REJLERS

Hack mot våra styrsystem

Nicklas Keijser

2018-01-31

REJLERS

TACK TILL SPONSORERNA

ABB

Power and productivity
for a better world™

westermo

Robust Industrial Data Communications – Made Easy

VARFÖR IT-SÄKERHET?

”Vi ser en asymmetri där samhällets beroende av IT-system blir allt större samtidigt som möjligheterna att ställa till skada i IT-systemen utvecklas så att det blir lättare för dom som vill skada oss.”
Generalmajor Gunnar Karlsson, Chef Militära underrättelse- och säkerhetstjänsten. Agenda 20161211

OCH VAD SÄGER KOLLEGAN PÅ FRA?

svt NYHETER

Nyheter | Lokalt | Sport | Kultur | Opinion | Väder

/ INRIKES

Utländska IT-spioner bakom 100.000 nätattacker förra året

För första gången berättar FRA:s ledning, och talespersonen Fredrik Wallin, om spionaget mot Sverige. Foto: SVT

Främmande makt har utfört över 100.000 nätattacker mot Sverige förra året och det är mycket svårt att skydda sig mot spionverksamheten. Det framgår när ledningen för Försvarets Radioanstalt för första gången berättar om omfattningen av IT-spionerіet mot Sverige.

Försvarets Radioanstalt, FRA är en av Sveriges mest hemliga organisationer. I en av Stockholms förorter ligger centrum för FRA:s avancerade signalspaning mot utlandet. Och nu visar det sig att IT-spionaget mot Sverige fullkomligt har exploderat.

Tidigare har alla dessa uppgifter varit hemligstämplade. Men nu berättar ledningen för första gången hur stor omfattningen är.

– Under en typisk månad kan vi se 10.000 aktiviteter från statliga utländska angripare mot svenska mål, säger FRA:s talesperson Fredrik Wallin. Och målen fördelar sig geografiskt över hela Sverige.

svt NYHETER

Nyheter | Lokalt | Sport | Kultur | Opinion | Väder

/ INRIKES

FRA: IT-spioner förbereder attack mot elnätet

Foto: TT

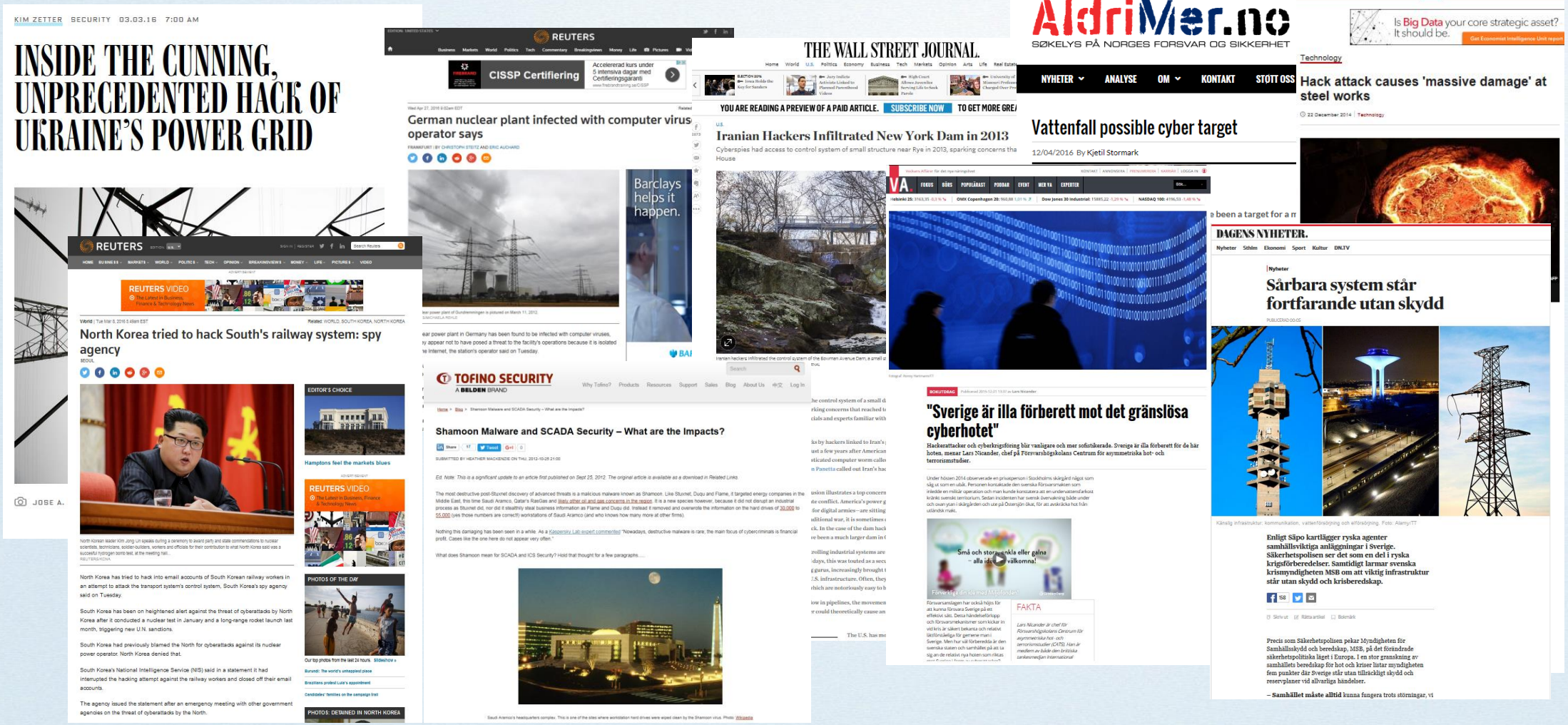
Utländska IT-spioner har gjort förberedelser för att slå ut svensk infrastruktur som elnät och kommunikationssystem. Det avslöjar Försvarets Radioanstalt i dag för SVT. Konsekvenserna om det svenska elsystemet slås ut blir dramatiska.
– Då skulle mycket av det normala samhällslivet bryta samman, säger Mikael Odenberg, generaldirektör för Svenska Kraftnät.

Äldre personer skulle sitta sex trappor upp i ett hyreshus utan fungerande hiss och utan ett fungerande trygghetslarm. Maten skulle ruttna i kyldiskarna. Det skulle inte gå att tanka bilen. Det skulle inte gå att få ut pengar på bankomaten. Efter en tid skulle inte telekommunikationerna fungera.

