterprise – **Threat Research**

Law Enforcement & Government - **Attribution**

CERT - **Disruption**

Evanta
a Gartner Company

Actionable Threat Intelligence – Q2 2020

17 Million
Botnet C&C attempts
THWARTED
PER MINUTE

565,000
SPAM
Blocked Per Day

URL
195,000
Malicious Website
ACCESSES
Blocked Per Minute

0
885
ZERO DAY
THREATS DISCOVERED

18 Million
NETWORK INTRUSION ATTEMPTS
resisted per minute

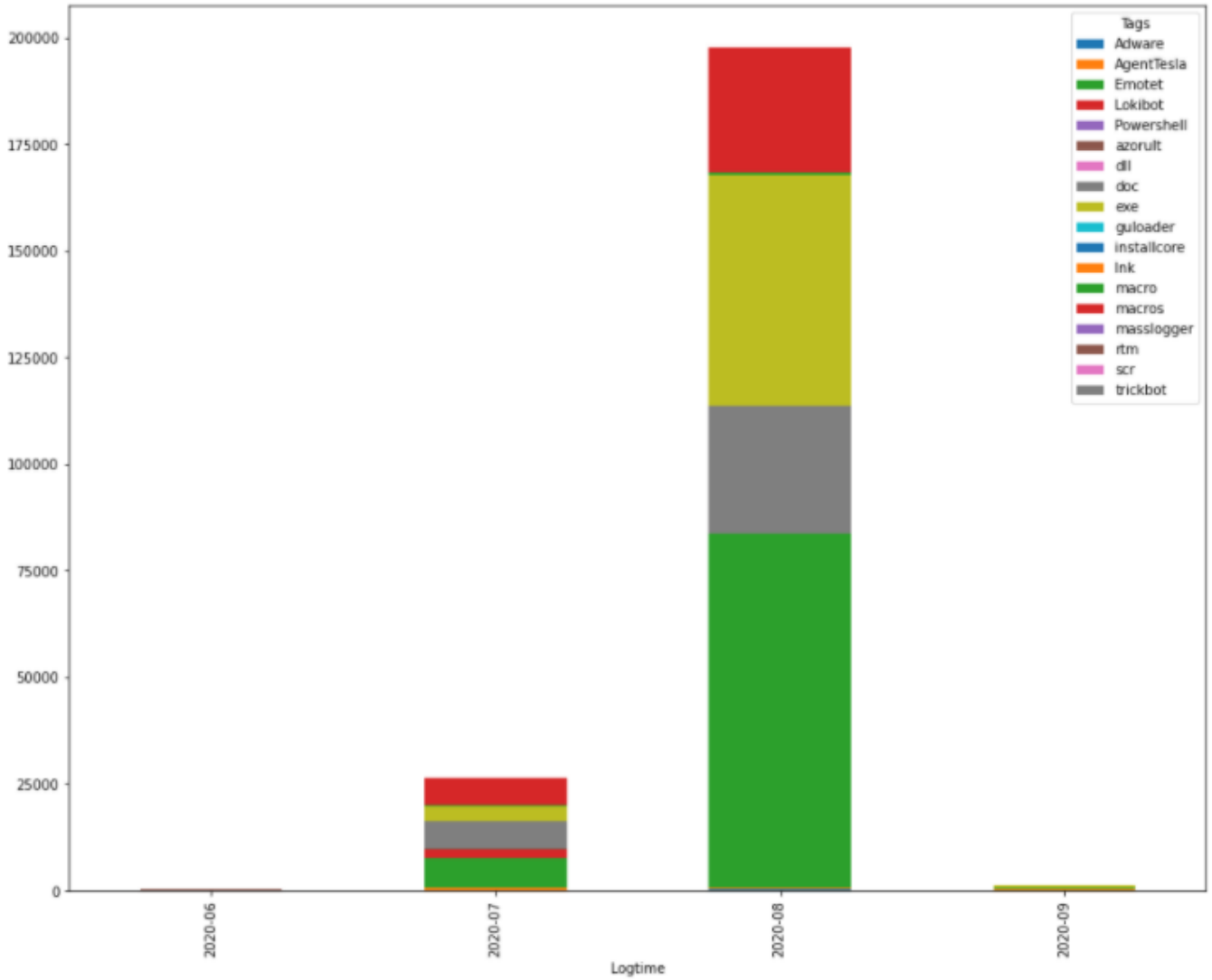
18 Million
PHISHING
Blocked Per Day

1.1
PB
Of Threat Samples

609,000
HOURS
of Threat Research
GLOBALLY PER WEEK

173,000
MALWARE PROGRAMS
Neutralized Per Minute

FortiGuard Labs & BI.Zone Sharing Stats



Monthly tracked sharing for intelligence relationship

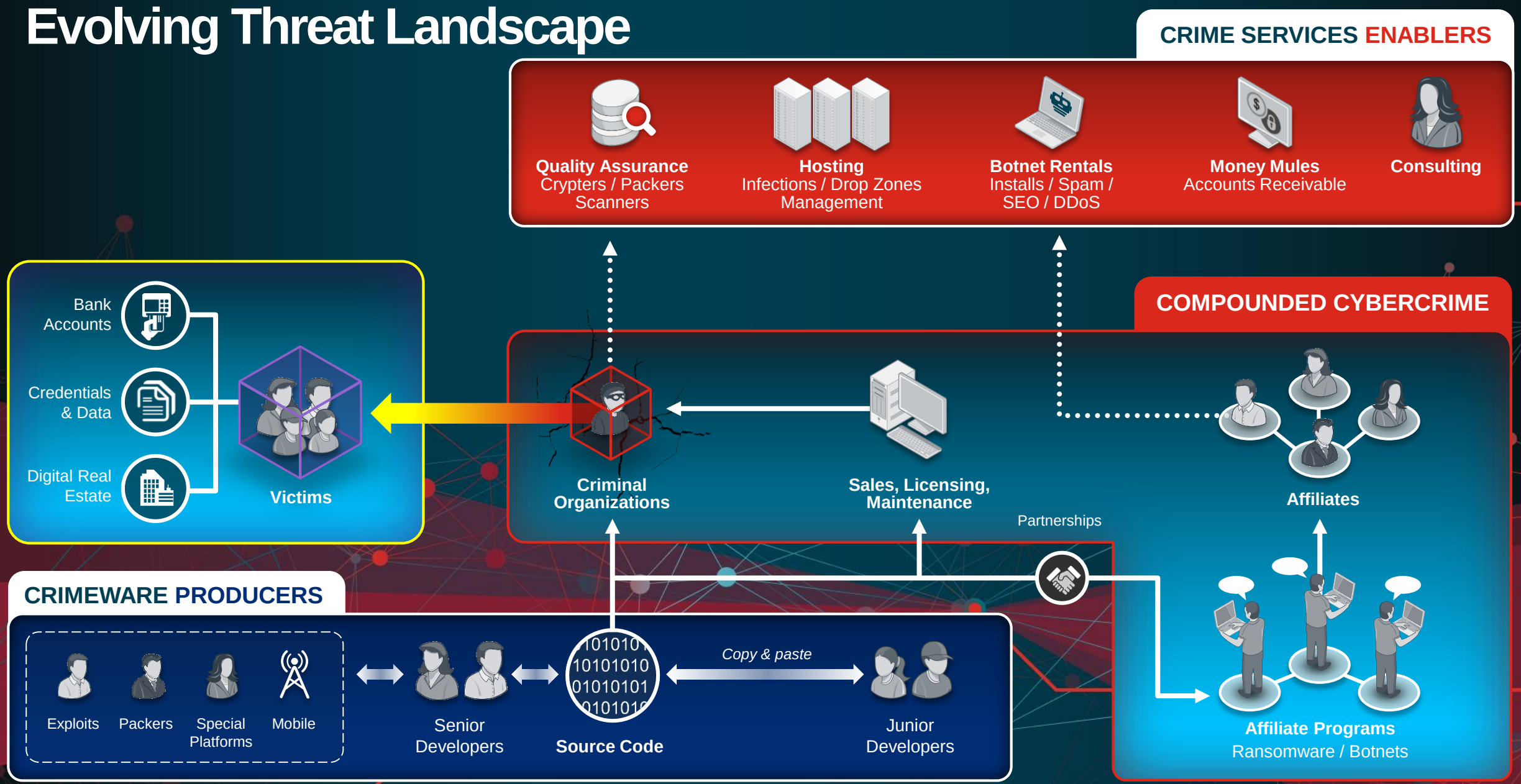
Bidirectional feedback capabilities

Heatmap creation based off fabric integrations from intelligence

