Sean Coyne | Consultant
Ryan Kazanciyan | Principal

MANDIANT®

The Getaway

Methods and Defenses for Data Exfiltration

Black Hat DC 2011

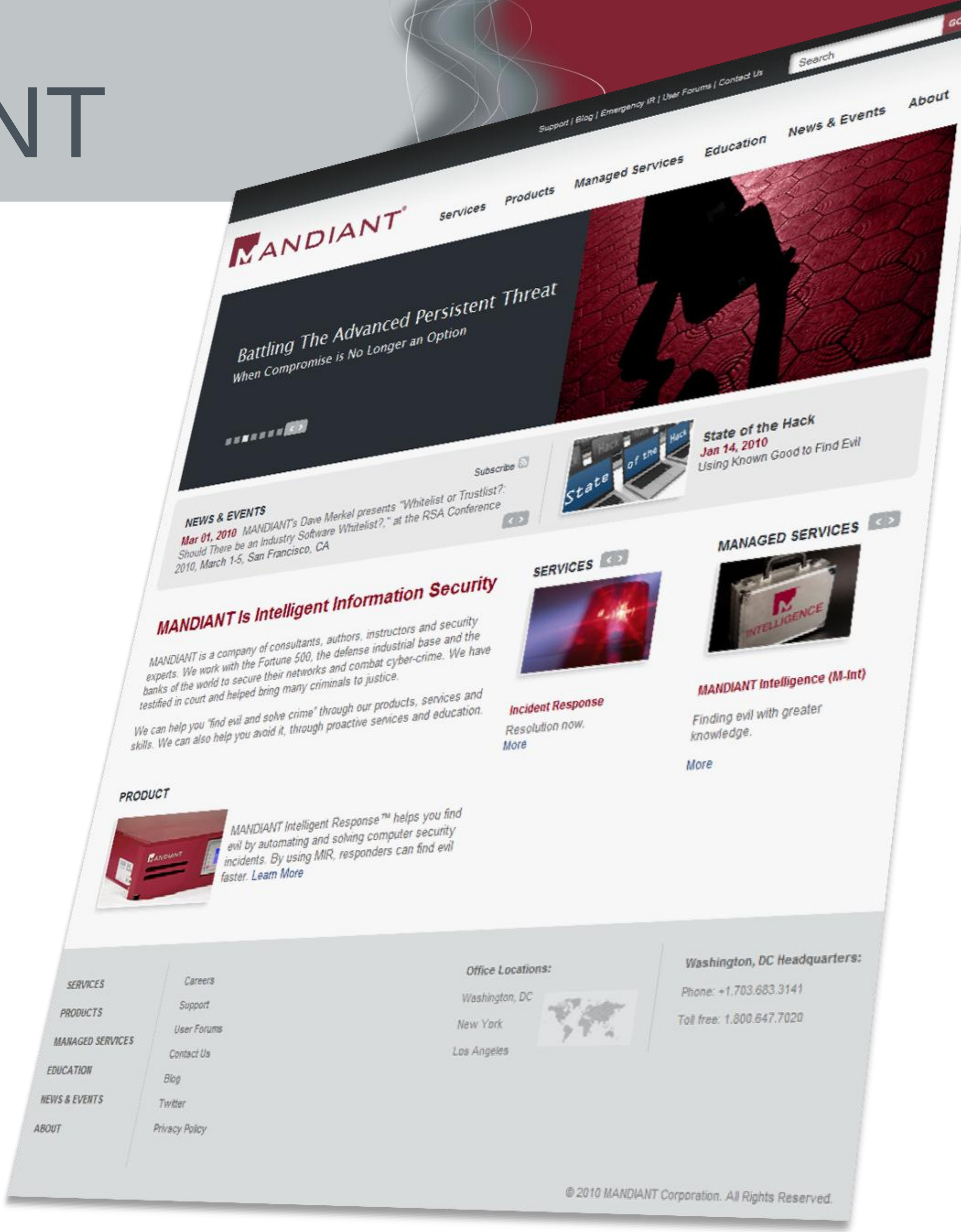
Important note

All information is derived from MANDIANT observations in non-classified environments

Some information has been sanitized to protect our clients' interests

We are MANDIANT

- VISA Qualified Incident Response Assessor (QIRA)
- APT and CDT experts
- Located in
  - Washington
  - New York
  - Los Angeles
  - San Francisco
- Professional and managed services, software and education



Battling The Advanced Persistent Threat

When Compromise is No Longer an Option

State of the Hack

Jan 14, 2010

Using Known Good to Find Evil

NEWS & EVENTS

Mar 01, 2010 MANDIANT's Dave Merkel presents "Whitelist or Trustlist?: Should There be an Industry Software Whitelist?," at the RSA Conference 2010, March 1-5, San Francisco, CA

MANDIANT Is Intelligent Information Security

MANDIANT is a company of consultants, authors, instructors and security experts. We work with the Fortune 500, the defense industrial base and the banks of the world to secure their networks and combat cyber-crime. We have testified in court and helped bring many criminals to justice.

We can help you "find evil and solve crime" through our products, services and skills. We can also help you avoid it, through proactive services and education.

Incident Response

Resolution now.

More

MANDIANT Intelligence (M-Int)

Finding evil with greater knowledge.

More

MANDIANT Intelligent Response™ helps you find evil by automating and solving computer security incidents. By using MIR, responders can find evil faster. Learn More

Office Locations:

Washington, DC

New York

Los Angeles

Washington, DC Headquarters:

Phone: +1.703.683.3141

Toll free: 1.800.647.7020

© 2010 MANDIANT Corporation. All Rights Reserved.

Introductions

RYAN KAZANCIYAN

[kah-ZAN-see-yan]

- Principal Consultant
- Incident response, forensics, penetration testing, application security
- Instructor for Black Hat, L.E. courses
- 9 large-scale investigations in 2010

Introductions

SEAN V. COYNE

[*coin*]

- Consultant
- Penetration-testing, Incident Response, Forensics, Training, Intelligence
- Instructor for L.E. courses
- 6 years security consulting for government/corporate clients.

The Getaway

- Overview and Definitions
- Data Preparation and Staging
- Data Exfiltration Fundamentals
- Case Studies
  - Naked file transfer through RDP
  - Malware checks its webmail
  - Down the tunnel, through the loop

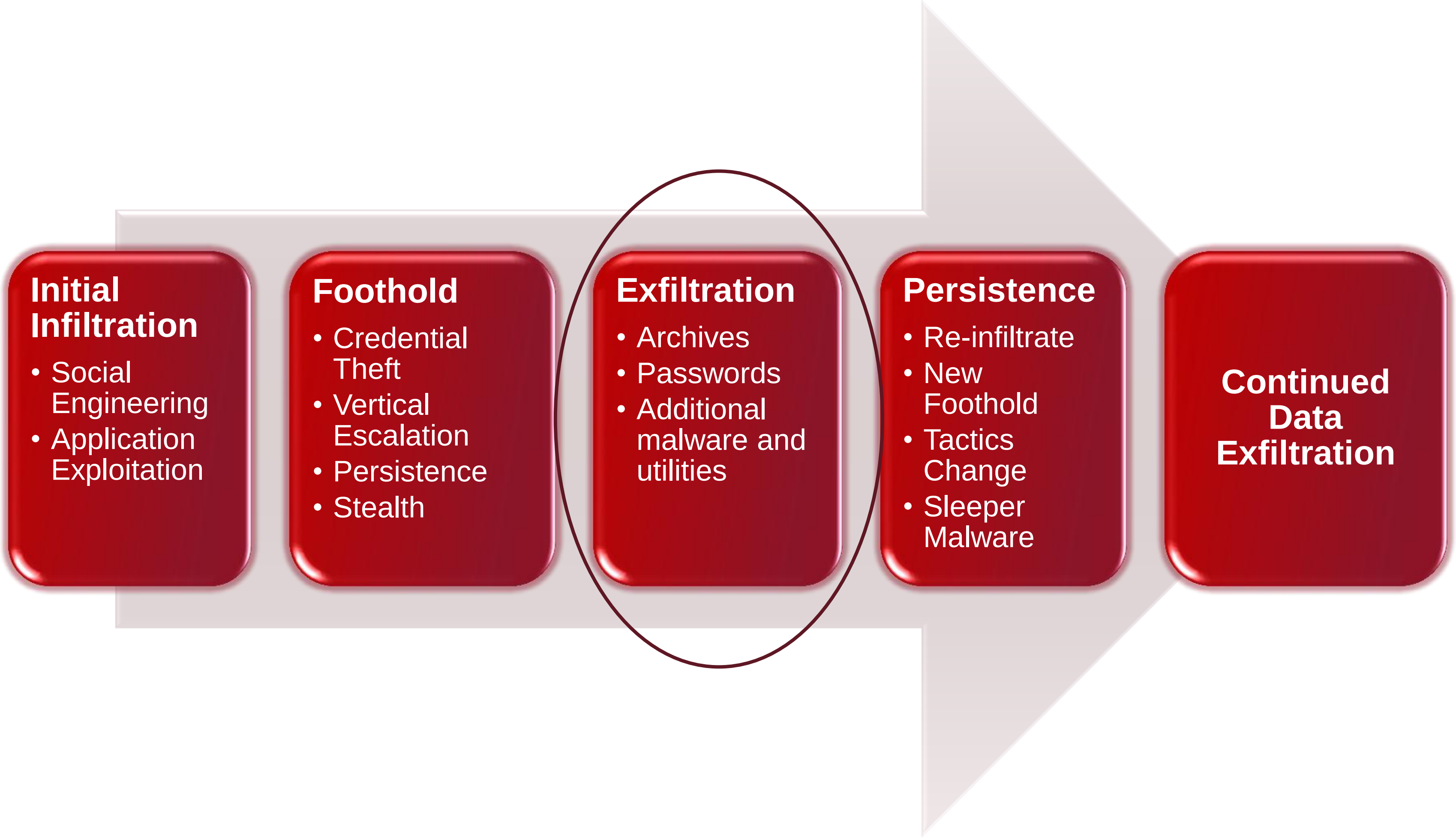
Overview and Definitions

What Are We Talking About?