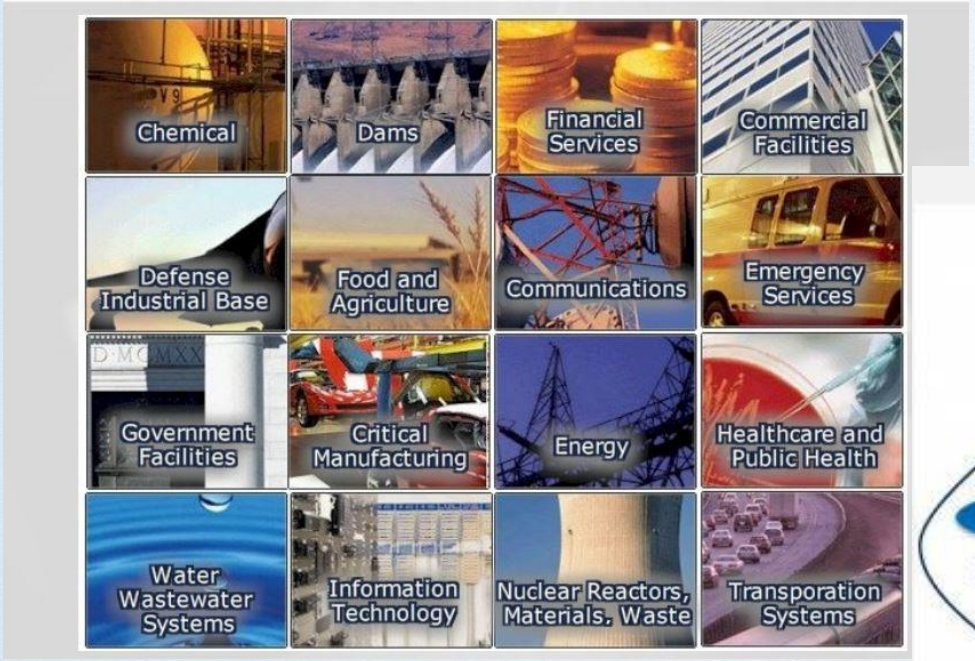
Problemet enligt Svenska Kraftnäts generaldirektör är att vi byggt upp ett allt mer sårbart samhälle som är beroende av att elen fungerar även i krissituationer.

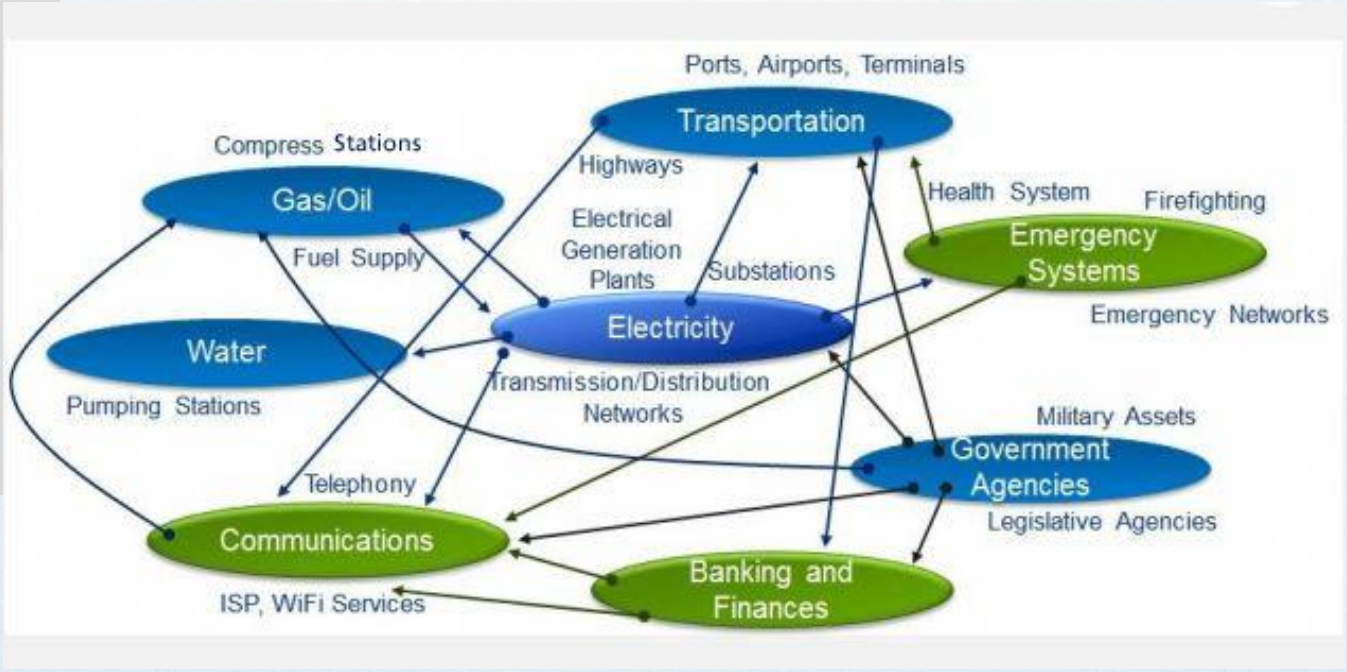
– I grunden behöver vi fundera på olika sätt att göra oss mindre elberoende så att vi kan upprätthålla viktiga samhällsfunktioner även när det är problem med elförsörjningen.

NY VÄRLD FÖR STYRSYSTEM

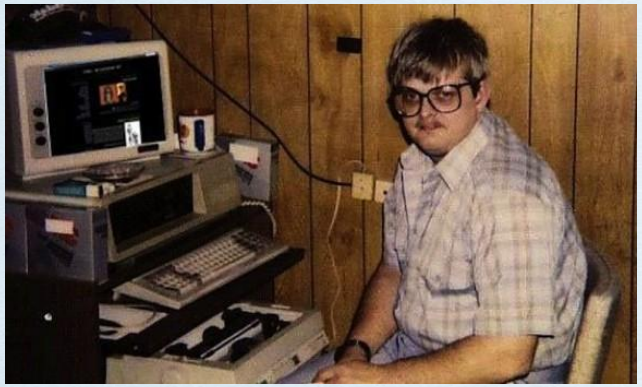


DET HÄNGER IHOP





FYRA TYPER AV AKTÖRER



Teknikintresserade

Kriminella

Ideologiska skäl

Stater

STORT INTRESSE AV TEKNIK

Hacker says he broke into Texas water plant, others

Annoyed with the downplaying of the risk to critical infrastructure systems, a hacker targets a water plant in South Houston following news of an Illinois water plant intrusion.

