

Into the Breach: Lessons Learned from Targeted Attacks

Introductions



Ryan Asanovic

- Technical Director @ Mandiant
- Incident response & forensics
- Targeted attacks, espionage & IP theft, nation-state threats
- Background in programming, application security
- Executive



David Dematt

- Managing Director @ Mandiant
- 11+ years experience
- Global life & experience
- Investigative
- Perceptive
- Executive

The State of the Hack



The headlines



All Threat Actors Are Not Equal



How Many?

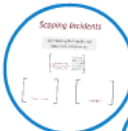


Hours of Detection



How Long is 'Post-breach'?

Common Challenges



Escaping Incidents



False Assumptions



Visibility



People & Process

What's Working?



Learn by Report



Train Like You Fight



Operational Maturity



Work in Public

Thank You!

ryan.asanovic@mandiant.com
@ryanas01

david.dematt@mandiant.com
@kingofthecrowns

Introductions



Ryan Kazanciyan

- Technical Director @ Mandiant
- Incident response & forensics
- Targeted attacks, espionage & IP theft, nation-state threats
- Background in pen-testing, application security
- Instructor



David Damato

- Managing Director @ Mandiant
- 12+ years experience
- Consulted 50+ companies
- Investigator
- Remediator
- Penetration tester
- IT administrator

The State of the Hack

The Headlines

Michael's Stores' Branch Involved 3 Million Customers

Attackers Exploit the Hottest OpenSSL Vulnerability to Circumvent Multi-Factor Authentication on VPNs

Anonymous DDoS Attack Hits Albuquerque Police Dept. In Response To Homeless Man James Boyd's 'Murder'

The Switchboard: Microsoft employees e-mailed hacked by Syrian Electronic Army

10 Target: Names, Emails, Phone Numbers on Up To 70 Million Customers Stolen

Individuals listed under "Found" below are listed as a "Call Center" discovered and were reported for reasons, including addressing phone numbers and e-mail addresses for up to 15 minutes before the call.

Adobe backed 3 million

Accounts hacked, 5 million accounts compromised

Journalists, media under attack from

hackers: Google researchers

Facebook | Twitter | YouTube | LinkedIn | Instagram | SoundCloud | RSS | About | Contact

All Threat Actors Are Not Equal

	NUISANCE	DATA THEFT	CYBER CRIME	INACTIVITY	NETFRAUD ATTACK
Impact	 Affects Properties	 Economic Political (stealing)	 Financial Data	 Cybercrime, Network Policy	 Corruption, Network Policy
Causes	 Economic & Policy	 Financial Property Theft	 Credit Card Theft	 Media Database	 System Glitch Infrastructure
Treated					
Character	 Audited	 Non-audited	 Transparent	 Closed source	 Good Cyber

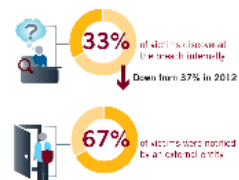
How do you respond? How do you remediate?

Now What?

What common characteristics help attackers compromise and persist in environments?

What are the key success factors to investigating and responding to these threats?

Means of Detection



Source: Mordant M-Trends 2014

How Long is "Persistent"?

Source: <http://www.mindgardens.com>

The Headlines

Michaels Stores' Breach Involved 3 Million Customers

By ELIZABETH A. HARRIS APRIL 18, 2014

Attackers Exploit the Heartbleed OpenSSL Vulnerability to Circumvent Multi-factor Authentication on VPNs

Anonymous DDoS Attack Hits Albuquerque Police Dept. In Response To Homeless Man James Boyd's 'Murder'

By *Dennis Lynch*
on March 30 2014 7:04 PM

f 284 t 38 in 8 g+ m

The Switchboard: Microsoft employee e-mail hacked by Syrian Electronic Army

BY BRIAN FUNG January 16 at 7:36 am

10 Target: Names, Emails, Phone Numbers on Up To 70 Million Customers Stolen

Nationwide retail giant Target today disclosed that a data breach discovered last month exposed the names, mailing addresses, phone number and email addresses for up to 70 million individuals.

Adobe hacked, 3 million accounts compromised

The massive attack exposes customer names, encrypted credit or debit card numbers, expiration dates, and other information relating to customer orders.

by Rachel King @rachelking / October 3, 2013 2:31 PM PDT

Journalists, media under attack from hackers: Google researchers

BY JEREMY WAGSTAFF
SINGAPORE Fri Mar 28, 2014 5:48am EDT

9 COMMENTS | Tweet 799 | Share 128 | Share this | 114 | Email | Print

All Threat Actors Are Not Equal

	NUISANCE	DATA THEFT	CYBER CRIME	HACKTIVISM	NETWORK ATTACK
Objective	 Access & Propagation	 Economic, Political Advantage	 Financial Gain	 Defamation, Press & Policy	 Escalation, Destruction
Example	Botnets & Spam	Intellectual Property Theft	Credit Card Theft	Website Defacements	Destroy Critical Infrastructure
Targeted	✗	✓	✓	✓	✓
Character	Automated	Persistent	Opportunistic	Conspicuous	Conflict Driven



How do you respond? How do you remediate?

How Long is "Persistent"?



