Preserving Evidence Before and After an Incident

Nathan Little
Gillware, Chief Investigator
nlittle@gillware.com

hipaacow.org

1

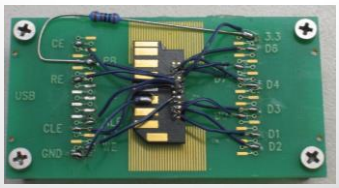
Gillware™ Digital Forensics

- Digital Forensics
  - HIPAA Security Incident Investigations
    - Determine Cause of Incident
    - Determine What Data Was Compromised
  - Data Breach Investigations
  - Criminal Investigations
  - Civil Litigation Support

2

Other Gillware Services

- Cyber Security Audits
- Data Recovery Services
  - Recovery of Data from any failed or corrupted media from SD Cards to multi-hundred terabyte RAID units.



3

Nathan Little

- Chief Investigator at Gillware
  - Contributed to Development of Gillware's Digital Forensics and Data Recovery Software
  - Day to day – specialize in leading incident response investigations, which are often times HIPAA Security incidents

4

Common Challenges in Investigations

- Organization does not preserve enough logs to investigate a situation.
- Logs are preserved in an organization, but are lost during incidents.
  - Logs/Evidence of incident is maliciously deleted by attacker/malicious users
  - Logs/Evidence of incident are lost due to encryption by ransomware

5

What the HIPAA Privacy Rule Says

- PART 164—SECURITY AND PRIVACY – SUBPART C—SECURITY STANDARDS FOR THE PROTECTION OF ELECTRONIC PROTECTED HEALTH INFORMATION

6

- § 164.308 Administrative Safeguards.
  - (a)(1)(ii)(D) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

7

- § 164.308 (a)(5)(ii)(B)- Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.

8

- § 164.308 (a)(5)(ii)(C) - Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.

9

- § 164.308 (a)(6)(ii) Implementation specification: Response and reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

10

- § 164.308 (b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

11

What HIPAA Says Summary

- Regularly review records of information system activity
- Detect and report malicious software
- Monitor successful and failed Logins
- Identify and respond to suspected or known security incidents
- Record and examine activity in information systems that contain or use electronic protected health information

12

What is a SIEM?

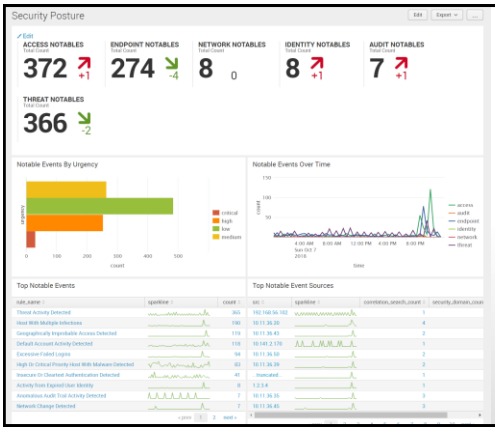
- Security and Incident Event Management
  - Aggregate Logs from All Systems
  - Create Baseline of Normal Activity
  - Detect Anomalies/Creates Security Alerts
  - Most Provide Some Level of Incident Detection
- SIEM Examples
  - Splunk
  - AlienVault
  - ArcSight
  - LogRhythm
  - Many More

13

Challenges with SIEMs

- Significant Management and Review Time
  - Constant Review and Analysis of Alerts
  - Frequent Configuration Changes
- SIEMs Often Require Dedicated Staff
- Large Amounts of Data to Collect
- Ingesting Logs/Events from Some Sources Can Require Custom Integrations

14



15

Quick Splunk Demo

- Live Demo: https://prd-p-9h2hq3hjt7gm.cloud.splunk.com/en-US/app/SplunkEnterpriseSecuritySuite/ess_home
- Splunk's Own Demo: https://www.splunk.com/es_es/resources/video.Uyc2VpbzrepKrXVuF4d0AmH_RD2Fuy-z.html

16

SIEM Solves Problems

- Log Retention in Separate Location
- Detect Security Incidents
- Manage Investigations
- Compliance Audits

17

Questions for SOC

- How would you break in?
- What type of incidents would you not detect?
- Does your incident response plan include network forensics?
- How quickly can you analyze your network traffic data?
- How far back in time can you investigate?
- How far back in time do you need to be able to look?

18

Network Forensics – During Incident

- What you need to be able to answer immediately?
  - What inbound connections came to this system?
  - What connections came out of this system?
  - Bonus: Use SIEM to determine what network connections are abnormal

19

Average Time to Detect an Incident

- 206 Days – 2018 Ponemon Institute Cost of Data Breach Study
- In addition to that, we commonly see vulnerabilities exploited more than once before detection

20

Average Log Retention (Never Long Enough)

- Many logs for organization roll over when space is needed – can be as little as 24 hours for some sources.
- Average log retention is 90 days.

