SecurityRisk ADVISORS

EMR Security

Presented by Mike Pinch

November, 2019

Table of Contents

1 Industry Threats

2 Assessing Your EMR Security Program

3 Recommendations

My Background

- **Director at Security Risk Advisors**
- **Other Experience**
  - Chief Information Security Officer – URMC 2012-2018
  - Chief Technology Officer – UR, Palladian Health
  - Medical Device Manufacturer CISO
  - PricewaterhouseCoopers

The Current State

- EMRs are the crown jewels of HDOs today, and often don’t receive dedicated, special attention from cyber security

- Penetration testing often shows not just access to the EMR, but it is often the easiest way to tunnel into the organization and go much deeper

- Basic controls, low hanging fruit, not often implemented

Industry Threats

Threats - Ransomware

- **Significant healthcare uptick again in 2019**
  - Predominantly Windows based systems
  - Workstations, Windows Servers, Windows Databases, Medical Databases

- **First-Ever Statistics on Data Breach Effects on Clinical Care**
  - 2019 Vanderbilt Study Showed the Following:
    - Hospitals that had data breaches showed 36 additional deaths per 10,000 heart attacks
    - https://onlinelibrary.wiley.com/doi/pdf/10.1111/1475-6773.13203

Trends in EMR Security

- Citrix/Virtualization isn’t patched
- Citrix/Virtualization breakout attack preventions aren’t implemented
- Rudimentary alerting of session breakout or tool misuse isn’t in place or integrated into SIEM
- Incident response workflows are not mature to handle clinical and patient safety incidents

Trends in EMR Security

- Privileged access management is weak or absent
- Data warehousing and reporting is over provisioned and under monitored
- Many organizations still aren’t running AV/EDR tools on the EMR
- Multi-Factor Authentication is still inconsistently in place

Quantifying Your Security Readiness

Metrics

- **Hygiene Metrics**
    - How well are your processes and protections configured to protect against compromise? Patches, Vulnerabilities, AV Coverage, Firewalling, etc
- **Hyperbole Metrics (bad)**
    - Noise that says nothing about your real world efficacy
        - Ex: We blocked 3 million attacks last month!
- **Defense Success Metrics (New!)**
    - How well will your system stand up to and respond to actual attacks

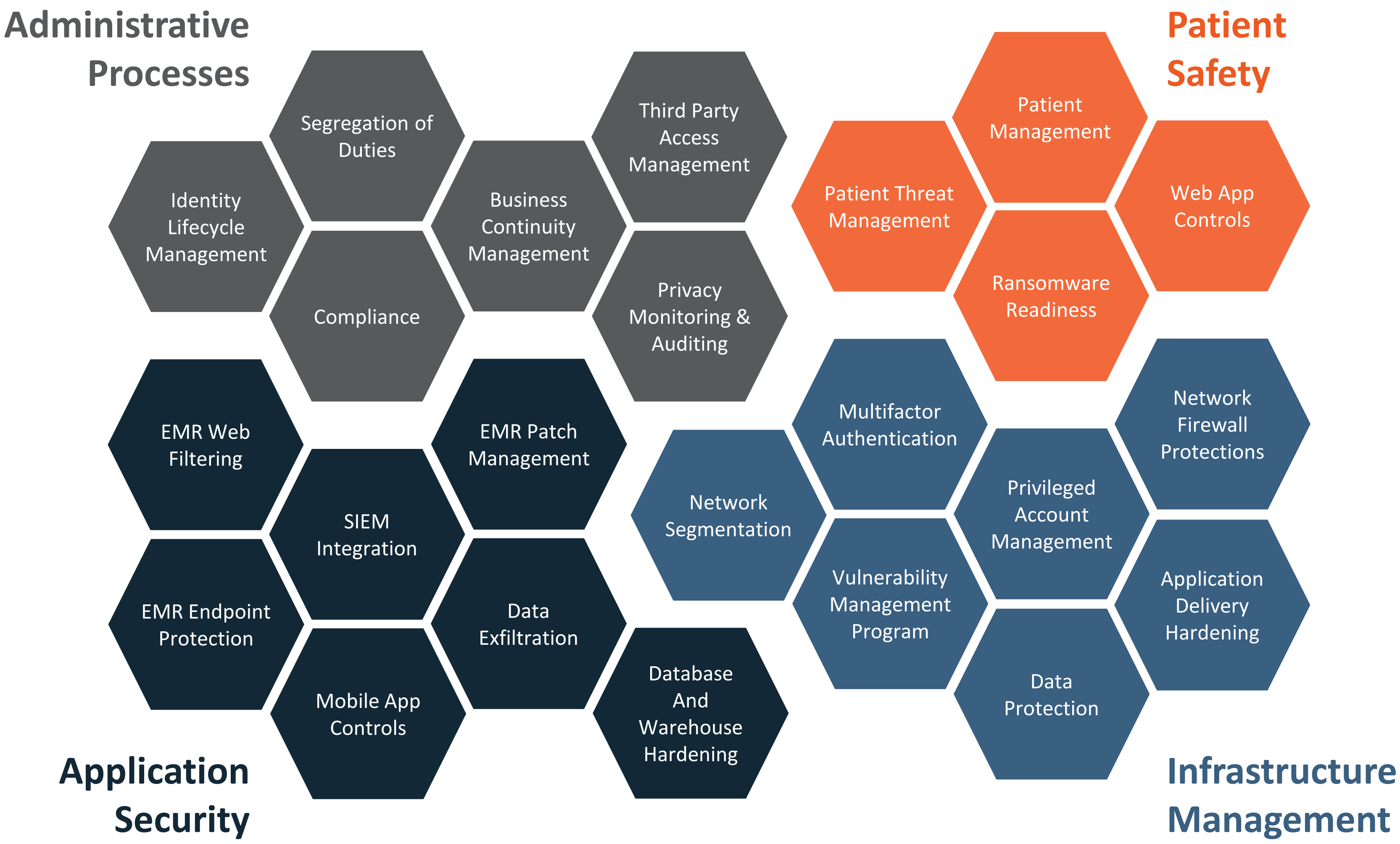
Metrics Takeaways

- **Hyperbole Metrics Bad**
  - At best drown out meaningful metrics, at worst unintentionally misleading
- **Hygiene Good**
  - Preparation against attack
- **Defense Success Metrics Good**
  - Resiliency against attack

Lets Dive Into the Good!

