Devonian Health Service

Introduction

It is an unfortunate fact that regional health services will suffer from cyber-attacks and are unable to dig deep into the underlying issues originally causing the breach. This is partially due to the complexity of health networks, but also because of the sensitivity and quantity of the data being collected limits the scope of post-breach investigations [1]. This creates a vicious cycle of breach to recovery, where health institutions can never truly recover from a cyber-attack, draining resources to maintain a losing battle against malicious actors. In a world where cyber-attacks are popular due to lack of enforcement against the perpetrators [2], not investigating is a dangerous move that can lead to proliferation of more cybercrime (and in turn, financial and reputational penalties) against the vulnerable organisation [3].

In this report, an investigative consultation plan for the Devonian Health Service (DHS) will be drafted up to show how an optimal, reactive forensic investigation would be executed. Using the Abstract Digital Forensics Modal (ADFM) [4], the investigation would be split up into several phases and stages. Beginning with acquisition of data, this stage will be critical at gathering key evidence of the means and methods the attackers used in the breach, followed by an examination phase and conclusion. Those two penultimate phases will publish the findings and draw meaningful recommendations for future investigations. This plan will consider financial and ethical concerns at every stage, as well as how effective a live examination would be several months after the initial attack.

Acquisition

Any such examination of data would require an initial point of collection of said data from as many affected sources as possible. The acquisition phase is the collection of that evidence, determining the course of the examination phase and what countermeasures should be deployed against the attackers. In DHS's case, only the Identification and Preparation stages had been performed.

Identification

The identification stage includes the searching and documentation of evidence that may be related to the recent attacks. This evidence can be digital, physical and/or volatile, so some evidence should be prioritised for gathering first if its nature is of high volatility. For example, the registers and cache of all potentially affected digital assets, along with any services DHS offloads to the cloud, should be gathered first since their contents are the most volatile [5]. The author would also include work mobile devices of employees into this prioritised group too, as they are easy to conceal and wipe [6]. Considering that the attacks have been ongoing for several months, the likelihood of recovering volatile evidence is slim, so volatile evidence would need to be gained from future attacks.

The methods of obtention would be many, but considering examples of recent attacks, it would be prudent to gather:

- Network and Intrusion Detection System (IDS) logs.
    - Includes logs for the wireless networks, as the possibility of an insider being present cannot be ruled out.
    - Alerts are often suppressed or ignored by network admins that may contain critical timeline details of how the attackers initially breached the system [7].

  - Analysis of these logs may indicate which machines they managed to successfully compromise.
- Application analysis.
  - Includes all operations performed on emails.
  - This is helpful to gather as it may indicate which accounts are compromised and even if there is an insider leaking information by contacting outsiders.
  - Care needs to be taken when analysing emails however, as it may violate the privacy of the account holder under the Data Protection Act 2018 [8]. Inadmissible evidence gathered without care of this may be invalidated and DHS sued for infringing upon laws of this type.
- Snapshots of machines
  - This includes everything stored on the machine on its original timeline in order to conduct dead analysis. Compared to a live analysis, this allows more freedom of investigation and no risk of malware execution [9].
  - The timeline analysis is particularly important as it may dictate the category of the attacker and where evidence should be gathered. An inaccurate or incomplete timeline may lead investigators to gather innocent suspects, wasting resources on chasing dead ends and putting the collection step at risk of gathering unintegral data [10].
  - So long as volatile data has already been secured, securing snapshots allows analysis of each potentially infected machine to be conducted in an isolated environment where it cannot be altered or deleted [11]. However, this is no substitute for live data which may only be accessible by bespoke programs on a booted machine.

