RSA Conference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: EXP 208R

The Six Most Dangerous New Attack Techniques and What's Coming Next

MODERATOR:

John Pescatore
Director
SANS Institute
@John_Pescatore

PANELISTS:

Ed Skoudis
SANS Instructor
Counter Hack Founder

Johannes Ulrich
CTO & Dean of Research
Internet Storm Center

Mike Assante
Director
SANS Institute

Topics Covered by Ed Skoudis

- Dribbling Breach Data
- Spanking Microsoft Kerberos
- Exploiting the Internet of Things

Dribbling Breach Data

- In the old days, stolen data was usually hoarded secretly or dropped all at once
- Now, there is an increased risk of it being released in dribs and drabs
  - The Sony breach is a perfect example
  - Andrew Breitbart's political releases followed a similar pattern
- This will likely become the new norm
  - Makes it harder for incident responders
- Add this kind of scenario to your incident response table top exercises

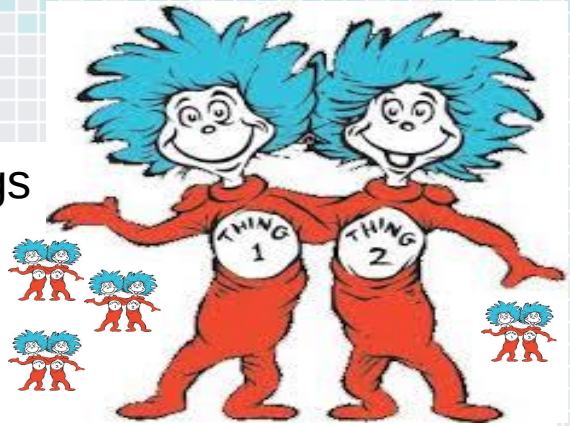
Spanking Microsoft Kerberos

- Over the past decade, attackers have had a field day attacking LANMAN hashes, NT hashes, LM C/R, NTLMv1, and NTLMv2
  - Sniffing, cracking, Rainbow Tables, Man-in-the-Middle (SMB Relay), Pass-the-Hash, etc.
- In the past year, attention has shifted to attacking Microsoft Kerberos
  - Used for authentication in large enterprise environments
  - Was viewed as safer than other Microsoft authentication protocols…
  - …due to lack of tools

Microsoft Kerberos Attacks

- Pass-the-Ticket Attack
  - Analogous to Pass-the-Hash
- Golden Ticket Attack
  - A crafted TGT created by attacker, hashed with the KRBTGT hash
  - Authenticate to *any* service as *any* user
  - Very persistent; hard to eradicate
- Silver Ticket Attack
  - Craft a service ticket with special perms

Exploiting the Internet of Things



- Pwnie Express industry report on Internet of (evil) Things

1) Self-Procured IT and BYOx
   - How can you secure it if you don't know it's there?

2) Proliferation of small, cheap, devices, often with:
   - No replay prevention in protocols, known plaintext repeated
   - XSS and Command Injection
   - These may not seem bad on the surface, but think about them… generating heat (fire?), bricking, and more

3) The Commoditization of Malicious Hardware
   - So low-cost, it becomes disposable hacking technology

Topics Covered by Johannes Ulrich

- Encryption: Security's #1 Frenemy
- DDoS: Size doesn't always matter

SSL is Dead (again)