EMR Security Hygiene

EMR Security Program Controls



Administrative Processes
Segregation of Duties
Third Party Access Management
Identity Lifecycle Management
Business Continuity Management
Compliance
Privacy Monitoring & Auditing
Patient Safety
Patient Management
Patient Threat Management
Web App Controls
Ransomware Readiness
EMR Web Filtering
EMR Patch Management
SIEM Integration
EMR Endpoint Protection
Data Exfiltration
Mobile App Controls
Database And Warehouse Hardening
Application Security
Multifactor Authentication
Network Firewall Protections
Network Segmentation
Privileged Account Management
Vulnerability Management Program
Application Delivery Hardening
Data Protection
Infrastructure Management

The “Honeycomb”

The EMR Security Program Controls, “Honeycomb”, diagram is a collection of processes and technical controls that should be implemented to enhance the security of the EMR application. This diagram was created to represent a mature EMR security program for organizations seeking to improve the maturity level of their program.

Each of the controls in this diagram will be evaluated against objective criteria and scored accordingly in subsequent slides. Additional honeycomb visuals will be presented to indicate the current state of each of these tiles with the goal of enabling management to prioritize investments to further protect the EMR environment.

Capability Assessment

Multifactor Authentication

Requiring multifactor authentication (MFA) to access EMR and perform privileged activity within the application will prevent an individual from performing unauthorized activity using compromised credentials.

Infrastructure Management – Multifactor Authentication

Rating	Controls Required	Meets
1 - Initial	Multifactor authentication is required for e-prescribing of controlled substances within EMR.	✓
2 - Baseline	Multifactor authentication required for all remote system access to EMR.	✓
3 - Par	Multifactor authentication required for all third-party connections into the network.	✓
4 - Leader	Multifactor authentication is used for privileged access and administrative functions within hyperspace.	
5 - Innovator	Risk-based authentication is used for all system access.	

Observed Strengths & Recommendations

Observed Strengths

- MFA is required for remote VPN access, Hypervisor’s EPCS function, and the MDM platform

Recommendations

- Information Security should leverage MFA capabilities in the upcoming EMR upgrade for related applications and systems such as MyChart, Haiku and Canto
- Information Security should implement MFA for systems that impact the security of the EMR application such as Active Directory

Capability Assessment

Effective Hyperspace breakout protections are critical to preventing misuse of the application and reduce the likelihood of an attacker being able to access underlying Epic infrastructure.

Hyperspace Breakout Protections

Application Security – Hyperspace Breakout Protections

Rating	Controls Required	Meets
1 - Initial	The organization is unaware of hyperspace breakout attacks and the possible root risks associated with them.	☑
2 - Baseline	The organization has attempted to reduce the likelihood of hyperspace breakouts by setting certain configurations such as sticky keys / accessibility mode to restrict breakouts.	□
3 - Par	The hyperspace environment has been been assessed to eliminate unnecessary underlying software that could provide an attacker the ability to move laterally inside the organization, such as PowerShell, RDP, F12 Developer Tools etc.	□
4 - Leader	The hyperspace environment has been configured to alert upon a successful hyperspace breakout or use of unauthorized software.	□
5 - Innovator	A formal incident response playbook has been defined and tested to identify a successful hyperspace breakout and respond by ending the user session, locking their account, and preserving forensic information from the image to aid in the investigation. Notifications should include a review by clinical leadership to determine if there was any patient risk by the actions of the attacker.	□

Observed Strengths & Recommendations

Observed Strengths

Recommendations

How to Design

- **Combine**
  - Common Security Frameworks (NIST, CIS etc)
  - EMR Infrastructure Inventory
  - Threat Modeling (STRIDE / DREAD)
  - Your technology stack
  - Business Outcomes
  - A maturity framework
    - CMMI
    - Bad, Good, Best

Examining the Full Infrastructure

- **Most testers see EMRs as just the clinicians app… but as you know, its so much more than that:**
  - Financials
  - Patient Portal
  - Patient Mobile App
  - FHIR Interface
  - API Server
  - Printers
  - Database
  - Data Warehouse
  - Business Intelligence
  - Share Drives
  - Domain Administrator Access
  - Host OS
  - Downtime PCs
  - Workstations on Wheels

EMR Security Resiliency

Why EMR Pen Testing?

- **We already have a penetration test performed almost every year…. What's the difference?**
  - Focus – In a traditional penetration test, you have thousands of assets, typically all with their own vulnerabilities. Penetration testing typically finds one (or a couple) ways in, but rarely has the time to focus on specific systems
  - Knowledge – Penetration testing an EMR typically requires deeper knowledge and experience with specific tools, as well as better understanding of clinical workflows to demonstrate effects of compromise
  - Risk – Quite simply, your EMR is likely the center of your clinical Universe. Organizations spend 8, 9, and even 10 figures to implement them, The **impact** factor of risk is extremely **high**
  - Weakness – EMR manufacturers off the shelf security configurations are often very weak and trivially easy to bypass, combined with the fact that they are often exposed on the internet. The **likelihood** factor of risk is extremely **high**

Establishing Safeguards

- **Safe penetration testing is mandatory**
- **Ask about fragile and weak assets**
  - Interface engines, for example, can often create performance or integrity issues if under hard scans or attacks
  - This inquiry phase may actually create your first ‘tabletop’ findings
- **Identify methods for safely testing a production system**
  - Identify and get provisioned access for both production and a non-production system
  - Non-prod needs to be most recent mirror of production and have common security controls employed in application and supporting infrastructure wherever possible
  - Testing performed in production until application access is obtained
  - Shift to non-production instance to demonstrate further attacks; when successful attacks are made, review with management before doing in production

