VESTIGE
Digital Investigations

Incident Response: from a Forensic Perspective

TURNING DIGITAL EVIDENCE INTO INTELLIGENCE™

NKU Cybersecurity Symposium
October 11, 2018

NKU NORTHERN KENTUCKY UNIVERSITY

5:00 AM

Agenda

1. Foundations
2. Preservation
3. Analysis
4. An Effective IR Plan

From Our Perspective

We are parachuted in to organizations to solve problems

- We are Electronic Evidence Experts
- Specialize in:
  Digital Forensics & CyberSecurity
  - 19 Years in CyberSecurity
  - 17 Years in Digital Forensics

  - Incident Response / Data Breach
    is a large percent of what we do.

Why?

Incident Response Planning

the most
important

It’s All Your Perspective

Operational

- What do we do?
- How do we get them outta here?
- Was this a career-altering event?

Leadership

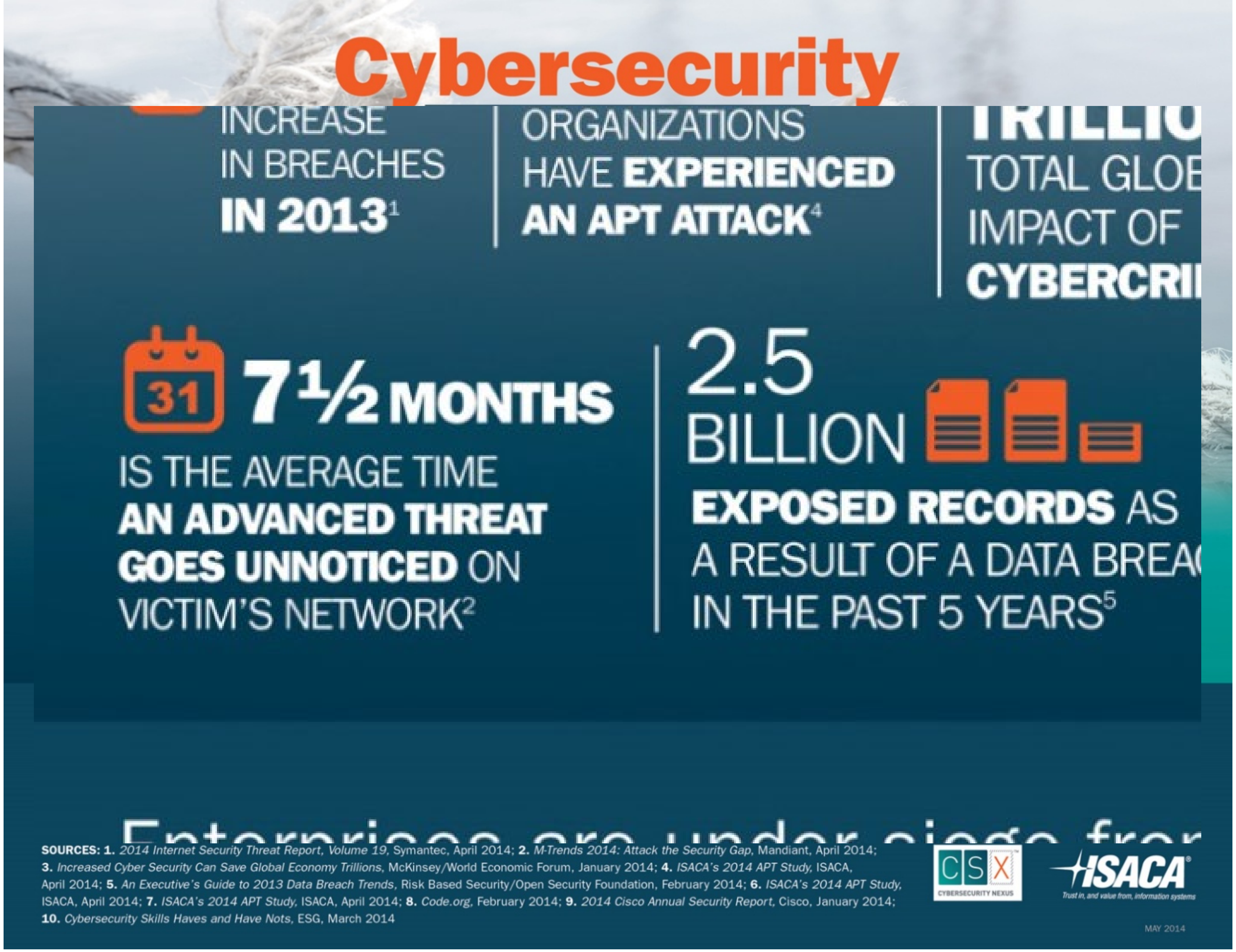
- How do we know we got everything?
- How bad was the compromise…really?
- What got compromised…exactly?
- What are our legal obligations?