Collection & Preservation

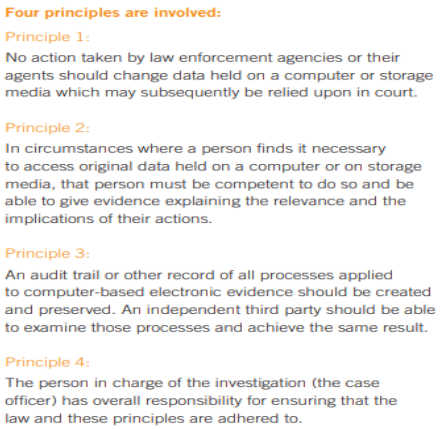

Figure 1: Principles of collecting electronic evidence [39]

As shown in Figure 1, the collection and preservation of the identified evidence is a complex and methodical process, that will determine how relevant the data is in the examination phase. In fact, DHS is currently without principle one and two as they have not sought to conduct the preservation of evidence from previous attacks. Instead, DHS is patching over the symptoms and continuing to use live systems. Since the operating system and its applications of each evidence machine has likely overwritten key information at this point, data integrity is non-existent. As such, the collection and preservation stage will attempt to obtain the identified evidence while ensuring it is admissible, authentic and believable in the context of a board setting. The last point is crucial as the results will need to be presented to a potentially computer illiterate CEO, who has the power to make changes at the highest level [12].

Considering the sensitivity and quantity of the information, this stage may take the longest due to the separate access levels that will be needed to access each level of evidence, ultimately concluding with customer data [13]. Each step of the process would be documented and audited by a lead investigator, to ensure no gaps are missed in the timeline and a singular point of responsibility for each piece of evidence is declared. This is so all evidence can be tracked and admissible according to ISO 27037 [14], albeit at significant financial cost [15].

All evidence should be stored securely using both physical (locked doors, limited access, etc) and digital (e.g. isolated from connectivity) protective measures. In addition, physical documents and access cards/keys should be stored in appropriate packaging, obscured from being directly read and preserves fingerprints. Machines should be plugged in to preserve their battery life but contained in protective materials to prevent damage and interference from electronic signals [16]. Ransomware has previously shown to propagate extremely quickly throughout networks that do not necessarily have the most up to

date software [17], so this connectivity blackout is extremely important. Considering this, significant financial assets may be required to maintain a facility that is capable of the specified requirements.

These measures may seem extreme, but file systems are constantly in flux and are very quick to unintentionally overwrite critical evidence if the opportunity appears. The Master File Table (MFT) and Master Boot Record (MBR) are the core culprits in this scenario, as they contain a record for every file and directory on the system and how it is booted. These files combined allow an investigator to map out a full file system from boot to shut down. But they are continually overwritten while the system is on and in use, so it is crucial that the machines are kept isolated and preferably powered off [18], but that will depend on the result of the initial identification assessment. After-all, databases in constant use cannot be easily seized as evidence for long periods of time. Hence why cold storage of image snapshots is so important early in the investigation.

This is before even considering potential anti-forensics measures the attackers have set up, which includes modifying the MFT and MBR to their own ends. If compromising data has not already been hidden and the machine is still accessible, attackers could connect to it and embed the data with steganographic material or move it into an unexpected location such as RAM or file slack [19]. This makes them a lot more difficult to recover with data carvers and would likely be out of the financial and chrono deadline scope of the DHS investigation.

In extremis, authorisation could be granted for data acquisition on confidential patient databases. This would come with severe restrictions and penalties however, as health information on individuals is heavily regulated [20]. A privacy impact assessment (PIA) evaluates this risk of evidence on the breach against potential financial, reputational and legal repercussions on processing patient data, with a summary action plan to reduce risk if permission is granted [21].

Examination

At this point in the process, incriminating evidence relating to the breach has not been identified, only the sources where it could lie. This is intentional, as it is hard to pinpoint a location of it on each source in a collection potentially hundreds of thousands of records in length after a cursory glance. This is where the examination phase comes in, judging the acquired evidence for its relevance, value and importance to the bigger picture [22]. The bigger picture is of course, halting or mitigating the known, constant cyber-attacks by identifying the root cause, so the examination phase focuses on the evidence relating to that goal.

DHS has seen corporate email accounts compromised that is likely tied into the information leakage issue. User accounts on one network are usually interlinked with several separate information services, so an attacker that has compromised the email account has likely compromised those other services too. Examination of where compromised accounts have logged into would therefore be important to conduct for timeline purposes. Using seized credentials or FTK, an investigator can search both email contents and attachments for evidence of information leakage, suspicious addresses and unexpected authentication attempts, beginning with the highest privileged accounts since these are the most likely to have been targeted [23]. This can be conducted on a dead sample of the system, but the investigation must ensure captured evidence from emails complies with standards that are of reliable relevance to the investigation [24] and to sensitive patient data.

