

# 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.







# IT'S HIP TO CHAT

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

Newspapers  
&  
Magazines

Websites

Social media

## Open-source intelligence

Open-source intelligence (**OSINT**) is intelligence collected from publicly available sources.

Paste sites

Government  
reports

Blogs



# OSINT

## POSITIVES

- Accessible
- Freely available
- Few (explicit) costs
- Wide range of sources:
  - Technical and non technical
  - Subject matter experts & general public
  - Official and "unofficial"

## NEGATIVES

- Overwhelming amount of information
- Easy to miss out on key insights
- Lack of source verifiability
- Wide variety of formats
- Difficult to filter
- Difficult to action

# CRITICAL INFRASTRUCTURE

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.”

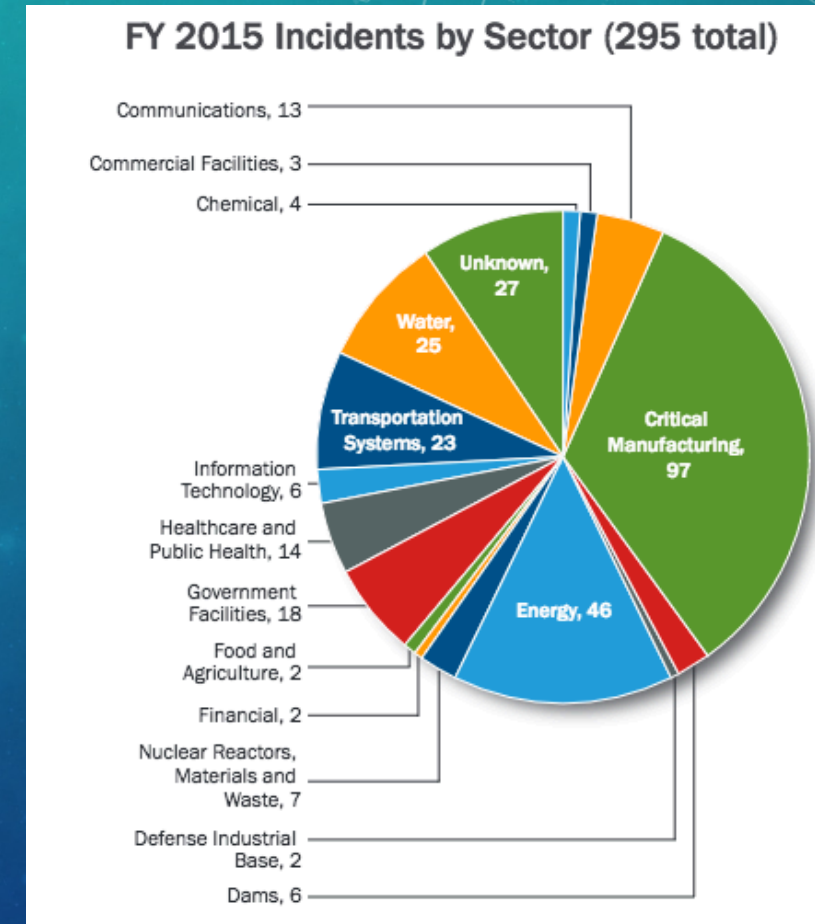
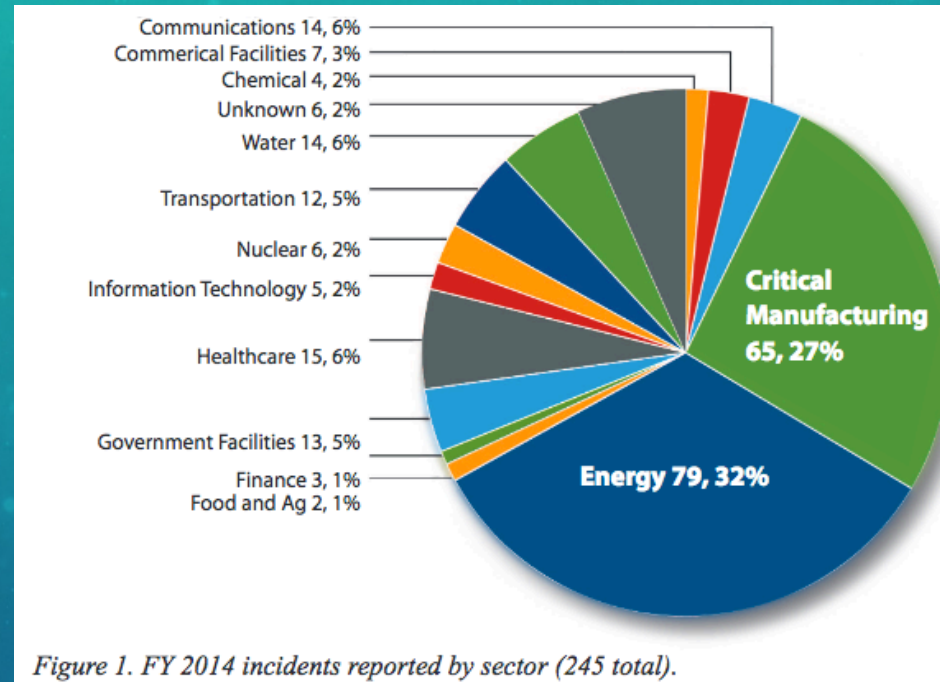
There are 16 critical infrastructure sectors including energy, food and agriculture, dams and chemicals.



