Anatomy of an Attack

Jay Mar-Tang – CISSP

Senior Solution Engineer – West Coast

Why this session?

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

– Sun Tzu, The Art of War

CYBERARK

The “Community’ of Attackers

Criminals

Petty criminals

Unsophisticated

Organized crime

Organized, sophisticated supply chains (PII, financial services, retail)

Non-state actors

Terrorists

PII, Government, critical infrastructure

Anti-establishment vigilantes

“Hacktivists” Targets of opportunity

Nation states

PII, government, defense industrial base, IP rich organizations

CYBERARK

Phases of the Intrusion Kill Chain

Intrusion Kill Chain Applied

Recon	Understand RSA (People & Technology), Identify Targets & lateral movement, SecurID knowledge
Weaponization	Package 0-day Flash Exploit in Excel
Delivery	Phishing Email
Exploitation	Exploit Flash process
Installation	Installed Poison Ivy RAT
C2	*.mincesur.com, *.hopto.org, *.cz88.net
Act on Objectives	Lateral Movement & FTP exfil with split .rar

CYBERARK

Security Practices – Critical Checklist

Business Risk Assessment

Identify most critical systems; ensure they are given the highest priorities for all hardening and monitoring activities

Active Directory Hardening

Minimize number of admins
Monitoring and alerting (Windows Event ID #566)
Two factor admin access from hardened VDI platform
Executable whitelisting on hardened DCs
Disable default account and rename key accounts
Complex passwords (9 & 15 Char)

Infrastructure & Logging

Full and detailed logging & analysis
Tighten VPN controls
Increase controls on crypto keys
Full packet capture at strategic network locations
Network segmentation
Team trained and focused on APT activity

Service Accounts

Review accounts for privilege creep
Change passwords frequently
Do not embed credentials into scripts
Minimize interactive login
Restrict login only from required hosts

Web Access

Block access to high risk and web filter categories
Click through on medium risk websites
Black hole dynamic DNS domains
Authenticated internet access
DNS traffic analysis

User Education

Increase security training for IT
Launch security improvement initiative
Regular education of users on phishing attacks
Regular education on social engineering
Increase mail filtering controls

User Machine Hardening

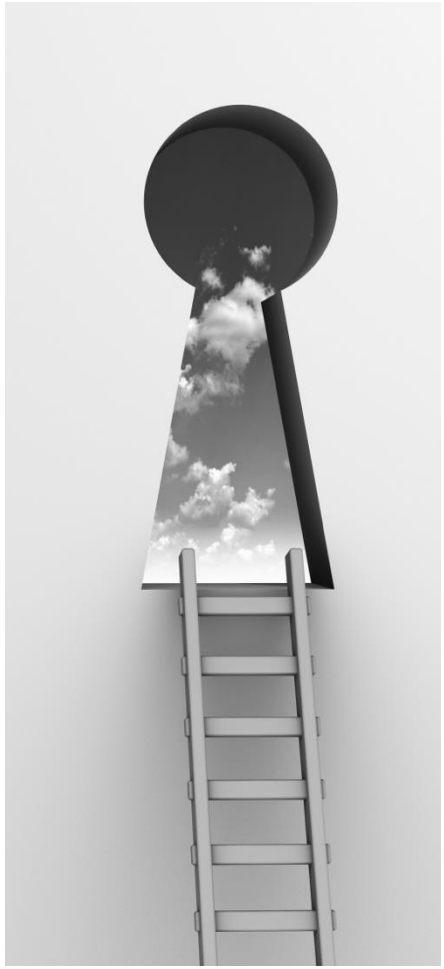
Limit local admin and randomize PW- change often
Increase patching regime
Enable security controls in applications
Deep visibility to identify lateral movement
Limit use of non-authorized software

Business Risk Assessments

- The first line of defense
  - Understanding the business is the first priority in securing it
  - Understand the data that you use
  - Understand the systems that house and protect that data
  - Understand the weaknesses in those systems and processes
  - Understand who wants this data
- Move beyond compliance