229

median number of days that
threat groups were present on a
victim's network before detection

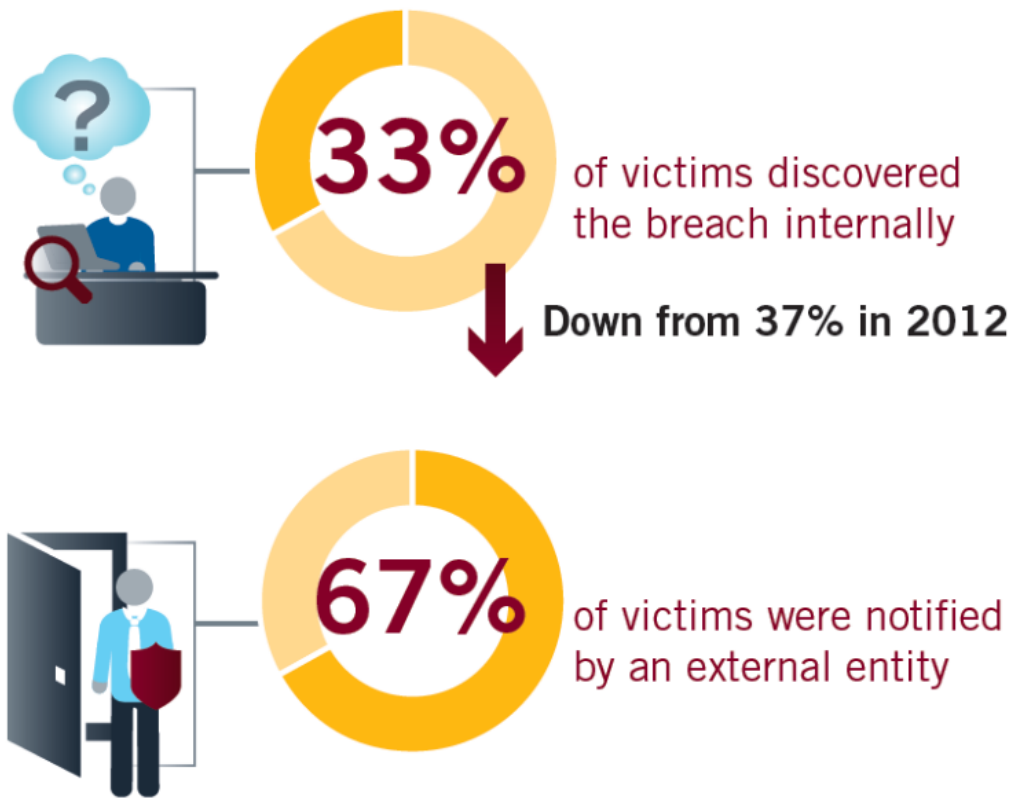


14 days less than 2012

Longest Presence: 2,287 days

Source: Mandiant M-Trends 2014

Means of Detection



Source: Mandiant M-Trends 2014

Now What?

What common characteristics help attackers compromise and persist in environments?

What are the key success factors to investigating and responding to these threats?

Common Challenges

Scoping Incidents

Determining the breadth and impact of a compromise



The Fundamental Problem

Organizations are struggling to protect environments that are

- Built incrementally
- Comprised of systems with inconsistent software & configurations
- Have too many interfaces
- Have too many privileged users
- Rely on "outside-in" defenses

People & Process

Leadership support

CSIRT team skills - employee misuse vs. incident response forensics

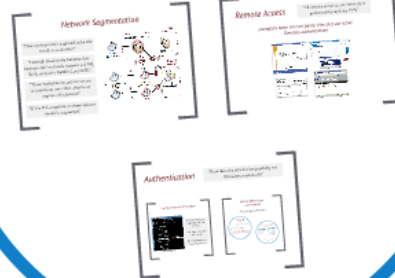
Lack of formal incident response plan or defined processes

Consensus on remediation strategy



False Assumptions

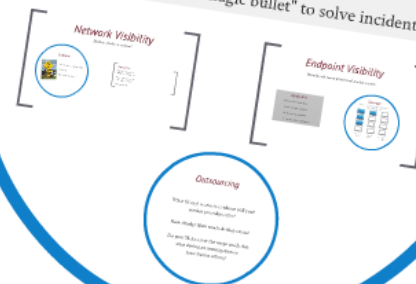
(or "how an attacker can teach you about your own network")



Visibility

You can't investigate what you can't see
(or what you don't even know you have)

There is no single "magic bullet" to solve incidents



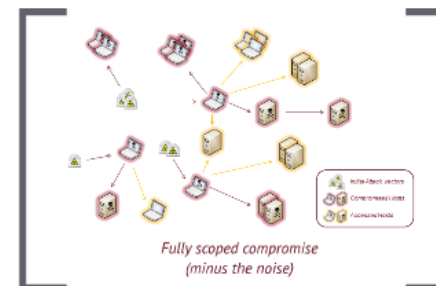
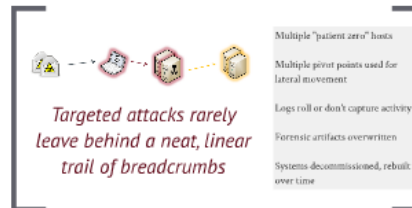
The Fundamental Problem

Organizations are struggling to protect environments that are

- Built incrementally
- Comprised of systems with inconsistent software & configurations
- Have too many interfaces
- Have too many privileged users
- Rely on "outside-in" defenses

