

# Hunting for Indicators of Compromise

Lucas Zaichkowsky  
Mandiant

Security in  
knowledge



# Agenda

Threat brief

Defensive strategy overview

Hunting for Indicators of Compromise

Live incident response

# — Question 1

When an **AV alert triggers on a host**, what do you do?

- Re-image the system
- Run multiple AV products
- Other



## Question 2

What question are you more interested in answering:

- Can a **pen-tester** get in?
- Is an **attacker** already in?



## Question 3

Is it possible to **stop** a determined attacker?

- **Yes**
- **No**



# We Have a Problem

## Nuisance

### Attacks are Opportunistic

You are targeted because you are vulnerable



## Insiders

### Trusted Insider Steals Data

Difficult to prevent, but attribution is possible



## Hackers

### Motivated by a Cause

Determined, but not always sophisticated



## Financial Criminals

### More Sophisticated Attacks

Typically target information for financial gain



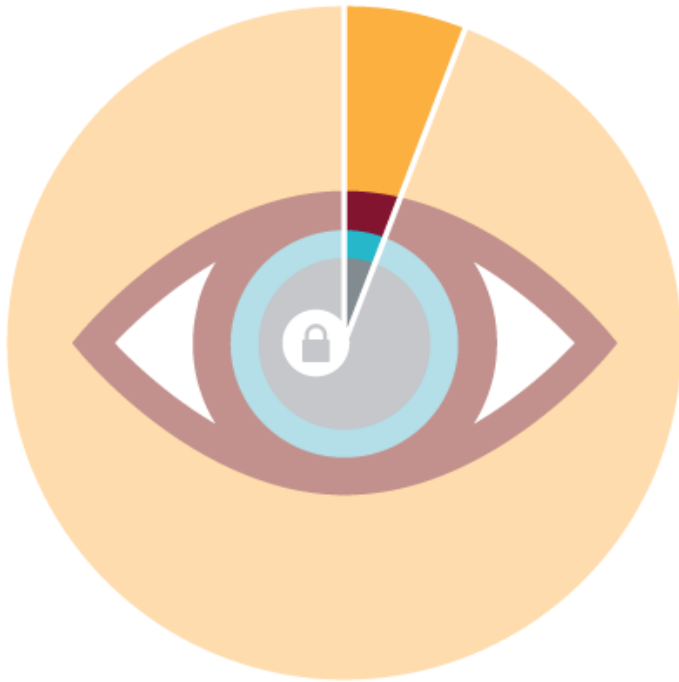
## State-Sponsored

### Persistent and Targeted

Attacks continue until targeted data is obtained



# Self-Detection Is Rare



▶ **6% Self-Detection**



• **94% External Entity**

Source: "M-Trends™ 2012: An Evolving Threat", Mandiant, 27 Feb 2012

<http://www.mandiant.com/resources/m-trends/>

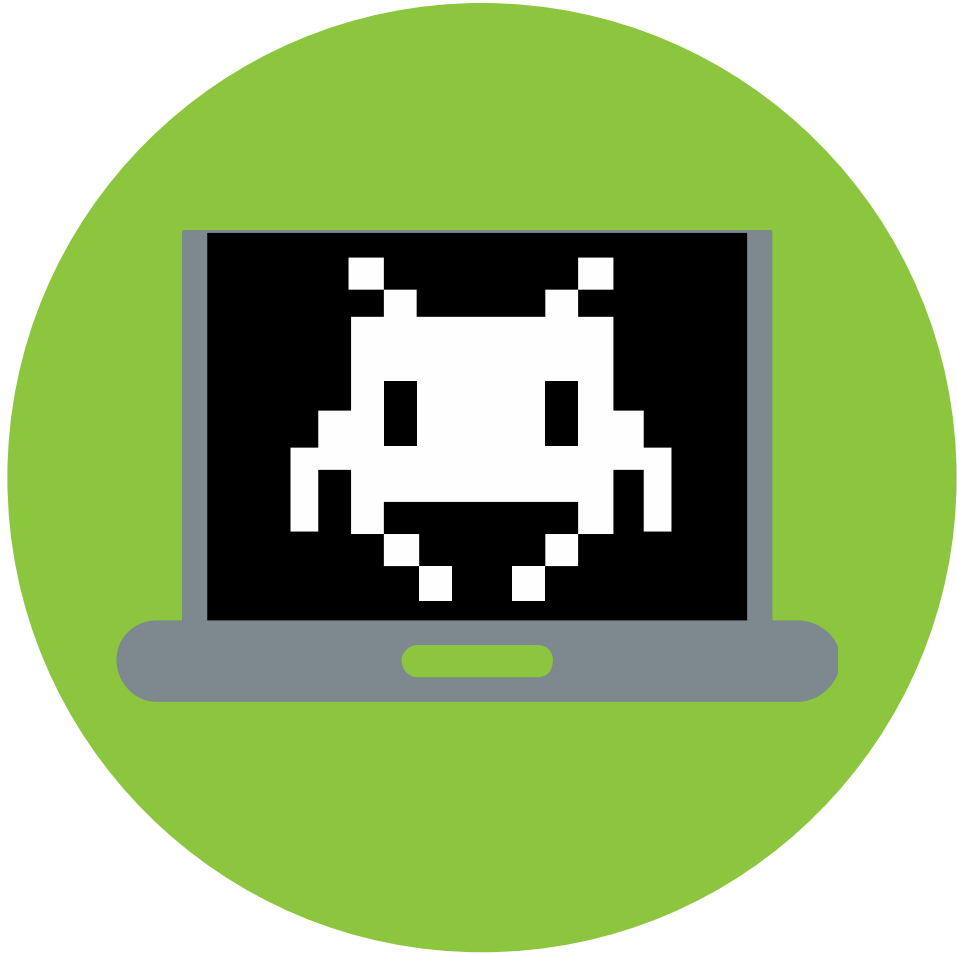
# Detection Time: 416 Days



Source: "M-Trends™ 2012: An Evolving Threat", Mandiant, 27 Feb 2012  
<http://www.mandiant.com/resources/m-trends/>



# Anti-Virus Software Updated



100%

Source: <http://www.mandiant.com/threat-landscape/>

# Attackers Used Valid Accounts



100%

Source: "M-Trends™ 2012: An Evolving Threat", Mandiant, 27 Feb 2012  
<http://www.mandiant.com/resources/m-trends/>

# How do breaches occur?

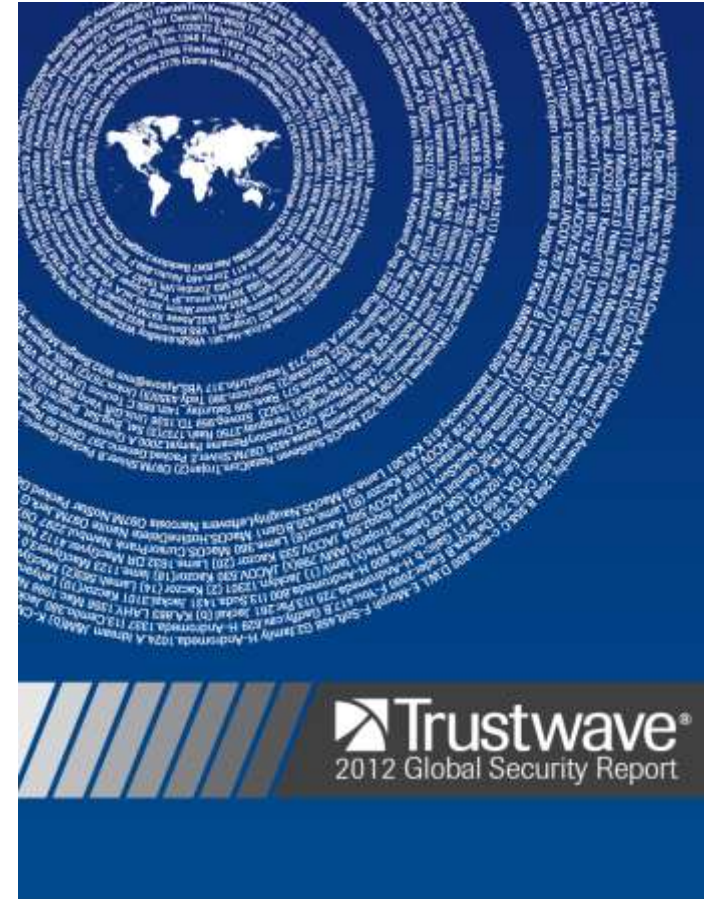
- 81% Utilized some form of hacking
- 69% Incorporated malware
- 10% Involved physical attacks
- 7% Employed social tactics
- 5% Resulted from privilege misuse