CYBERARK

Active Directory Hardening



- IT Admins never cede privilege
  - Rein them in for their safety!
  - Understand the weak link
- Harden DC & access to it
  - Proxy/Jump Server Access
  - Whitelisting
  - Change defaults (passwords/accounts)
- Disguise Labeling in AD
  - AD, great for employees and attackers!
  - Opportunity for simple honeypot

Machine & Network Hardening

- Pull the plug on local admin access
- 0-Day Detection ≠ AT Tool
- Whitelisting Applications
- Boost end user controls
  - VPN endpoints/concentrators
  - Crypto keys
- VDI is a GREAT solution for this!
  - And solves BYOD concerns
  - Think about Hollywood's depiction!
- Network segmentation with ACLs

CYBERARK

Comprehensive Visibility

- Full log capture capabilities
  - And analysis across all of it!
- Boosted visibility across the gamut
  - Devices
  - Networks
  - Sessions
- Full packet capture at key network locations
- Team focused on AT

CYBERARK

Service Accounts

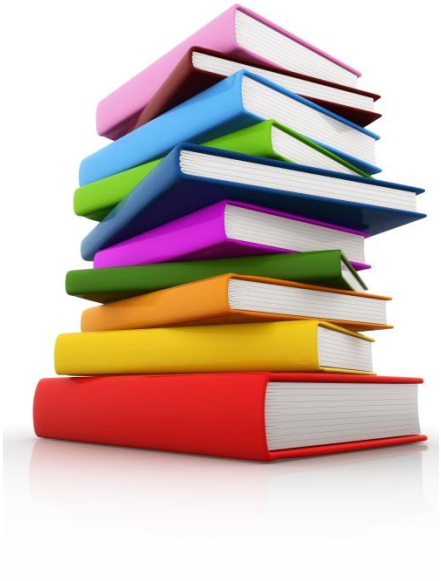
- Watch out for developers!
  - We’re crafty individuals
  - And we’re under tons of pressure
- Review accounts for privilege creep
- Fix authentication
  - Don’t embed credentials in code
  - Don’t even use passwords (use SSH/SSL)
  - Don’t allow interactive login
- Restrict login from required hosts

CYBERARK

Web Access

- Turn up filtering and blocking!
- Allow some access to medium risk:
  - Facebook/Social Media
- DNS
  - Use a black hole!
  - Analyze for indicators of compromise
- Authenticate all internet access
  - And watch your access go down!
- Can we push personal traffic to iOS?

Education



- Board-level expectation setting is crucial
- You can’t train the effects of ATs away
- Take education seriously
  - Reach out to users on the WHY
  - Have security professionals learn how business users engage with systems
  - Train on social eng./phish your employees
- Increase mail filtering
  - But in smart ways!
  - Block .exe? No problem, I will Gmail!

CYBERARK

Security Practices – Critical Checklist

Business Risk Assessment

Identify most critical systems; ensure they are given the highest priorities for all hardening and monitoring activities

Active Directory Hardening

Minimize number of admins
Monitoring and alerting (Windows Event ID #566)
Two factor admin access from hardened VDI platform
Executable whitelisting on hardened DCs
Disable default account and rename key accounts
Complex passwords (9 & 15 Char)

Infrastructure & Logging

Full and detailed logging & analysis
Tighten VPN controls
Increase controls on crypto keys
Full packet capture at strategic network locations
Network segmentation
Team trained and focused on APT activity

Service Accounts

Review accounts for privilege creep
Change passwords frequently
Do not embed credentials into scripts
Minimize interactive login
Restrict login only from required hosts

Web Access

Block access to high risk and web filter categories
Click through on medium risk websites
Black hole dynamic DNS domains
Authenticated internet access
DNS traffic analysis

User Education

Increase security training for IT
Launch security improvement initiative
Regular education of users on phishing attacks
Regular education on social engineering
Increase mail filtering controls

User Machine Hardening

Limit local admin and randomize PW- change often
Increase patching regime
Enable security controls in applications
Deep visibility to identify lateral movement
Limit use of non-authorized software