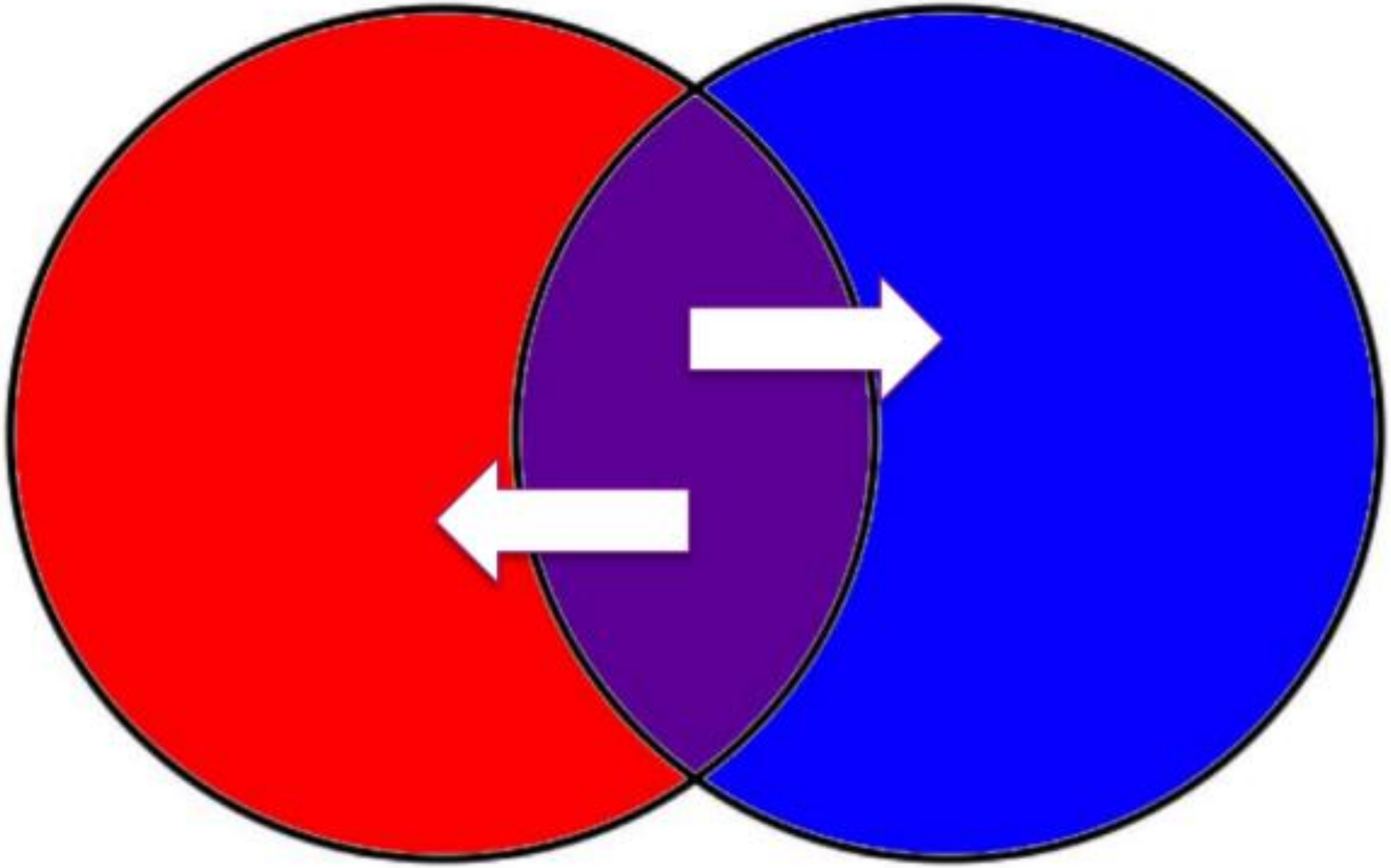
Introducing Purple Teams

- **Purple Teams is *an open-book-exam process that prioritizes and shows <u>quantifiable</u> improvements in defenses over time*.**

- Vulnerability Assessment
- Reconnaissance
- Penetration Testing
- Social Engineering
- Data Exfiltration

- Threat Intelligence
- Incident Response
- Forensics
- Active Monitoring
- Process Improvement

How we make Purple



What is Purple Team Testing?

SecurityRisk ADVISORS

Live, cooperative attack and defense events that focus on collaborative improvement and optimization of prevention, detection, and response

Red team plans an attack that exercises different phases of the kill chain

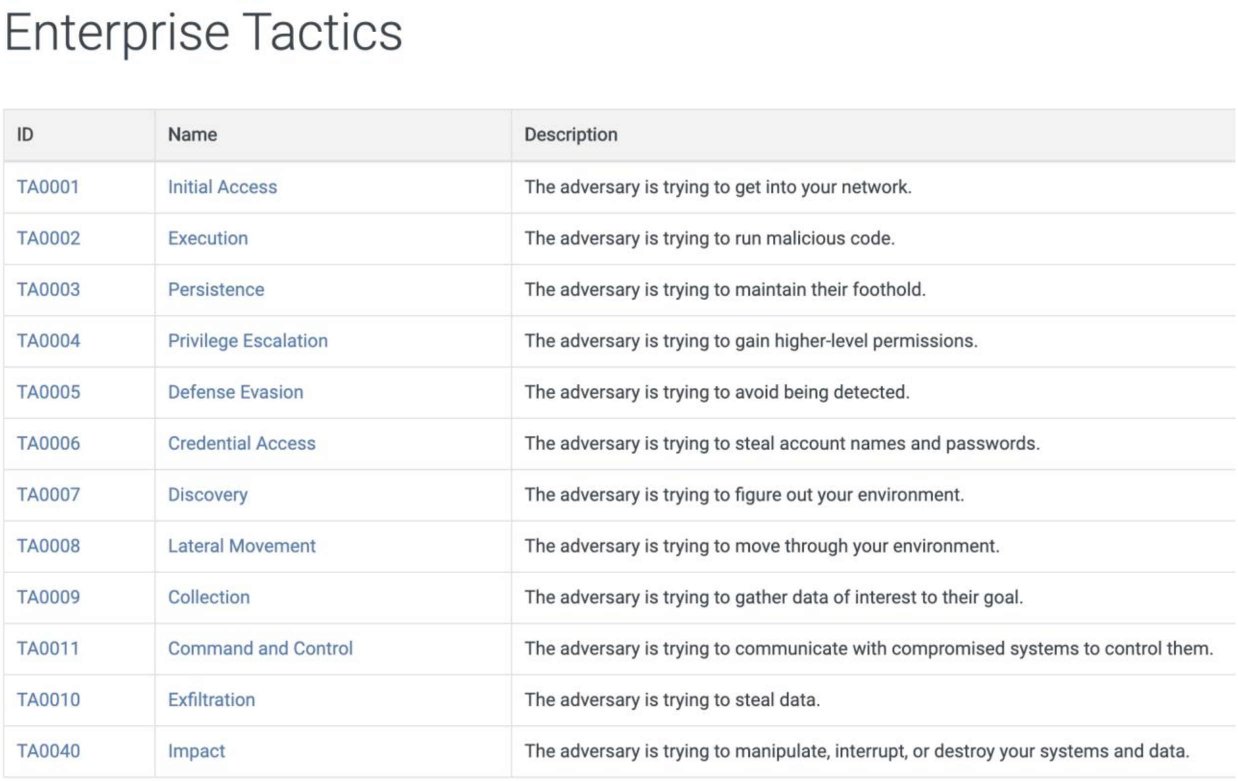
Red team executes attack while announcing / sharing their activities with blue team

