HIDING IN PLAIN SIGHT: LEVERAGING OPEN SOURCE INFORMATION FOR GREATER SECURITY
IT’S INTERACTIVE

Please submit your questions through the GoToWebinar Control Panel to get answers LIVE from our panelists.
EnergySec is hosting an online chat to accompany this webinar which is open to all registered EnergySec Community participants.

To join the chat as a guest, visit:
https://hipchat.energysec.org/g0kGNyQRW

If you have a HipChat account already, join us in the room.
Note: Registered users have access to the chat history, file attachments, and links
PANELISTS

- Sean Maloney, EnergySec
- Charlotte Goreing, SiloBreaker
- Darrell Johnston, SiloBreaker
AGENDA

1. What is OSINT?
2. OSINT – positives and negatives
3. What is critical infrastructure?
4. Problems faced by critical infrastructure
5. OSINT as a solution
6. Critical Infrastructure: Recent threats & outcomes
7. Investigating critical infrastructure security threats using OSINT tool
8. Q&A
Open-source intelligence (OSINT) is intelligence collected from publicly available sources.
<table>
<thead>
<tr>
<th>POSITIVES</th>
<th>NEGATIVES</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Accessible</td>
<td>• Overwhelming amount of information</td>
</tr>
<tr>
<td>• Freely available</td>
<td>• Easy to miss out on key insights</td>
</tr>
<tr>
<td>• Few (explicit) costs</td>
<td>• Lack of source verifiability</td>
</tr>
<tr>
<td>• Wide range of sources:</td>
<td>• Wide variety of formats</td>
</tr>
<tr>
<td>o Technical and non technical</td>
<td>• Difficult to filter</td>
</tr>
<tr>
<td>o Subject matter experts &amp; general public</td>
<td>• Difficult to action</td>
</tr>
<tr>
<td>o Official and &quot;unofficial&quot;</td>
<td></td>
</tr>
</tbody>
</table>
The Department of Homeland Security defines critical infrastructure as:

The essential services that underpin American society and serve as the backbone of our nation’s economy, security, and health.

“We know it as the power we use in our homes, the water we drink, the transportation that moves us, the stores we shop in, and the communication systems we rely on to stay in touch with friends and family.”

There are 16 critical infrastructure sectors including energy, food and agriculture, dams and chemicals.
CYBER THREATS BY SECTOR

Top sectors under attack:
Critical Manufacturing & Energy

Courtesy of ICS-CERT

Figure 1. FY 2014 incidents reported by sector (245 total).

Has the number of successful cyberattacks your organization has experienced increased in the past 12 months?

Yes

No

Electric utilities and companies in the oil, gas and other energy sectors have seen a rash of cyberattacks, information technology workers say.

COURTESY TRIPWIRE
CORE THREATS & ENERGY INDUSTRY

• Generic malware
• Hacktivism
• Vulnerabilities
• Human error
• State-sponsored activity
Case Study: Lansing Board of Water and Light (April 2016)

- One of the first examples of a utility being hit with ransomware
- Corporate network was infected via a phishing email
- ICS environment remained secure but corporate network was shut down in response

Case Study: Phishing campaigns against AGL customers (May 2016)

- Phishing emails notified customers of a ‘new’ monthly bill service
- Following the link would lead to a malicious .zip file containing Cryptolocker
- Up to 10,000 Australian customers were targeted

An AGL phishing email
Available Intelligence

New strains of ransomware & generic malware
- IOCs can be used to update AV and firewalls.
- Analysis and reporting to maintain an awareness of the threat landscape.

Reports of spam mail or malware
- Track and respond to spam campaigns targeting customers and clients.

Exploit kit activity
- Monitor EK popularity, associated malware and packaged vulnerabilities.
Concerns:

• Legacy systems
  • Designed for durability, longevity, and consistent uptime
  • Not easily replaced, or patched

• Technical information on products is often available online, giving malicious actors a head start.
Available Intelligence

New vulnerabilities in ICS equipment
- Track exploitable/critical vulnerabilities
- Monitor, prepare & remediate

Malicious actors & vulnerability usage
- Detect and evaluate unusual attention
- Spot emerging issues
**OSINT ➔ HACKTIVISM**

- OpNoDapl- Anonymous hijacking Native American protests against Dakota Access Pipeline.
- Threatening DDoS and general petty cyber attacks against ‘all those associated with the pipeline’
- Posting target lists and attack instructions on sites such as Pastebin.
OSINT > HUMAN ERROR

• Unable to breach the computer network of a major oil company, a hacker group targeted the human link, using a watering hole attack to infiltrate the businesses network.

• Using a malware fragment (.exe file), disguised as a PDF, the employees opened and browsed the fake menu, even accepting a prompt asking for access (it’s a familiar menu on a familiar site), and the hackers gained access to the businesses computer network.

• Industry specialists who dealt with the breach did not disclose details of the case, but the message is clear: even the most secure system is only as strong as its weakest link.

• Industry consensus is that human error is the major cause of data and system breaches; “52% of security breaches are caused by human error” (CompTIA)
• EnergySec ISAO team currently evaluating SiloBreaker
• Network tool - Invaluable visualization aid
• Extremely rich set of Entities
• The “SEIM” of OSINT
QUESTIONS?
THANK YOU!