Scoping Incidents

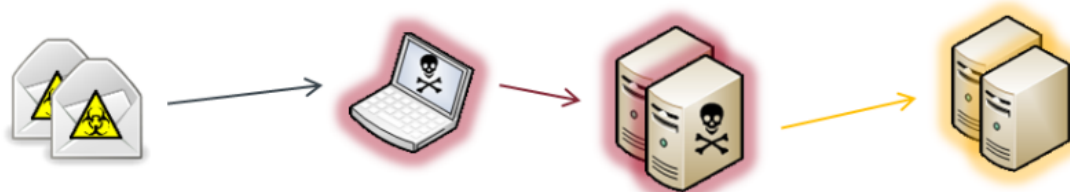
Determining the breadth and impact of a compromise



Fa

(or "how an

Network S



*Targeted attacks rarely
leave behind a neat, linear
trail of breadcrumbs*

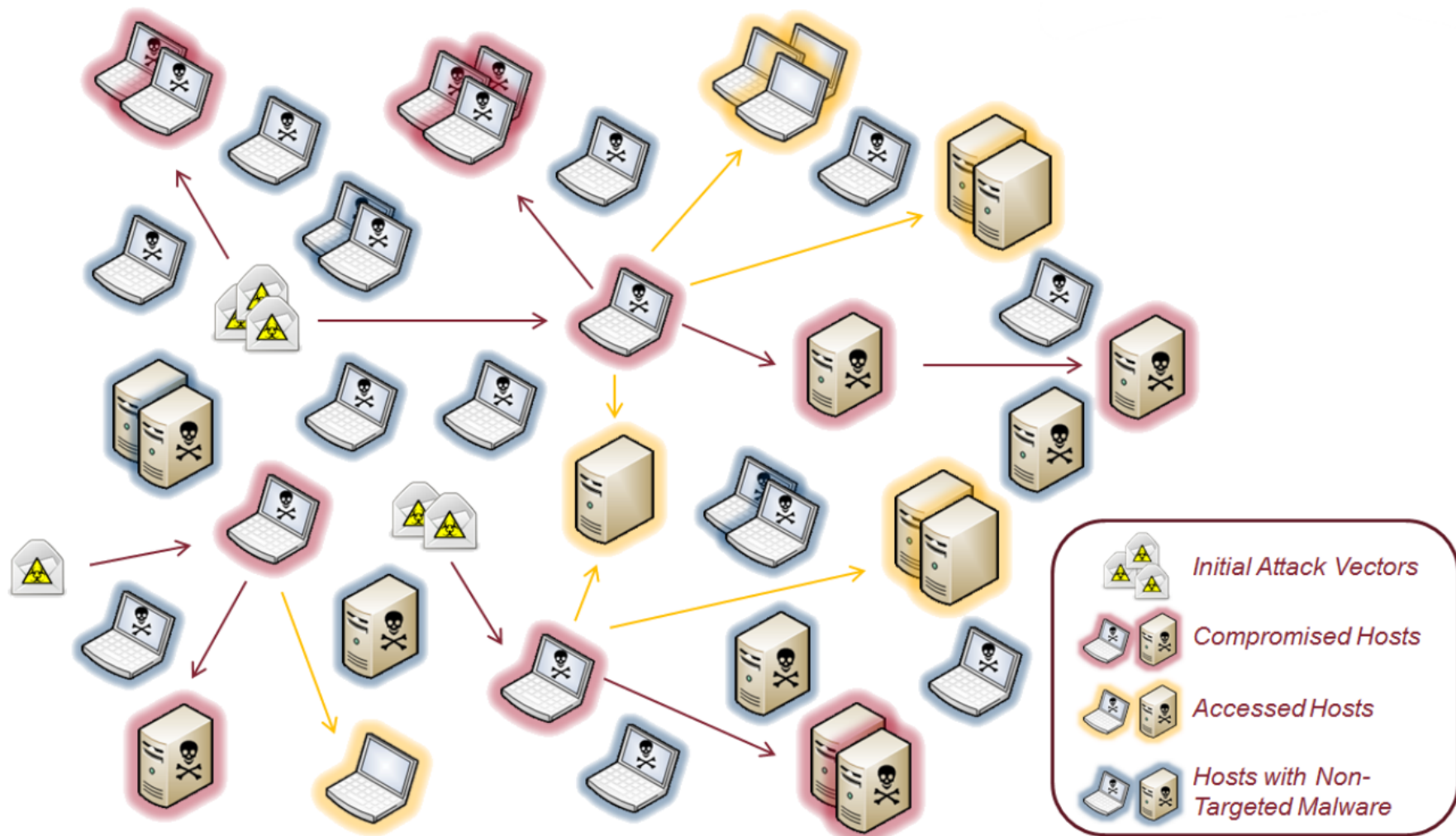
Multiple "patient zero" hosts

Multiple pivot points used for
lateral movement

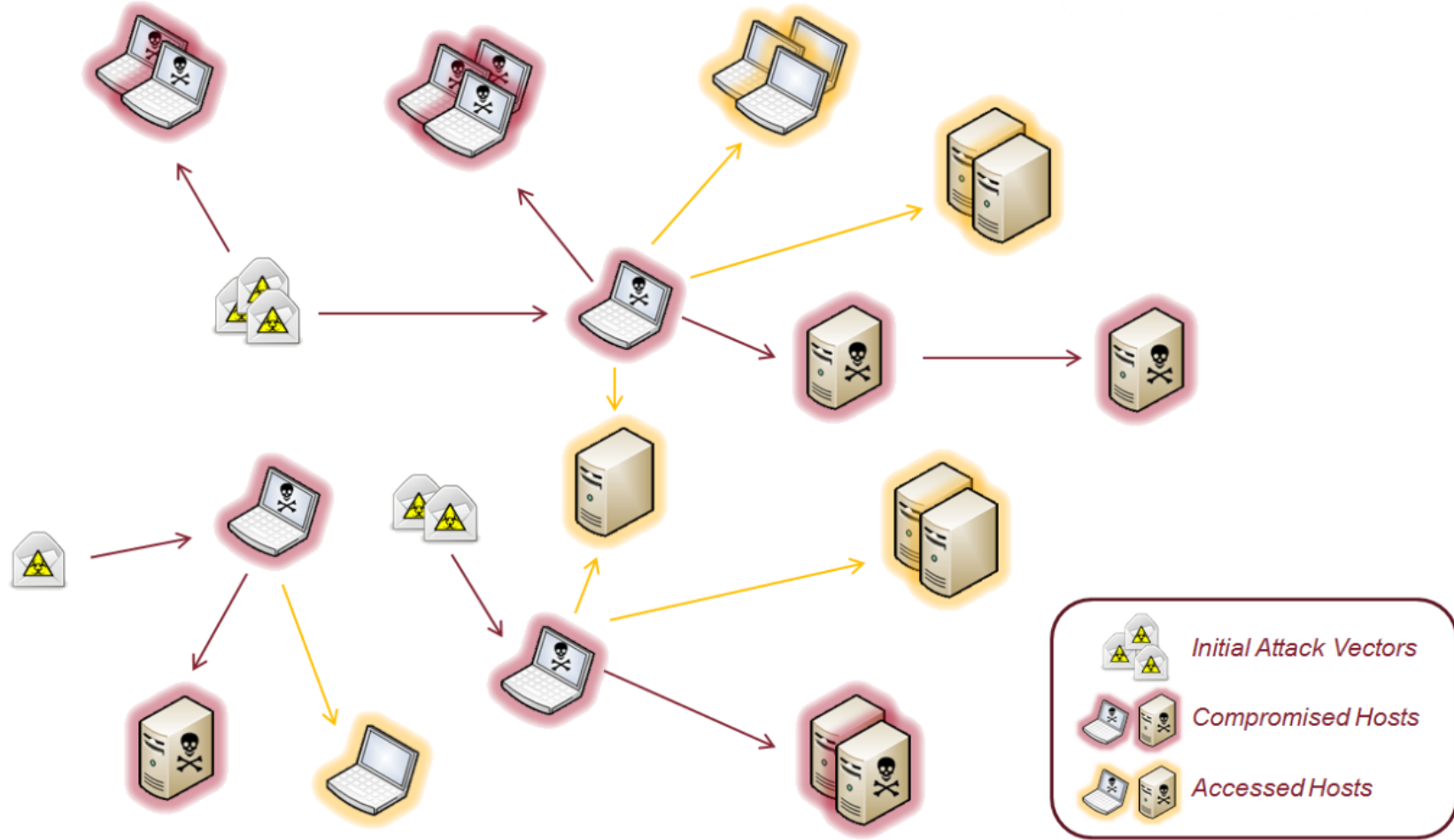
Logs roll or don't capture activity

Forensic artifacts overwritten

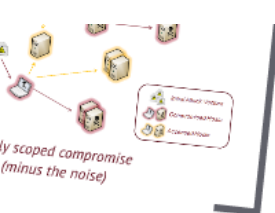
Systems decommissioned, rebuilt
over time



They usually look more like this...



*Fully scoped compromise
(minus the noise)*

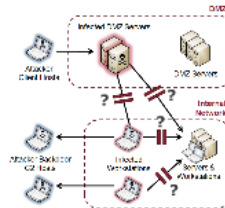


False Assumptions

(or "how an attacker can teach you about your own network")

Network Segmentation

- "Those systems aren't supposed to be able to talk to each other"
- "Firewalls block traffic between that business unit's network segment and HQ. Well, except for NetBIOS and SMB."
- "Those workstations and servers are isolated from one other...they're on separate AD domains"
- "We're PCI compliant, so those systems should be segmented"



Remote Access

"All remote access to our network is protected through the VPN"

(except for these Internet-facing sites that use Active Directory authentication)



Authentication

"How does the attacker keep getting our Windows credentials?"

"Our Passwords are Unbreakable"



This is a password that was cracked from a hash. Can you tell how we got the hash? We use a password that was cracked from a hash.