Source: "2012 Data Breach Investigations Report",  
Verizon, 29 Mar 2012  
<http://www.verizonbusiness.com/about/events/2012dbir/>

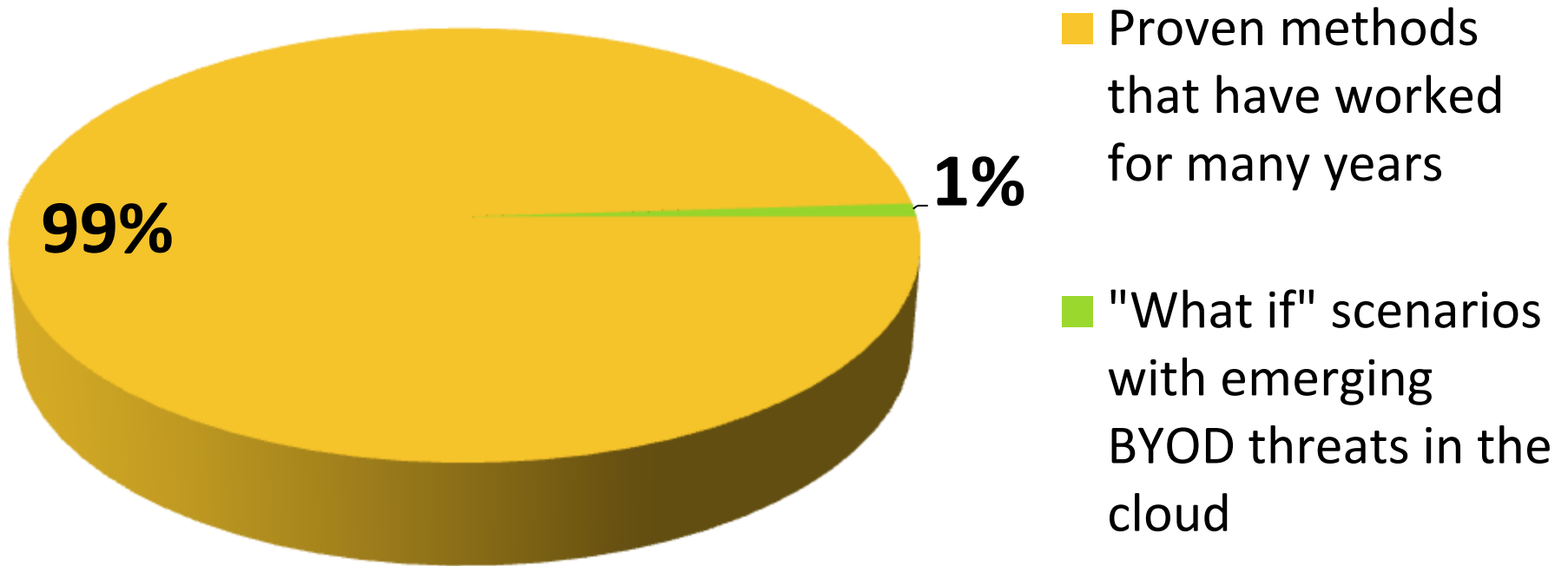
# Top three methods of propagation

- 80% Use of weak administrative credentials
- 15% Default hidden administrative shares
- 5% Remote access solution credential caching