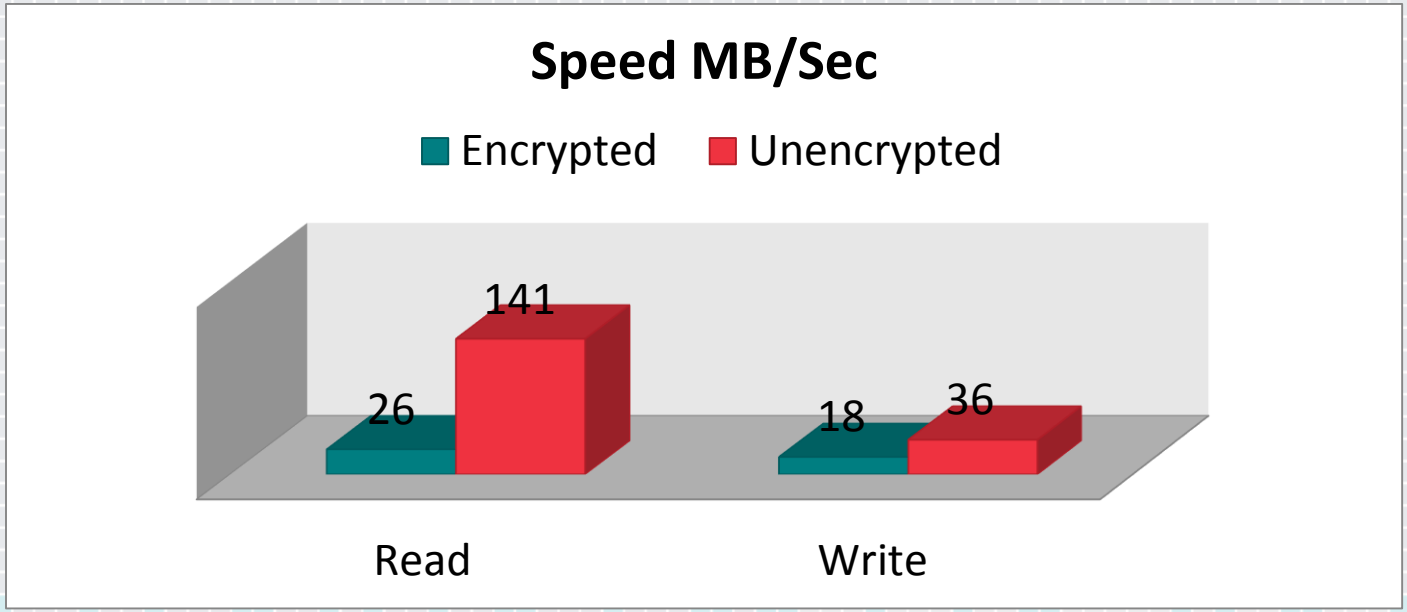
CRIME (2012)

BEAST (2013)

Lucky 13 (2014)

POODLE (2014)

Android: Missing Drivers



Missing Validation / Outdated Code

Threatpost.com

Millions of mobile app users are still exposed to SSL vulnerabilities.

Crypto Ransom-Ware

2014: Desktop cryto ransom-ware becoming a major problem:

- Cryptolocker: ~ 500k victims, > $3million extorted
- Cryptowall: 625k victims, > $1million extorted
- Torrentlocker

SynoLocker™

Automated Decryption Service

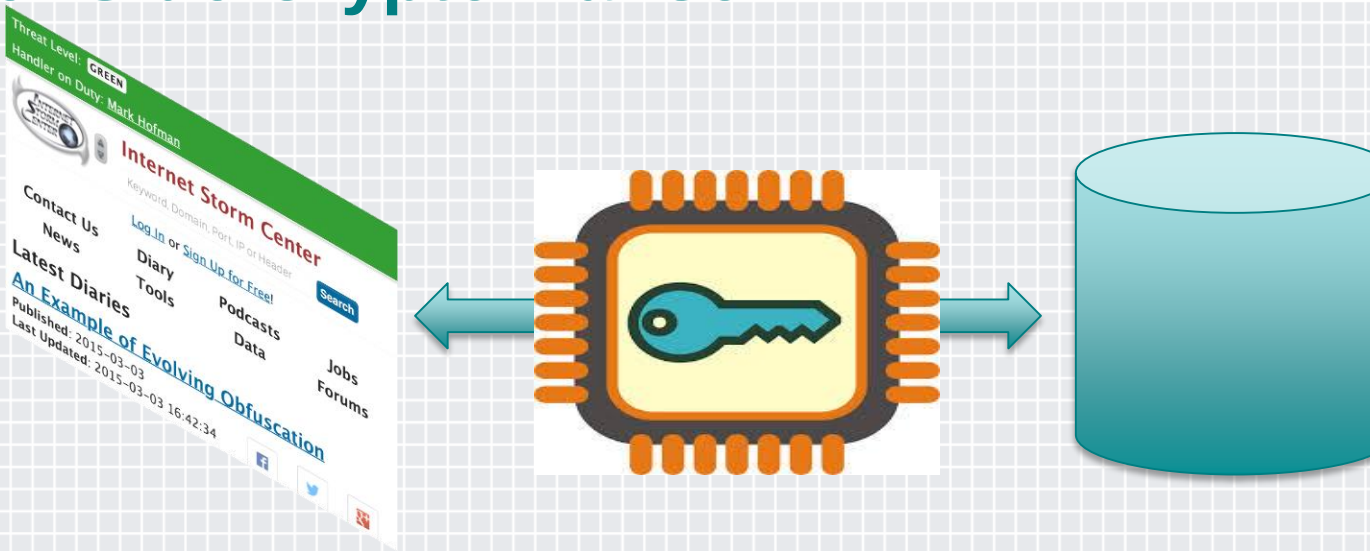
All important files on this NAS have been encrypted using strong cryptography