- Exfiltrate [eks-fil-treyt]. *verb*,:
  - *To surreptitiously move personnel or materials out of an area under enemy control.*

- In computing terms, exfiltration is the unauthorized removal of data from a network.

What Are We Talking About?



Initial Infiltration

- Social Engineering
- Application Exploitation

Foothold

- Credential Theft
- Vertical Escalation
- Persistence
- Stealth

Exfiltration

- Archives
- Passwords
- Additional malware and utilities

Persistence

- Re-infiltrate
- New Foothold
- Tactics Change
- Sleeper Malware

Continued Data Exfiltration

Why Do We Care?

- ‘It’s the ~~Economy~~ Data, Stupid.’
  - Personally identifiable information (PII), financial data, ***trade secrets, source code, intellectual property***
- Data Disclosure Laws:
  - The Data Breach Notification Act
  - The Personal Data Privacy and Security Act of 2009
- Contractual Obligations
  - Clients
  - Business partners
- Closing the barn door after the cow is gone.

Why Do We Care?

- Impact hard to quantify
  - R&D costs? Trade Secrets? Loss of market share?
  - Consumer confidence, stock price?
  - % of victims who do not report, or never know?
  - Quantity of data != impact
- One of our larger recent breaches
  - Over 120 GBs, 105 multi-part RARs
  - Spread across 6 staging areas

Data Preparation and Staging

Let’s Pack it Up.

- Easier to move things in a box
  - RAR, ZIP, and CAB files.
  - Makecab built-in to Windows
- Staging areas
  - Locations to aggregate data before sending it out
  - Easier to track tools and stolen data
  - Fewer connections to external drops
  - Typically workstations – plenty of storage space

Common Staging Points

- %systemdrive%\RECYCLER
  - Recycle Bin maps to subdirectories for each user SID
  - Hidden directory
  - Root directory shouldn’t contain any files
- %systemdrive%\System Volume Information
  - Subdirectories contain Restore Point folders
  - Hidden directory
  - Access restricted to SYSTEM by default
  - Root directory typically only contains “tracking.log”

Common Staging Points

- %systemroot%\Tasks
  - “Special” folder – Windows hides contents in Explorer
  - Root directory only contains scheduled .job files, “SA.dat” and “desktop.ini”
- Countless other hiding spots…
  - %systemroot%\system32
  - %systemroot%\debug
  - User temp folders
  - Trivial to hide from most users
  - Staging points vary on OS, attacker privileges

Playing with Extensions

Attacker responds to custom HIPS rule blocking RAR file creation…

Host	Event	Date / Time
Victim1	McAfee AccessProtectionLog Entry: **Blocked by Access Protection rule** Victim1\user C:\WINDOWS\system32\cmd.exe \Device\LanmanRedirector\1.2.3.4\ **c$\WINDOWS\addins\Data.rar**	4/1/2010 08:34:11
Victim1	McAfee AccessProtectionLog Entry: **Blocked by Access Protection rule** Victim1\user C:\WINDOWS\system32\cmd.exe **Z:\WINDOWS\addins\Data.rar**	4/1/2010 08:35:14
Victim1	McAfee AccessProtectionLog Entry: Blocked by Access Protection rule Victim1\user C:\WINDOWS\system32\cmd.exe **Z:\WINDOWS\addins\MoreData.part01.rar**	4/1/2010 08:35:45
Victim2	File Created: **C:\RECYCLER\Data**	4/1/2010 09:17:37
Victim2	File Created: **C:\RECYCLER\MoreData.part01**	4/1/2010 09:29:08

Data Exfiltration Fundamentals

Data Exfil 101

MANDIANT®

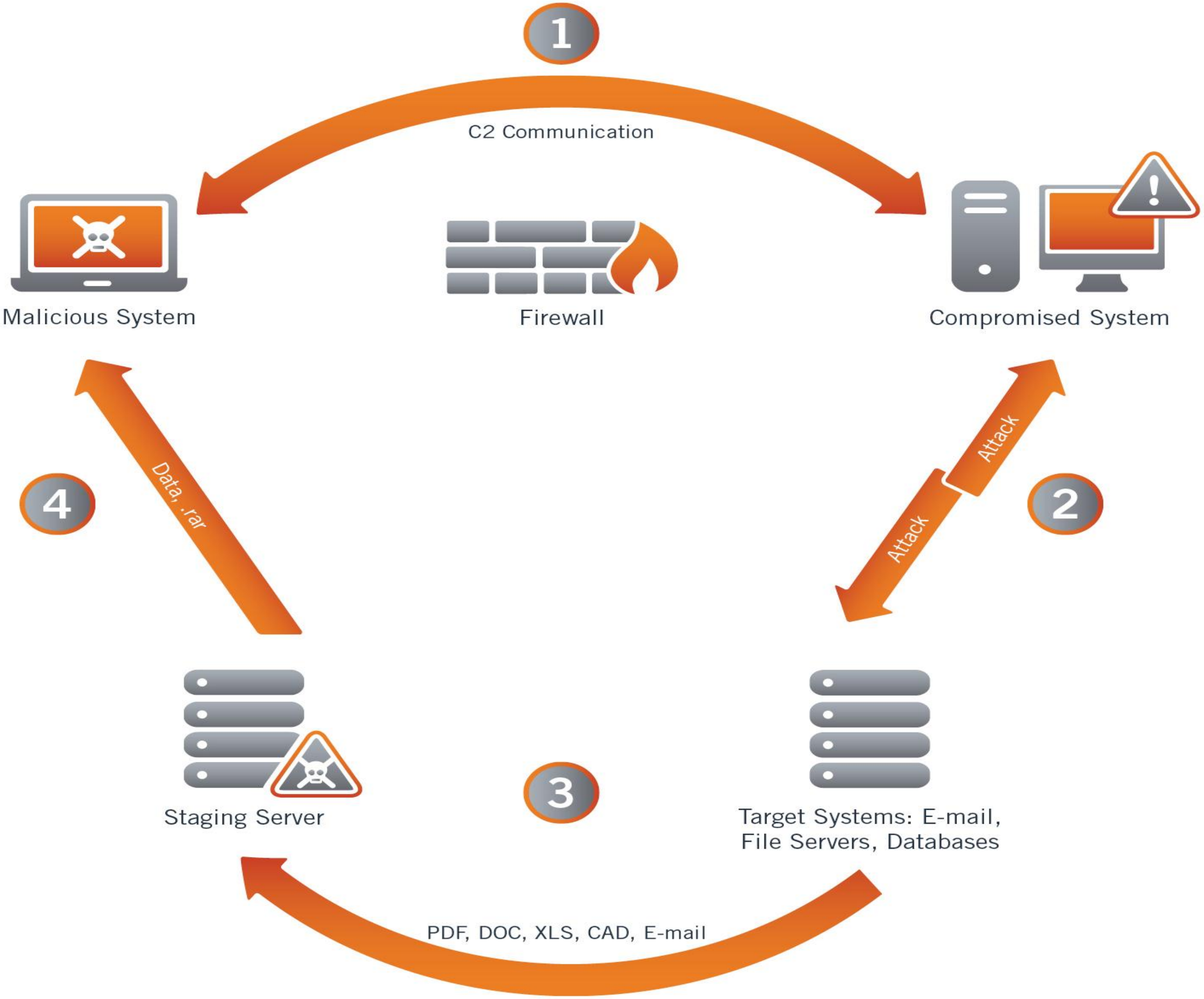
DATA EXFILTRATION METHODOLOGY

Step One: C2 Communication
The malware contacts C2 servers for instructions, such as downloading and executing new malware or opening a reverse backdoor — allowing the attacker full access to the compromised system, bypassing firewall restrictions.