Blue team must prevent / detect / respond

- Inability to meet expected outcome creates an action or task to remediate

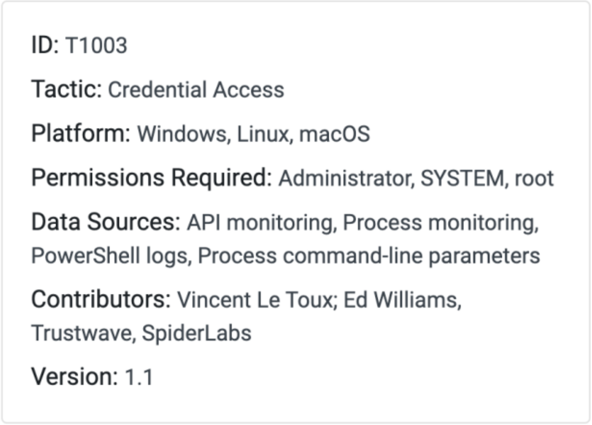
Aligning with MITRE ATT&CK

- **The MITRE ATT&CK Framework is a collection of granular attacker tactics, catalogued in a variety of useful fashions**



Enterprise Tactics

ID	Name	Description
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.



ID: T1003

Tactic: Credential Access

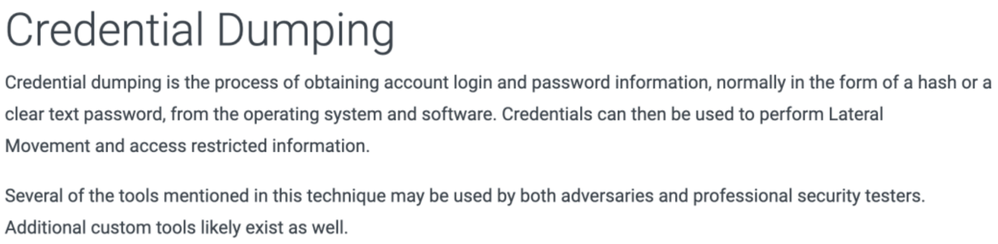
Platform: Windows, Linux, macOS

Permissions Required: Administrator, SYSTEM, root

Data Sources: API monitoring, Process monitoring, PowerShell logs, Process command-line parameters

Contributors: Vincent Le Toux; Ed Williams, Trustwave, SpiderLabs

Version: 1.1



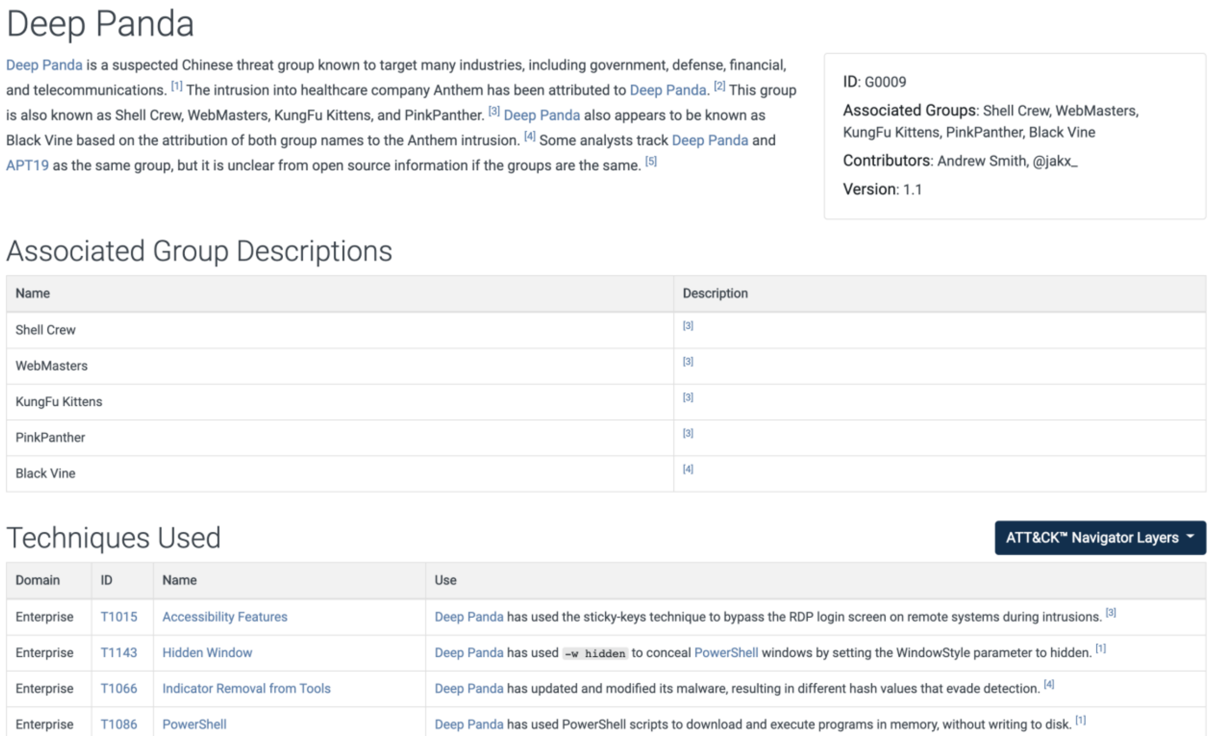
Credential Dumping

Credential dumping is the process of obtaining account login and password information, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information.

Several of the tools mentioned in this technique may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

MITRE Usage

- ATT&CK Framework provides 100s of technical tactics that can be tested to show your overall resilience to attacks
- Tactics can be sorted a number of different ways, including the actual bad guys….