List of encrypted files available here.

Follow these simple steps if files recovery is needed:

1. Download and install Tor Browser.
2. Open Tor Browser and visit http://cypherxffttr7hho.onion. This link works **only** with the Tor Browser.
3. Login with your identification code to get further instructions on how to get a decryption key.
4. Your identification code is **1LQgMhfRu4HdnC7dinccWtMSQ5toMFsSnV** (also visible here).
5. Follow the instructions on the decryption page once a valid decryption key has been acquired.

Server Side Crypto Ransom




```
if(isset($result['user_password'])){
 $result['user_password'] = $cipher->decrypt($result['user_password']);
}
if(isset($result['user_email'])){
 $result['user_email'] = $cipher->decrypt($result['user_email']);
}
```

New DDoS Threats

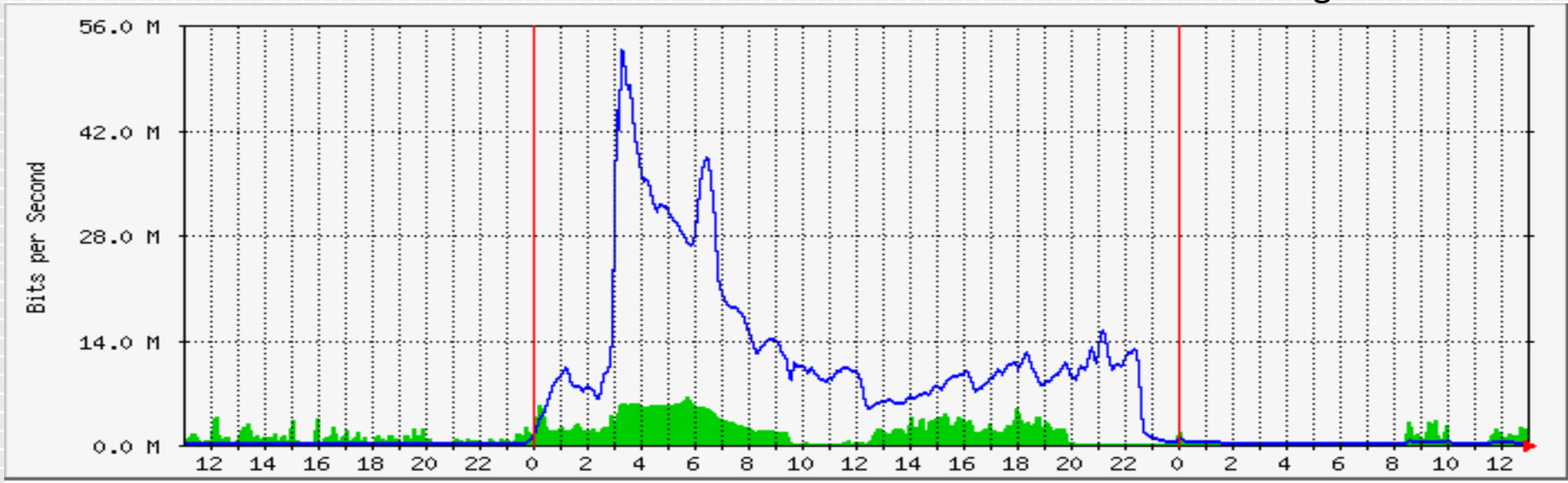
- Enterprise learn how to deal with “simple” packet floods, even at sizes exceeding 100 GBps (“buy anti-DDoS protection”)
- Currently few large scale disruptions caused by traditional packet flood DDoS