We Use Multi-Factor Authentication



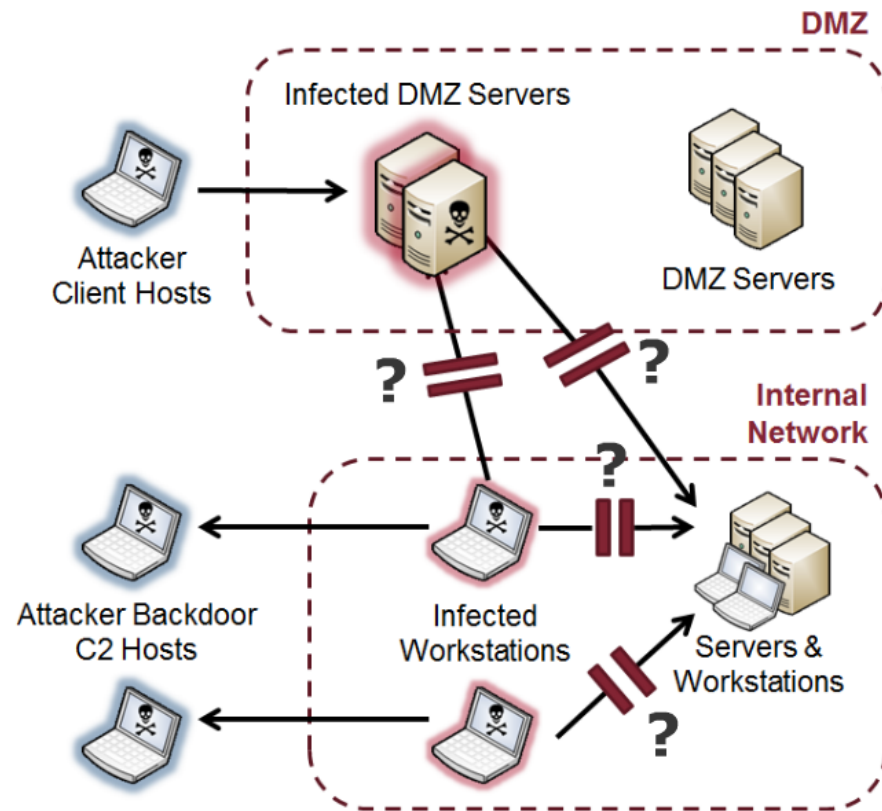
Network Segmentation

"Those systems aren't supposed to be able to talk to each other!"

"Firewalls block traffic between that business unit's network segment and HQ. Well, except for NetBIOS and SMB."

"Those workstations and servers are isolated from one other...they're on separate AD domains"

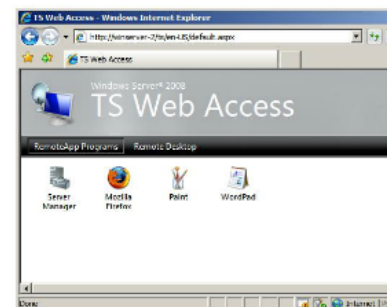
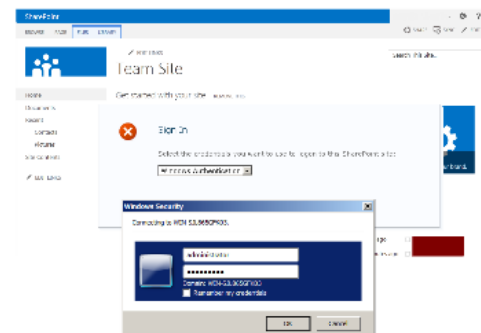
"We're PCI compliant, so those systems should be segmented"



Remote Access

"All remote access to our network is protected through the VPN"

(except for these Internet-facing sites that use Active Directory authentication)



Microsoft



Microsoft Office Outlook Web Access

Provided by Microsoft Exchange Server 2003

User name:

Password:

Client ([what's this?](#))

☒ Premium

☐ Basic

Security ([what's this?](#))

☒ Public or shared computer

☐ Private computer

To protect your account from unauthorized access, Outlook Web Access automatically closes its connection to your mailbox after a period of inactivity. If your session ends, refresh your browser, and then log on again.

SharePoint

BROWSE PAGE FILES LIBRARY

EDIT LINKS

Team Site

Home Get started with your site REMOVE THIS

Documents

Recent

Contacts

Pictures

Site Contents

EDIT LINKS

Sign In

Select the credentials you want to use to login to this SharePoint site:

Windows Authentication

Windows Security

Connecting to WIN-SJL865GFK03.

administrator

Domain: WIN-SJL865GFK03

☒ Remember my credentials

OK Cancel

Web Interface for MetaFrame® Presentation Server

Login [?](#) **Welcome**

Username:

Password:

Domain:

TS Web Access - Windows Internet Explorer

http://winserver-2/ts/en-US/default.aspx

TS Web Access

Windows Server® 2008

TS Web Access

RemoteApp Programs Remote Desktop

Server Manager

Mozilla Firefox

Paint

WordPad

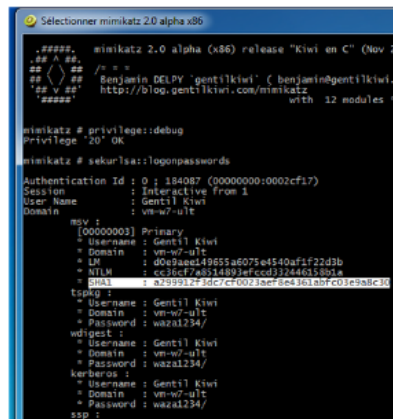
Done

Internet | Protec

Authentication

"How does the attacker keep getting our Windows credentials?"