Attractive Environments

- What Makes YOUR Environment Attractive to an Attacker?
  - Highly Confidential Intellectual Property?
  - Credit Card Data?
  - Other Financial Resources & Transactions?
  - Personally Identifiable Information?
  - Health Information?

Still think you’re not a target?

- “…though there were initial questions as to why a foodbank would be targeted...[he] quickly came to learn that such hacks are perpetrated by robots who do not see information as having belonged to the food bank, but rather a vulnerable IP address.”



Cybersecurity

INCREASE IN BREACHES **IN 2013**[1]

ORGANIZATIONS HAVE **EXPERIENCED AN APT ATTACK**[4]

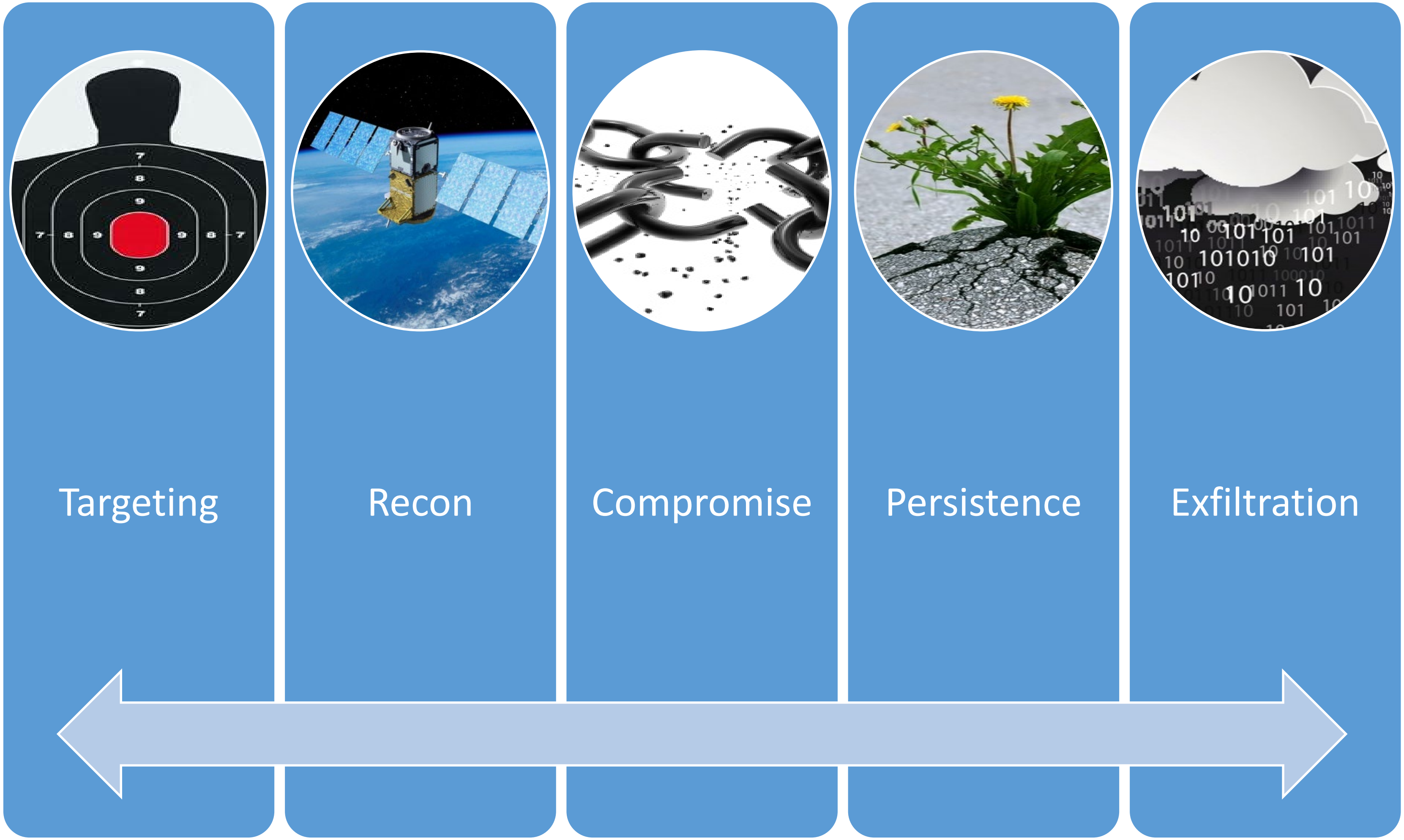
TRILLIO
TOTAL GLOB
IMPACT OF
CYBERCRI

7½ MONTHS
IS THE AVERAGE TIME **AN ADVANCED THREAT GOES UNNOTICED** ON VICTIM'S NETWORK[2]

2.5 BILLION
EXPOSED RECORDS AS A RESULT OF A DATA BREA