Security

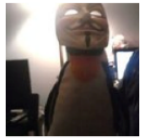
November 18, 2011

by Elinor Mills

A twentysomething hacker said today that he hacked into a South Houston water utility to show that it can easily be done, after U.S. officials downplayed the risks from a report yesterday of an intrusion at an Illinois water plant.

The hacker, using the alias "pr0f," said he has hacked other SCADA (supervisory control and data acquisition) systems too.

He tweeted on November 5 links to public posts with what he identified as PLC configurations for a Polish waste-water treatment plant; SCADA data from an HMI (human-machine interface) box possibly for a generator used for research purposes at Southern Methodist University; and what he believes are water metering control system files from Spain or Portugal.



The Twitter profile picture of the hacker who says he compromised a Texas water plant and others to show how easy it is.

pr0f

"Basically, people have no idea what's going on in terms of industrial control, groups like ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) are too slow don't have enough power to react to situations," he wrote in an e-mail to CNET. "There's a lot of rubbish information out there that's being treated seriously, etc. Lot of crap. So I'm putting information out there to show people what kind of systems are vulnerable to basic attacks."

He said his actions were prompted by the U.S. government's response to a report from an Illinois Statewide Terrorism and Intelligence Center that said intruders compromised a water utility in the state last week, burning out a pump. Industry expert Joe Weiss blogged about the report and provided more information to CNET yesterday. The Department of Homeland Security initially identified the location as Springfield, but a local official today reportedly confirmed that it happened in nearby Curran-Gardner Townships Public Water District, but the official could not say whether it was a hacking incident.

A DHS representative responded to the report with this comment: "At this time there is no credible corroborated data that indicates a risk to critical infrastructure entities or a threat to public safety."

That government response irked pr0f.

"I dislike, immensely, how the DHS tend to downplay how absolutely F***ED the state of national infrastructure is," he wrote in a Pastebin post. "I've also seen various people doubt the possibility that an attack like this could be done."

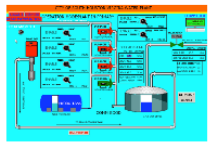
Then he provided screenshots of what look like diagrams of water and waste-water treatment facilities in South Houston, Texas.

Fred Gonzalez, superintendent of the South Houston water plant, told CNET, "We're still checking into the whole problem and seeing what's going on."

A DHS representative said he would look into the purported Texas incident.

"I'm not going to expose the details of the box," pr0f wrote in his Pastebin post. "No damage was done to any of the machines; I don't really like mindless vandalism. It's stupid and silly.

"On the other hand, so is connecting interfaces to your SCADA machinery to the Internet," he added. "I wouldn't even call this a hack, either. Just to say. This required almost no skill and could be reproduced by a two-year-old with a basic knowledge of Simatic," which is automation software from Siemens that's used to control equipment in industrial production.



This is one of the screenshots provided by pr0f as proof of his intrusion into a South Houston water utility.

pr0f

Asked how he gets into systems, pr0f said: "As for how I did it, it's usually a

IDEOLOGISKA

The Washington Times

HOME \ NEWS \ SECURITY

Islamic State hacker sentenced for assisting terrorist group with 'kill list'

A 20-year-old computer science student from Kosovo described by the Justice Department as "the first terrorist hacker convicted in the United States" was sentenced Friday to two decades in prison for providing the Islamic State with a "kill list" containing the personal information of roughly 1,300 U.S. military members and government employees.

Federal prosecutors had asked U.S. District Judge Leonie M. Brinkema to sentence Ardit Ferizi to 25 years in prison after the hacker pleaded guilty in June to two charges brought as a result of his role with the terror group.

Mr. Ferizi acknowledged hacking an Illinois-based company in June 2015 and illegally obtaining the personally identifiable information of tens of thousands of its customers. He then parsed those records for individuals with military and government email accounts before providing their details to a Junaid Hussain, an Islamic State recruiter who administered the group's cyber operations and had previously published a similar "kill list" containing the names and addresses of 100 U.S. military personnel, according to court documents.

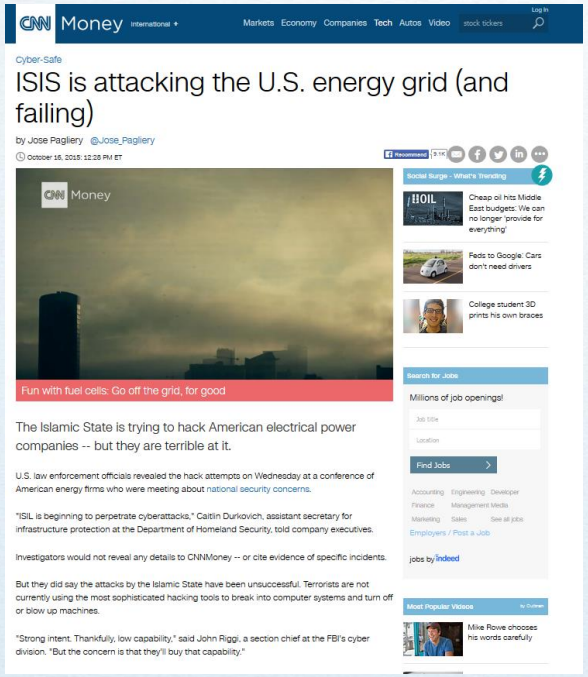
Mr. Hussain was ultimately killed by a U.S. drone strike in August 2015. Two weeks prior to his death, however, he took Ferizi's hacked data and released it online in the form of a new list containing the information of approximately 1,300 U.S. government and military targets.

"[W]e are extracting confidential data and passing on your personal information to the soldiers of the khilafah, who soon with the permission of Allah will strike at your necks in your own lands!" reads an excerpt from a statement that accompanied the second kill list when it was tweeted by Hussain in mid August.