Step Two: Attack
The attacker (through the reverse backdoor) compromises multiple sources of interest, such as database servers, email servers, and file share servers.

Step Three: Data Staging
The attacker sends data to a staging server. Once the data is set, the attacker then compresses the data (using the rar.exe utility) and password protects it.

Step Four: Data Exfiltration
The attacker uses malware to send the data through an encrypted tunnel to a malicious external IP address.



Basic Techniques

- Exfiltration via outbound FTP or HTTPS most common, blends in
- Simple works best!
- Out-of-band: distinct from C2 channels and endpoints
  - Maintain separate external drop points
  - C2 resilience if data exfil channel detected

Drinking from a fire hose

- Attackers have distinct data collection strategies
  - Take it all, process offline
    - XCOPY file server directories
    - 100s of GBs of archived data

-or-

  - Examine and filter in-place
    - Probe for data of interest
    - Obtain recursive directory listings
    - Return later to retrieve small sets of specific files
- Can draw inferences on attacker motivations, planning, and resources

Case Studies

Three Tales of Woe and Loss

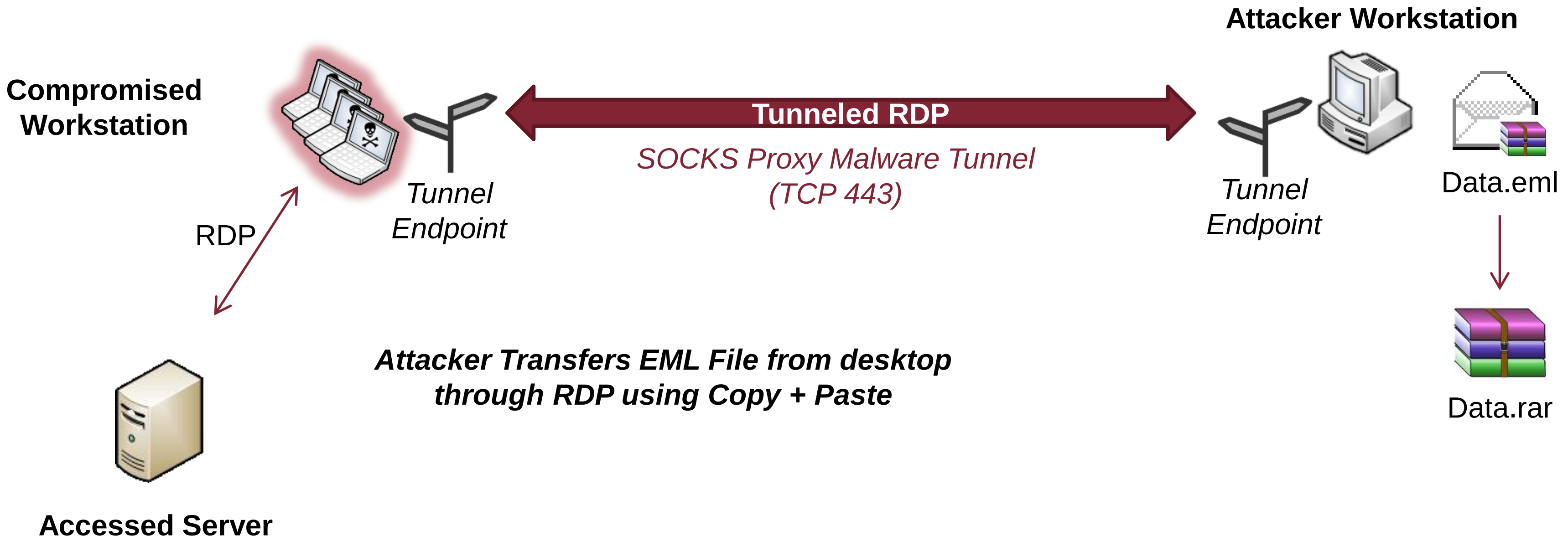
- Creative approaches to data theft
- Highly targeted attacks
- All initiated by phishing e-mails
- Most victims notified by law enforcement
- Long-term persistence (multi-year)
- Goal: Consider strategies for both detection and post-incident investigation

Case # 1: Naked file transfer through RDP

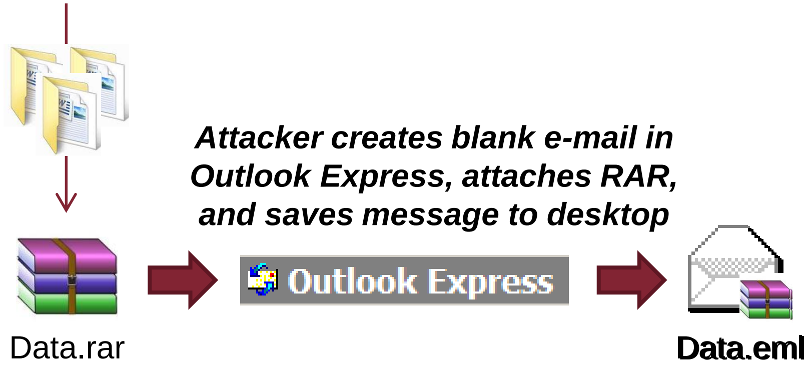
The Scenario

- Medium sized defense contractor with about 5,000 hosts
- Proactive analysis for indicators of compromise
- Identified one attack group active in the environment
- ~25 compromised hosts

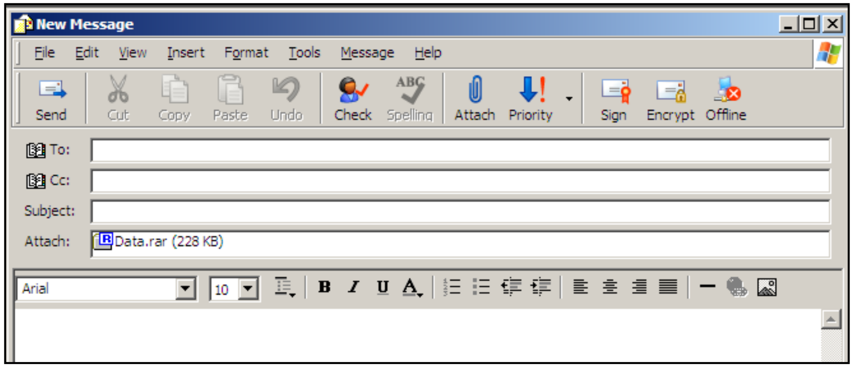
Using and Abusing Tunneled RDP



Attacker Transfers EML File from desktop through RDP using Copy + Paste



Attacker creates blank e-mail in Outlook Express, attaches RAR, and saves message to desktop


New Message
File Edit View Insert Format Tools Message Help
Send Cut Copy Paste Undo Check Spelling Attach Priority Sign Encrypt Offline
Arial
10
B I U A

To:

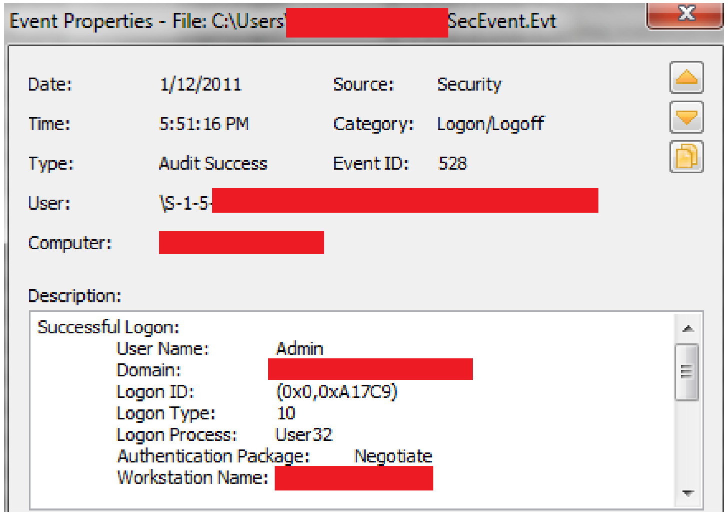
Cc:

Subject:

Attach: Data.rar (228 KB)

Sources of Evidence

- Timeline analysis of events following attacker RDP login using local admin credentials
- Records of .EML file (deleted) in user’s index.dat
- Prefetch record: first execution of MSIMN.EXE (Outlook Express) during this period

