

Morgan Stanley



Finding the Needle in the Needle Stack

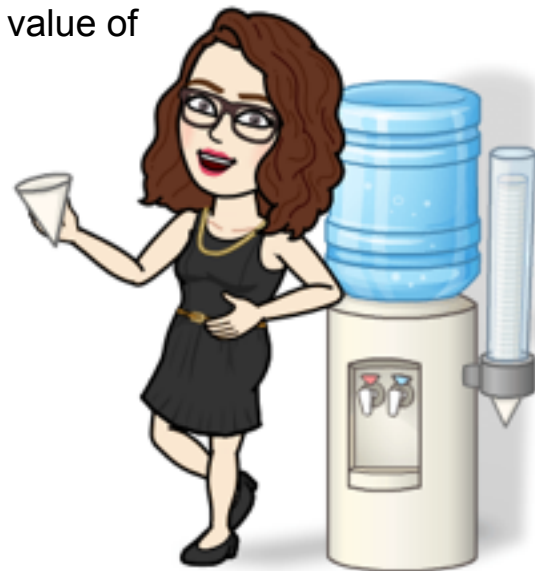
Creative Approaches to Insider Threat Investigations

Emily Wicki

Digital Forensics Examiner, Morgan Stanley

The Needle Stack: Insiders

- Insiders are members of an organization who have information that those outside their organization do not have
- They have authorized access to their organization's systems and data
- They understand how their organization's systems work as well as the value of the data and the value of their work product



Threat Scope

- Organizations come in all sorts of sizes, but each is comprised of people with varied
 - Roles
 - Skills
 - Knowledge
 - Access
 - Influence/s
- Insiders are influenced by their emotions, circumstances, and environmental stressors
- Understanding these variances is instrumental in understanding the scope of insider threats
- The characteristics that make someone valuable as an employee are the same characteristics that would make them dangerous as an insider threat actor

The Needle: Insider Threat Actors

Unintentional Threat Actors

“Accidental Insiders”



Types of Insider Threats

Data theft

Sabotage

Credential/session sharing

Misuse of Firm systems

Policy/security violations

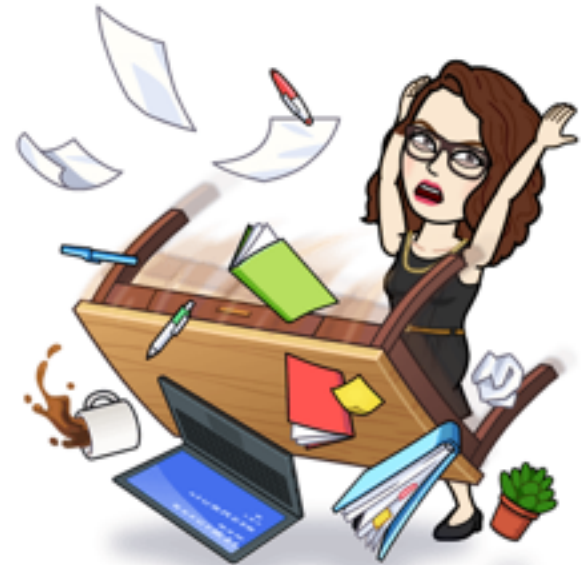
Insider trading/fraud

Harassment, missing persons,
physical threats

Employee poaching/collusion

Intentional Threat Actors

“Malicious Insiders”



Mitigation Efforts

Environmental

Positive organization culture and environment

Healthy/effective management and staff relations

Anticipation of emotional/environmental triggers

Confidential reporting systems

Security and policy training

Technical

Rules of least privilege and properly managed entitlements

Monitoring/anomaly detection

Understanding of the environment

Data hygiene



These mitigation efforts only get us so far...

- Some insider threat actors act with good intentions
- Enabling anomaly detection and/or other monitoring at a large scale enterprise is not as simple as just turning it on
 - Monitoring can be limited by privacy requirements and regulations
 - Not everything can be monitored
- Insider threats are not always anomalous or triggered by distinct events

Insider Threat Forensics Investigations

- Investigations provide us with opportunities to
 - Better understand how insiders interact and behave within our environment
 - Improve monitoring, analytics, controls, and policies
 - Generate a playbook to increase efficiency of response and mitigation
- All of these benefits contribute significantly to the overall goal of
 - Preventing, detecting, and responding to Insider Threats originating from the misuse of authorized access to systems and information



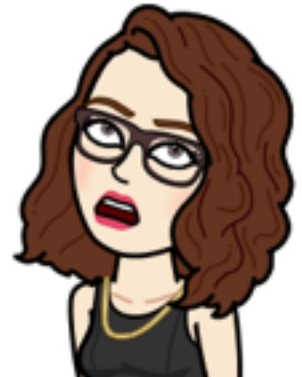
Insider Threat Forensics Investigations Toolset