Live ransomware may not be easily examined outside of a dynamic environment when the code is running, since the code is usually obfuscated and resistant to reverse engineering [25]. Nevertheless, DHS has seen

ransomware attacks from the attackers on the system, so it is assumed that machines infected with ransomware would have been acquired for examination. The first steps would be to create a controlled, sandbox, testbed environment based off the compromised services, where both static and dynamic analysis can be conducted safely. This environment depends on the capabilities and configuration of DHS's network layout, but should reflect the operating systems, structure and update state as closely as possible. It should also be easily restorable to its default state, as it is assumed the ransomware would sabotage it, and easily scalable as it would need to reflect the dynamic nature of the large organisation [26]. Using such an environment evidence can be extracted from the ransomware at runtime and rest, including information on the suspect and ransomware type. From this, DHS can build a profile on the attacker to pass over to prosecution services, as well as how to counter the ransomware already on the network with existing weaknesses [27].

Analysis

Analysis of the gathered evidence will vary wildly depending on the type, but it is without doubt that all would be analysed for its worth and relevance to the investigation's goal. This is penultimate stage where a hypothesis is formed to be presented to the CEO of DHS on how and why the breaches continue to take place [28].

One step in this stage would be the data carve reassemble of deleted and hidden data on the seized machines and captured images. Even if anti-forensics has not been implemented in the recent attacks, deleted or corrupted data will need to be recovered from DHS's machines as it can reveal clues and fill gaps in the timeline of attacks. While time consuming and unreliable, data carving can recover an extraordinary quantity of detailed information, which may also include deleted decryption keys for the ransomware and bundles of deleted emails containing incrimination information. DHS can use this knowledge to recover from the cyber-attacks and seek out those responsible. To ensure time conserved and reliability is as high as possible, considerations will need to be taken when carving out the data and evaluating its worth afterwards. For example, if a carved file indicates a suspect uploaded Ransomware to DHS via USB stick on 22nd May, but they were not shown to be in the office on that day, it cannot be ruled out that incomplete carving resulted in a malformed result. Therefore, for each piece of evidence carved, corroborating evidence from the suspect or DHS would need to put forward to verify its validity or invalidity [29]. The reach of data carving is limited however, as modern synchronisation technologies on both mobile and desktop systems means data is constantly uploaded and downloaded from the cloud. Some text and instant message, backup or patient data is included in this, often being encrypted in transit and at rest too. If the data is not held on DHS's cloud instance, they will find that it can take considerable time and effort to gain a warrant for evidence that may no longer be at that facility [30]. Even if it is, encrypted evidence would need to be cracked or exploited to gain access [31] which, while possible, would need to take into consideration the time and effort needed to do so to be relevant to the investigation.

On the topic of cracking authentication, it is possible that investigators may not be able to gain instant access to user accounts that attracted their attention. Whether it is deliberate or not, secured accounts will need to be unlocked in order to conduct any data carving or other evidence extraction methods (e.g. keyword search, regex, etc) can be conducted on them. In instances where these accounts in DHS's network have high privileges, obtaining access may not be possible using existing admin accounts. Therefore, these accounts would need to be broken into using password cracking techniques. Depending on the strength of the password regulations set by DHS, cracking can take an exceedingly long time on a slow machine, so it is possible the investigation will require financial aid in securing a password cracking rig

for the duration of the investigation. To otherwise narrow down the potential password space, the investigator could specialise their password dictionary and ruleset to DHS's industry (e.g. including excessive words relating to health and wellbeing) [32]. Controversially, there is a legal grey area concerning social reconnaissance and engineering techniques on a subject to discover clues on the structure of a targeted password [33]. This will also narrow down the search space since clues are being obtained directly from the target, but does arguably violate privacy laws mentioned above, leaving the evidence open to scrutiny or prosecution [34].