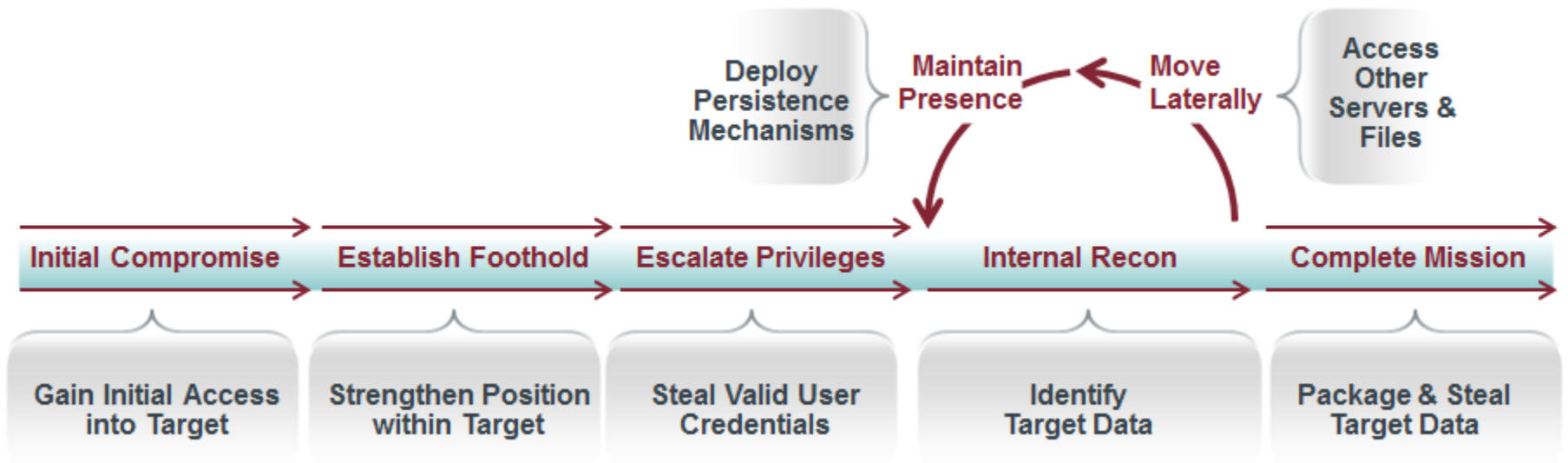
Source: "2012 Global Security Report", Trustwave, 7 Feb 2012  
<https://www.trustwave.com/global-security-report>

# How Orgs Are Compromised



# Anatomy of an Attack

Attackers move methodically from system to system. They take steps along the way to ensure ongoing access.





# Attack Demonstration

# Why the Attackers Are Winning

**Most organizations are unprepared to detect and respond to targeted intrusions.**

**Pervasive failures:**

- Traditional defenses do not work
- Security tunnel vision on vulnerabilities & preventing victim zero
- Underdeveloped IR processes
- Human resource commitment





# — WARNING

## ▶ **Stopping malware and 0-days is not a cure**

- Attackers are not malware
- 0-day exploits are typically reserved for organizations that excel at vulnerability and patch management.

## ▶ **No product can stop innovative human attackers**

- In 1996, IBM Deep Blue beat Garry Kasparov at chess in the first game of a series in Philadelphia **BUT...**
  - ...Kasparov rebounded to claim the rest of the series fairly easily.
- Products are governed by a set of rules, attackers are not
- Attackers evolve as the need arises, altering tactics and increasing levels of sophistication

# Technology Company

30,000 TOTAL SYSTEMS

63 COMPROMISED SYSTEMS

**12 SYSTEMS HAD HACKING TOOLS OR BACKDOORS**

QTY	TYPE OF BACKDOOR OR UTILITY
-----	-----------------------------

3	Proprietary only
---	------------------

9	Poison Ivy (Active Backdoor)
---	------------------------------

6	Windows Credential Editor (Credential Stealer)
---	--

9	Psexec (Admin Tool)
---	---------------------

**51 SYSTEMS HAD NO HACKING TOOLS OR BACKDOORS**

Source: "M-Trends™ 2012: An Evolving Threat", Mandiant, 27 Feb 2012  
<http://www.mandiant.com/resources/m-trends/>

# High Tech Defense

6,000 TOTAL SYSTEMS

102 COMPROMISED SYSTEMS

## 56 SYSTEMS HAD HACKING TOOLS OR BACKDOORS

QTY	TYPE OF BACKDOOR OR UTILITY
-----	-----------------------------

16	Proprietary only
----	------------------

18	Gh0st (Active Backdoor)
----	-------------------------

3	ASPXSpy (Passive Backdoor)
---	----------------------------

7	GetHashes (Credential Stealer)
---	--------------------------------

12	Psexec (Admin Tool)
----	---------------------

## 46 SYSTEMS HAD NO HACKING TOOLS OR BACKDOORS

Source: "M-Trends™ 2012: An Evolving Threat", Mandiant, 27 Feb 2012  
<http://www.mandiant.com/resources/m-trends/>