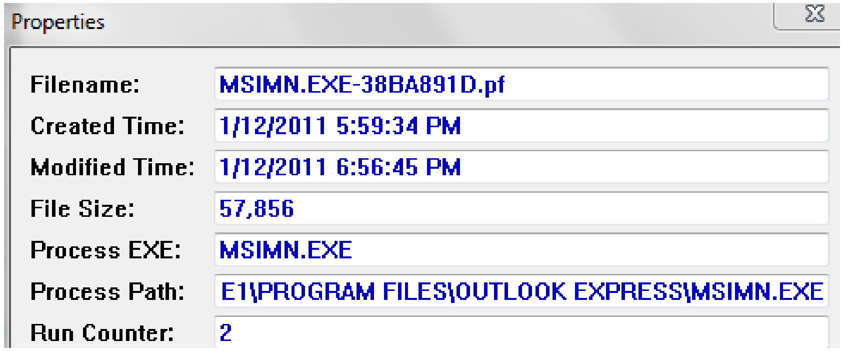


Event Properties - File: C:\Users\[redacted]SecEvent.Evt

Date: 1/12/2011 Source: Security
Time: 5:51:16 PM Category: Logon/Logoff
Type: Audit Success Event ID: 528
User: \S-1-5-[redacted]
Computer: [redacted]

Description:

Successful Logon:
User Name: Admin
Domain: [redacted]
Logon ID: (0x0,0xA17C9)
Logon Type: 10
Logon Process: User32
Authentication Package: Negotiate
Workstation Name: [redacted]



Properties

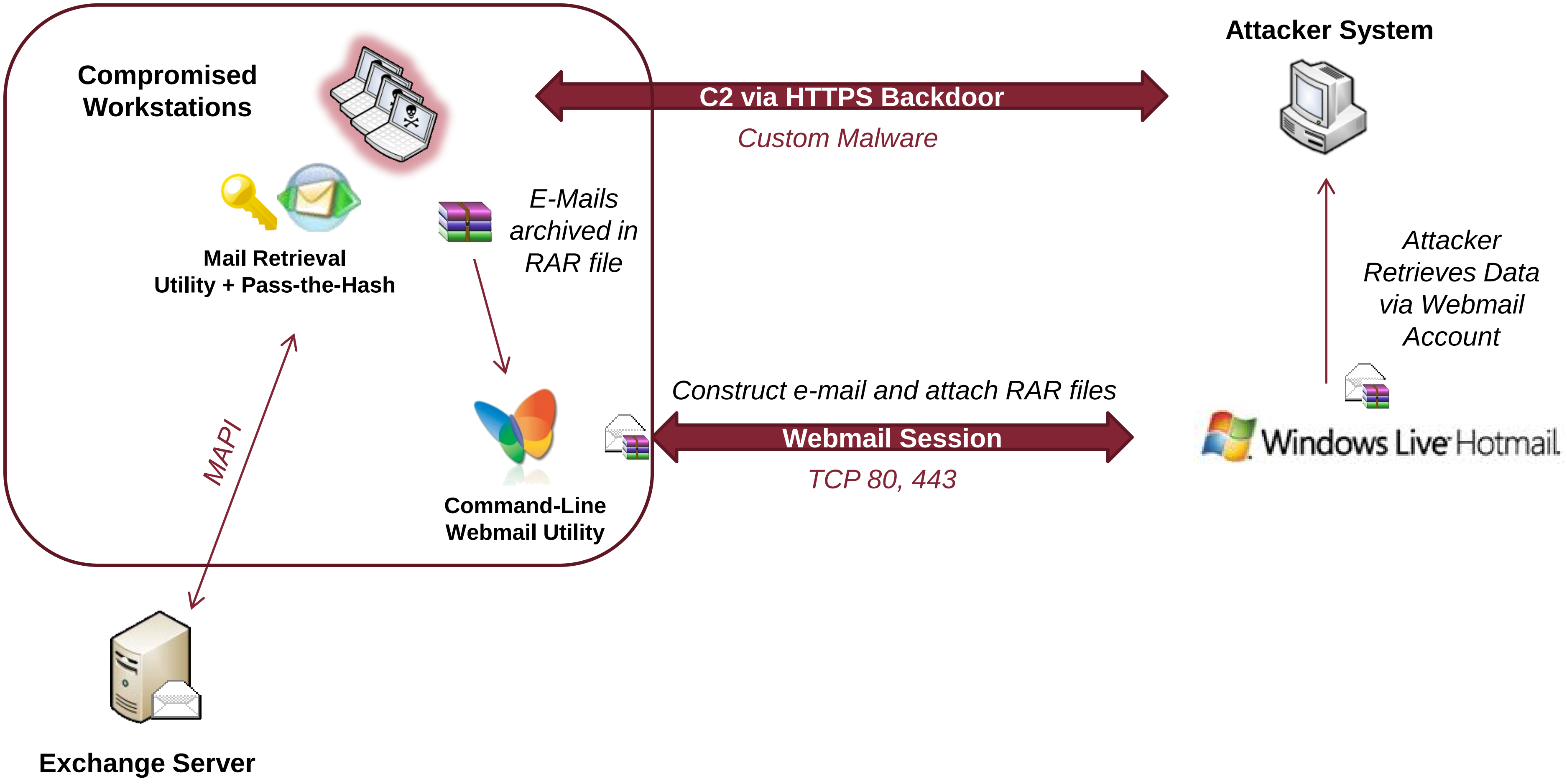
Filename: MSIMN.EXE-38BA891D.pf
Created Time: 1/12/2011 5:59:34 PM
Modified Time: 1/12/2011 6:56:45 PM
File Size: 57,856
Process EXE: MSIMN.EXE
Process Path: E1\PROGRAM FILES\OUTLOOK EXPRESS\MSIMN.EXE
Run Counter: 2

Case #2: Malware Checks its Webmail

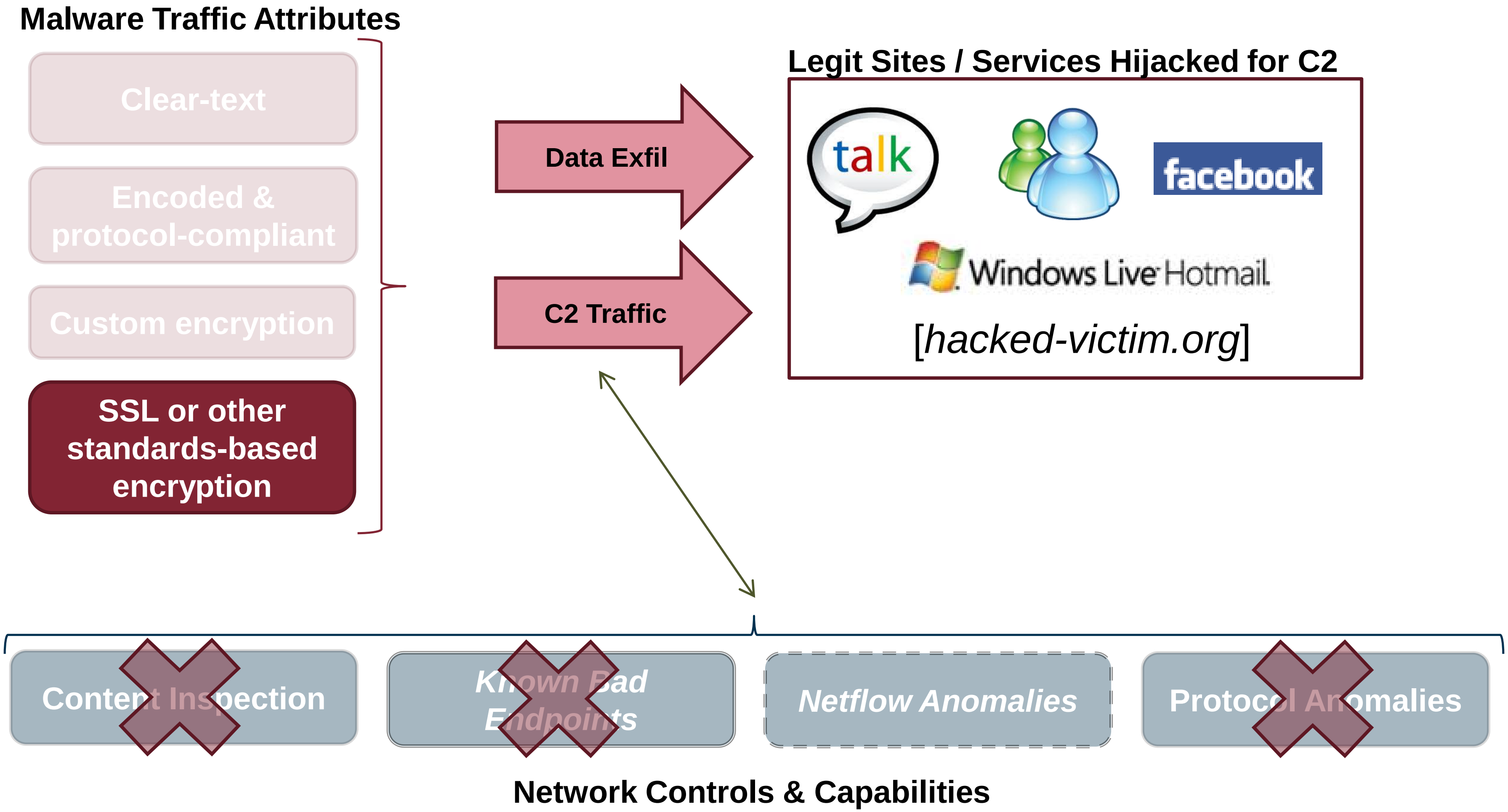
The Scenario

- Medium sized enterprise of ~ 7,000 hosts
- Attack activity attributed to one attack group
- Over 50 compromised hosts
- Targeted data: e-mails

Malware Checks its Webmail


Compromised Workstations
Attacker System
C2 via HTTPS Backdoor
Custom Malware
Mail Retrieval Utility + Pass-the-Hash
E-Mails archived in RAR file
Attacker Retrieves Data via Webmail Account
Construct e-mail and attach RAR files
Webmail Session
TCP 80, 443
Windows Live Hotmail
MAPI
Command-Line Webmail Utility
Exchange Server

What's a "bad" endpoint?