Federal investigators soon after identified Mr. Ferizi as the perpetrator of the Illinois hack and arranged to have him arrested in Sept. 2015 in Malaysia where he had been attending college. He was formally charged the following

Click to Read More

RECOMMENDED



CNN Money

Cyber-Safe

ISIS is attacking the U.S. energy grid (and failing)

by Jose Pagliery @Jose_Pagliery

October 16, 2015: 12:28 PM ET

Fun with fuel cells: Go off the grid, for good

The Islamic State is trying to hack American electrical power companies -- but they are terrible at it.

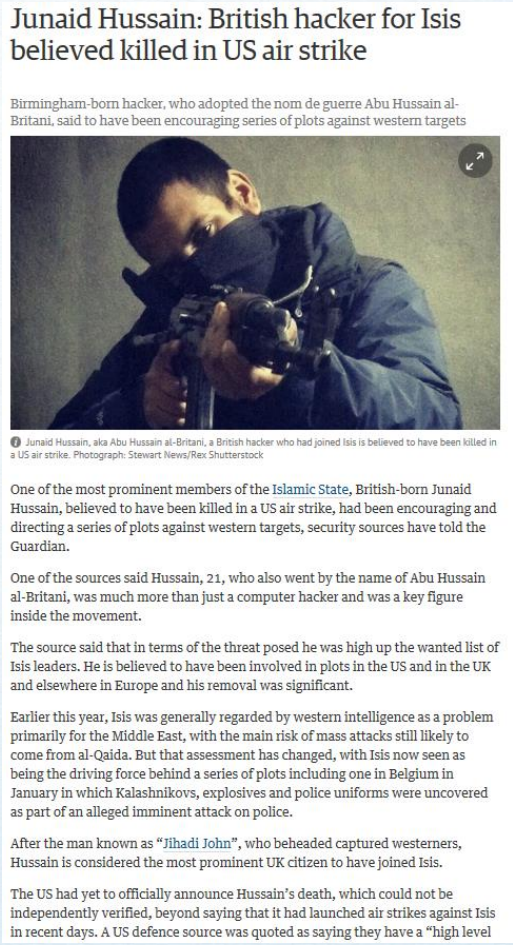
U.S. law enforcement officials revealed the hack attempts on Wednesday at a conference of American energy firms who were meeting about national security concerns.

"ISIL is beginning to perpetrate cyberattacks," Caitlin Durkovich, assistant secretary for infrastructure protection at the Department of Homeland Security, told company executives.

Investigators would not reveal any details to CNNMoney -- or cite evidence of specific incidents.

But they did say the attacks by the Islamic State have been unsuccessful. Terrorists are not currently using the most sophisticated hacking tools to break into computer systems and turn off or blow up machines.

"Strong intent. Thankfully, low capability," said John Riggi, a section chief at the FBI's cyber division. "But the concern is that they'll buy that capability."



Junaid Hussain: British hacker for Isis believed killed in US air strike

Birmingham-born hacker, who adopted the nom de guerre Abu Hussain al-Britani, said to have been encouraging series of plots against western targets

Junaid Hussain, aka Abu Hussain al-Britani, a British hacker who had joined Isis is believed to have been killed in a US air strike. Photograph: Stewart News/Rex Shutterstock

One of the most prominent members of the Islamic State, British-born Junaid Hussain, believed to have been killed in a US air strike, had been encouraging and directing a series of plots against western targets, security sources have told the Guardian.

One of the sources said Hussain, 21, who also went by the name of Abu Hussain al-Britani, was much more than just a computer hacker and was a key figure inside the movement.

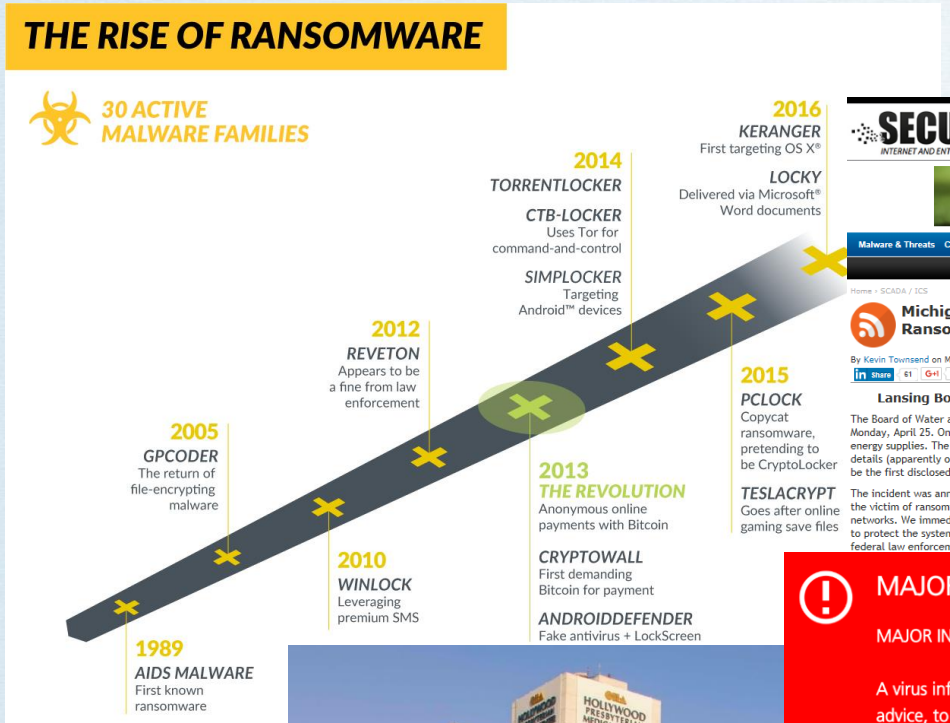
The source said that in terms of the threat posed he was high up the wanted list of Isis leaders. He is believed to have been involved in plots in the US and in the UK and elsewhere in Europe and his removal was significant.