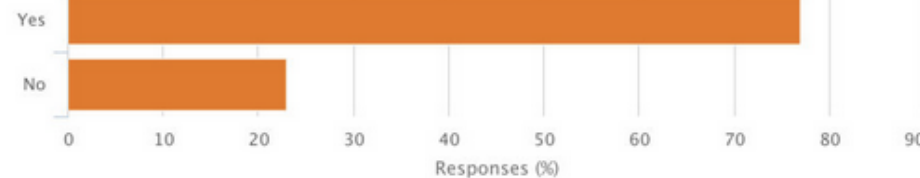
# CYBER THREATS BY SECTOR

Top sectors under attack:  
Critical Manufacturing  
&  
Energy

Courtesy of ICS-CERT



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



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



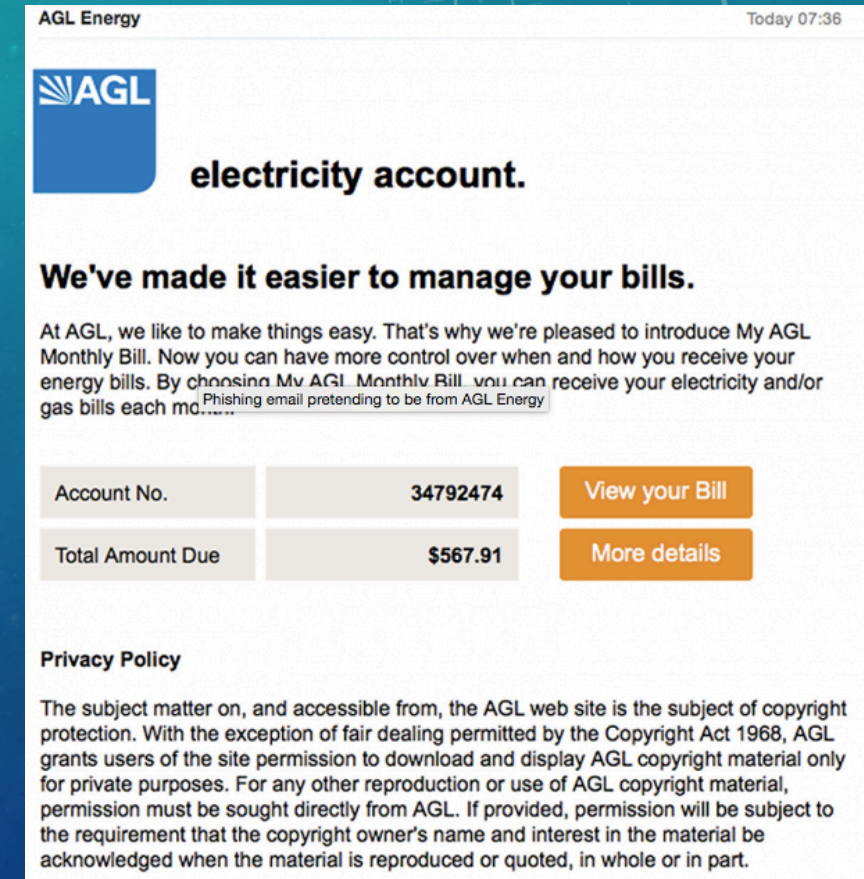
# OSINT > GENERIC MALWARE/CAMPAIGNS (1)