Malware Traffic Attributes

Clear-text

Encoded & protocol-compliant

Custom encryption

SSL or other standards-based encryption

Data Exfil

C2 Traffic

Legit Sites / Services Hijacked for C2

[*hacked-victim.org*]

Content Inspection

Known Bad Endpoints

Netflow Anomalies

Protocol Anomalies

Network Controls & Capabilities

This can only get worse…

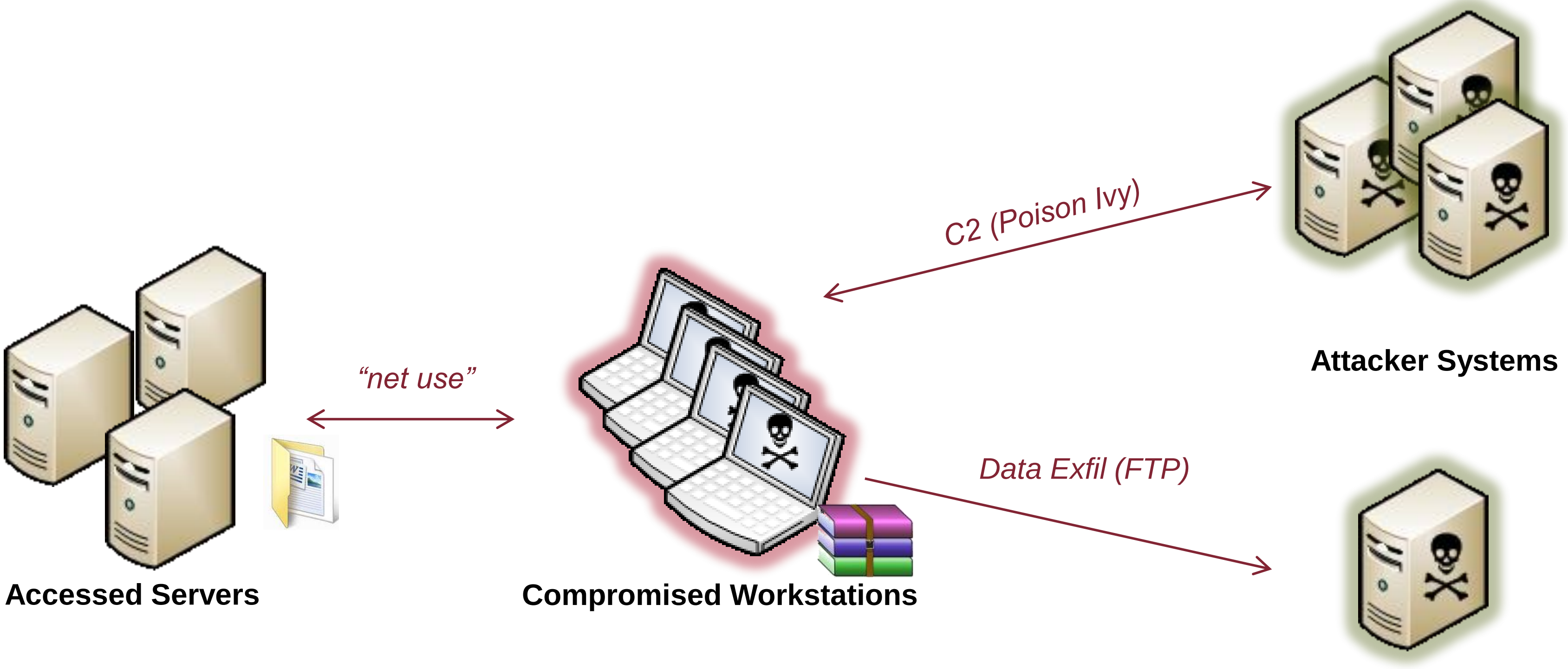
- Why even maintain your own infrastructure for targeted attacks?
- Webmail or social sites for C2
- Online storage sites (Dropbox, Sugarsync, Google Docs) or webmail for file transfer
- Detection vs. anonymity?

Case #3:
Down the Tunnel,
Through the Loop

The Scenario

- Small enterprise of about 2,000 hosts
- Attack activity attributed to one group
- Over 150 compromised hosts

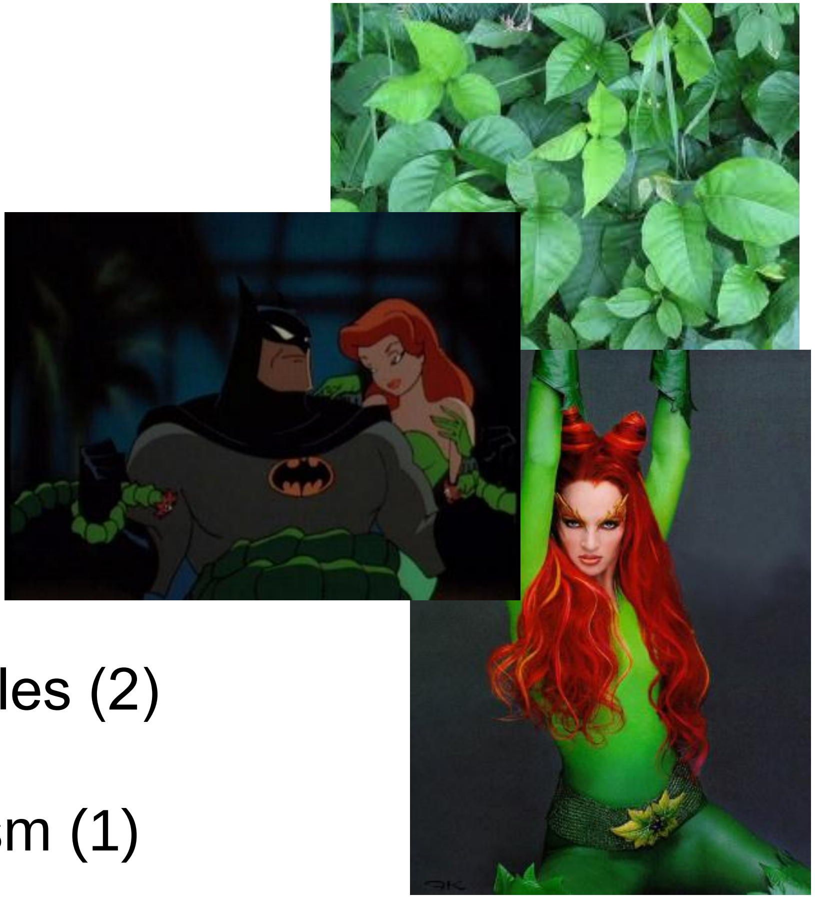
Incident Phase 1



- 150 compromised systems – mainly workstations
- 38 malware variants incl. 10 Poison Ivy variants
- ~20 C2 DNS and IP endpoints
- Exfil via 2GB multi-part RAR files staged on workstations and uploaded via FTP