Actionable Threat Intelligence

Red & Blue Playbooks

Evolving Threat Landscape



Traditional Challenges

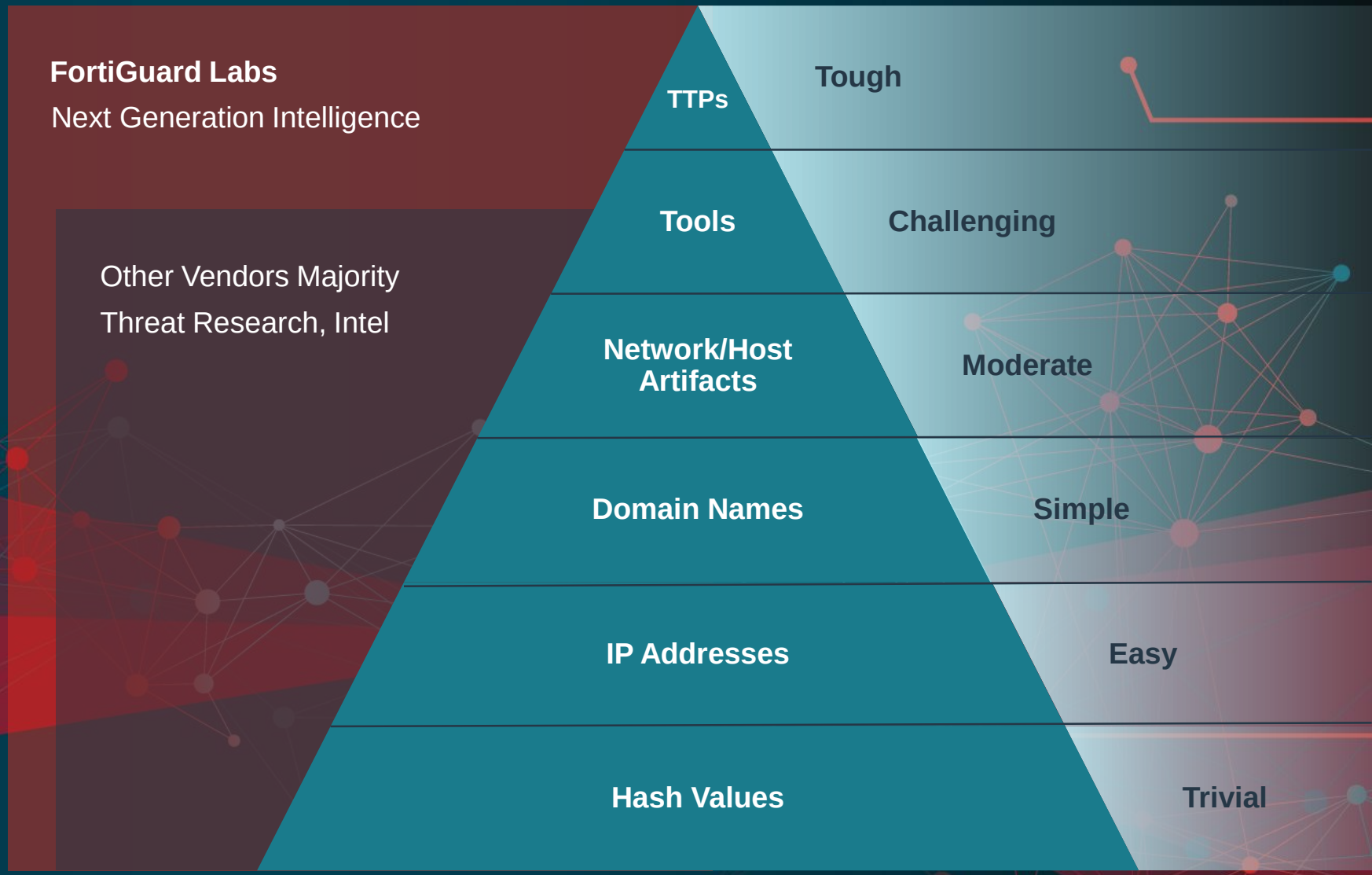
Pyramid of Pain

Platform adoption

Real time collaboration

False positives

Skills gap



Fortinet & INTERPOL: Project Knightrider

$61M of funds stolen in 3 month period through Business Email Compromise

$100k - $10M+ USD transactions through payment diversion

61 days of information reviewed

35-50% payment to money laundering on funds transferred through service (high amount, high risk); local and overseas

4 main players, including kingpin, laundering manager, hacker head, and forger

Largest group was hacking group

Many more involved in laundering network

Adversarial Playbooks

The complete collection of tools, techniques, and steps that adversaries goes through to complete their cyber mission.