"Our Passwords are Uncrackable"



```
.##### mimikatz 2.0 alpha (x86) release "Kiwi en C" (Nov 2014)
#####
## ^ ##
## / ##
## \ ## Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## v ## http://blog.gentilkiwi.com/mimikatz
##### with 12 modules

mimikatz # privilege:debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 : 184087 (00000000:0002cf17)
Session           : Interactive from 1
User Name         : Gentil Kiwi
Domain            : vm-w7-ult

msv :
[00000003] Primary
+ Username : Gentil Kiwi
+ Domain   : vm-w7-ult
+ LM       : d089aed49855a6075e4540af1f22d3b
+ NtLm     : cc36cf7a8514891efcd33244615891e
+ SHA1     : a79991273dc7cf0021ae78e4361abf03e9a8c14

lsass :
+ Username : Gentil Kiwi
+ Domain   : vm-w7-ult
+ Password : wazai234/

wdigest :
+ Username : Gentil Kiwi
+ Domain   : vm-w7-ult
+ Password : wazai234/

kerberos :
+ Username : Gentil Kiwi
+ Domain   : vm-w7-ult
+ Password : wazai234/

ssp :
```

Mimikatz by @gentilkiwi

Trivial to recover clear-text credentials from memory

Can always fall back on pass-the-hash

No easy mitigations for most environments

We Use Multi-Factor Authentication

But how reliable is your second factor?

The Risks of Soft Certificates

⚡ volatility [can be dumped from memory]

[can be dumped from protected storage]

If your 2nd factor is stored on a compromised endpoint...it's compromised!

Smart Cards Don't Fix Everything (in Active Directory)

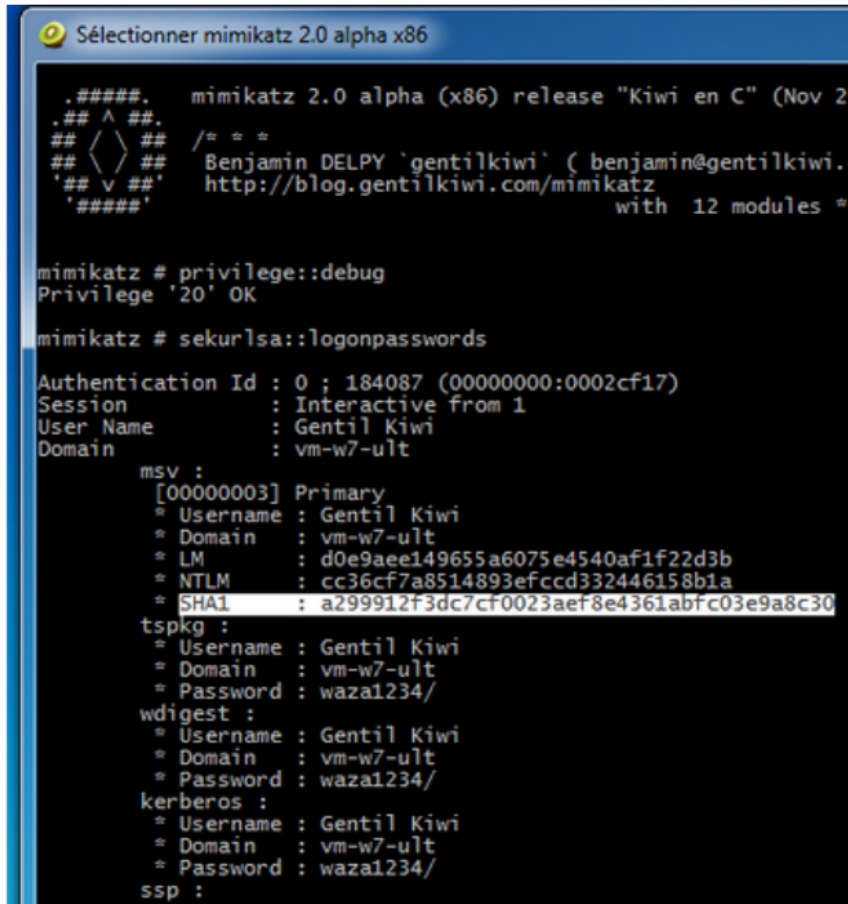
Smart Cards Do

Enhance security for local & RDP logins

Smart Cards Don't

Prevent pass-the-hash for network logons - the authenticator is still an NT hash!

"Our Passwords are Uncrackable"



```
##### mimikatz 2.0 alpha (x86) release "Kiwi en C" (Nov 29 2013)
.## ^ ##.
## < \ ##
## < \ ## Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
'## v ##' http://blog.gentilkiwi.com/mimikatz
##### with 12 modules *

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 184087 (00000000:0002cf17)
Session           : Interactive from 1
User Name         : Gentil Kiwi
Domain            : vm-w7-ult

msv :
[00000003] Primary
* Username : Gentil Kiwi
* Domain   : vm-w7-ult
* LM       : d0e9aee149655a6075e4540af1f22d3b
* NTLM     : cc36cf7a8514893efccd332446158b1a
* SHA1     : a299912f3dc7cf0023aef8e4361abfc03e9a8c30

tspkg :
* Username : Gentil Kiwi
* Domain   : vm-w7-ult
* Password : waza1234/

wdigest :
* Username : Gentil Kiwi
* Domain   : vm-w7-ult
* Password : waza1234/

kerberos :
* Username : Gentil Kiwi
* Domain   : vm-w7-ult
* Password : waza1234/

ssp :
```

Mimikatz by @gentilkiwi

Trivial to recover clear-text credentials from memory

Can always fall back on pass-the-hash

No easy mitigations for most environments

We Use Multi-Factor Authentication

But how reliable is your second factor?

The Risks of Soft Certificates

 volatility [can be dumped from memory]

[can be dumped from protected storage] 

If your 2nd factor is stored on a compromised endpoint...it's compromised!

Smart Cards Don't Fix Everything (in Active Directory)

Smart Cards Do

Enhance security
for local & RDP
logins

Smart Cards Don't

Prevent pass-the-hash
for network logons -
the authenticator is
still an NT hash!