Deep Panda

Deep Panda is a suspected Chinese threat group known to target many industries, including government, defense, financial, and telecommunications. [1] The intrusion into healthcare company Anthem has been attributed to Deep Panda. [2] This group is also known as Shell Crew, WebMasters, KungFu Kittens, and PinkPanther. [3] Deep Panda also appears to be known as Black Vine based on the attribution of both group names to the Anthem intrusion. [4] Some analysts track Deep Panda and APT19 as the same group, but it is unclear from open source information if the groups are the same. [5]

ID: G0009

Associated Groups: Shell Crew, WebMasters, KungFu Kittens, PinkPanther, Black Vine

Contributors: Andrew Smith, @jakx_

Version: 1.1

Associated Group Descriptions

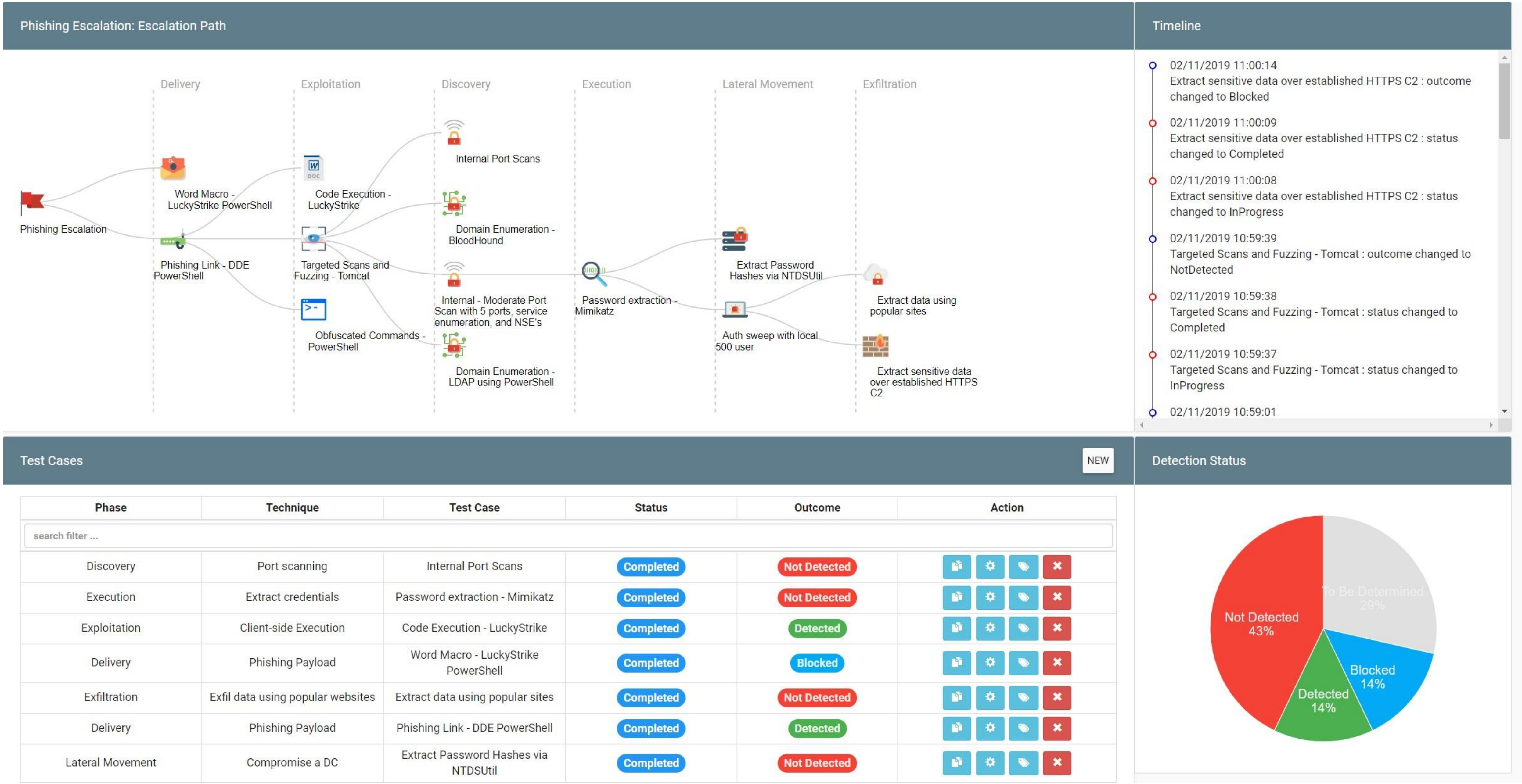
Name	Description
Shell Crew	[3]
WebMasters	[3]
KungFu Kittens	[3]
PinkPanther	[3]
Black Vine	[4]

Techniques Used

Domain	ID	Name	Use
Enterprise	T1015	Accessibility Features	Deep Panda has used the sticky-keys technique to bypass the RDP login screen on remote systems during intrusions. [3]
Enterprise	T1143	Hidden Window	Deep Panda has used `-w hidden` to conceal PowerShell windows by setting the WindowStyle parameter to hidden. [1]
Enterprise	T1066	Indicator Removal from Tools	Deep Panda has updated and modified its malware, resulting in different hash values that evade detection. [4]
Enterprise	T1086	PowerShell	Deep Panda has used PowerShell scripts to download and execute programs in memory, without writing to disk. [1]

Running Purple Teams

- **Start small, simple**
  - ICS Cert Advisory
  - Email Phish
  - Wireless Attack
  - Data Exfiltration – cloud storage
  - Data Loss – Email
  - Virtual Currency Mining
  - Password Spray Attack
  - Permissions Change
  - Excessive Internal Logins
- **VECTR Purple Team Platform for Growth and Metrics**


Phishing Escalation: Escalation Path
Delivery
Exploitation
Discovery
Execution
Lateral Movement
Exfiltration
Phishing Escalation
Word Macro - LuckyStrike PowerShell
Phishing Link - DDE PowerShell
Code Execution - LuckyStrike
Targeted Scans and Fuzzing - Tomcat
Obfuscated Commands - PowerShell
Internal Port Scans
Domain Enumeration - BloodHound
Internal - Moderate Port Scan with 5 ports, service enumeration, and NSE's
Domain Enumeration - LDAP using PowerShell
Password extraction - Mimikatz
Extract Password Hashes via NTDSUtil
Auth sweep with local 500 user
Extract data using popular sites
Extract sensitive data over established HTTPS C2
Timeline

02/11/2019 11:00:14
Extract sensitive data over established HTTPS C2 : outcome changed to Blocked

02/11/2019 11:00:09
Extract sensitive data over established HTTPS C2 : status changed to Completed

02/11/2019 11:00:08
Extract sensitive data over established HTTPS C2 : status changed to InProgress

02/11/2019 10:59:39
Targeted Scans and Fuzzing - Tomcat : outcome changed to NotDetected

02/11/2019 10:59:38
Targeted Scans and Fuzzing - Tomcat : status changed to Completed