Intelligent DDoS

- Find “slow” (= high resource) API function
- Create randomized queries to send requests to this function
- Use hijacked browsers (CSRF) to send requests
- Mobile clients may participate
- No “malware” required

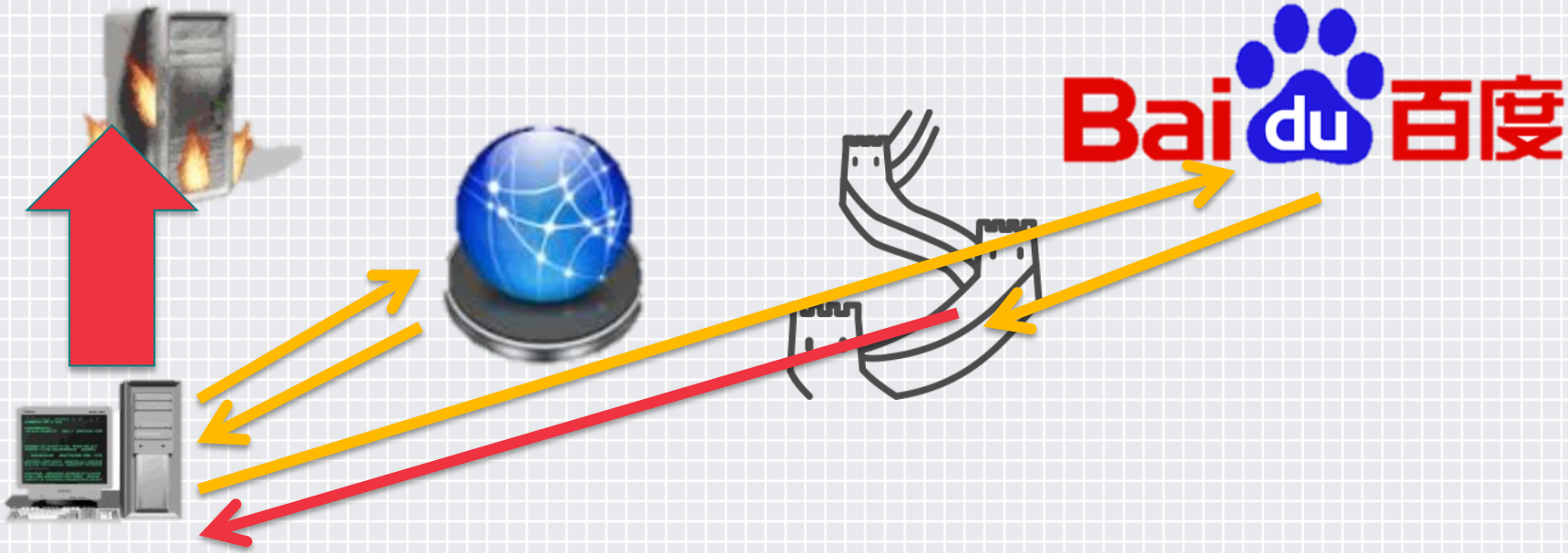
Chinese Firewall Misconfiguration

Furbo.org



	Max	Average	Current
In	6332.0 kb/s (0.6%)	1375.6 kb/s (0.1%)	1747.1 kb/s (0.2%)
Out	52.6 Mb/s (5.3%)	6400.0 kb/s (0.6%)	107.7 kb/s (0.0%)