(even Microsoft says so!)

Source: "Mitigating Pass-the-Hash", Microsoft

The Risks of Soft Certificates

 volatility [can be dumped from memory]

[can be dumped from protected storage] 

If your 2nd factor is stored on a
compromised endpoint...it's compromised!

Smart Cards Don't Fix Everything (in Active Directory)

Smart Cards Do

Enhance security
for local & RDP
logins

Smart Cards Don't

Prevent pass-the-hash
for network logons -
the authenticator is
still an NT hash!

(even Microsoft says so!)

Other mitigation	Effectiveness	Effort required	Privilege escalation	Lateral movement
Disable the NTLM protocol	Minimal	High	-	-
Smart cards and multifactor authentication	Minimal	High	-	-

Source: "Mitigating Pass-the-Hash", Microsoft

(even Microsoft says so!)

Other mitigation	Effectiveness	Effort required	Privilege escalation	Lateral movement
Disable the NTLM protocol	Minimal	High	-	-
Smart cards and multifactor authentication	Minimal	High	-	-

Source: "Mitigating Pass-the-Hash", Microsoft

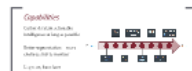
Visibility

You can't investigate what you can't see
(or what you don't even know you have)

There is no single "magic bullet" to solve incidents

Network Visibility

Monitor attacks "en masse"



Endpoint Visibility

Identify both recent & historical attacker activity



Outsourcing

What (if any) access to evidence will your service providers offer?

How timely? How much do they retain?

Do your SLAs cover the surge needs that arise during an investigation or remediation efforts?

Network Visibility

Monitor attacks "in motion"

Coverage



Internet ingress and egress points

VPN traffic

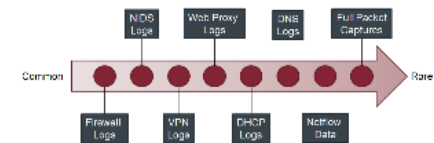
Zone & trust boundaries

Capabilities

Gather & retain actionable intelligence as long as possible

Better segmentation = more choke-points to monitor

Log now, hunt later



Coverage



Internet ingress and egress points

VPN traffic

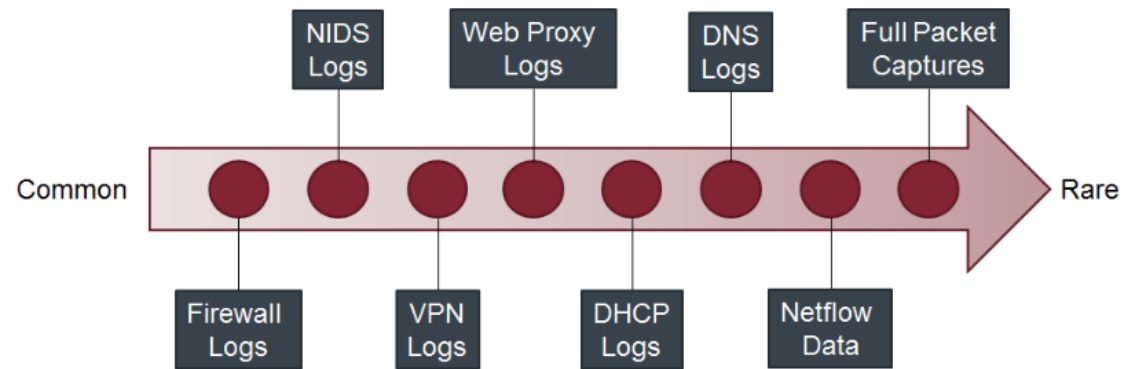
Zone & trust boundaries

Capabilities

Gather & retain actionable intelligence as long as possible

Better segmentation = more choke-points to monitor

Log now, hunt later



Endpoint Visibility

Identify both recent & historical attacker activity

Capabilities

Remote "live" system triage

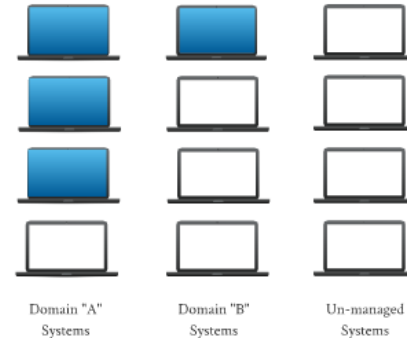
Remote forensic acquisition

On-site forensic acquisition

At-scale searching & aggregation

Coverage

Across what percentage of your endpoints can you exercise these capabilities?