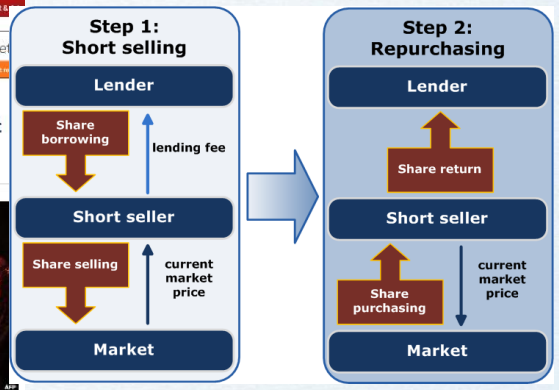
Earlier this year, Isis was generally regarded by western intelligence as a problem primarily for the Middle East, with the main risk of mass attacks still likely to come from al-Qaida. But that assessment has changed, with Isis now seen as being the driving force behind a series of plots including one in Belgium in January in which Kalashnikovs, explosives and police uniforms were uncovered as part of an alleged imminent attack on police.

After the man known as "Jihadi John", who beheaded captured westerners, Hussain is considered the most prominent UK citizen to have joined Isis.

The US had yet to officially announce Hussain's death, which could not be independently verified, beyond saying that it had launched air strikes against Isis in recent days. A US defence source was quoted as saying they have a "high level

KRIMINELLA





MAJOR INCIDENT - UPDATE

MAJOR INCIDENT – APPOINTMENTS CANCELLED

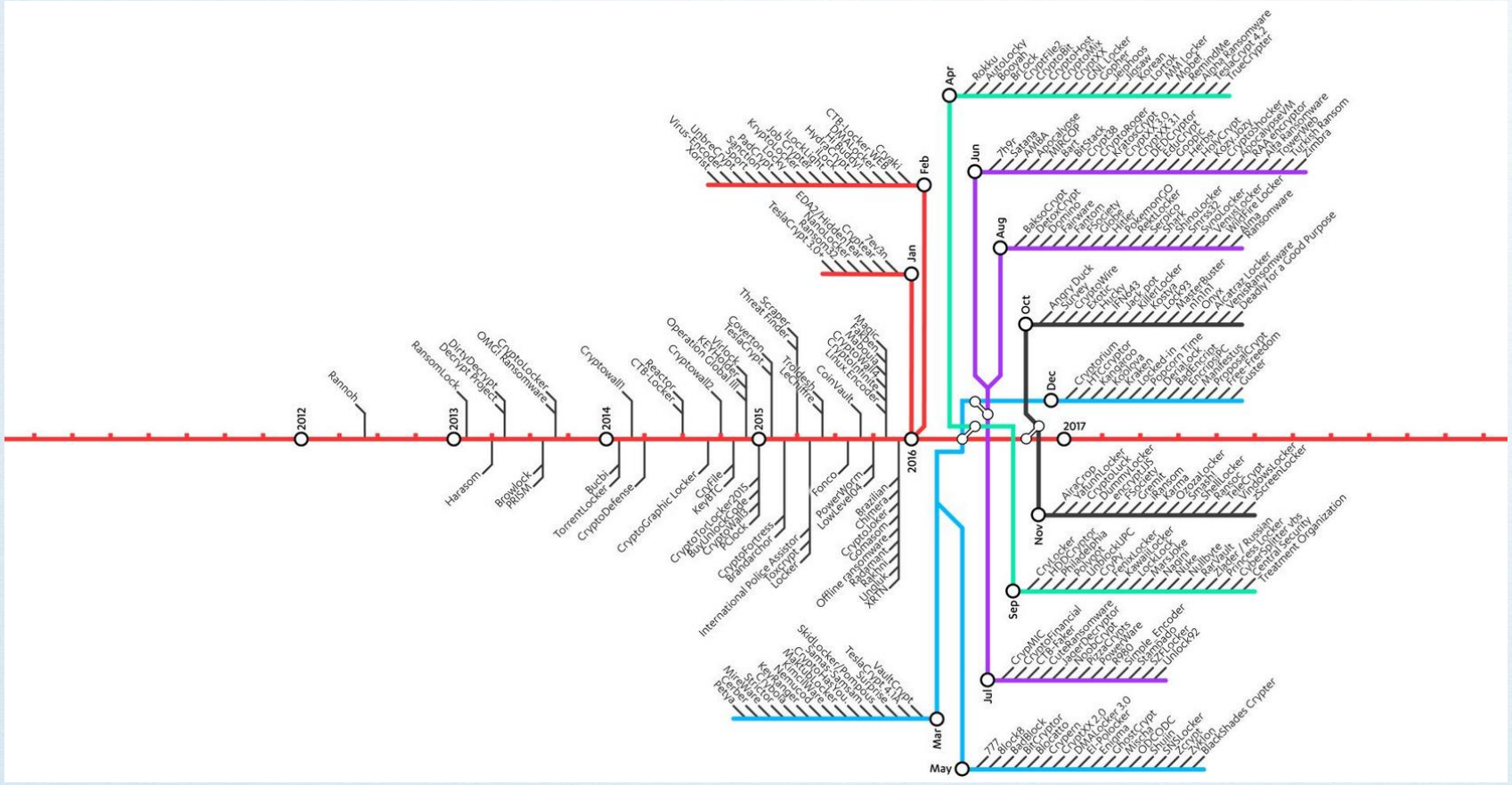
A virus infected our electronic systems on Sunday October 30 and we have taken the decision, following expert advice, to shut down the majority of our systems so we can isolate and destroy it.

All planned operations, outpatient appointments and diagnostic procedures have been cancelled for Wednesday November 2 with a small number of exceptions as follows:

- Audiology
- Physiological measurements
- Antenatal
- Community and therapy
- Chemotherapy
- Paediatrics