THREAT RESEARCH
CTA Adversary Playbook: Goblin Panda

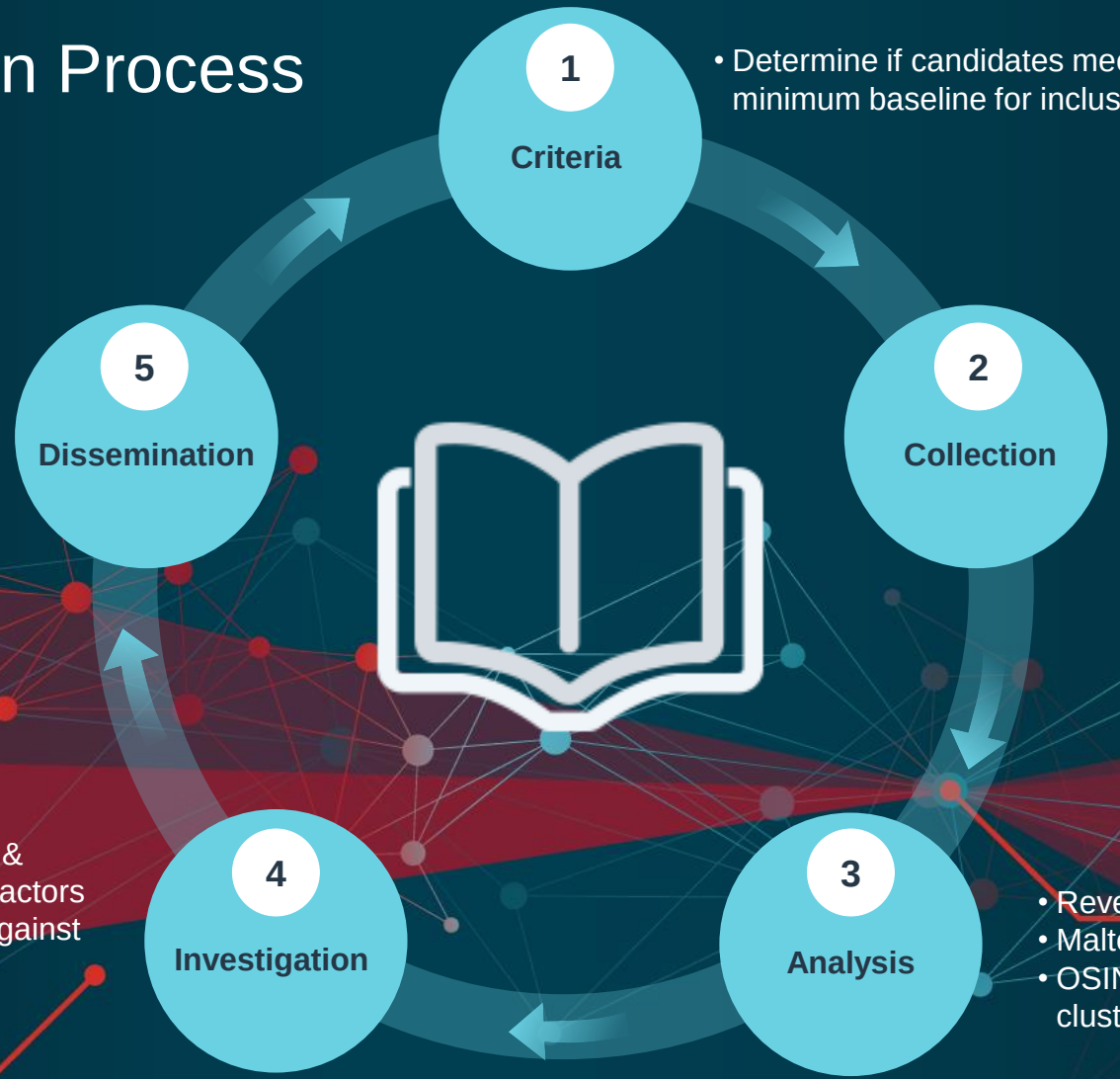
THREAT RESEARCH
Silence Group Playbook

THREAT RESEARCH
Zegost from Within – New Campaign Targeting Internal Interests

THREAT RESEARCH
Emotet – Jack of All Trades

Operationalizing MITRE ATT&CK

Playbook Creation Process



- Determine if candidates meet minimum baseline for inclusion.

- Fortinet research
- Hunting via yara rules
- Samples in ST3/VT/OSINT