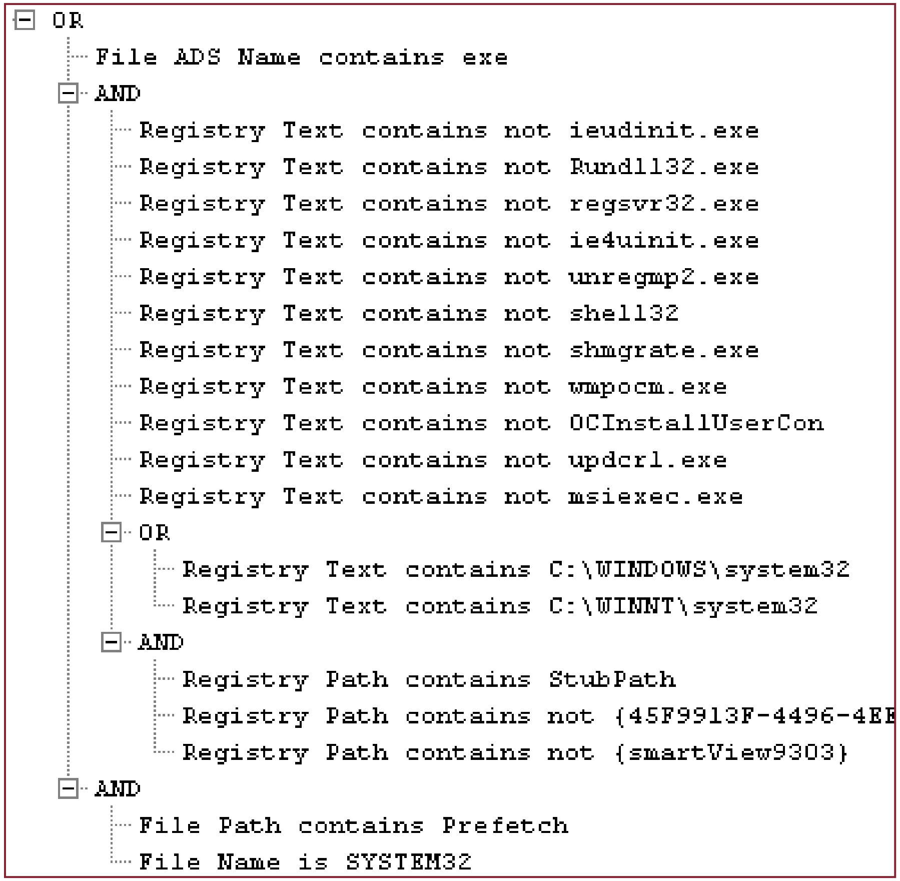
Mixing it up

- Poison Ivy Variations (> 12 samples)
  - MD5s
  - File sizes
  - File names
  - Packing methods
  - Hard-coded C2 addresses
  - Network encryption keys
  - Mutant handles in memory
- Consistencies
  - Installer path (1)
  - Alternate Data Stream “host” files (2)
  - Injected process (2)
  - Registry persistence mechanism (1)



Poison Ivy IOC

- Developed specific and generic Indicators of Compromise (IOCs) based on characteristics in memory, disk, and registry
- Examined each host in the environment for these indicators

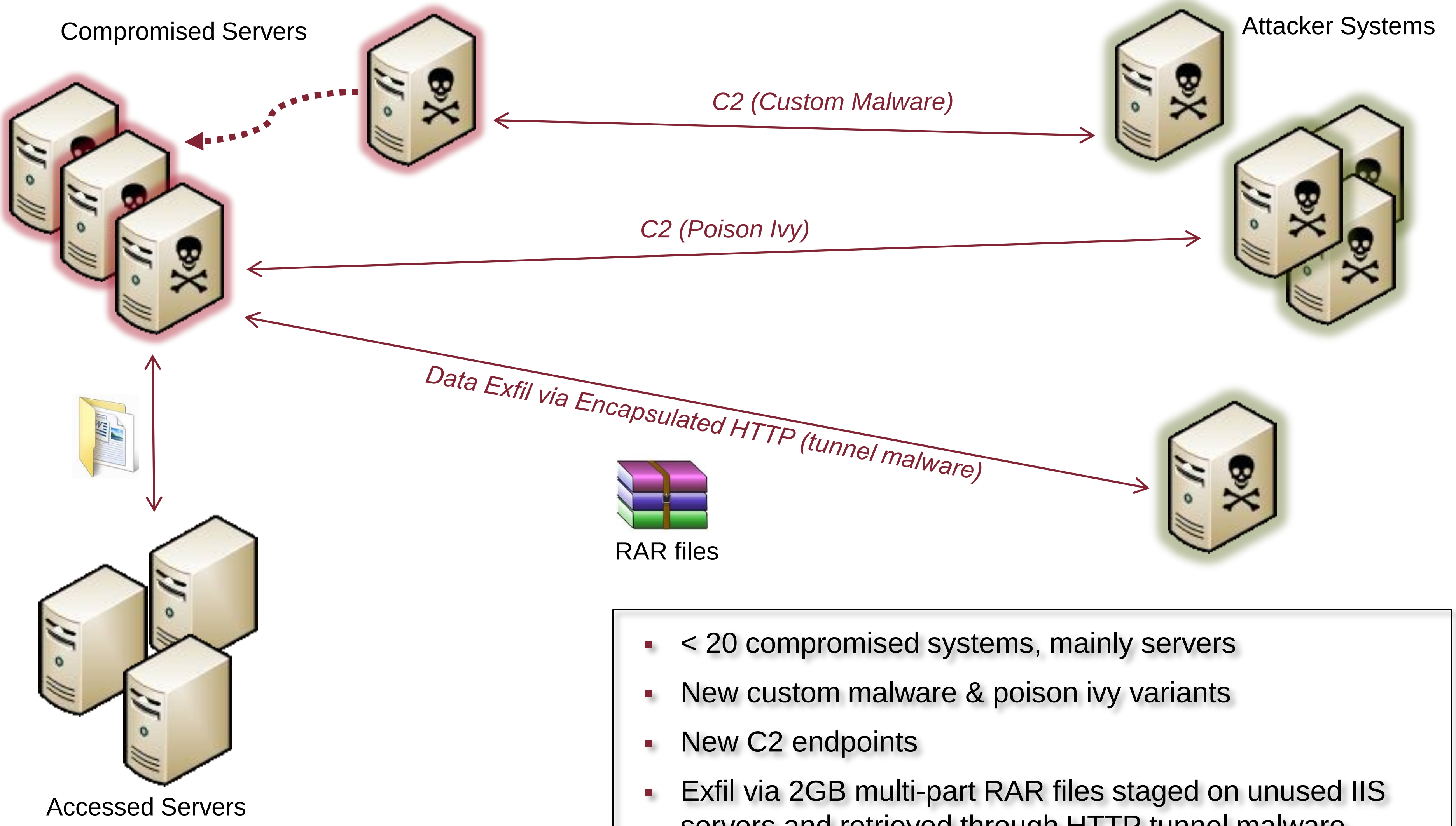


```
OR
    File ADS Name contains exe
    AND
        Registry Text contains not ieudinit.exe
        Registry Text contains not Rundll32.exe
        Registry Text contains not regsvr32.exe
        Registry Text contains not ie4uinit.exe
        Registry Text contains not unregmp2.exe
        Registry Text contains not shell32
        Registry Text contains not shmgrate.exe
        Registry Text contains not wmpocm.exe
        Registry Text contains not OCInstallUserCon
        Registry Text contains not updcrl.exe
        Registry Text contains not msiexec.exe
        OR
            Registry Text contains C:\WINDOWS\system32
            Registry Text contains C:\WINNT\system32
        AND
            Registry Path contains StubPath
            Registry Path contains not {45F9913F-4496-4EE
            Registry Path contains not {smartView9303}
    AND
        File Path contains Prefetch
        File Name is SYSTEM32
```

Phase 1: Remediation

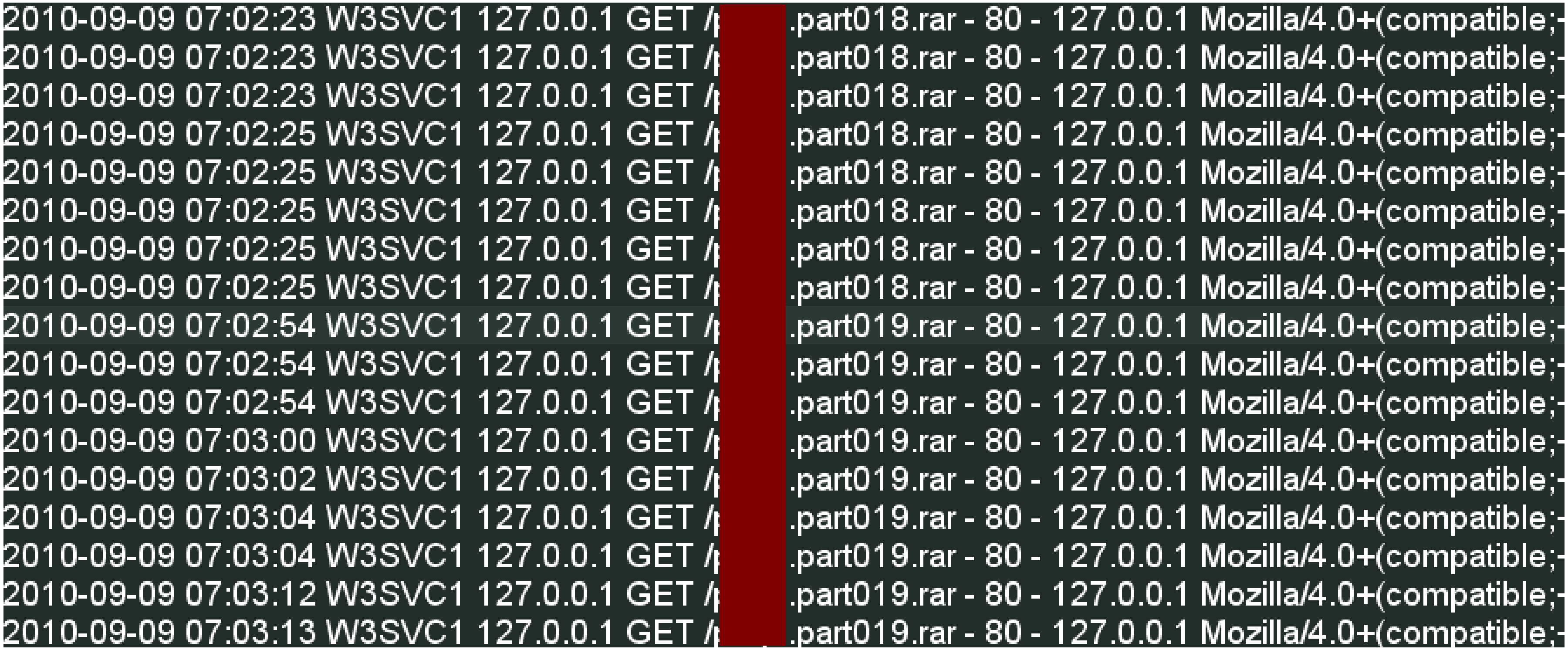
- Victim conducted thorough remediation
  - Rebuilt all systems
  - Changed all local and domain passwords
  - Implemented enhanced network controls and segmentation
  - Implemented enhanced host-based controls
- Attacker regained access to environment several months later