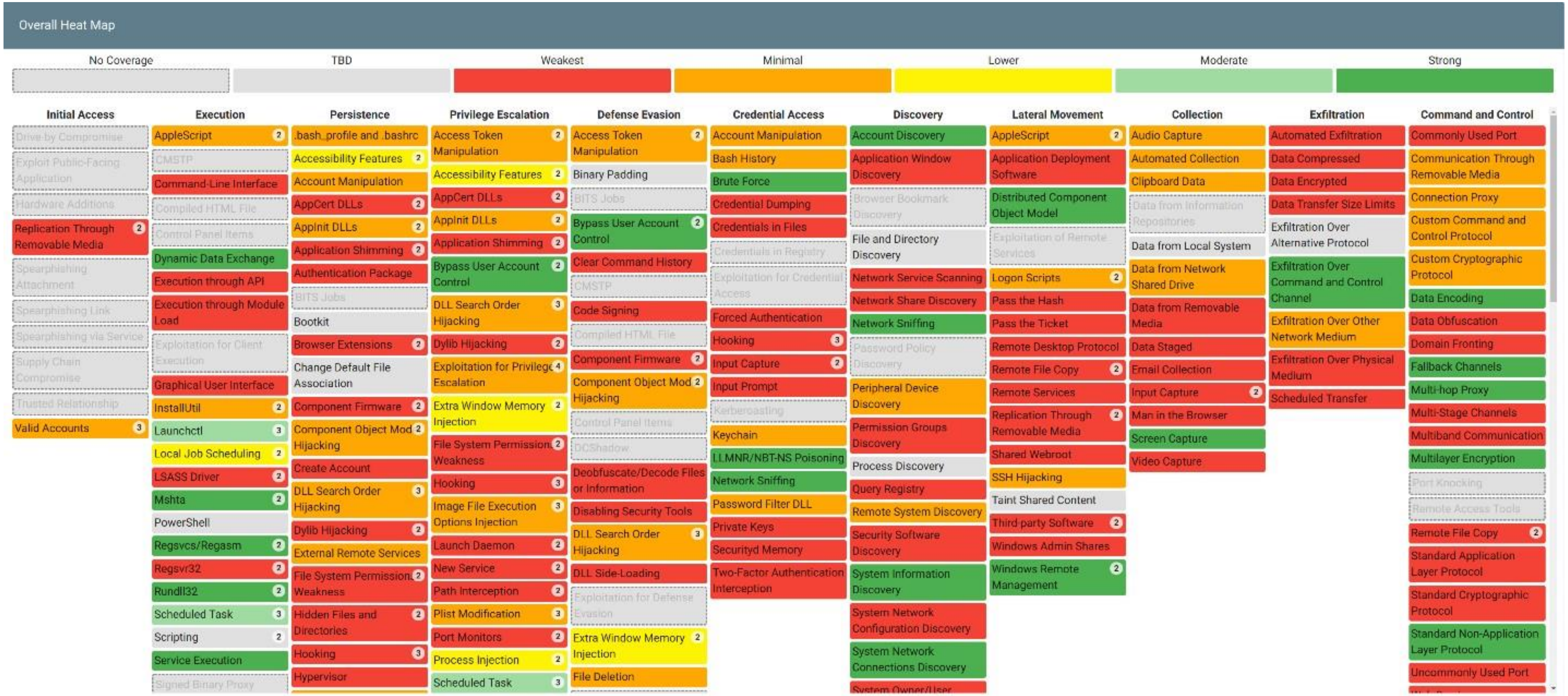
02/11/2019 10:59:37
Targeted Scans and Fuzzing - Tomcat : status changed to InProgress

02/11/2019 10:59:01

search filter ...

Phase	Technique	Test Case	Status	Outcome	Action
Discovery	Port scanning	Internal Port Scans	Completed	Not Detected	⧉ ⚙ 🏷 ✖
Execution	Extract credentials	Password extraction - Mimikatz	Completed	Not Detected	⧉ ⚙ 🏷 ✖
Exploitation	Client-side Execution	Code Execution - LuckyStrike	Completed	Detected	⧉ ⚙ 🏷 ✖
Delivery	Phishing Payload	Word Macro - LuckyStrike PowerShell	Completed	Blocked	⧉ ⚙ 🏷 ✖
Exfiltration	Exfil data using popular websites	Extract data using popular sites	Completed	Not Detected	⧉ ⚙ 🏷 ✖
Delivery	Phishing Payload	Phishing Link - DDE PowerShell	Completed	Detected	⧉ ⚙ 🏷 ✖
Lateral Movement	Compromise a DC	Extract Password Hashes via NTDSUtil	Completed	Not Detected	⧉ ⚙ 🏷 ✖

https://vectr.io



Overall Heat Map

No Coverage	TBD	Weakest	Minimal	Lower	Moderate	Strong
⬚	⬜	🟥	🟧	🟨	▧	🟩

Initial Access

- ⬚ Drive-by Compromise
- ⬚ Exploit Public-Facing Application
- ⬚ Hardware Additions
- 🟥 Replication Through Removable Media 2
- ⬚ Spearphishing Attachment
- ⬚ Spearphishing Link
- ⬚ Spearphishing via Service
- ⬚ Supply Chain Compromise
- ⬚ Trusted Relationship
- 🟧 Valid Accounts 3

Execution

- 🟧 AppleScript 2
- ⬚ CMSTP
- 🟥 Command-Line Interface
- ⬚ Compiled HTML File
- ⬚ Control Panel Items
- 🟩 Dynamic Data Exchange
- 🟥 Execution through API
- 🟥 Execution through Module Load
- ⬚ Exploitation for Client Execution
- 🟥 Graphical User Interface
- 🟧 InstallUtil 2
- ▧ Launchctl 3
- 🟨 Local Job Scheduling 2
- 🟥 LSASS Driver 2
- 🟩 Mshta 2
- ⬜ PowerShell
- 🟩 Regsvcs/Regasm 2
- 🟥 Regsvr32 2
- 🟩 Rundll32 2
- ▧ Scheduled Task 3
- ⬜ Scripting 2
- 🟩 Service Execution
- ⬚ Signed Binary Proxy