IN THE PAST 5 YEARS[5]

Enterprises are under siege fro

SOURCES: 1. *2014 Internet Security Threat Report, Volume 19*, Symantec, April 2014; **2.** *M-Trends 2014: Attack the Security Gap*, Mandiant, April 2014; **3.** *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; **4.** *ISACA's 2014 APT Study*, ISACA, April 2014; **5.** *An Executive's Guide to 2013 Data Breach Trends*, Risk Based Security/Open Security Foundation, February 2014; **6.** *ISACA's 2014 APT Study*, ISACA, April 2014; **7.** *ISACA's 2014 APT Study*, ISACA, April 2014; **8.** *Code.org*, February 2014; **9.** *2014 Cisco Annual Security Report*, Cisco, January 2014; **10.** *Cybersecurity Skills Haves and Have Nots*, ESG, March 2014



Targeting

Recon

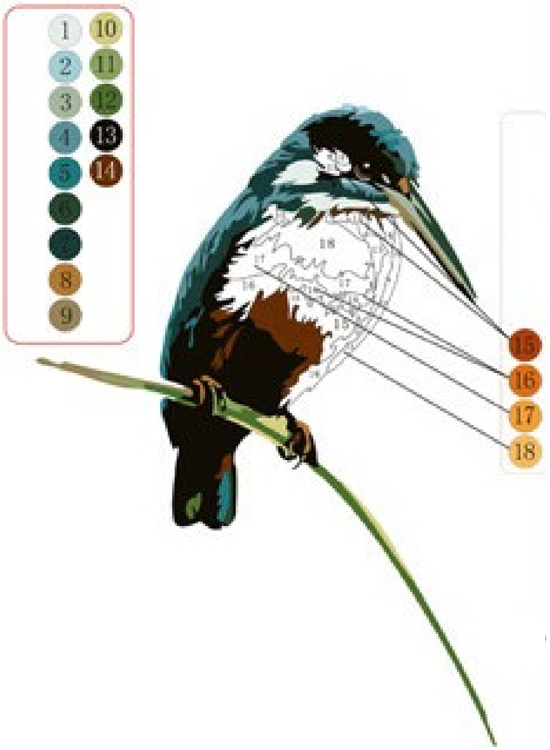
Compromise

Persistence

Exfiltration

THE BEST TIME TO
PLANT A TREE IS
20 YEARS AGO.