Incident Phase 2 (Re-Compromise)



- < 20 compromised systems, mainly servers
- New custom malware & poison ivy variants
- New C2 endpoints
- Exfil via 2GB multi-part RAR files staged on unused IIS servers and retrieved through HTTP tunnel malware

Sources of Evidence

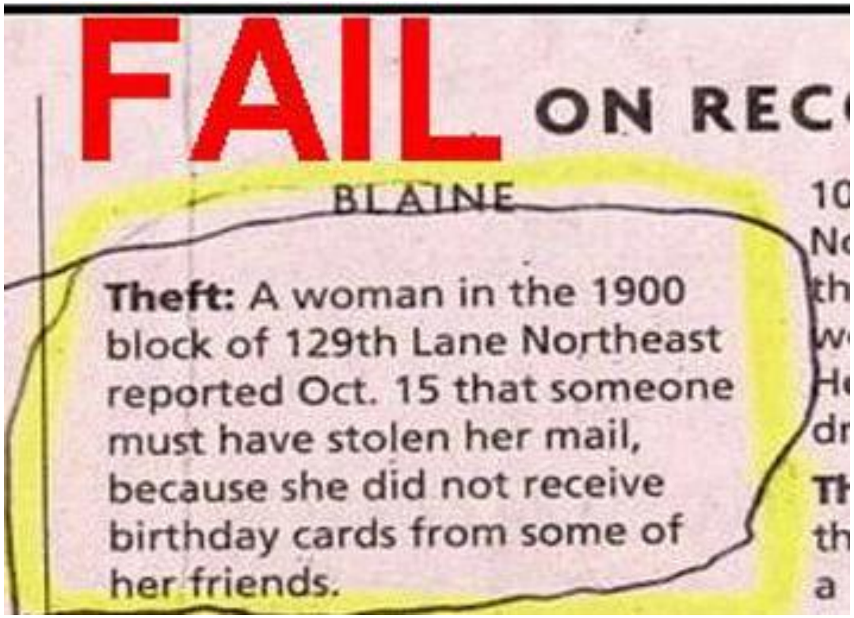


```
2010-09-09 07:02:23 W3SVC1 127.0.0.1 GET /[redacted].part018.rar - 80 - 127.0.0.1 Mozilla/4.0+(compatible;-
2010-09-09 07:02:23 W3SVC1 127.0.0.1 GET /[redacted].part018.rar - 80 - 127.0.0.1 Mozilla/4.0+(compatible;-
2010-09-09 07:02:23 W3SVC1 127.0.0.1 GET /[redacted].part018.rar - 80 - 127.0.0.1 Mozilla/4.0+(compatible;-
2010-09-09 07:02:25 W3SVC1 127.0.0.1 GET /[redacted].part018.rar - 80 - 127.0.0.1 Mozilla/4.0+(compatible;-
2010-09-09 07:02:25 W3SVC1 127.0.0.1 GET /[redacted].part018.rar - 80 - 127.0.0.1 Mozilla/4.0+(compatible;-
2010-09-09 07:02:25 W3SVC1 127.0.0.1 GET /[redacted].part018.rar - 80 - 127.0.0.1 Mozilla/4.0+(compatible;-
2010-09-09 07:02:25 W3SVC1 127.0.0.1 GET /[redacted].part018.rar - 80 - 127.0.0.1 Mozilla/4.0+(compatible;-
2010-09-09 07:02:25 W3SVC1 127.0.0.1 GET /[redacted].part018.rar - 80 - 127.0.0.1 Mozilla/4.0+(compatible;-
2010-09-09 07:02:54 W3SVC1 127.0.0.1 GET /[redacted].part019.rar - 80 - 127.0.0.1 Mozilla/4.0+(compatible;-
2010-09-09 07:02:54 W3SVC1 127.0.0.1 GET /[redacted].part019.rar - 80 - 127.0.0.1 Mozilla/4.0+(compatible;-
2010-09-09 07:02:54 W3SVC1 127.0.0.1 GET /[redacted].part019.rar - 80 - 127.0.0.1 Mozilla/4.0+(compatible;-
2010-09-09 07:03:00 W3SVC1 127.0.0.1 GET /[redacted].part019.rar - 80 - 127.0.0.1 Mozilla/4.0+(compatible;-
2010-09-09 07:03:02 W3SVC1 127.0.0.1 GET /[redacted].part019.rar - 80 - 127.0.0.1 Mozilla/4.0+(compatible;-
2010-09-09 07:03:04 W3SVC1 127.0.0.1 GET /[redacted].part019.rar - 80 - 127.0.0.1 Mozilla/4.0+(compatible;-
2010-09-09 07:03:04 W3SVC1 127.0.0.1 GET /[redacted].part019.rar - 80 - 127.0.0.1 Mozilla/4.0+(compatible;-
2010-09-09 07:03:12 W3SVC1 127.0.0.1 GET /[redacted].part019.rar - 80 - 127.0.0.1 Mozilla/4.0+(compatible;-
2010-09-09 07:03:13 W3SVC1 127.0.0.1 GET /[redacted].part019.rar - 80 - 127.0.0.1 Mozilla/4.0+(compatible;-
```

Source and client IPs are both the same

Aftermath

- Detected data theft while attacker was transferring part 30 of a ~72 part encrypted RAR set
- 2GB per part
- Incomplete multi-part encrypted archive = useless!



FAIL ON REC

BLAINE

Theft: A woman in the 1900 block of 129th Lane Northeast reported Oct. 15 that someone must have stolen her mail, because she did not receive birthday cards from some of her friends.

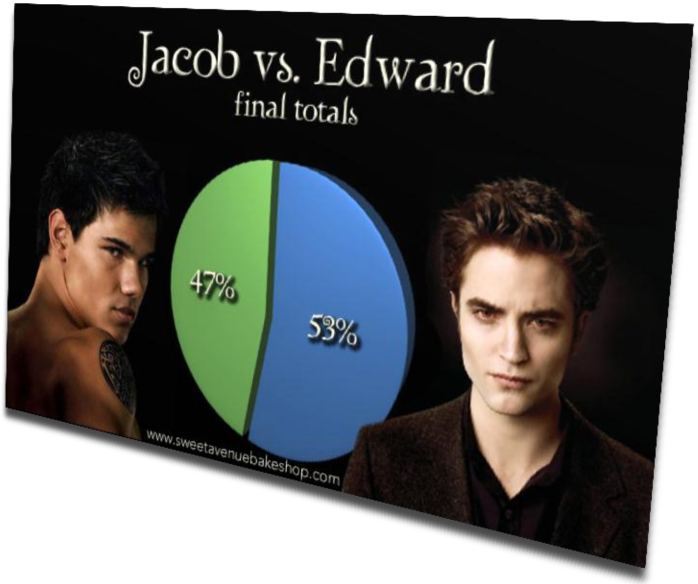
All is Not Lost

Investigating and Preventing Data Theft

- “What was taken?” is often extremely difficult to answer
- Staging is not proof of data theft!
- Long-term, undetected network occupation and data theft is common
- Different strategies for:
  - Single host investigation
  - Enterprise scale investigation
  - Detection and prevention

Host or Network Analysis?