- Open source tools are exactly what we need:
 - Fast
 - Cheap
 - Flexible
 - Mutable
 - Lightweight
 - Dependable
- This talk will highlight use of:
 - Kansa
 - log2timeline
 - Kibana
 - Autopsy



Finding the Needle in the Needle Stack: **Session Sharing**

- Alice suspects that Bob may have inappropriately accessed restricted information while he was using her machine
- Alice reports that she lent her session to Bob who was reportedly having issues printing, but returned to her session to find that the HR portal was open in Chrome
- Our objectives are to determine
 - Whether there is digital evidence to support that Bob used Alice's session
 - What activity Bob engaged in using Alice's session



Finding the Needle in the Needle Stack: **Session Sharing**

- Use Kibana to review Windows event logs
 - Bob's PC session status
 - Alice's PC session status
 - Print events for both user accounts for the relevant time range
- Collect potentially relevant artifacts from Alice's PC
- Use log2timeline to parse
 - WebCacheV*.dat
 - Identify any documents with file names that match those printed
 - Note access count
 - Chrome Artifacts
 - Review whether the HR portal was accessed
 - Note the method and any other relevant proximity events

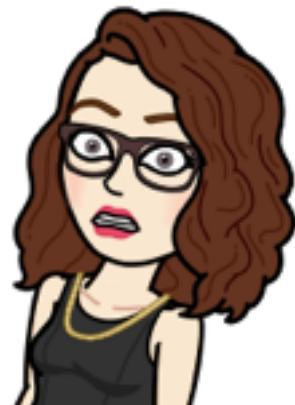
Finding the Needle in the Needle Stack: **Session Sharing**

Time	Event
11:19:12	Alice PC session unlocked
12:00:53	Bob PC session locked
12:01:00	Alice browses to "Shared Network Path\Document1" in the file explorer
12:01:09	Alice prints "Document 1"
12:01:38	Alice browses to "Shared Network Path\Document 2" in the file explorer
12:02:24	Alice prints "Document 2"
12:02:35	Alice browses to "Shared Network Path\Document 3" in the file explorer
12:02:43	Alice prints "Document 3"
12:03:06	Alice browses to the HR Portal using Google Chrome
12:06:58	Alice PC session locked
12:07:16	Bob PC session unlocked
12:10:00	Bob PC session locked
12:47:34	Alice PC session unlocked



Finding the Needle in the Needle Stack: Suspicious Proxy Activity

- Anomaly detection reports a significant number of requests going to a website
- Triage review of proxy logs confirms traffic and indicates one user is generating 99% of traffic
- Our objectives are to determine
 - The nature of this activity
 - Whether there is any data leakage



Finding the Needle in the Needle Stack: Suspicious Proxy Activity

- Use Kibana to review logs
 - Confirm the alert
 - Verify running programs
- Use Kansa to acquire Chrome logs from user's PC
- Parse Chrome logs using log2timeline

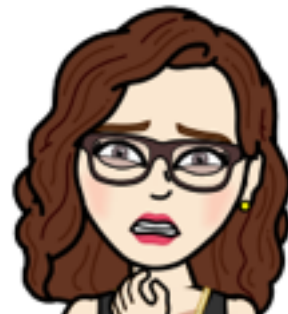
Finding the Needle in the Needle Stack: Suspicious Proxy Activity

- log2timeline output:
 - 06/06/2018, 02:56:01,UTC,.A.,WEBHIST,Chrome History,Page Visited,-,https://superactuallylegitsite.com (Super Actually Legit Site) [count: 0] Host: superactuallylegitsite.com Type: **[RELOAD - The user reloaded the page eg by hitting the reload button or restored a session] (URL not typed directly - no typed count)**,2,OS:C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History,-,sqlite/chrome_history,sha256_hash:39fea74fbe4367f25d1944591cd0d90c849de3c2acfe9e17ce41994de5c98d9b
 - User had over three hundred unique tabs open



Finding the Needle in the Needle Stack: **Employee Poaching**

- An employee was observed printing several documents prior to resigning
- There is concern that they may have taken confidential client information with them upon their resignation
- Our objectives are to
 - Recover copies of the files that had been printed for review
 - Confirm whether this behavior is anomalous for this user
 - Determine if there is any evidence of data leakage by means other than printing



Finding the Needle in the Needle Stack: **Employee Poaching**

- Use Autopsy to
 - Find drive mappings
 - May indicate location of documents, spreadsheets, code, PDFs
 - Search across machine for filename strings
 - Identify emails sent
 - Attachments, keyword hits, direction of mail
 - Review local Internet history
 - Share Point access, etc.
 - Timeline activity throughout interval of printing
 - Identify recent activity
 - Recently accessed files and recent browsing could indicate where non-descript files originated

Finding the Needle in the Needle Stack: Investigation Take-Aways

- Reminder that not everyone has a “security mindset”
- The world record for number of Chrome tabs open is 2,012 tabs
 - (just a few more than 300 😞)