BEING
BAD
AT ART


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18

Helpful Evidence

- Disk
- Logs
- RAM
- Configuration Settings
- Network Traffic
- Temporal Information

Importance of Preservation

- Change to 2013 HIPAA omnibus rule

[Incident] “is presumed to be a breach, unless the covered entity can demonstrate that there is a low probability that the PHI has been compromised”

- Expect others to follow

Case Study:
That Shouldn’t Be There!

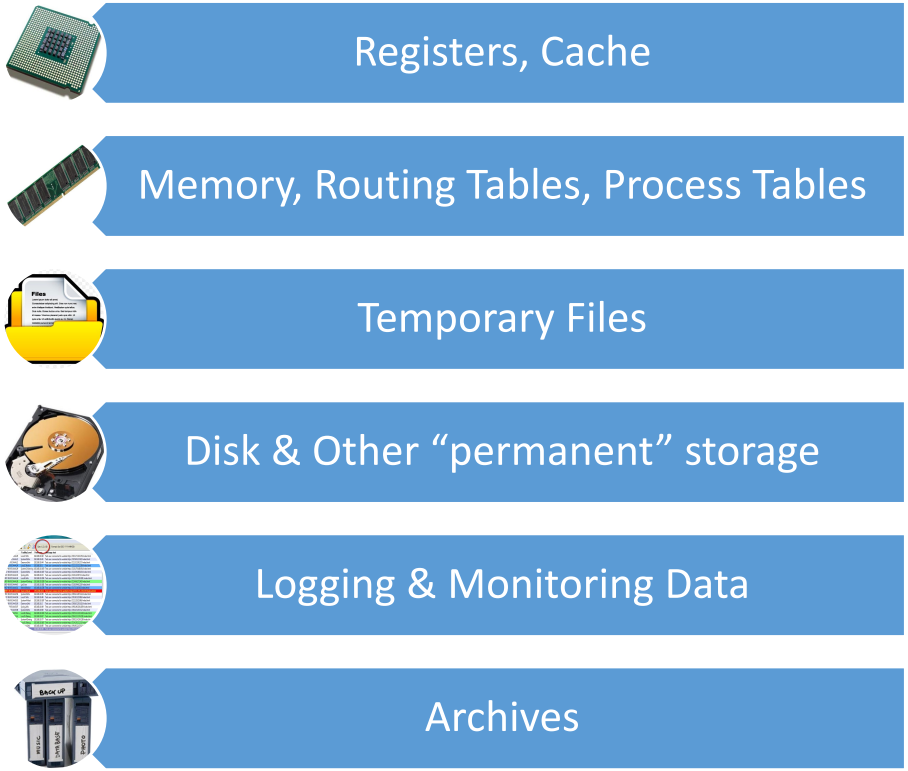
- Financial services company is informed of client list indexed by Google
- Contains SSN, DOB…
- Loss of major client as a result of disclosure
- But, there’s a silver lining…