- Often subject to heated debate…
- Need to be adept at both!
- Distinct set of skills and technologies to address each challenge
- Most organizations prioritize network-centric detection



Investigation Techniques

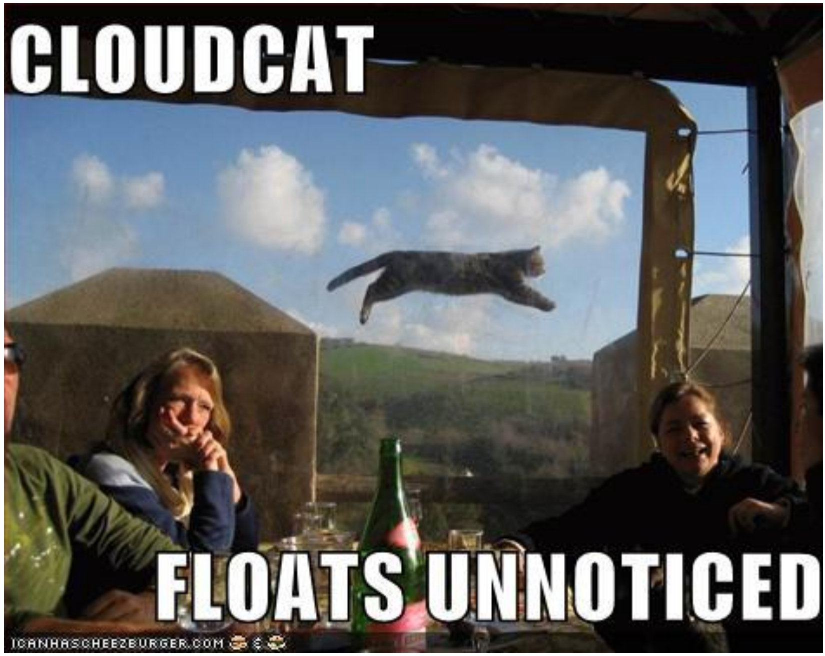
- Single host analysis
  - Traditional file system forensics
  - Directory index records
  - Search & carve archives from unallocated space
  - Examine ShellBags, MRU registry keys
  - ...etc...

Investigation Techniques

- Enterprise scale (e.g. 1,000s of systems)
- Lightweight data suitable for stacking and searching. Examples:
  - Evidence of deleted attacker tools
    - Prefetch analysis
    - Restore point analysis
  - Remnants in staging directories
    - Easy to whitelist common “hiding spots” in Windows
    - e.g. “C:\RECYCLER”, “%SYSTEMROOT%\Tasks”, etc.
  - Local logon events implicating lateral movement

Network Logs

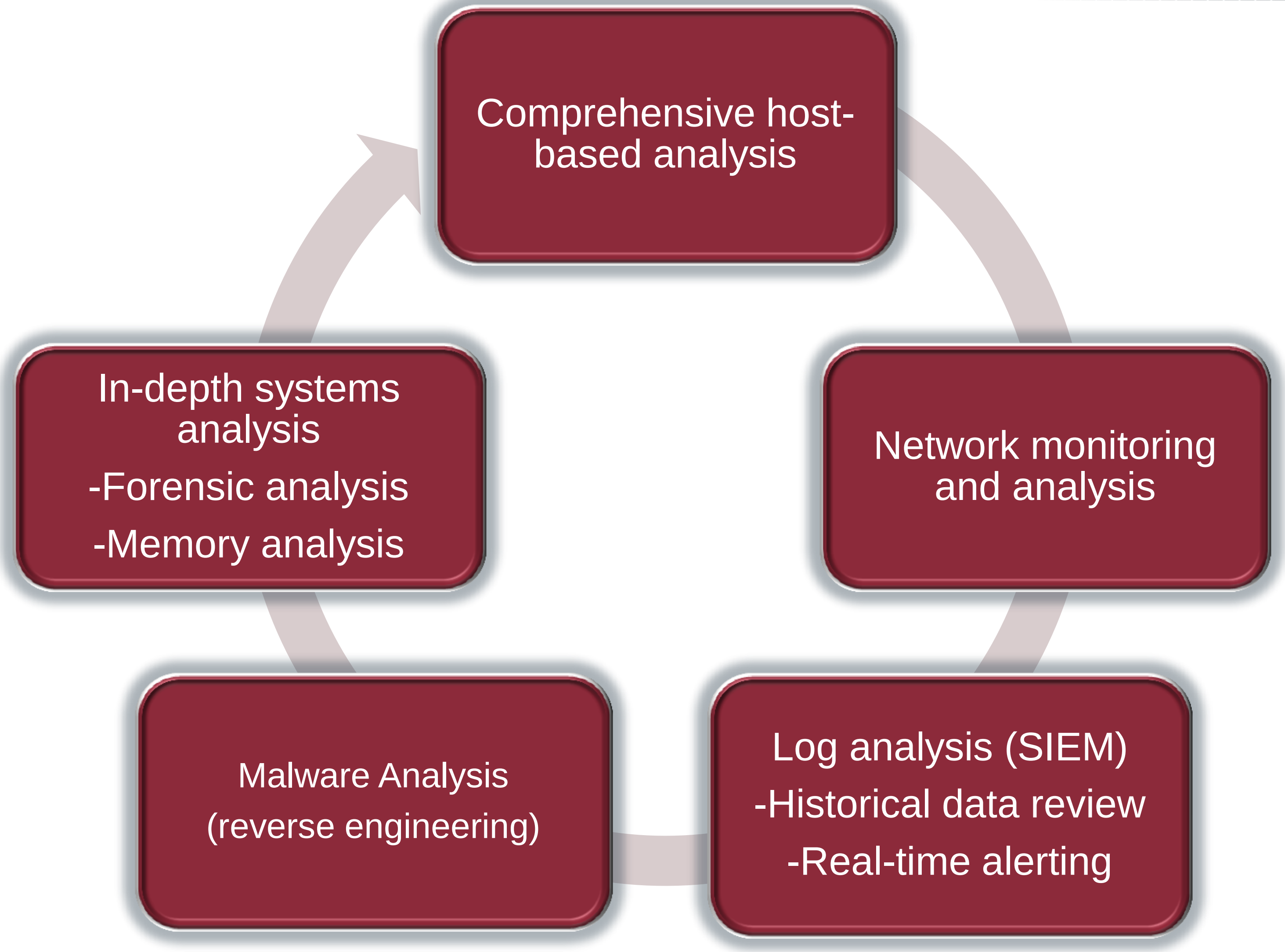
- High-volume data transfers usually detected *after the fact*
- Next steps often unclear
  - Can you map the traffic back to a single / several offending hosts?
    - DHCP logging?
    - DNS logging?
    - Web proxy logs?
    - Log retention?
  - What's the threshold for identifying "anomalous" volumes of data to an Internet endpoint?
    - Via FTP?
    - Via HTTPS?



Detection via Netflow: Look within…

- It is often easier to detect data theft through *internal* netflow monitoring
- Workstations are almost always both the initial entry points and staging points
- Baseline “normal” netflows between workstations and servers / server segments

Investigative approach



Comprehensive host-based analysis

Network monitoring and analysis

Log analysis (SIEM)

-Historical data review

-Real-time alerting

Malware Analysis

(reverse engineering)

In-depth systems analysis

-Forensic analysis

-Memory analysis

Windows Security 101

- Inhibit lateral movement to limit data theft opportunities
- Internal network segmentation
  - Host-to-host
  - Host-to-server
  - Admin LANs
- Lock down Local Admin
  - Remove Local Admin from ordinary domain users
  - Unique Local Admin passwords on each system

Don’t Panic!

- Avoid knee-jerk responses to detected breaches
- You probably only know a small piece of a larger puzzle
  - Compromised systems
  - Accessed systems
  - Malware and utilities in place
  - Malicious network endpoints
- Incomplete response ensures attacker adaptation and persistence

Marathon, not a sprint

- Truths about targeted attacks
  - They were there for a reason
  - They will try to come back
- Plan for their return
- Maximize the costs of exploitation, data theft & persistence

Resources

The bad guys have them, do you?

Free resources

- Free tools
  - IOCe
  - Memoryze
  - Audit Viewer
  - Highlighter
  - Red Curtain
  - Web Historian
  - First Response

- Resources
  - M-trends
  - M-unition
    - blog.mandiant.com

- Webinar series

www.mandiant.com

Special Thanks

- Matt Oldham
- Anne Mroczynski
- Kevin Albano
- Bob Sengupta
- Kyle Dempsey
- Nick Harbour
- Steve Davis
- Christina Padron
- Jed Mitten
- Wendi Rafferty
- Christopher Glyer
- The Whole MANDIANT Team

Q&A

MANDIANT is hiring

- Positions in
  - Consulting, federal and managed services
  - Product development
  - Sales
- Locations
  - Washington
  - New York
  - Los Angeles
  - San Francisco
- http://www.mandiant.com

Sean Coyne | Consultant

Ryan Kazanciyan | Principal

MANDIANT®

The Getaway

Methods and Defenses for Data Exfiltration

Black Hat DC 2011