Chinese Firewall: DDoS Tool



Topics Covered by Mike Assante

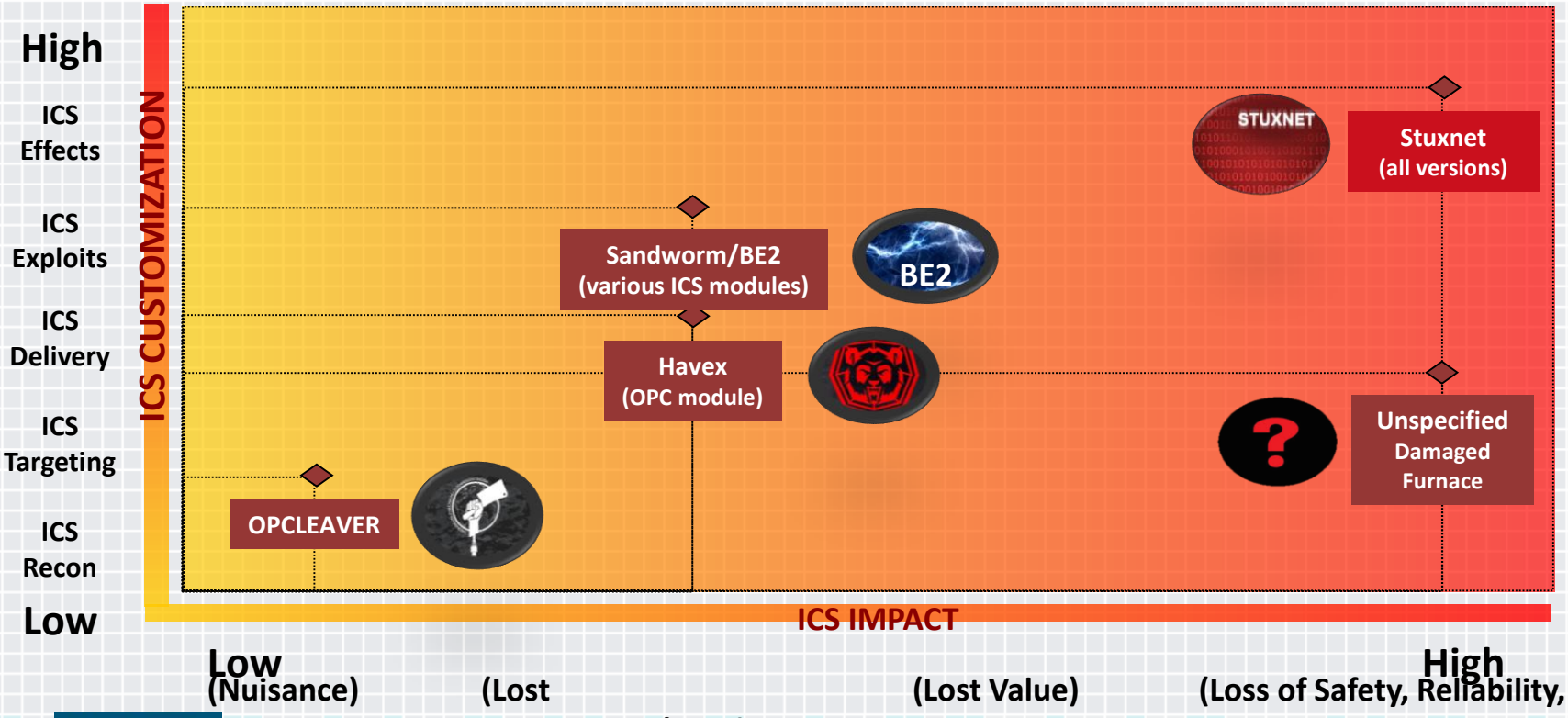
- ICS Threats
- ICS Incidents
- ICS Defense

Most Dangerous New to ICS Attack Techniques

1. Greatest number of ICS cyber incidents continue to be non-targeted malware, but…
2. Emergence of targeted ICS attacks
3. Custom ICS exploits & features
4. Gaps & segmentation are expected
5. Targeting trusted ICS relationships

”With Stuxnet, Havex, and BE2 we have moved from the era of accidental infections and insiders to targeted and ICS-customized attacks”