- Reversing for baseline discovery
- Maltego analysis
- OSINT of network IOC's and hashes to cluster families

- Understand the motives & distribution of the threat actors
- Analysis and research against MITRE ATT&CK

- Stage internal playbook viewer via STIX
- Early partner sharing
- Public release

Silence Group

May 2018 to December 2018

Intrusion Set

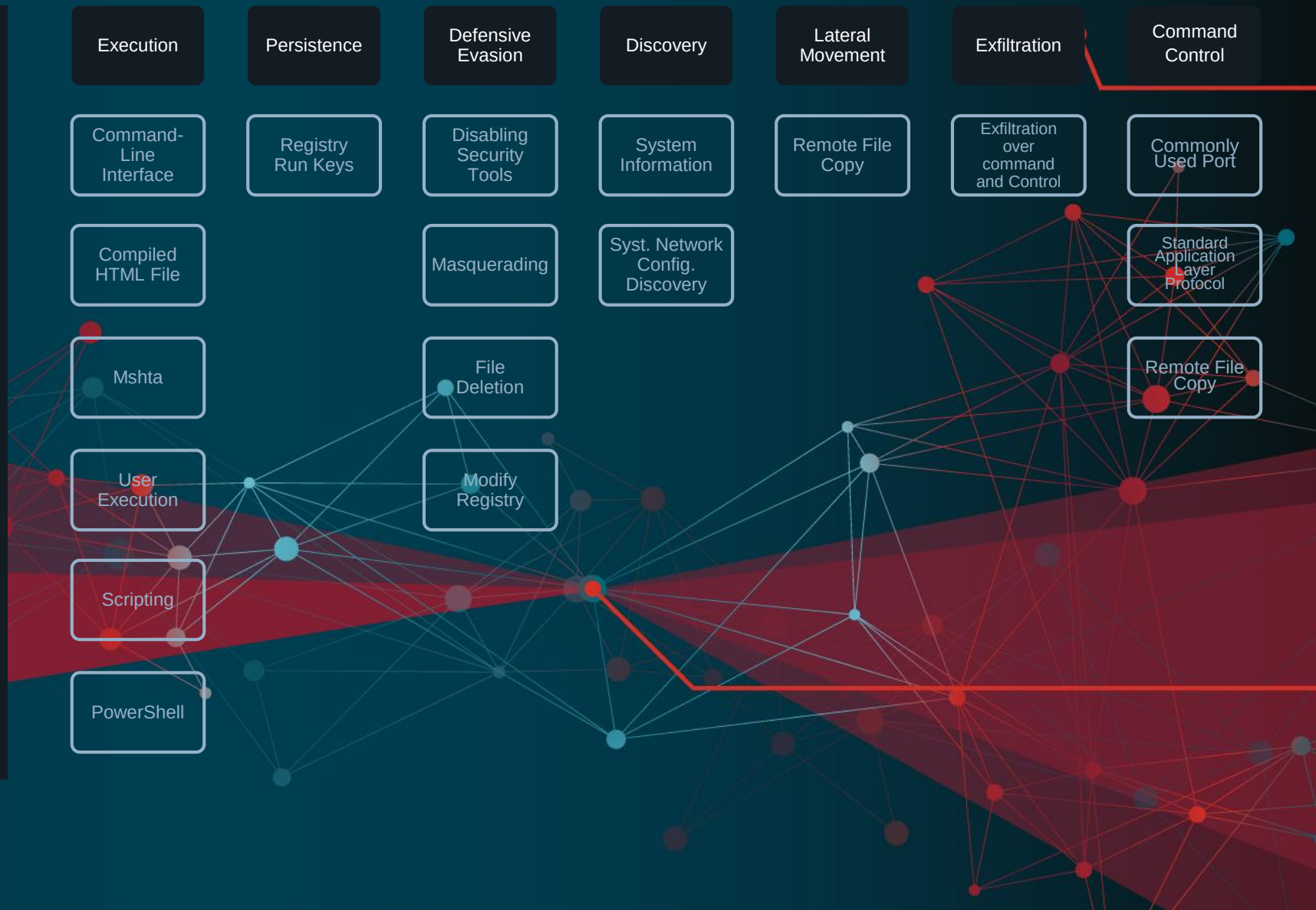
- 5 Campaigns
- 436 Indicators
- 15 Vulnerabilities
- 86 Attack Patterns