## 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*



# OSINT > GENERIC MALWARE/CAMPAIGNS (2)

## 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.

```
60. Malware:
61. - encoded on download, filesize 163332
62. 557ecdd50394a5d7f8c4ab8a601181daab05c546ad1f46f7e0b1e2ecfdc8774b http___charge2go.com_coplbr
63. bbb7ddaa902d8b841fa61d19b1d660c700cafddec6b2d5e053869b013b748b730 http___dangras.net_3geg2zj
64. dd08228c392f453fca3c2a7ce9704f459adfb877a11dc8678f28780c0b23b7a5 http___dangras.net_5edbite
65. dc5af8dedfd5bfd7aba3835016b5c2dd0dedf32c9cd573f87821d4b874bce334 http___dangras.net_6lebt
66. b930bd9a83872fef9f0998d68ba06bce89443fa0a4c53cccef43e54efe8bb29 http___dotcom-enterprises.com_cpqskvx9
67. 980ec589d5235ceddb6b9386104179dadd257e80f7b59b196d8b56e6b56bc1a http___eskrow.ru_gk2sabe
68. 734f88817afd59964e6996a3adacc3578fbb9a2dfb521eb25b18dbc2dfe595b0 http___ferumusky.com_229k9z
69. b101235e9d617498e55d40688ef4482d642ea93a8be9bca1139242582d14ec14 http___ferumusky.com_5o11b5s
```

SPAM CAMPAIGNS EDIT ✕

Q ransomware AND spam AND Locky

**Nicolas Raus** @Nicolas Raus  
Subjects "[Scan] 2016-1003 15:26:26" / "Sent with Genius Scan for iOS." leads to #Locky #Ransomware #Spam #Mail  
[blog.dynamoo.com/2016/10/malwar...](http://blog.dynamoo.com/2016/10/malwar...)  
Oct 03 2016 14:03

**Nicolas Raus** @Nicolas Raus  
Subject "please sign" leads to #Locky #Ransomware #Spam [blog.dynamoo.com/2016/10/malwar...](http://blog.dynamoo.com/2016/10/malwar...)  
Oct 03 2016 14:02

Save Article Add to Report Give feedback

### RIG Replaces Neutrino in Massive Malvertising Campaigns

Security Week - Sep 28 2016 19:50

The RIG exploit kit (EK) might be moving up the social ladder to become the top threat in its segment and leave Neutrino behind, recently observed malvertising campaigns suggest. A malvertising incident that affected the popular website answers.com ...

Entities: Malvertising, Locky Ransomware, Afraidgate, RIG Exploit Kit

[Read Full Article](#)



# OSINT > VULNERABILITIES (1)

## Concerns:

- Legacy systems
  - Designed for durability, longevity, and consistent up-time
  - Not easily replaced, or patched
- Technical information on products is often available online, giving malicious actors a head start.