National Health Service's Lincolnshire and Goole

RANSOMWARE


2012
2013
2014
2015
2016
2017
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Rannoh
Harasom
BrowLock
PRISM
BucBi
TorrentLocker
CryptoDefense
CryptoGraphic Locker
CryptoTorLocker2015
PClock
CryptoFortress
International Police Assistor
Fonco
PowerWorm
LowLevelOrm
Offline ransomware
Brazilian
Chimera
Comaware
Rabbit
Radamant
Unlock-it
XRTN
Locker
Troldesh
LeChiffre
CoinVault
Linux.Encoder
Magic
Rabbit
Cryptorbit
Coverton
TeslaCrypt
Virlock
KeyHolder
Operation Global III
Cryptowall2
Cryptowall
CTB Locker
Reactor
CryptoLocker
OMG! Ransomware
DirtyDecrypt
DecrypTile Project
RansomLock
Scraper
Threat Finder
CTB-Locker
Critroni
EDA2/HiddenTear
TeslaCrypt 3.0
Jigsaw
Cryptear
7ev3n
Ransom32
Kraken
Locky
Troldesh
Shade
Encoder.858
Cryptesla
Cryptodefense
Cryptolocker.F
Xorist
Virus Encoder
Unbreakable
Sanction
PadCrypt
CryptoMix
CryptoTorLocker2015
Critroni
CryptoLocker.F
Hydracrypt
Cryptodefense
Cryptolocker.F
Cryptesla
Jobcrypter
Rokku
AutoLocky
Bergmania
BitCryptor
CryptoFile2
CryptoHost
CryptoMix
CryptoMix V3
Evil Locker
Jigsaw
Koolova
Lortok
WM Locker
Mobef
Remind Me
Alpha Ransomware
TeslaCrypt 4.2
TrueCrypter
7ltgr
Satana
AMBA
Anonymous
MIRCOP
Bart
BitStack
CryptoBlue
CryptoRogger
KatoCrypt
CryptoXXX 3.0
CryptoXXX 3.1
DFDCryptor
EduCrypt
Google
Herbst
HolyCrypt
Kozy.Jozy
CryptoShocker
NoobCrypt
NAA encryptor
Alfa Ransomware
PowerWeb
Turkish Ransom
Zimbra
BaksoCrypt
DirtonCrypt
Domino
Fairware
Fantom
Foggety
Globe
Hitler
PokemonCO
RectLocker
Sarpoco
Sharp
ShinoLocker
Smrss32
SmokeLocker
VenusLocker
Wildfire Locker
Alma Ransomware
Ransomware
Angry Duck
Survey
CryptoWire
EvilLocky
HiddenTear
Jack.pot
KillerLocker
Kostya
Lock93
MasterBuster
nmnm
Onyx
Alcatraz Locker
VenusRansomware
Deadly for a Good Purpose
Cryptorium
HCCryptor
Kangaroo
Koolova
Kraken
Locked-in
Popcorn Time
PoshLock
BadEncript
NMoreEncrypt
NMSLusus
ProposalCrypt
FreeFreedom
Custer
AiraCrop
VaultLocker
CryptoLuck
DummyLocker
FenixLocker
Globeimposter
Phantom
Radamant
CryptoLocker
SpecialLocker
RansomCrypt
TeleCrypt
WindowsLocker
XSweetLocker
CryLocker
DMALocker
Philadelphia
PolskiLocker
PolskiLockUPC
CryPy
EvilLocker
KawaiiLocker
MarsJoke
Nemty
Nullbyte
BadVault
Hader / Russian
Princess Locker
CyberSplitter .vhs
Central Security
Treatment Organization
CryptoFinancial
CTB Locker
Ransomweb
SpeedCrypt
PowerWare
Simple Encoder
Stampado
XTPLocker
Unlock92
777
Blocke
BadBlock
BitCryptor
Bocato
Cryptem
CryptXX 2.0
DMALocker 3.0
EnkripsiPC
Enigma
GhostCrypt
Mischa
OMGDDC
Shuiin
SNSLocker
Zyklon
BlackShades Crypter
Skull Locker
TeslaCrypt 4.1/Pony
Vault Crypt
Cryptas
Karmen
Karmen Ransom
Kimcilware
Mircop
Petya
Satan
Scatter
Xpan

WANNACRY ELLER

IUQERFSODP9IFJAPOSDFJHGOSURIJFAEWRWERGWEA.COM

Mer än 150 länder drabbade.

Över 300.000 datorer.

Bland drabbade företag finns NHS, Nissan, Renault, Deutsche Bahn, Fedex och mobiloperatören Telefonica samt i Sverige Sandvik och Timerå kommun.

NOTPETYA

NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million

Lee Mathews, CONTRIBUTOR

Observing, pondering, and writing about tech. Generally in that order. FULL BIO

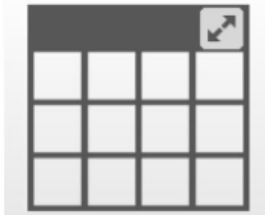
Opinions expressed by Forbes Contributors are their own.

In June, the NotPetya ransomware hit companies in the U.S. and throughout Europe. One of those hardest hit was Copenhagen-based shipping giant A.P. Moller-Maersk, which moves about one-fifth of the world's freight. Operations at Maersk terminals in four different countries were impacted, causing delays and disruption that lasted weeks.

A Maersk shipping container/Wikipedia

Kevin Beaumont @GossiTheDog Följ

After Merck say they are having manufacturing issues from Petya, CDC say Merck Hepatitis vaccine not being distributed.

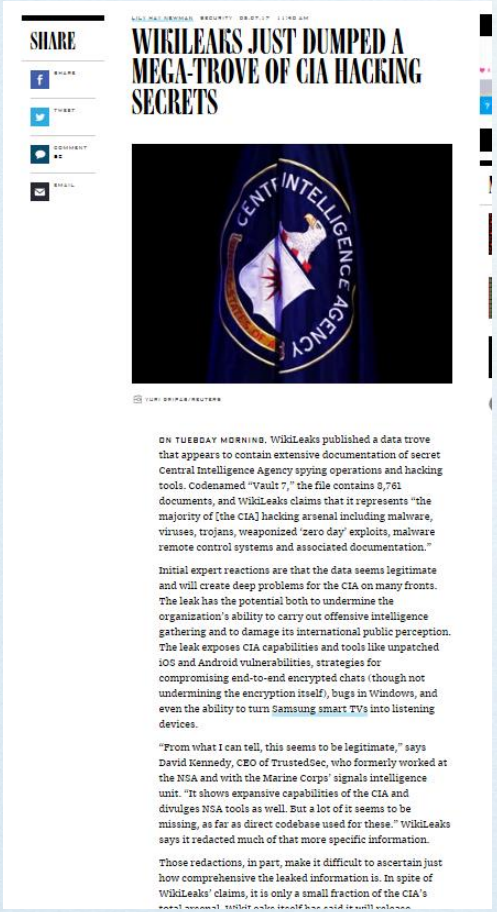


Note[1]: Merck is not currently distributing its adult Hepatitis B vaccine and does not expect to be distributing adult Hepatitis B vaccine between now and the end of 2018. Additionally, Merck anticipates that its pediatric Hepatitis B vaccine will be unavailable between early August 2017 and early 2018. Merck's supply of the dialysis formulation of Hepatitis B vaccine, however, is not affected and is expected to remain available. GSK has sufficient supplies of adult and pediatric Hepatitis B vaccines to address these anticipated gap in Merck's supply of adult and pediatric Hepatitis B vaccines during these time periods:

STATER

Billigt, effektivt och lätt att förneka

WIKILEAKS VS CIA



SHARE

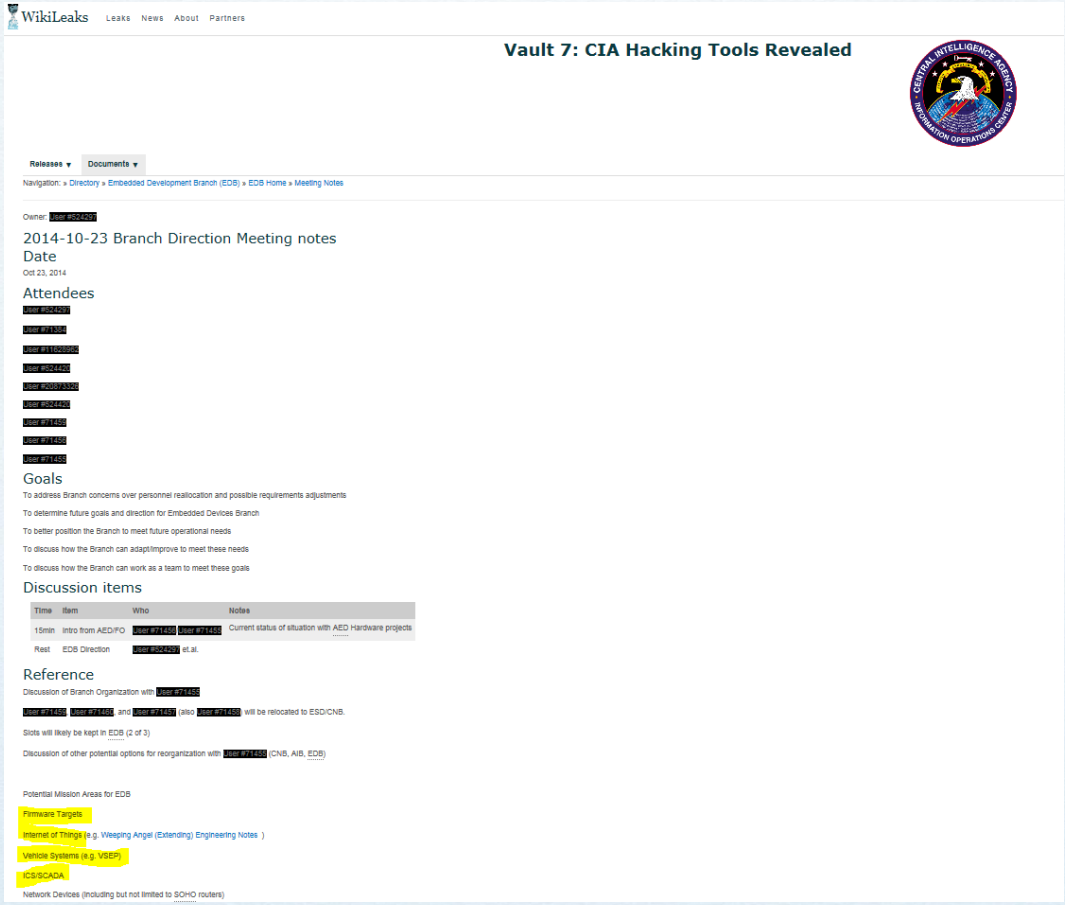
WIKILEAKS JUST DUMPED A MEGA-TROVE OF CIA HACKING SECRETS

ON TUESDAY MORNING, WikiLeaks published a data trove that appears to contain extensive documentation of secret Central Intelligence Agency spying operations and hacking tools. Codenamed "Vault 7," the file contains 8,761 documents, and WikiLeaks claims that it represents "the majority of [the CIA] hacking arsenal including malware, viruses, trojans, weaponized 'zero day' exploits, malware remote control systems and associated documentation."

Initial expert reactions are that the data seems legitimate and will create deep problems for the CIA on many fronts. The leak has the potential both to undermine the organization's ability to carry out offensive intelligence gathering and to damage its international public perception. The leak exposes CIA capabilities and tools like unpatched iOS and Android vulnerabilities, strategies for compromising end-to-end encrypted chats (though not undermining the encryption itself), bugs in Windows, and even the ability to turn Samsung smart TVs into listening devices.

"From what I can tell, this seems to be legitimate," says David Kennedy, CEO of TrustedSec, who formerly worked at the NSA and with the Marine Corps' signals intelligence unit. "It shows expansive capabilities of the CIA and divulges NSA tools as well. But a lot of it seems to be missing, as far as direct codebase used for these." WikiLeaks says it redacted much of that more specific information.

Those redactions, in part, make it difficult to ascertain just how comprehensive the leaked information is. In spite of WikiLeaks' claims, it is only a small fraction of the CIA's



WikiLeaks Leaks News About Partners

Vault 7: CIA Hacking Tools Revealed

Releases ▾ Documents ▾

Navigation: » Directory » Embedded Development Branch (EDB) » EDB Home » Meeting Notes

Owner: User #524297

2014-10-23 Branch Direction Meeting notes

Date

Oct 23, 2014

Attendees

User #524297

User #71458

User #1162305

User #524429

User #2087309

User #524442

User #71458

User #71458

User #71458

Goals

To address Branch concerns over personnel reallocation and possible requirements adjustments

To determine future goals and direction for Embedded Devices Branch

To better position the Branch to meet future operational needs

To discuss how the Branch can adapt/improve to meet these needs

To discuss how the Branch can work as a team to meet these goals

Discussion items

Time	Item	Who	Notes
15min	Intro from AED/FO	User #71458 User #71458	Current status of situation with AED Hardware projects
Rest	EDB Direction	User #524297 et.al.	

Reference

Discussion of Branch Organization with User #71458

User #71458, User #71458, and User #71457 (also User #71458) will be relocated to ESD/CNB.