Targets

- Banks & Banking Infrastructure

4 Modules

- Main Module
- Proxy Module
- Monitor Module
- ATM Module



Silence Group

May 2018 to December 2018

Intrusion Set

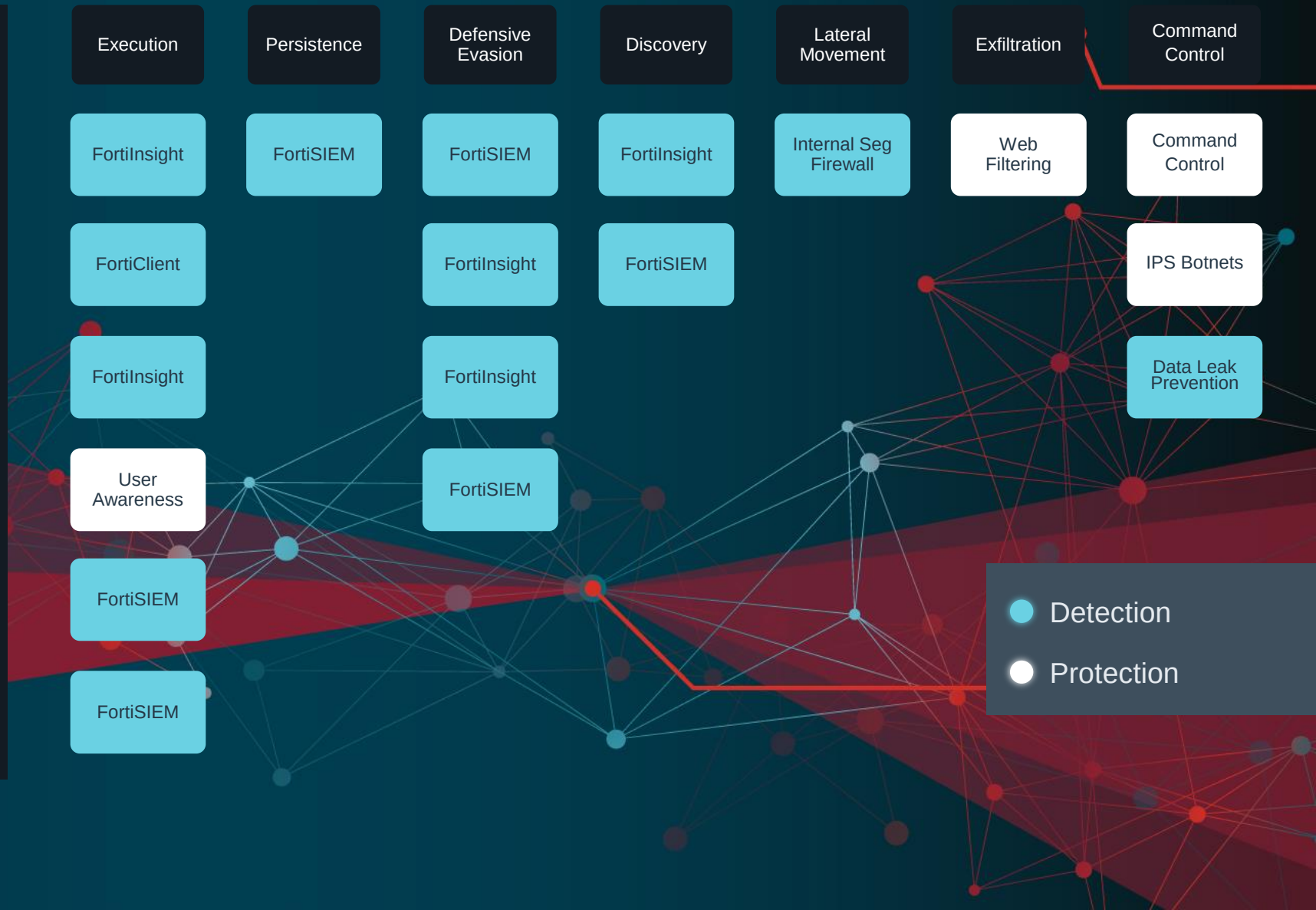
- 5 Campaigns
- 436 Indicators
- 15 Vulnerabilities
- 86 Attack Patterns