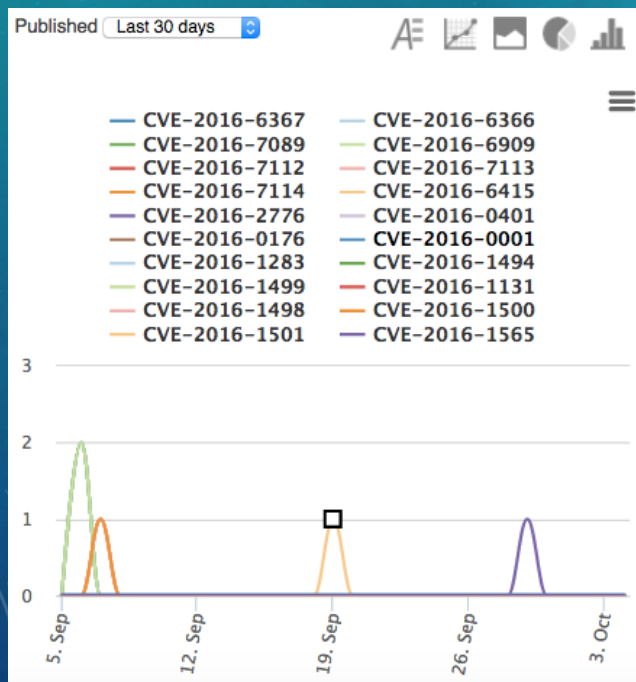
6	Vendor	Device	Default password
7	ABB	AC 800M	service:ABB800xA
8	ABB	SREA-01	admin:admin
9	Adcon Telemetry	Telemetry Gateway A840 and Wireless Modem A440	root:840sw
10	Adcon Telemetry	addVANTAGE Pro 6.1	root:root

# OSINT > VULNERABILITIES (2)

## Available Intelligence

### New vulnerabilities in ICS equipment

- Track exploitable/critical vulnerabilities
- Monitor, prepare & remediate



### Reports (2)

EXPLOIT AVAILABLE - VULNERABILITIES

[View results in Silobreaker](#)

#### Epson WorkForce Multi-Function Printer Firmware Update Handler POST Request privilege escalation

vuldb.com - Sep 26 2016 14:52

A vulnerability was found in Epson WorkForce Multi-Function Printer (the affected version is unknown). It has been declared as critical. This vulnerability affects an unknown function of the component Firmware Update Handler. The manipulation ...

#### OpenSSL 1.1.0a Message Handler buffer overflow

vuldb.com - Sep 26 2016 14:52

A vulnerability was found in OpenSSL 1.1.0a. It has been rated as critical. This issue affects an unknown function of the component Message Handler. The manipulation with an unknown input leads to a buffer overflow vulnerability. Impacted is ...

### Malicious actors & vulnerability usage

- Detect and evaluate unusual attention
- Spot emerging issues

### TOP STORIES

EXPORT

#### Kaspersky Lab Discovers Important Vulnerability In Popular Energy Equipment

Information Security Buzz - Jun 28 2016 05:14

**SIEMENS**

The ISBuzz Post : This Post Kaspersky Lab Discovers Important Vulnerability In Popular Energy Equipment appeared first on Information Security Buzz . While performing a security assessment for one of its clients in the critical infrastructure ...