Persistence

- 🟧 .bash_profile and .bashrc
- 🟨 Accessibility Features 2
- 🟧 Account Manipulation
- 🟥 AppCert DLLs 2
- 🟧 AppInit DLLs 2
- 🟥 Application Shimming 2
- 🟥 Authentication Package
- ⬚ BITS Jobs
- ⬜ Bootkit
- 🟥 Browser Extensions 2
- ⬜ Change Default File Association
- 🟥 Component Firmware 2
- 🟧 Component Object Mod Hijacking 2
- 🟥 Create Account
- 🟧 DLL Search Order Hijacking 3
- 🟥 Dylib Hijacking 2
- 🟧 External Remote Services
- 🟥 File System Permission Weakness 2
- 🟥 Hidden Files and Directories 2
- 🟥 Hooking 3
- 🟥 Hypervisor

Privilege Escalation

- 🟧 Access Token Manipulation 2
- 🟨 Accessibility Features 2
- 🟥 AppCert DLLs 2
- 🟧 AppInit DLLs 2
- 🟥 Application Shimming 2
- 🟩 Bypass User Account Control 2
- 🟧 DLL Search Order Hijacking 3
- 🟥 Dylib Hijacking 2
- 🟧 Exploitation for Privilege Escalation 4
- 🟨 Extra Window Memory Injection 2
- 🟥 File System Permission Weakness 2
- 🟥 Hooking 3
- 🟧 Image File Execution Options Injection 3
- 🟥 Launch Daemon 2
- 🟥 New Service 2
- 🟥 Path Interception 2
- 🟧 Plist Modification 3
- 🟥 Port Monitors 2
- 🟨 Process Injection 2
- ▧ Scheduled Task 3

Defense Evasion

- 🟧 Access Token Manipulation 2
- ⬜ Binary Padding
- ⬚ BITS Jobs
- 🟩 Bypass User Account Control 2
- 🟥 Clear Command History
- ⬚ CMSTP
- 🟥 Code Signing
- ⬚ Compiled HTML File
- 🟥 Component Firmware 2
- 🟧 Component Object Mod Hijacking 2
- ⬚ Control Panel Items
- ⬚ DCShadow
- 🟥 Deobfuscate/Decode Files or Information
- 🟥 Disabling Security Tools
- 🟧 DLL Search Order Hijacking 3
- 🟥 DLL Side-Loading
- ⬚ Exploitation for Defense Evasion
- 🟨 Extra Window Memory Injection 2
- 🟧 File Deletion

Credential Access

- 🟧 Account Manipulation
- 🟧 Bash History
- 🟩 Brute Force
- 🟥 Credential Dumping
- 🟥 Credentials in Files
- ⬚ Credentials in Registry
- ⬚ Exploitation for Credential Access
- 🟥 Forced Authentication
- 🟥 Hooking 3
- 🟥 Input Capture 2
- 🟥 Input Prompt
- ⬚ Kerberoasting
- 🟧 Keychain
- 🟩 LLMNR/NBT-NS Poisoning
- 🟩 Network Sniffing
- 🟧 Password Filter DLL
- 🟥 Private Keys
- 🟥 Securityd Memory
- 🟥 Two-Factor Authentication Interception

Discovery

- 🟩 Account Discovery
- 🟥 Application Window Discovery
- ⬚ Browser Bookmark Discovery
- ⬜ File and Directory Discovery
- 🟥 Network Service Scanning
- 🟥 Network Share Discovery
- 🟩 Network Sniffing
- ⬚ Password Policy Discovery
- 🟧 Peripheral Device Discovery
- 🟥 Permission Groups Discovery
- ⬜ Process Discovery
- 🟥 Query Registry
- 🟧 Remote System Discovery
- 🟥 Security Software Discovery
- 🟩 System Information Discovery
- 🟥 System Network Configuration Discovery
- 🟩 System Network Connections Discovery
- 🟥 System Owner/User

Lateral Movement

- 🟧 AppleScript 2
- 🟥 Application Deployment Software
- 🟩 Distributed Component Object Model
- ⬚ Exploitation of Remote Services
- 🟧 Logon Scripts 2
- 🟥 Pass the Hash
- 🟥 Pass the Ticket
- 🟥 Remote Desktop Protocol
- 🟥 Remote File Copy 2
- 🟥 Remote Services
- 🟥 Replication Through Removable Media 2
- 🟥 Shared Webroot
- 🟧 SSH Hijacking
- ⬜ Taint Shared Content
- 🟥 Third-party Software 2
- 🟥 Windows Admin Shares
- 🟩 Windows Remote Management 2

Collection

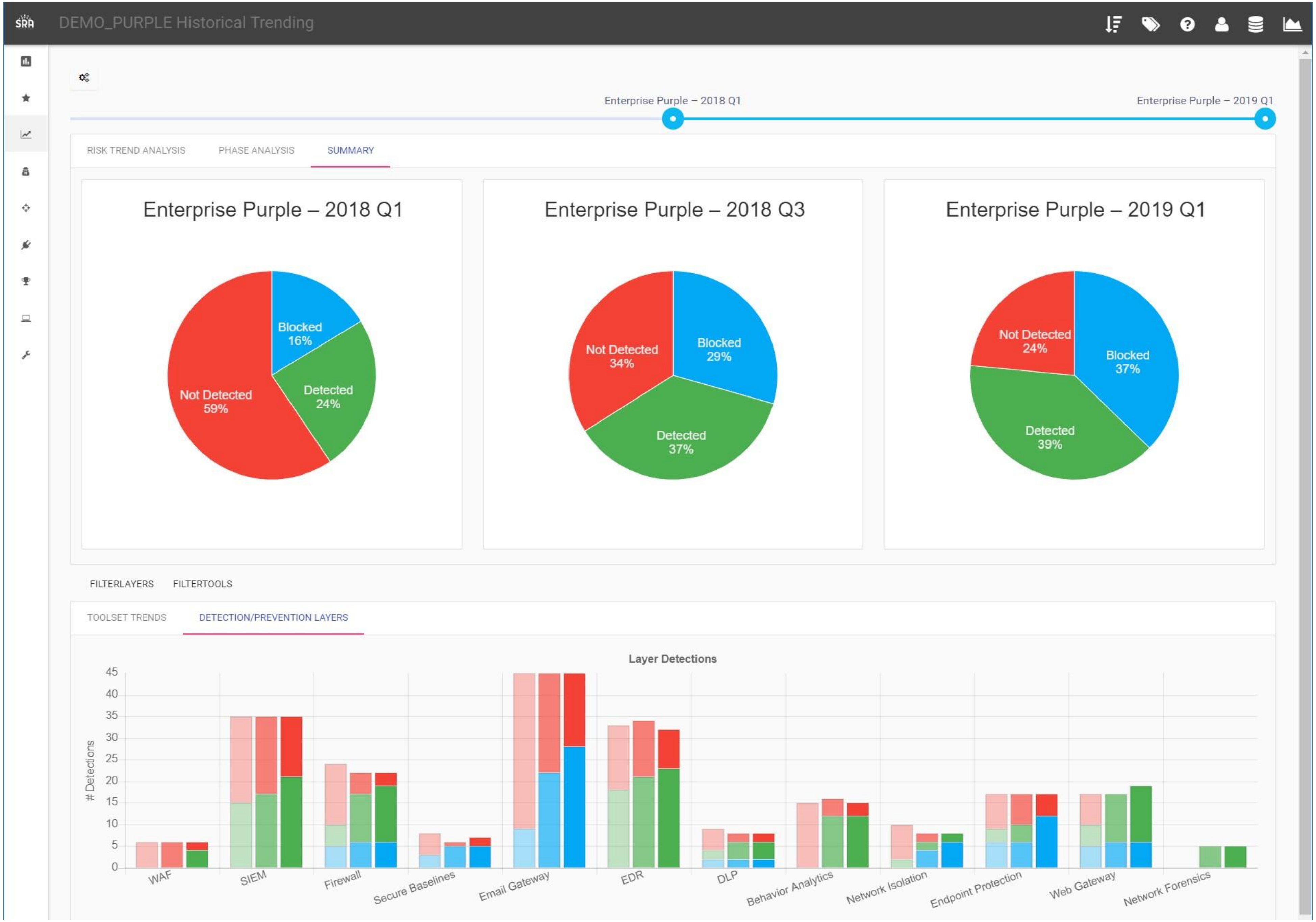
- 🟧 Audio Capture
- 🟧 Automated Collection
- 🟧 Clipboard Data
- ⬚ Data from Information Repositories
- ⬜ Data from Local System
- 🟧 Data from Network Shared Drive
- 🟥 Data from Removable Media
- 🟥 Data Staged
- 🟥 Email Collection
- 🟥 Input Capture 2
- 🟥 Man in the Browser
- 🟩 Screen Capture
- 🟥 Video Capture