Preservation

Your Key to Digital Time Travel

Evidence Volatility

- Rate at which evidence disappears



Registers, Cache

Memory, Routing Tables, Process Tables

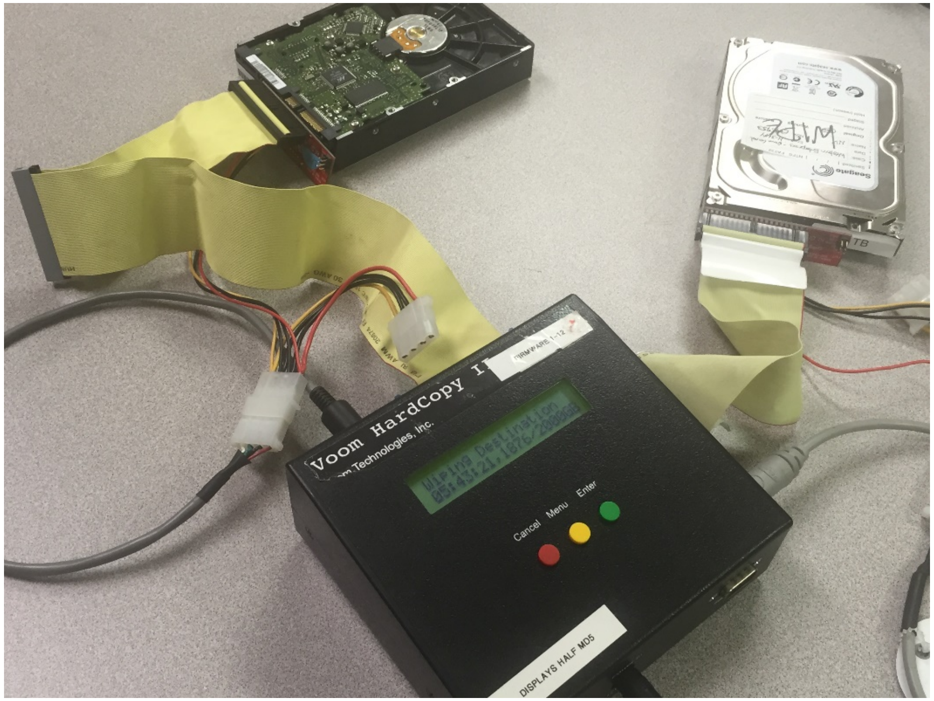
Temporary Files

Disk & Other “permanent” storage

Logging & Monitoring Data

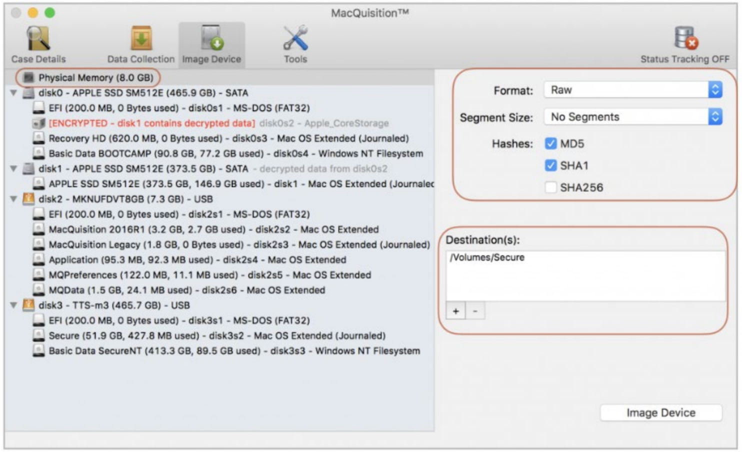
Archives

Evidence Preservation



RAM Preservation

- FTK Imager
- Magnet Forensics Ram Capture
- Belkasoft Live RAM Capturer
- Mandiant Memoryze
- DumpIt
- MacQuisition
- Recon for Mac
- LiME



```
Physical Memory (8.0 GB)
▼ disk0 - APPLE SSD SM512E (465.9 GB) - SATA
    EFI (200.0 MB, 0 Bytes used) - disk0s1 - MS-DOS (FAT32)
    [ENCRYPTED - disk1 contains decrypted data] disk0s2 - Apple_CoreStorage
    Recovery HD (620.0 MB, 0 Bytes used) - disk0s3 - Mac OS Extended (Journaled)
    Basic Data BOOTCAMP (90.8 GB, 77.2 GB used) - disk0s4 - Windows NT Filesystem
▼ disk1 - APPLE SSD SM512E (373.5 GB) - SATA - decrypted data from disk0s2
    APPLE SSD SM512E (373.5 GB, 146.9 GB used) - disk1 - Mac OS Extended (Journalec
▼ disk2 - MKNUFDVT8GB (7.3 GB) - USB
    EFI (200.0 MB, 0 Bytes used) - disk2s1 - MS-DOS (FAT32)
    MacQuisition 2016R1 (3.2 GB, 2.7 GB used) - disk2s2 - Mac OS Extended
    MacQuisition Legacy (1.8 GB, 0 Bytes used) - disk2s3 - Mac OS Extended (Journaled)
    Application (95.3 MB, 92.3 MB used) - disk2s4 - Mac OS Extended
    MQPreferences (122.0 MB, 11.1 MB used) - disk2s5 - Mac OS Extended
    MQData (1.5 GB, 24.1 MB used) - disk2s6 - Mac OS Extended
▼ disk3 - TTS-m3 (465.7 GB) - USB
    EFI (200.0 MB, 0 Bytes used) - disk3s1 - MS-DOS (FAT32)
    Secure (51.9 GB, 427.8 MB used) - disk3s2 - Mac OS Extended (Journaled)
    Basic Data SecureNT (413.3 GB, 89.5 GB used) - disk3s3 - Windows NT Filesystem
```