# Financial Company

30,000 TOTAL SYSTEMS

63 COMPROMISED SYSTEMS

**12 SYSTEMS HAD HACKING TOOLS OR BACKDOORS**

QTY	TYPE OF BACKDOOR OR UTILITY
-----	-----------------------------

3	Proprietary only
---	------------------

9	Poison Ivy (Active Backdoor)
---	------------------------------

6	Windows Credential Editor (Credential Stealer)
---	--

9	Psexec (Admin Tool)
---	---------------------

**51 SYSTEMS HAD NO HACKING TOOLS OR BACKDOORS**

Source: "M-Trends™ 2012: An Evolving Threat", Mandiant, 27 Feb 2012  
<http://www.mandiant.com/resources/m-trends/>

# There Is Hope





# Defense Against the Dark Arts

# Detection and Response

Hunting for Indicators of Compromise (IOCs) is an effective way to combat advanced attackers.

## Secret Formula:

1. Document attacker tools and methodology (a.k.a. intelligence)
2. Use the intelligence to proactively hunt for attacker activity
3. Investigate incidents to increase intelligence & scope compromise
4. Remediate
5. Lather, rinse, repeat



# Step 1: Document Intelligence

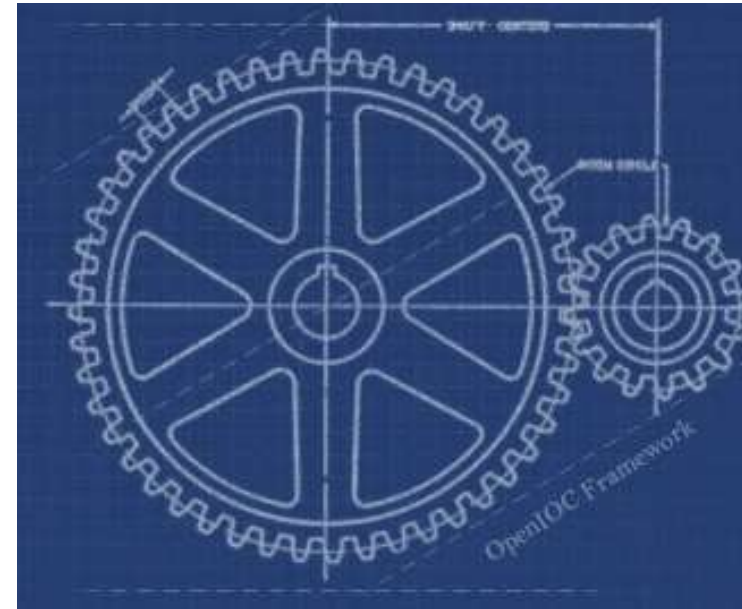
- ▶ Red and white stripes
- ▶ Beanie
- ▶ Long sleeves
- ▶ Blue pants
- ▶ Walking cane
- ▶ Smug grin





# Indicators of Compromise

- **Document attacker tools and methodology**
  - Network DNS, IP, and traffic protocol patterns
  - Logfile entries
  - Host forensic artifacts and live memory
- **Metadata is efficient for hunting**
- **Analyze attacker tools to create highly effective IOCs**
- **IOC authoring is an art. Practice with a creative mindset**



<http://www.openioc.org>

# Gh0st RAT Community IOC

Name: Gh0st RAT

Author: raustin

GUID: 4f57b99a-7802-4f4e-9ee4-f380bb993a5c

Created: 2012-05-15 15:28:35Z

Modified: 2012-06-28 20:14:27Z

T..	R..

Description:  
This IOC details system changes that occur on a machine that has been infected with the Gh0st RAT variant that was delivered as a result of the compromise to Amnesty International's web site. This IOC covers both the initial dropper executable and the Gh0st variant that is installed. For Windows XP only.