Presentation

At this point in the investigation, the built case contains a detailed account of the investigation and cause of the continuous breaches, as well as recommendations for change identified from the analysis step. This account is likely unreadable to a non-technically savvy audience. Therefore, the ultimate step in the investigation is to restructure the evidence, showing to DHS executives who can digest the streamlined information and draw meaningful impacts, causes, statuses and recommendations from the investigation. The conclusions and lessons that are drawn from this data is what will go on to be used in future training for DHS's employee's [35].

Referring to figure 1, the presentation of data should align closely with principles 1 and 3, meaning data should be presented in as close a format as possible to the original (even if it has been streamlined) and tracked from identification to presentation. The evidence must be able to stand in a court setting since DHS may wish to prosecute the attacker in the future and cannot do that if they submit inconclusive evidence to the jury. On the same note, evidence that is overly complex or indigestible to a member of the public is also likely to be inadmissible in court, since the judge and jury would not be able to understand it [36]. For example, showing logs of intrusive authentication attempts straight from DHS's router may be confusing to a jury, but showing an email thread that shows a suspect leaking information to a media news outlet may not be. In summary, evidence must be sanitised but not changed irrevocably from its original format.

The presentation phase also includes the submission of change recommendations to DHS's current security and operational practices. The recommendations should be tied into the formatted evidence and ideally should source relevant material where the recommendations applied and were effective [37]. For instance, one recommendation could be to set up honeypots of fake, "valuable" information and follow up on who tries to access it in order to leak the fake information. While effective, it will need to be limited in scope and any follow-up action to avoid repercussions from the target [38]. However, it is handled sensibly, it could lead to successful criminal investigations.

Conclusion

Cyber-attacks are an almost constant thorn in the side of organisations, so much so that investigations into each individual cyber-attack is nearly impossible as when one ends, another starts, and attention is diverted away. However, DHS has seen the opposite side of this, where not investigating leads to further and more damaging attacks after the original breach. It is crucial for organisations to investigate thoroughly every successful network breach in order to protect both themselves and customers from ethical, financial, reputational and even life-threatening consequences.

When investigating, there must always be multiple routes to take in order to achieve a successful result and accountability of both evidence and people so that a full timeline can be provided in a court setting. In

the chaos of the aftermath of a data breach, this may be a difficult but pinnacle step to closing the security hole. DHS should consider pre-processing their sensitive health and operational data prior to any investigation, while ensuring full co-operation to verify no stone remains unturned in the search for the attackers and their entrance points.

Works Cited

[1] G. Grispos, W. B. Glisson and K.-K. R. Choo, "Medical Cyber-Physical Systems Development: A Forensics-Driven Approach," 19 7 2017. [Online]. Available: https://ieeexplore.ieee.org/document/8010623. [Accessed 24 5 2021].

[2] Anthony, "Why Is It So Hard To Catch Cybercriminals?," 6 1 2020. [Online]. Available: https://blog.tmb.co.uk/why-is-it-so-hard-to-catch-cyber-criminals. [Accessed 24 5 2021].

[3] N. Goud, "Authorities fail to investigate over 90% of Cyber Crime cases in the UK," 2017. [Online]. Available: https://www.cybersecurity-insiders.com/authorities-fail-to-investigate-over-90-of-cyber-crime-cases-in-the-uk/. [Accessed 24 5 2021].

[4] G. Shrivastava and K. Sharma, "FORENSIC COMPUTING MODELS: TECHNICAL OVERVIEW," 10 2012. [Online]. Available: https://www.researchgate.net/publication/242524844_FORENSIC_COMPUTING_MODELS_TECHNICAL_OVERVIEW. [Accessed 24 5 2021].

[5] Computer Forensics, "Order of Volatility," 29 6 2016. [Online]. Available: https://www.computer-forensics-recruiter.com/order-of-volatility/. [Accessed 24 5 2021].

[6] R. Ayers, S. Brothers and W. Jansen, "Guidelines on Mobile Device Forensics," 5 2014. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf. [Accessed 29 5 2021].