Format: Raw

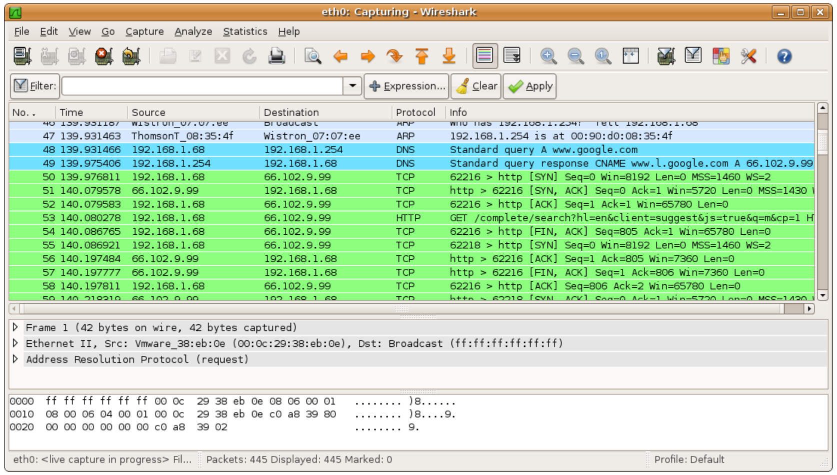
Segment Size: No Segments

Hashes: ☑ MD5 ☑ SHA1 □ SHA256

Destination(s): /Volumes/Secure

Network Traffic

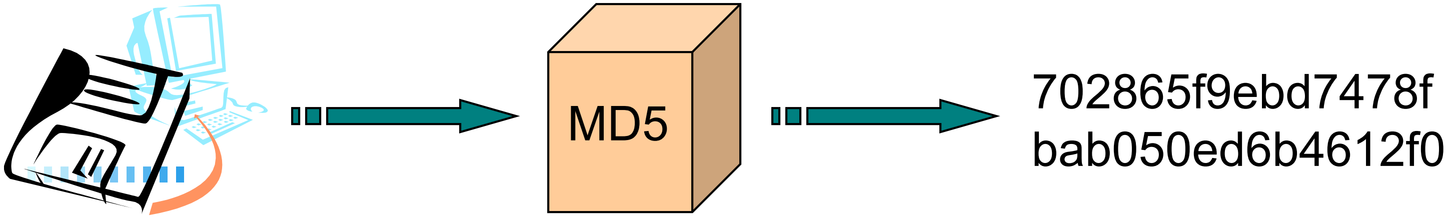
- WireShark
- TCPDump


eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply

```
No. .  Time        Source            Destination       Protocol  Info
    47 139.931463  ThomsonT_08:35:4f Wistron_07:07:ee  ARP       192.168.1.254 is at 00:90:d0:08:35:4f
    48 139.931466  192.168.1.68      192.168.1.254     DNS       Standard query A www.google.com
    49 139.975406  192.168.1.254     192.168.1.68      DNS       Standard query response CNAME www.l.google.com A 66.102.9.99
    50 139.976811  192.168.1.68      66.102.9.99       TCP       62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
    51 140.079578  66.102.9.99       192.168.1.68      TCP       http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
    52 140.079583  192.168.1.68      66.102.9.99       TCP       62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
    53 140.080278  192.168.1.68      66.102.9.99       HTTP      GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
    54 140.086765  192.168.1.68      66.102.9.99       TCP       62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
    55 140.086921  192.168.1.68      66.102.9.99       TCP       62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
    56 140.197484  66.102.9.99       192.168.1.68      TCP       http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
    57 140.197777  66.102.9.99       192.168.1.68      TCP       http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
    58 140.197811  192.168.1.68      66.102.9.99       TCP       62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0

▷ Frame 1 (42 bytes on wire, 42 bytes captured)
▷ Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 0c  29 38 eb 0e 08 06 00 01   ........ )8......
0010  08 00 06 04 00 01 00 0c  29 38 eb 0e c0 a8 39 80   ........ )8....9.
0020  00 00 00 00 00 00 c0 a8  39 02                     ........ 9.

eth0: <live capture in progress> Fil...  Packets: 445 Displayed: 445 Marked: 0        Profile: Default
```