Add: AND OR Item ▾

- OR
  - Network DNS contains shell.xhhow4.com
  - UrlHistory URL contains shell.xhhow4.com
  - UrlHistory URL contains www.48groupclub.org
  - Snort Rule, double click to view or edit
  - Snort Rule, double click to view or edit
- OR
  - File MD5 is 3EC4DE9EF2E158473208842F4631236A
    - AND
      - File Name is sethc.exe
      - File Size is 206168
      - File Detected Anomalies is contains\_eof\_data
      - File Compile Time is 2012-02-14T12:10:59Z
      - File EntryPoint Sig Name contains Microsoft Visual C++ 6.0
      - File PE Type is Executable
      - File PE Subsystem contains GUI
      - File Digital Signature Exists is false
    - OR
      - AND
        - File PEInfo Resource Info Type contains DIALOG
        - File PEInfo Resource Info Language contains Chinese (PRC)
        - File PEInfo Resource Info Name is 102

Source: <https://forums.mandiant.com/forum/general-7>

# Example Methodology IOC

Name: WINDOWS HELP (METHODOLOGY) T.. R..

Author: lucas@mandiant.com

GUID: 7a6b481b-a492-4f55-80e0-b74a4047d4c2

Created: 2012-12-26 18:21:42Z

Modified: 2013-01-22 11:46:25Z

Description:  
This indicator finds unexpected files in the Windows Help directory.

Add: AND OR Item ▾

- OR
  - AND
    - File Extension is not H1V
    - File Extension is not H1T
    - File Extension is not stp
    - File Extension is not h1s
    - File Extension is not H1K
    - File Extension is not h1f
    - File Extension is not chm
    - File Extension is not h1c
    - File Extension is not chq
    - File Extension is not cnt
    - File Extension is not hlp
    - File Extension is not htm
    - File Extension is not wmv
    - File Extension is not js
    - File Extension is not css
    - File Extension is not hta
    - File Extension is not gif
    - File Extension is not wav
    - File Extension is not jpg
    - File Full Path contains not \HELP\bnts.dll
    - File Full Path contains not \HELP\sniffpol.dll
    - File Full Path contains not \HELP\sstube.dll
    - File Full Path contains not \HELP\tshoot.dll
    - File Full Path contains not \HELP\Tours\mmTour\
    - File Attribute is not Directory
  - OR
    - File Full Path contains C:\Winnt\Help\
    - File Full Path contains C:\Windows\Help\



# IOC Hunting Demonstr ation

# Step 3: Investigate Incidents

- **Start with what you know**
  - System, IP, DNS, user, timestamp, etc.
- **Time lining**
  - What else happened?
  - Look through anything with timestamps – e.g., logs, files, registry
- **Search for incident specific IOCs**
  - Exhibited patterns - e.g., working directories
  - Hosts and accounts being used



# — Live IR



1. Quickly pull metadata from live hosts
  - Automation is your friend
2. Investigate the data
3. Pull individual files and memory sections as needed from live hosts

# Investigative Loop Using IOCs





# Investigati on Demonstr ation



# — Step 4: Remediation

## 1. Identify all:

- ▶ Compromised hosts and accounts (user, service, all of AD, etc.)
- ▶ Active (beaconing) and passive (listening) backdoors
- ▶ Other entry points like web servers, VPN, & terminal services

## 2. Perform the following over a “remediation weekend”:

- ▶ Reset passwords
- ▶ Remove backdoors
- ▶ Fix vulnerable systems they’re exploiting for access

## 3. Continue hunting for IOCs to ensure remediation worked and to identify when the attacker returns

# Alert Handling Guideline

## Initial alert

1. Quarantine on network
2. Perform live IR to identify what happened and related activity

## Larger compromise

1. Scope completely
2. Remediate all at once



# Freeware

- **IOC authoring and searching**
- **Live IR**
- **Timelining**
- **Memory analysis**



**Redline**



**IOCe**

<http://www.mandiant.com/resources/downloads>

# — Takeaways

## **Are you compromised right now?**

Accept that attackers will maneuver past your defenses

Hire or train people to hunt for IOCs and investigate alerts

Invest in technologies to support those people

# Questions?

Lucas Zaichkowsky

Lucas@Mandiant.com

Twitter: @LucasErratus