[7] D. B. CARRIER, "Make Better Use of IDS Alerts for Incident Response," 18 2 2016. [Online]. Available: https://www.cybertriage.com/2016/make-better-use-of-ids-alerts-for-incident-response/. [Accessed 24 5 2021].

[8] Legislation UK Government, "Data Protection Act 2018," 2018. [Online]. Available: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted. [Accessed 24 5 2021].

[9] P.-H. Yen, C.-H. Yang and T.-N. Ahn, "Design and Implementation of a Live-analysis Digital Forensic System," 8 2009. [Online]. Available: https://core.ac.uk/download/pdf/206718996.pdf. [Accessed 29 5 2021].

[10] M. K. Rogers, "Psychological profiling as an investigative tool for digital forensics," 2016. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/timeline-analysis. [Accessed 24 5 2021].

[11] M. Kolhe and P. Ahirao, “Live Vs Dead Computer Forensic Image Acquisition,” 2017. [Online]. Available: https://ijcsit.com/docs/Volume%208/vol8issue3/ijcsit2017080331.pdf. [Accessed 24 5 2021].

[12] S. Bommisetty, R. Tamma and H. Mahalik, “Practical Mobile Forensics: Rules of evidence,” 7 2014. [Online]. Available: https://subscription.packtpub.com/book/application_development/9781783288311/1/ch01lvl1sec12/rules-of-evidence. [Accessed 24 5 2021].

[13] KPMG, “BUILDING CYBER RESILIENCE IN ASSET MANAGEMENT,” 5 2018. [Online]. Available: https://assets.kpmg/content/dam/kpmg/uk/pdf/2018/04/building-cyber-resilience-in-asset-management.pdf. [Accessed 24 5 2021].

[14] International Standards Organisation, “ISO/IEC 27037:2012,” 2018. [Online]. Available: https://www.iso.org/standard/44381.html. [Accessed 24 5 2021].

[15] Lineal, “What is the Chain of Custody in Digital Forensics?,” 2021. [Online]. Available: https://www.linealservices.com/what-is-the-chain-of-custody-in-digital-forensics/. [Accessed 24 5 2021].

[16] K. J. Mahoney, “Collecting Evidence,” 2019. [Online]. Available: https://www.relentlessdefense.com/forensics/preserving-collecting-evidence. [Accessed 24 5 2021].

[17] J. M. Ehrenfeld, “WannaCry, Cybersecurity and Health Information Technology: A Time to Act,” 24 5 2017. [Online]. Available: https://link.springer.com/article/10.1007/s10916-017-0752-1. [Accessed 24 5 2021].

[18] C. Tilbury, “NTFS $I30 Index Attributes: Evidence of Deleted and Overwritten Files,” 10 9 2011. [Online]. Available: https://www.sans.org/blog/ntfs-i30-index-attributes-evidence-of-deleted-and-overwritten-files/. [Accessed 24 5 2021].

[19] H. Berghel, “Hiding Data, Forensics, and Anti-Forensics,” 4 2007. [Online]. Available: https://cacm.acm.org/magazines/2007/4/5676-hiding-data-forensics-and-anti-forensics/fulltext. [Accessed 24 5 2021].

[20] Information Commisioners Office, “Special category data,” 2018. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data. [Accessed 24 5 2021].

[21] M. Seyyar and Z.J.M.H.Geradts, “Privacy impact assessment in large-scale digital forensic investigations,” 6 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281720300263. [Accessed 24 5 2021].

[22] I. O. Ademu, D. C. O. Imafidon and D. D. S. Preston, “A New Approach of Digital Forensic Model for Digital Forensic Investigation,” 2011. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.233.1707&rep=rep1&type=pdf. [Accessed 25 5 2021].

[23] A. Spadafora, “Office 365 phishing attacks targets admin accounts,” 2020. [Online]. Available: https://www.techradar.com/uk/news/office-365-phishing-attacks-targets-admin-accounts. [Accessed 25 5 2021].

[24] OUT-LAW GUIDE, “Email as court evidence,” 1 8 2008. [Online]. Available: https://www.pinsentmasons.com/out-law/guides/email-as-court-evidence. [Accessed 25 5 2021].