Recent ICS Threat & Actor Landscape

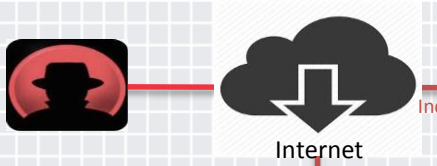


Observed ICS Discovery & Delivery Techniques

E-mail

Spear Phishing [BE2 & Havex]

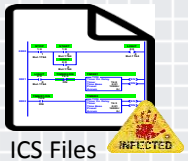
Enterprise Network



ICS Webpages

Water Holing [Havex]

OPC Server Module [Havex]
ICS scanning [Havex]



ICS Files

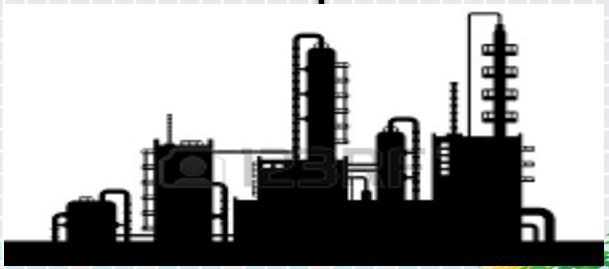
Trojanized Software [Havex]
Infected Files [Stuxnet]

ICS searches [BE2]

Local HMI
(Internet Facing)

direct

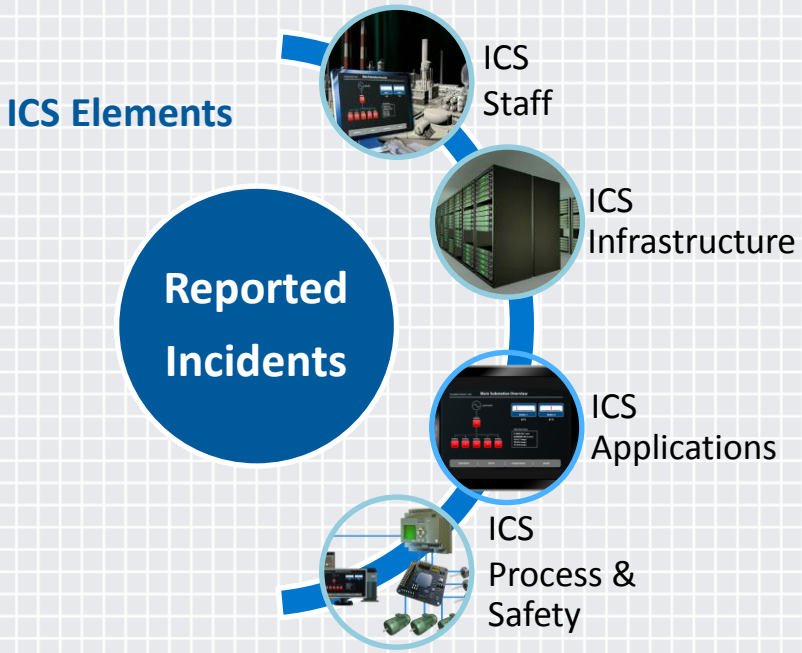
ICS Exploits [BE2]

