ISASecure Web Conference

End User Perspectives

ISASecure®

About the Speaker

- James Hobbs
- Sr. ICS Cybersecurity Advisor, EM
- 27 years of IT experience
- Managed numerous Cybersecurity Investigations
- Architect for ICS Cybersecurity transformation

ISA Security Compliance Institute

Threats

- Nation States
- Organized Crime
- Social Collectives
- Insiders
- Mistakes
- C&C, Beacons

STUXnet — 2010 – DESTRUCTION. Cyber Worm disrupted PLC's of more than 1000 centrifuges in Iran.

HAVEX / ENERGETIC BEAR — 2013 – ESPIONAGE. RAT targeted Energy, used OPC to conduct recon, & supply chain

2015 - DESTRUCTION. Took down part of Ukraine power grid. C&C, Wiper.

Crash Override — 2016 - DESTRUCTION. Took down part of Ukraine power substation. C&C, Wiper. Evolution of B.E.

TRISIS — 2017

HELLO CWT_company ！
IF YOU ARE READING THIS, IT'S MEAN YOUR DATA WAS ENCRYPTED AND YOU SENSITIVE PRIVATE INFORMATION WAS STOLEN!
READ CAREFULLY THE WHOLE INSTRUCTION NOTES TO AVOID DIFFICULTIES WITH YOUR DATA

by RAGNAR_LOCKER ！
YOU HAVE TO CONTACT US via LIVE CHAT IMMEDIATELY TO RESOLVE THIS CASE AND MAKE A DEAL
(contact information you will find at the bottom of this notes)

!!!!! WARNING !!!!!

DO NOT Modify, rename, copy or move any files or you can DAMAGE them and decryption will be impossible.
DO NOT Use any third-party or public Decryption software, it also may DAMAGE files.
DO NOT Shutdown or Reset your system, it can DAMAGE files

There is ONLY ONE possible way to get back your files - contact us and pay for the special DECRYPTION KEY !
For your GUARANTEE we will decrypt 2 of your files FOR FREE, as a proof that it works.
Don't waste your TIME, the link for contact us will be deleted if there is no contact made in closest time and you will NEVER restore your DATA.
!!! HOWEVER if you will contact us within 2 day since get penetrated - you can get a very SPECIAL PRICE.

! WARNING !
Whole your network was fully COMPROMISED!

We has DOWNLOADED more than 2 TB of your PRIVATE SENSITIVE Data, including your Billing info, Insurance cases, Financial reports,
Business audit, Banking accounts! Also we have corporate correspondence, information about your clients such as AXA Equitable, Abbot Laboratories, AIG, Amazon,
Boston Scientific, Facebook, J & J, SONOCO, Estee Lauder and many others.
We got even more info about your partners and even about your staff, there are some screenshots just as a proofs of what we got on you.
Screenshots:
http://prntscr.com/tolino (from here was downloaded almost every file)
https://prnt.sc/tolkqq
https://prnt.sc/tollbp
https://prnt.sc/tnzooz   your trial balances in USD
https://prnt.sc/tnzqxf
https://prnt.sc/tozqlx
http://prnt.sc/tozrab

Whole data that gathered from your private files and directories could be published in MASS MEDIA for BREAKING NEWS! Yours partners, clients and investors would be notified about
LEAK.
However if we make a deal everything would be kept in secret and all your data will be restored.

You can take a look for some more examples of what we have, right now it's a private hidden page, but it could become accessable for Public View if you decide NOT pay.
Use TOR Browser to open the link: http://p6o7m7JujalhgkIv.onion/?Batxqawm8rKxIP16ZIxB
to view the page's content use password: GME8sYUND6

ISA **Security Compliance Institute**

Threat Surface

- Any Network connection into ICSE
  - Wireless
  - Telco
- Removable Media
- Hardware, chipsets
- Patches, firmware

- Increasing Technology complexity
- Increasing demand on firewalls
- Increasing legislation

For there to be a threat, there must be a vulnerability and an exploit.

ISA Security Compliance Institute

Supply Chain

▶ What if bad things are in the hardware?

▶ Supply chain is not easy to attack

▶ We innovate faster than supply chain cyber can keep up with

▶ Build the capability to identify Supply Chain threats yourself?

▶ Have industry develop standards and certifications

▶ We want to know that what we use is safe

ISA Security Compliance Institute