[25] G. Kaur and B. Nagpal, “Malware Analysis & its Application to Digital Forensic,” 4 4 2012. [Online]. Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.640.1723&rep=rep1&type=pdf. [Accessed 25 5 2021].

[26] M. A. Ahmad, S. Woodhead and D. Gan, “The V-Network Testbed for Malware Analysis,” 2016. [Online]. Available: https://gala.gre.ac.uk/id/eprint/15871/7/15871%20WOODHEAD_V-Network_Testbed_2016.pdf. [Accessed 25 5 2021].

[27] MalwareTech, “Finding the kill switch to stop the spread of ransomware,” 13 5 2017. [Online]. Available: https://www.ncsc.gov.uk/blog-post/finding-kill-switch-stop-spread-ransomware-0. [Accessed 25 5 2021].

[28] M.D.Kohn, M.M.Eloff and J.H.P.Eloff, “Integrated digital forensic process model,” 10 2013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404813000849. [Accessed 26 5 2021].

[29] NIST, “Forensic File Carving Tool Test Assertions and Test Plan,” 4 2014. [Online]. Available: https://www.nist.gov/system/files/documents/2017/05/09/fc-atp-public-draft-01-of-ver-01.pdf. [Accessed 27 5 2021].

[30] D. G. Cantrell and J. R. Through, “TEACHING DATA CARVING USING THE REAL-WORLD PROBLEM OF TEXT MESSAGE EXTRACTION FROM UNSTRUCTURED MOBILE DEVICE DATA DUMPS,” 4 2020. [Online]. Available: https://commons.erau.edu/cgi/viewcontent.cgi?article=1603&context=jdfsl. [Accessed 27 5 2021].

[31] V. n. Singh, “Computer Forensics: A Forensic Approach to Recover Encrypted Data from Digital Evidences,” 1 2015. [Online]. Available: https://www.researchgate.net/publication/277814857_Computer_Forensics_A_Forensic_Approach_to_Recover_Encrypted_Data_from_Digital_Evidences. [Accessed 27 5 2021].

[32] Computerphile, “Password Cracking - Computerphile,” 13 7 2016. [Online]. Available: https://www.youtube.com/watch?v=7U-RbOKanYs. [Accessed 27 5 2021].

[33] M. James, “How Is Social Engineering Used In Ethical Hacking?,” 4 10 2018. [Online]. Available: https://www.theselfemployed.com/article/how-is-social-engineering-used-in-ethical-hacking/. [Accessed 27 5 2021].

[34] Erdal, “Forensic investigation of a Social Engineering attack, from real life,” 7 5 2021. [Online]. Available: https://www.erdalozkaya.com/forensic-investigation-of-a-social-engineering-attack-from-real-life/. [Accessed 27 5 2021].

[35] M. Grobler and S. v. Solms, “FUSING BUSINESS, SCIENCE AND LAW: PRESENTING DIGITAL EVIDENCE IN COURT,” 2009. [Online]. Available: https://journals.co.za/doi/pdf/10.10520/EJC51043. [Accessed 28 5 2021].

[36] Forensic Science Simplified, “Evidence that May be Gathered Digitally,” 2013. [Online]. Available: http://www.forensicsciencesimplified.org/digital/how.html. [Accessed 28 5 2021].

[37] Magnet Forensics, “8 Tips for Presenting Digital Evidence in Court,” 2014. [Online]. Available: http://sarahmackinnonwrites.com/wp-content/uploads/2017/07/Digital-Forensics-Whitepaper-2.pdf. [Accessed 28 5 2021].

[38] M. R. Overly, “Avoiding the pitfalls of operating a honeypot,” 25 11 2019. [Online]. Available: https://www.csoonline.com/article/3455187/avoiding-the-pitfalls-of-operating-a-honeypot.html. [Accessed 29 5 2021].

[39] Association of Chief Police Officers, “Good Practice Guide for Computer-Based Electronic Evidence,” 2021. [Online]. Available: https://www.7safe.com/docs/default-source/default-document-library/acpo_guidelines_computer_evidence_v4_web.pdf. [Accessed 24 5 2021].