Capabilities

Remote "live" system triage

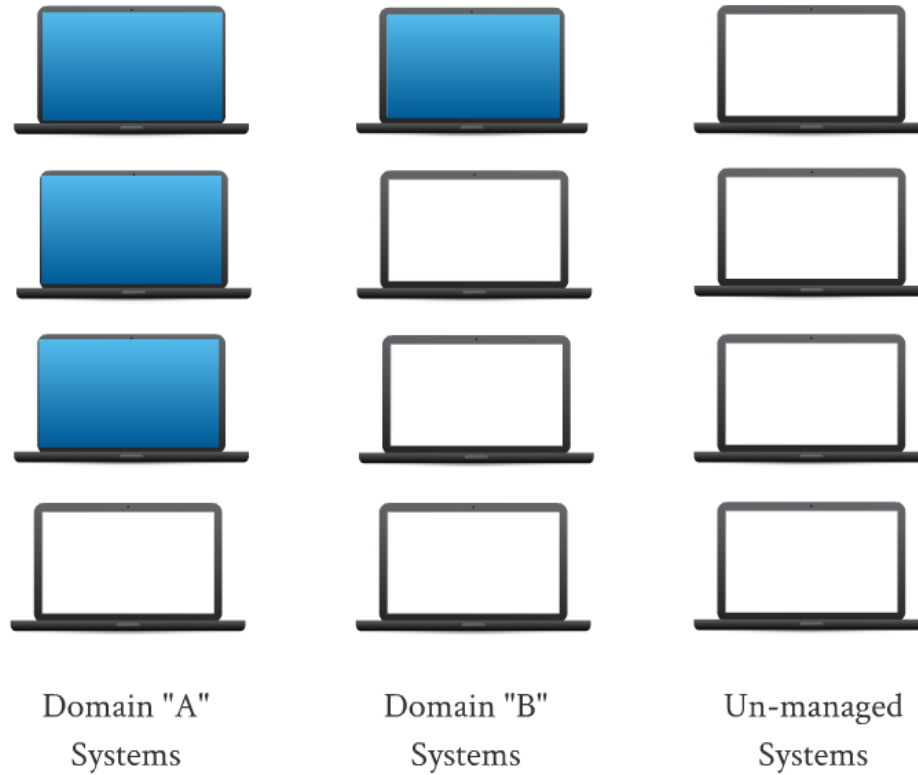
Remote forensic acquisition

On-site forensic acquisition

At-scale searching & aggregation

Coverage

Across what percentage of your endpoints can you exercise these capabilities?



Outsourcing

What (if any) access to evidence will your service providers offer?

How timely? How much do they retain?

Do your SLAs cover the surge needs that arise during an investigation or remediation efforts?

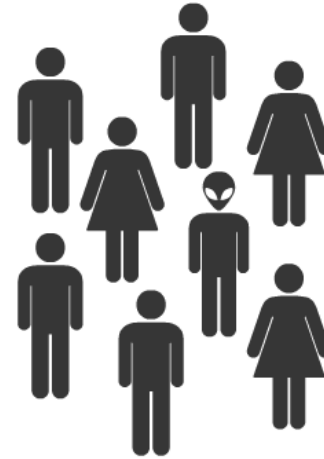
People & Process

Leadership support

CSIRT team skills - employee misuse
vs. incident response forensics

Lack of formal incident response plan
or defined processes

Consensus on remediation strategy



What's Working?

Learn to Hunt



CIRT teams should constantly examine their environment for indicators of compromise

Host & network-based data

Baseline activity, learn what's "normal"

Proactively eliminate false positives

Use Intelligence Intelligently

Who's behind the keyboard?
Who's tasking the operators?
What's really important?



Focus on What's Important

Use a reliable tool, make sure you're using it right

Don't get lost in the noise

Identify threats and assess their impact

What's going on? (What's the story?)

Train Like You Fight



Make your security assessments and pen-tests realistic

Assume attacker will gain initial entry and escalate privileges - what now?

Containment vs. initial entry vector

Invest in People

Never underestimate the power of smart people with coding skills

Buy shiny toys to help smart people work at greater scale

Learn to Hunt



CIRT teams should constantly examine their environment for indicators of compromise

Host & network-based data

Baseline activity, learn what's "normal"

Proactively eliminate false positives

Train Like You Fight



thegrugq
@thegrugq



Following

Let you guys in on a secret: there is always a critical Internet Explorer 0day being exploited in the wild.



Gabe The Engineer @gdbassett · Apr 28

@thegrugq @jaysonstreet yeah. If 0days change your infosec strategy, you're doing something wrong. Everyone knows they're out there.

[View conversation](#)



Reply



Retweeted



Favorite



More



Make your security assessments and pen-tests realistic

Assume attacker will gain initial entry and escalate privileges - what now?

Containment vs. initial entry vector



the grugq

@thegrugq



Following

Let you guys in on a secret: there is always a critical Internet Explorer 0day being exploited in the wild.



Gabe The Engineer @gdbassett · Apr 28

@thegrugq @jaysonstreet yeah. If 0days change your infosec strategy, you're doing something wrong. Everyone knows they're out there.



View conversation



Reply



Retweeted



Favorite



More



Make your security assessments and pen-tests realistic

Assume attacker will gain initial entry and escalate privileges - what now?

Containment vs. initial entry vector

Use Intelligence Intelligently

Who's behind the keyboard?
Who's tasking the operators?
What's really important?

APT Alphabet Soup



<http://www.flickr.com/photos/whitexpts/images/5215904872/>

Focus on What's Important

Learn attacker tools, tactics, procedures **regardless of attribution**

Derive indicators of compromise

Identify the data and assets most likely to be targeted

Identify gaps in visibility ("Could we have detected that?")

APT Alphabet Soup



<http://www.flickr.com/photos/whitneyinchicago/5215904693/>

Focus on What's Important

Learn attacker tools, tactics, procedures **regardless of attribution**

Derive indicators of compromise

Identify the data and assets most likely to be targeted

Identify gaps in visibility ("Could we have detected that?")

Invest in People

Never underestimate the power of
smart people with coding skills

Buy shiny toys to help smart people
work at greater scale

Thank You!

ryan.kazanciyan@mandiant.com

 @ryankaz42

david.damato@mandiant.com

 @ArigatoDamato