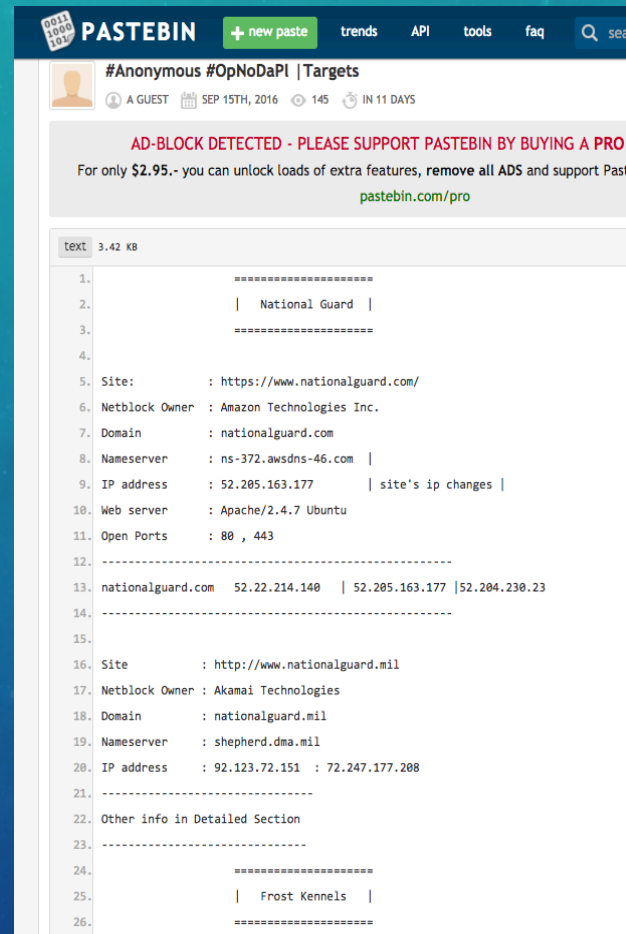
First reported Jun 28 2016 05:14 - 1 reports

Entities: Kaspersky Labs, Vulnerability (Computing), Siemens AG, Security



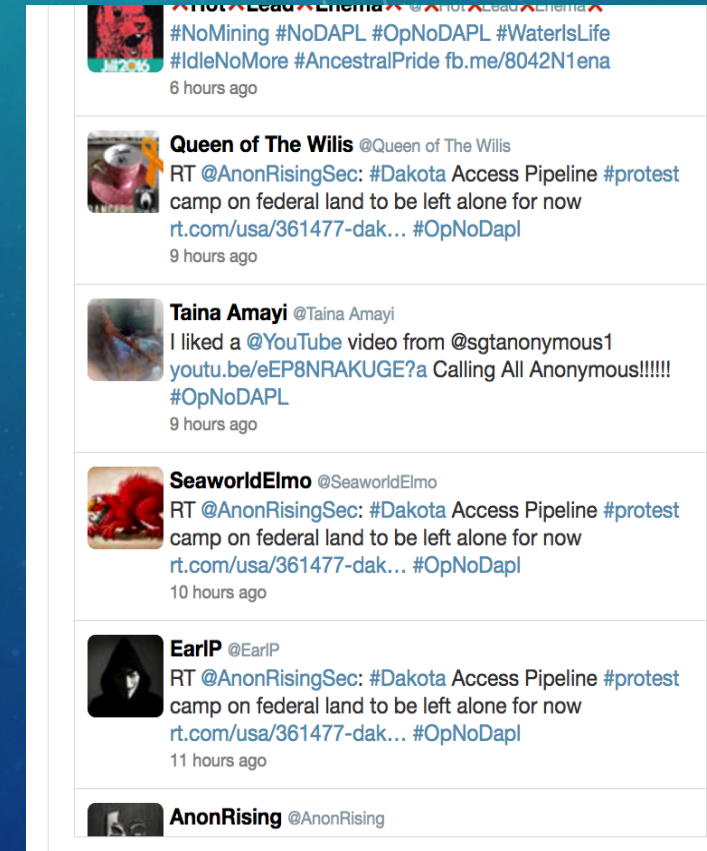
# OSINT>HACKTIVISM

- 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.