21

Absolute Must Logs

- Login Events (Desktop, Web App, VPN)
- File/Data Access – File Share, 3rd Party Cloud, Web Applications (Not always files)
- Malware Infections
- Network Activity

22

Case 1: An Example of Bad Logging

- Windows XAMP Server Hosting ePHI Configured Incorrectly and Allows Unauthenticated Access
- Access is wide open for four months
- Breach is detected by ePHI being found in Google Index

23

Case 1: Pitfalls

- Proper logging could have detected either increase in ePHI access or the access from new IP addresses
- Data access logging was not set up correctly, only HTTP GET and POST Requests were logged, but not what was returned

24

Case 1: Malicious Get Requests

- GET requests are logged in Apache log file
  - Ex: GET https://compromisedapi.com?set=1
- Based on "set" parameter, a set of ePHI would be returned

25

Case 1: The Challenge in Determining What was Compromised

- Breach went on for four months
- The sets of data returned are different every week – This means that the result returned for "set=2" on September 1is different than the data set returned on September 8

26

Case 1: Incident Response Solution

- The Good
  - Apache Logs were retained forever.
  - The client had weekly backups of the server.
- Parsed the Apache Logs from before mis-config to determine which IP addresses had logged into which users in the past.
  - Any IP that had made authenticated requests previous to mis-config was excluded from breach.

27

Case 1: Incident Response Solution Cont.

- We restored the data folder from each weekly backup.
- Implemented logs to track the patients IDs that were returned based on each query.
- Replayed all Apache access events from IPs that hadn't previously authenticated.
- Inventoried all patient IDs that were in responses to unauthenticated IP addresses.

28

Case 2: The Good Example

- Windows Server 2003 Running IIS is compromised with ransomware
- Company had all internal and external network activity tracked
- Company had all file access logged and imported into SIEM
- We were able to query SIEM and immediately determine that the malware came through compromised FTP credentials

29

Case 2: The Good Example Cont.

- We were able to query the SIEM to determine that there was not unauthorized outbound internet activity – indicating no data was exfiltrated.
- File Access Logging – showed that the compromised FTP user was only used to push the malware onto the system, not exfiltrate data.
- File Access Logging – Showed that the ransomware was deployed when an authorized user access malicious file.

30

Responding To an Incident

- Preserve evidence.
- Evidence is used to prove that it is unlikely that protected health information was not compromised.
- Often, we see systems reformatted after an incident before evidence is collected.

31

Preserve Forensic Images

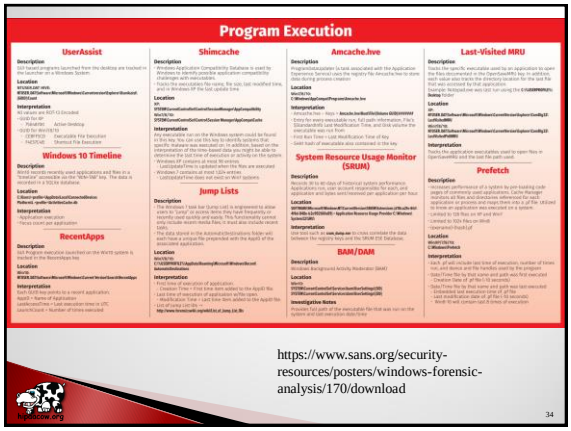
- Collect forensic images (bit for bit clone including free space).
- Common pitfall is to use an application that only backs up active data or user data, which does not contain evidence of deleted data system files.

32

So Logging Wasn't Set up. Now What?

- We use the wealth of Digital Forensic Artifacts left behind on Windows Systems.
- Many Security Analysts are not aware of these sources of data.
- https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download

33



https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download

https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download

Case 3: Remote Desktop Compromise Without Logging

- Workstation with access to ePHI is compromised via RDP access that is open to the world.
- No Object Access Logging enabled on the File Share.

Case 3: Internet Explorer History to the Rescue

IE|Edge file://

Description

A little known fact about the IE History is that the information stored in the history files is not just related to Internet browsing. The history also records local, removable, and remote (via network shares) file access, giving us an excellent means for determining which files and applications were accessed on the system, day by day.

Location

Internet Explorer:

- IE6-7: %USERPROFILE%\Local Settings\History\ History.IE5
- IE8-9: %USERPROFILE%\AppData\Local\Microsoft\Windows\History\History.IE5
- IE10-11: %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat

Interpretation

- Stored in index.dat as: file:///C:|directory/filename.ext
- Does not mean file was opened in browser

Case 3: Result

- Able to use Forensic Artifacts to determine exactly which programs were run and which files were accessed.

Forensic Analysis Demo

- If time permits. Live Demo of Forensic Analysis to prove data exfiltration.

Questions?

- Contact Info
  - Nathan Little
  - nlittle@gillware.com

40