Targets

- Banks & Banking Infrastructure

4 Modules

- Main Module
- Proxy Module
- Monitor Module
- ATM Module



PLAYBOOK VIEWER

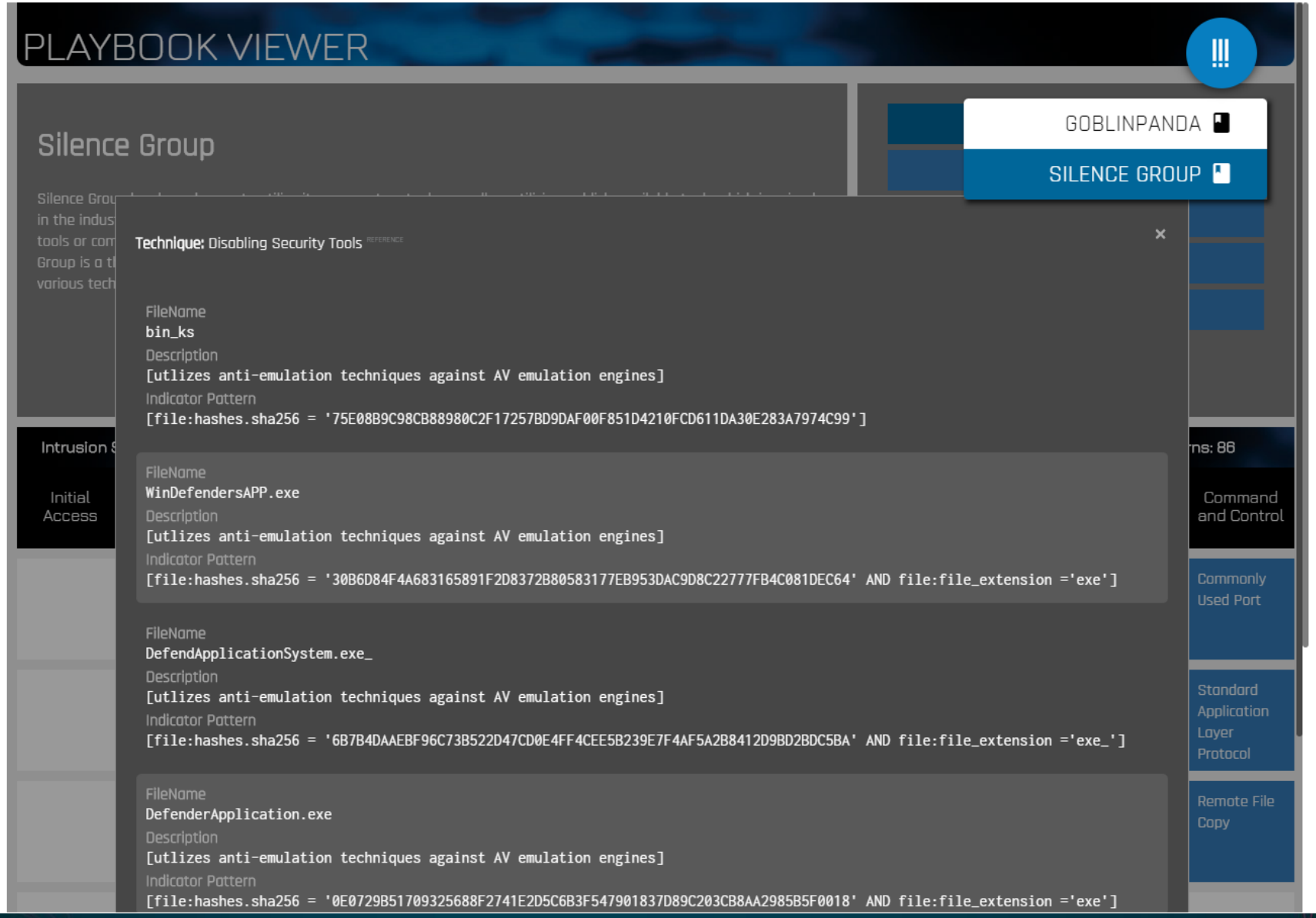
Silence Group

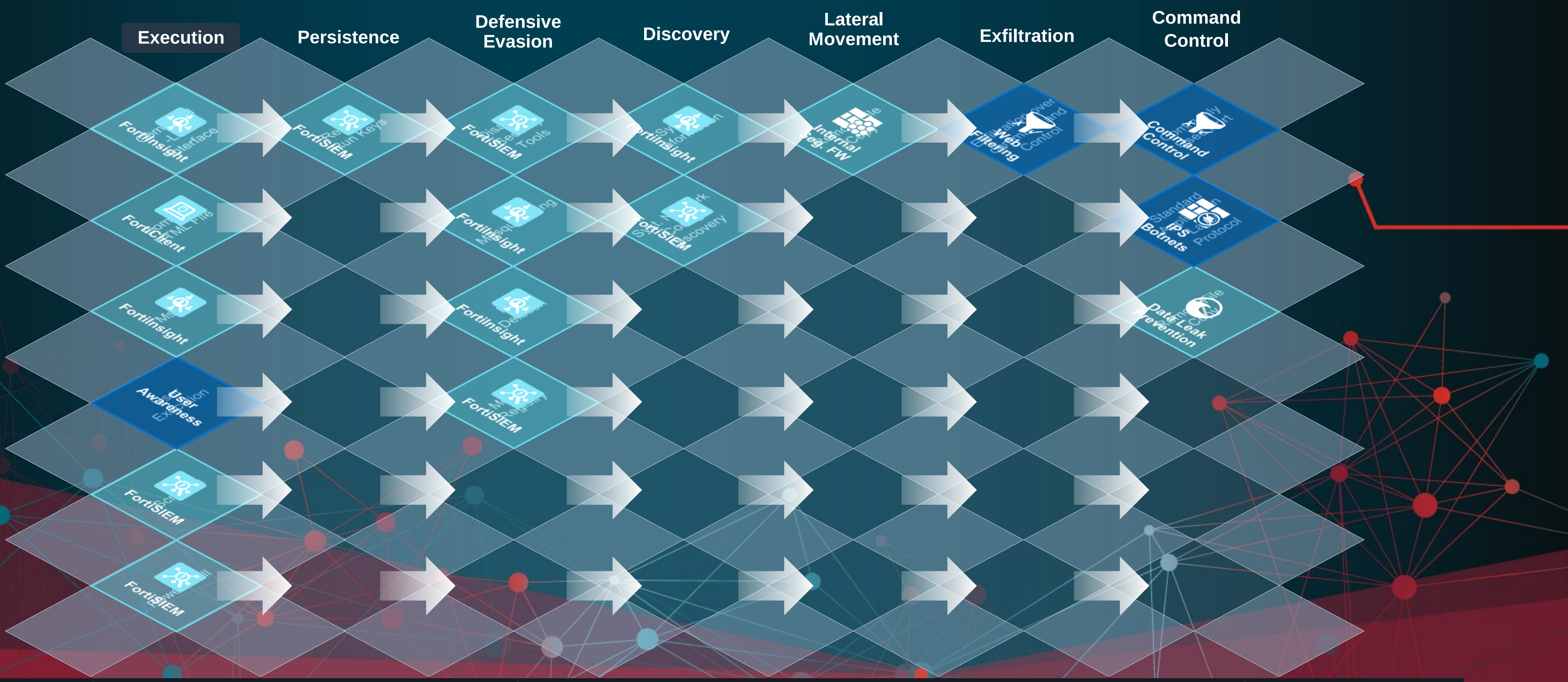
Silence Group has been known to utilize its own custom tools as well as utilizing publicly available tools which is coined in the industry as living off the land. What this means essentially is to operate as long as possible using preexisting tools or commands built into the operating system of the target. Suspected Attribution: Unknown. Targets: Silence Group is a threat actor that focuses primarily on attacking banks and banking infrastructure to embezzle funds via various technological means. Synonims:Silence Banker

GOBLINPANDA
SILENCE GROUP
July 2017 to November 2017
December 2016 to June 2017
June 2016 to December 2016

Intrusion Set: Silence Group **Campaigns: 5** **Indicators: 436** Vulnerabilities: 15 **Attack Patterns: 86**

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
	Command-Line Interface	Registry Run Keys / Startup Folder		Disabling Security Tools		System Information Discovery	Remote File Copy		Exfiltration Over Command and Control	Commonly Used Port
	Compiled HTML File			Masquerading		System Network Configuration Discovery				Standard Application Layer Protocol
	Mshta			File Deletion						Remote File Copy
	User			Modify						