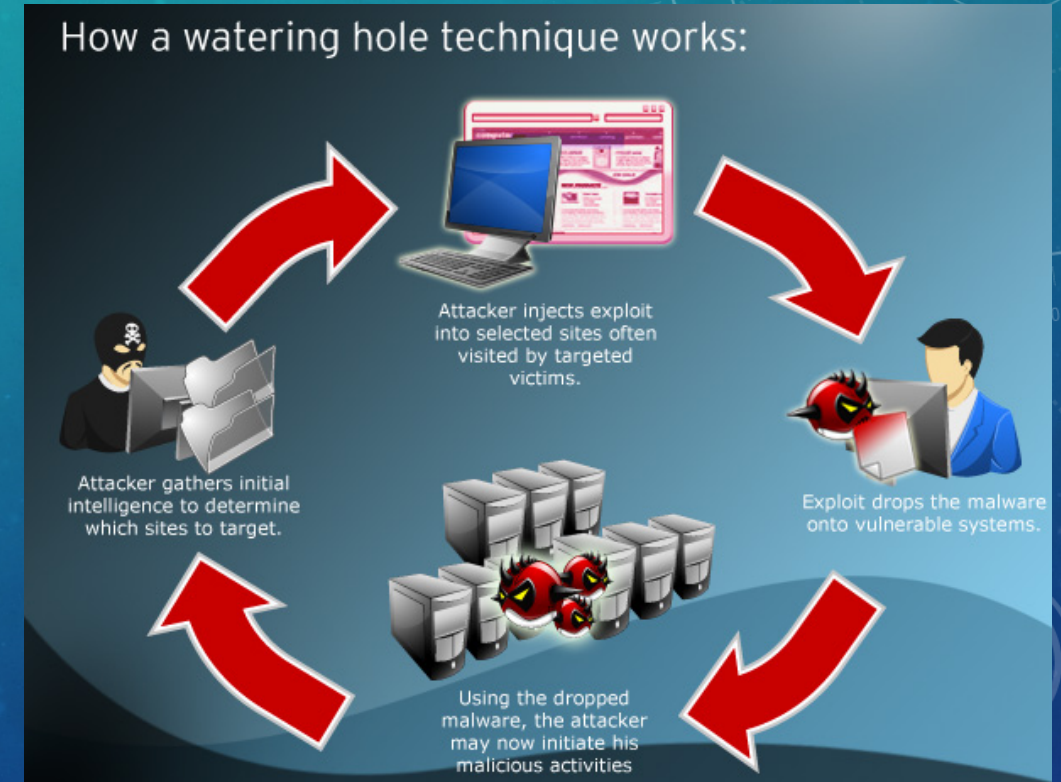
The screenshot shows a Pastebin page with the title "#Anonymous #OpNoDaPl |Targets". The post is by a guest user, dated September 15th, 2016, and has 145 views. A red banner at the top says "AD-BLOCK DETECTED - PLEASE SUPPORT PASTEBIN BY BUYING A PRO A". The main content is a list of targets for the Dakota Access Pipeline protests, including National Guard, Amazon Technologies Inc., and Akamai Technologies. The list includes details such as Site, Netblock Owner, Domain, Nameserver, IP address, Web server, and Open Ports.

```
1. #####
2. | National Guard |
3. #####
4.
5. Site: : https://www.nationalguard.com/
6. Netblock Owner : Amazon Technologies Inc.
7. Domain : nationalguard.com
8. Nameserver : ns-372.awsdns-46.com |
9. IP address : 52.205.163.177 | site's ip changes |
10. Web server : Apache/2.4.7 Ubuntu
11. Open Ports : 80 , 443
12. -----
13. nationalguard.com 52.22.214.140 | 52.205.163.177 | 52.204.230.23
14. -----
15.
16. Site : http://www.nationalguard.mil
17. Netblock Owner : Akamai Technologies
18. Domain : nationalguard.mil
19. Nameserver : shepherd.dma.mil
20. IP address : 92.123.72.151 : 72.247.177.208
21. -----
22. Other info in Detailed Section
23. -----
24. #####
25. | Frost Kennels |
26. #####
```



# 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)





# CLOSING

- EnergySec ISAO team currently evaluating SiloBreaker
- Network tool - Invaluable visualization aid
- Extremely rich set of Entities
- The “SEIM” of OSINT



QUESTIONS?



SILObreaker

**THANK YOU!**