Exfiltration

- 🟥 Automated Exfiltration
- 🟥 Data Compressed
- 🟥 Data Encrypted
- 🟥 Data Transfer Size Limits
- ⬜ Exfiltration Over Alternative Protocol
- 🟩 Exfiltration Over Command and Control Channel
- 🟧 Exfiltration Over Other Network Medium
- 🟥 Exfiltration Over Physical Medium
- 🟥 Scheduled Transfer

Command and Control

- 🟥 Commonly Used Port
- 🟧 Communication Through Removable Media
- 🟧 Connection Proxy
- 🟧 Custom Command and Control Protocol
- 🟧 Custom Cryptographic Protocol
- 🟩 Data Encoding
- 🟥 Data Obfuscation
- 🟥 Domain Fronting
- 🟩 Fallback Channels
- 🟩 Multi-hop Proxy
- 🟥 Multi-Stage Channels
- 🟥 Multiband Communication
- 🟩 Multilayer Encryption
- ⬚ Port Knocking
- ⬚ Remote Access Tools
- 🟥 Remote File Copy 2
- 🟥 Standard Application Layer Protocol
- 🟥 Standard Cryptographic Protocol
- 🟩 Standard Non-Application Layer Protocol
- 🟥 Uncommonly Used Port


DEMO_PURPLE Historical Trending
Enterprise Purple – 2018 Q1
Enterprise Purple – 2019 Q1
RISK TREND ANALYSIS
PHASE ANALYSIS
SUMMARY
Enterprise Purple – 2018 Q1
Blocked 16%
Detected 24%
Not Detected 59%
Enterprise Purple – 2018 Q3
Blocked 29%
Detected 37%
Not Detected 34%
Enterprise Purple – 2019 Q1
Blocked 37%
Detected 39%
Not Detected 24%
FILTERLAYERS
FILTERTOOLS
TOOLSET TRENDS
DETECTION/PREVENTION LAYERS
Layer Detections
# Detections
0
5
10
15
20
25
30
35
40
45
WAF
SIEM
Firewall
Secure Baselines
Email Gateway
EDR
DLP
Behavior Analytics
Network Isolation
Endpoint Protection
Web Gateway
Network Forensics

Recommendations

Tabletop Exercises

SecurityRisk ADVISORS

- Tabletop exercises (TTX) are some of the best exercises to simulate events and get better at soft skills
- Focus on small, relevant scenarios
- Start “left of boom”, early stages of attack to think through communication and escalation
- Take notes, make improvements

Backup Security

- Your most critical security control for ransomware
- If your backup systems run on Windows and are bound to your domain; be very afraid!
- Conduct dedicated hardening projects; multi-factor auth, configuration change alerts, consider removing remote logons
- Don’t disregard the value of tape/offline backups

HIPAA Risk Analysis

- You NEED to do this every year
- Don’t just focus on assessing controls
- Include
  - ePHI Inventory
  - Mapping your controls to HIPAA
  - How you address “addressable” controls
  - Risk quantification (impact * likelihood)
  - Current Industry Threats
  - Risk Management Plan

Multi-Factor Authentication

- You NEED this everywhere….
- EVERY external facing authentication source
  - VPN
  - EMR
  - Email
- For everyone, no exceptions

Privileged Access Management

- Nearly every successful attack campaign compromises domain administrator credentials
- Make local administrator password one-time use & strong with MS LAPS (free)
- Make one time use passwords for domain admin accounts, use privileged account management tools ($)
- 2 Factor Authentication on servers is a red-herring – there are other ways in!

Summary

- **We’ve turned a corner and can now correlate patient safety and security**
- **Consider a dedicated focus to customize markers and metrics around your EMR program**
    - Communicate at the board level, show progress and growth
- **Dedicated Pen Testing is great, Purple is better**
    - DIY can be highly effective to get started
- **Drop metrics that don’t matter**
- **Focus on the most critical items**
    - Multifactor Authentication
    - Privileged Access Management
    - Tabletop Exercises

Questions?

Mike.Pinch@SecurityRiskAdvisors.com

Resources

- Purple Team Platform – https://vectr.io
- Purple Team Approach - https://securityriskadvisors.com/blog/purple-teams-and-defense-success-metrics/
- DIY Red Teaming - https://atomicredteam.io/
- Vanderbilt Study - https://onlinelibrary.wiley.com/doi/pdf/10.1111/1475-6773.13203