PLAYBOOK VIEWER
Silence Group
GOBLINPANDA
SILENCE GROUP
Technique: Disabling Security Tools
FileName
bin_ks
Description
[utlizes anti-emulation techniques against AV emulation engines]
Indicator Pattern
[file:hashes.sha256 = '75E08B9C98CB88980C2F17257BD9DAF00F851D4210FCD611DA30E283A7974C99']
FileName
WinDefendersAPP.exe
Description
[utlizes anti-emulation techniques against AV emulation engines]
Indicator Pattern
[file:hashes.sha256 = '30B6D84F4A683165891F2D8372B80583177EB953DAC9D8C22777FB4C081DEC64' AND file:file_extension ='exe']
FileName
DefendApplicationSystem.exe_
Description
[utlizes anti-emulation techniques against AV emulation engines]
Indicator Pattern
[file:hashes.sha256 = '6B7B4DAAEBF96C73B522D47CD0E4FF4CEE5B239E7F4AF5A2B8412D9BD2BDC5BA' AND file:file_extension ='exe_']
FileName
DefenderApplication.exe
Description
[utlizes anti-emulation techniques against AV emulation engines]
Indicator Pattern
[file:hashes.sha256 = '0E0729B51709325688F2741E2D5C6B3F547901837D89C203CB8AA2985B5F0018' AND file:file_extension ='exe']
Initial Access
Command and Control
Commonly Used Port
Standard Application Layer Protocol
Remote File Copy



ATT&CK Gameboard

Build Adversarial Playbook

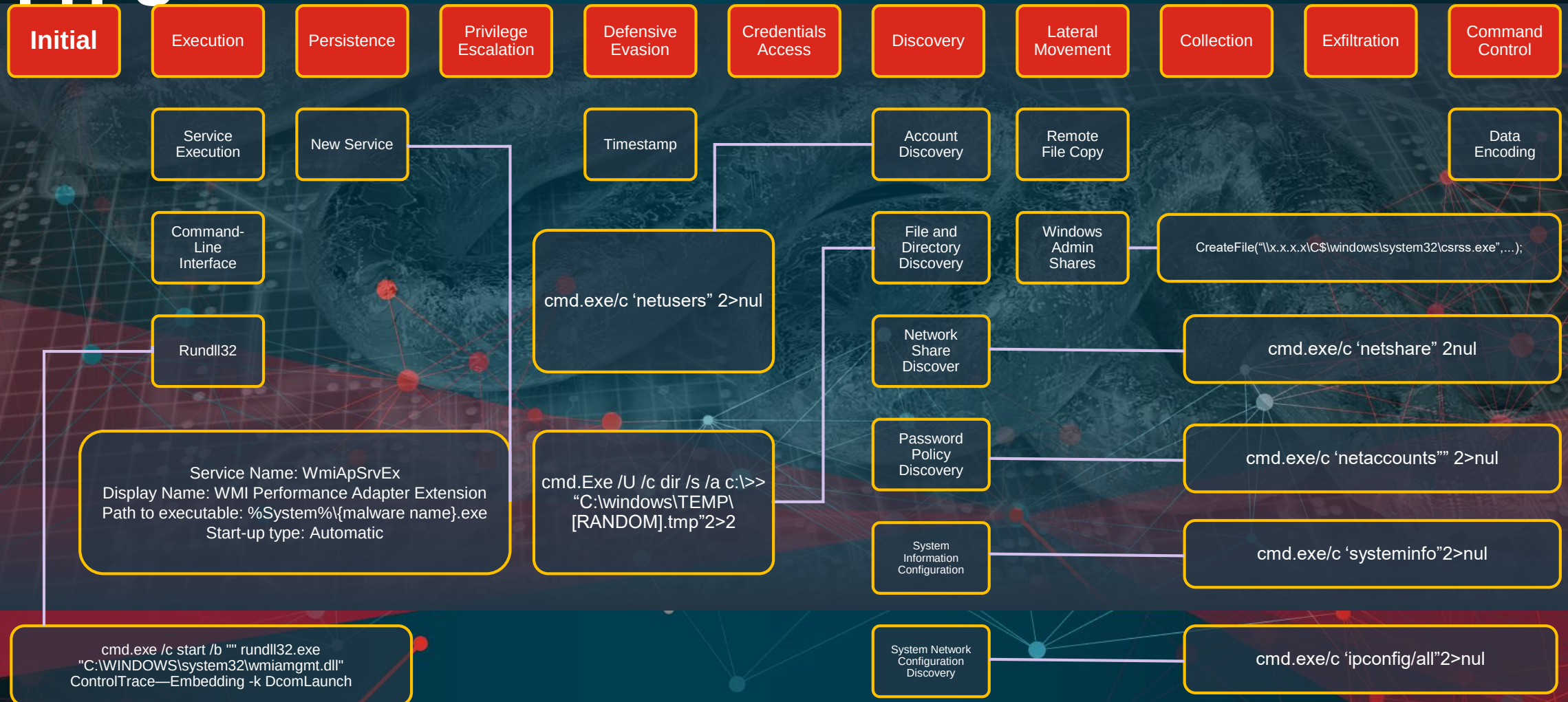
Track Left->Right Movement

Build Defensive Playbook

Detection

Protection

Orangeworm Attack—Mitre Attack TTPs



MITRE ATT&CK Implemented Heatmap on Live Sightings (Fortinet)

Since: 1 week Go Date range Go 2020-04-01 2020-06-10

MITRE ATT&CK Matrix™ (Enterprise) for duration 2020-04-01 -> 2020-06-10

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


FORTINET®
VIRTUAL
SECURITY
DAY