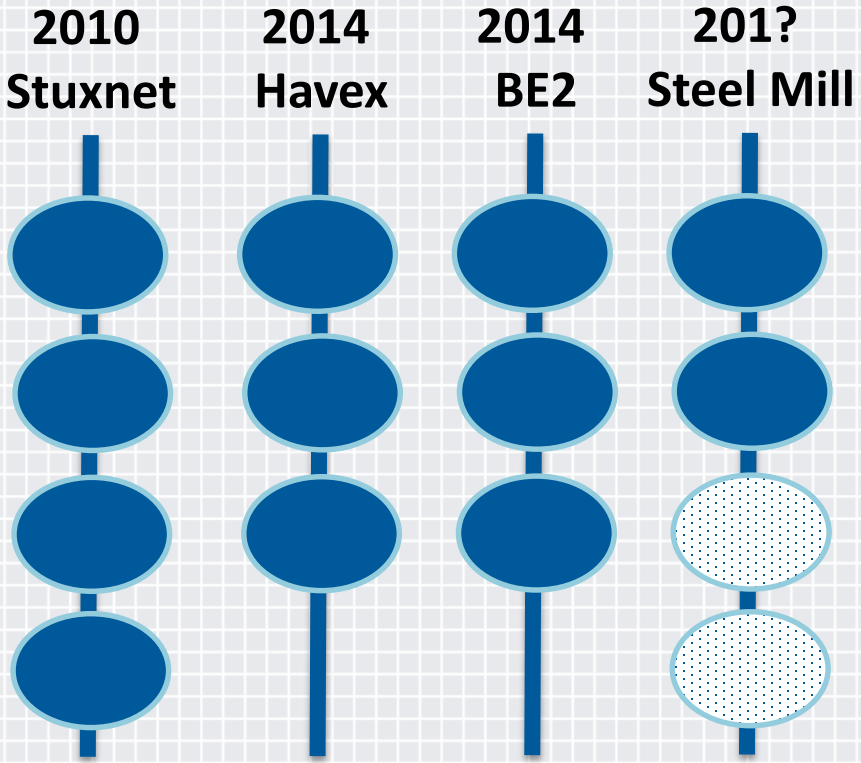


Industrial Control System Networks

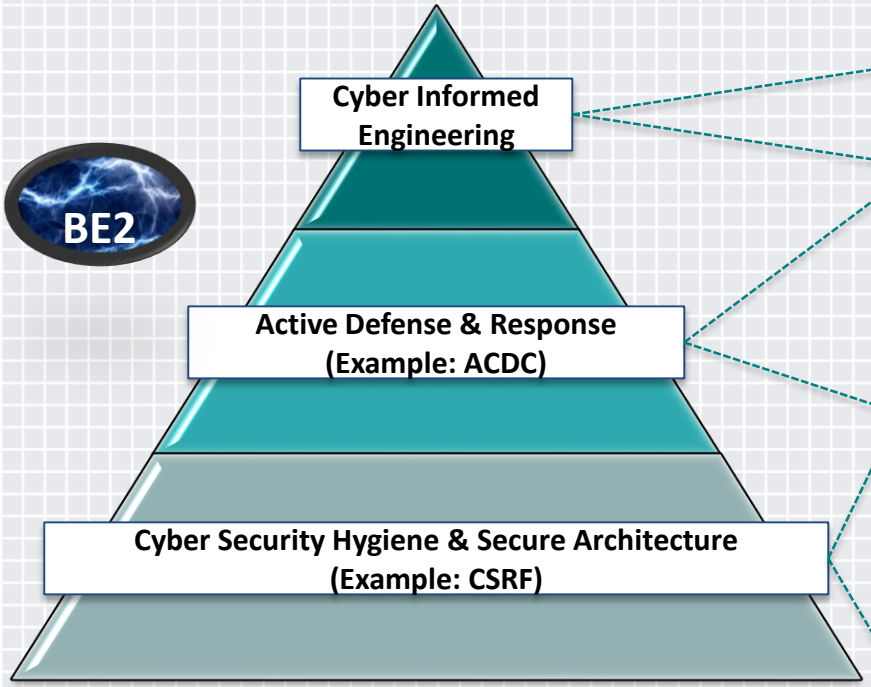
SANS

Discovered ICS Cyber Incidents





Targeted ICS Attack Defenses [BE2]



- Consequence & safety analysis
- Trust model modifications

- Presumption of guilt for vuln ICS
- Identify ICS hotspots & egress NSM
- Threat intel & analysis (IoCs, TTPS)
- Internal ICS traffic baseline & NSM
- Strong points & software vaults

- Educate employees on spear phishing
- Use e-mail anti-phishing tools
- Patch browsers, OS, ICS Apps
- Proper ICS segmentation
- Police Internet-facing ICS components

For More Information

- SANS Institute – http://www.sans.org
- NetWars CyberCity - http://www.sans.org/netwars/cybercity
- Internet Storm Center - https://isc.sans.edu/
- Industrial Control Systems Security - http://ics.sans.org/
- SANS “What Works”/Critical Security Controls - https://www.sans.org/critical-security-controls/vendor-solutions