Authenticate

- Our Methodology
  - MD5 Hash – Digital Fingerprint



MD5

702865f9ebd7478f
bab050ed6b4612f0

Authentication

- Authenticate:
  - Prove “no change”
  - Prove Clones ARE the Same
- Method
  - MD5 Hash (digital fingerprint)
    - Industry-standard, industry-recognized
    - 128-bit
    - 1 in 1x10^{38} chance for deceiving
      - 1 in 100,000,000,000,000,000,000,000,000,000,000,000,000
      - DNA Evidence is 1 in 1,000,000,000

Analysis

RAM Analysis

- What you can expect to find:
  - Encryption Keys (AES, RSA)
  - Passwords (Plaintext and encrypted)
  - Running processes
  - Keywords
  - Configuration settings
  - Malware, Rootkits, Worms

Case Study – What card would you like to use?

- Client provides shopping cart services for numerous clients
- Attacker used vulnerability to gain access
- Attempted to email credit card and other personally identifiable information (PII)

FileSystem Analysis

- What you can expect to find:
  - Evidence of persistence
  - Malware
  - Temporal data
  - Time-stomped MACE dates
  - Log files

Traffic Analysis

- Virtualization
  - Open Ports & Listeners
  - Processes
  - File, Registry & Memory Monitoring
- SandBox
  - Beaconing
  - Ingress/Egress traffic analysis

Effective IR Plans

The 6 Ps

IR Plan Basics

- Who has lead responsibility
  - PR
  - IT
  - Legal
- 24x7 contact information
  - How to proceed if unreachable
- Update Cadence
- Prioritization of IT assets
- Preservation steps

IR Plan Basics

- Understand the criteria for notification
- Procedures for notifying LE or other organizations

Best Practices for Victim Response and Reporting of Cyber Incidents. US DOJ Cybersecurity Unit. April 2015.

Protect and Monitor

- Educate your users – repeatedly
- Collect and monitor logs
- Conduct periodic audits
  - Your environment and those connected to you

The Response

- Follow your plan
  - You do have one, right?!

The Response – Plan B

- Strike a balance between remediation and preservation
  - IT wants to remediate
  - Legal and IR team want and need to preserve
- Involve investigation team right away
- Understand the type of data on the compromised devices
    - Is the data encrypted?

The Response – Plan B

- Understand the genesis of the attack
- Understand what data was compromised
- Attempt to determine where the data went
    - Difficult when attack is from unknown entities

The Response – Plan B

- Create a signature of the threatening files
  - Scan environment to reveal additional infections

IR - Expected Time Frame

- IR team is usually on site same day or next day
  - However, this is dependent on up front planning
- “Bleeding” of data stopped in hours
  - May depend on appetite for shutting down internet connection

IR - Expected Time Frame

- Days to weeks to determine:
  - How incident occurred
  - What data was leaked
  - Where data went
- Again, heavily dependent on up front work

Conclusion

- Start with the **end in mind**.
- Up front planning is essential to achieving a proper and expedient response with **manageable costs**
- Ensure you're capturing, saving and managing data **long enough**.
- IR team needs to be consulted immediately **before** any **clean-up** occurs
- Proper preparations for any attack can give your company an advantage

Q&A

Damon S. Hacker, MBA, CCE, CISA, CSXF

Vestige Digital Investigations

Cleveland | Columbus | Pittsburgh
330.721.1205
dhacker@vestigeltd.com
www.vestigeltd.com