Slots will likely be kept in EDB (2 of 3)

Discussion of other potential options for reorganization with User #71458 (CNB, AIB, EDB)

Potential Mission Areas for EDB

Firmware Targets

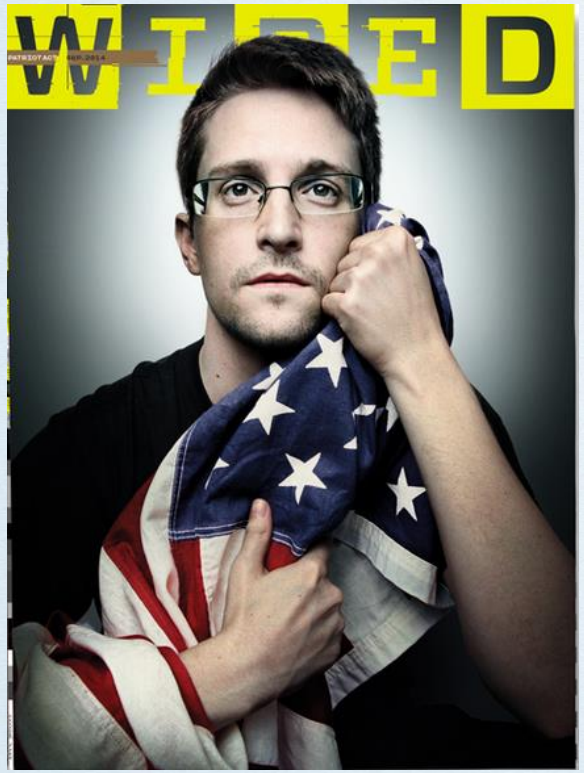
Internet of Things (e.g. Weeping Angel (Extending) Engineering Notes)

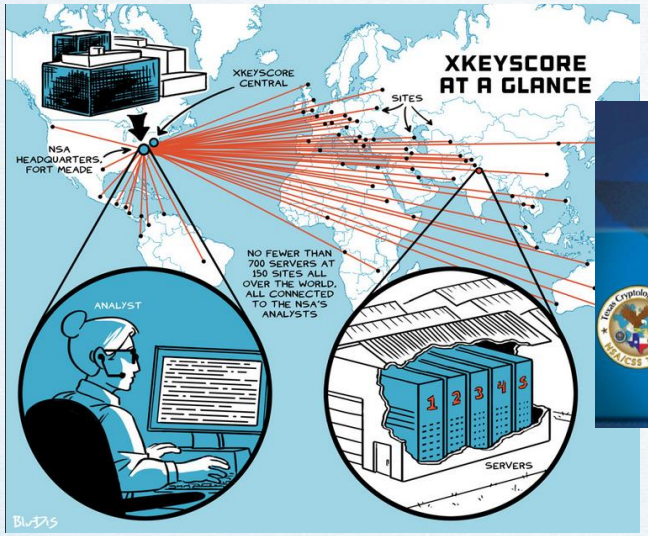
Vehicle Systems (e.g. VSEP)

ICS/SCADA

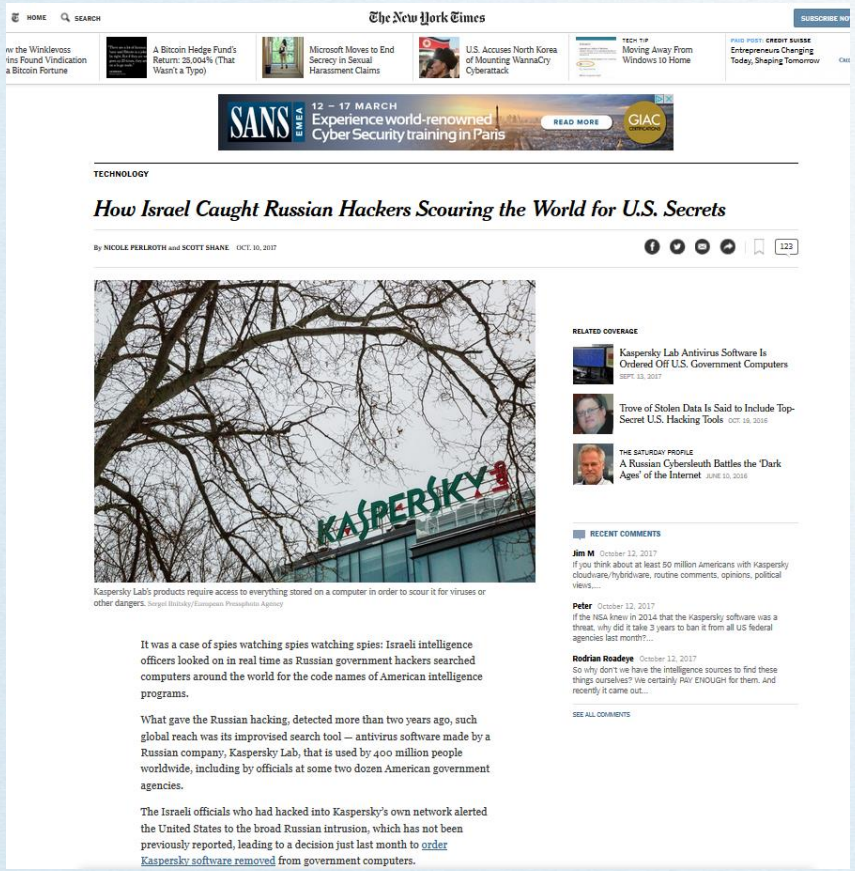
Network Devices (including but not limited to SOHO routers)

SNOWDEN VS NSA





KASPERSKY VS DHS & GCHQ



The New York Times

A Bitcoin Hedge Fund's Return: 25,004% (That Wasn't a Typo)

Microsoft Moves to End Secrecy in Sexual Harassment Claims

U.S. Accuses North Korea of Mounting WannaCry Cyberattack

Moving Away From Windows 10 Home

SANS 12 – 17 MARCH Experience world-renowned Cyber Security training in Paris READ MORE GIAC

TECHNOLOGY

How Israel Caught Russian Hackers Scouring the World for U.S. Secrets

By NICOLE PERLROTH and SCOTT SHANE OCT. 10, 2017

Kaspersky Lab's products require access to everything stored on a computer in order to scour it for viruses or other dangers. Sergei Ilnitsky/European Pressphoto Agency

It was a case of spies watching spies watching spies: Israeli intelligence officers looked on in real time as Russian government hackers searched computers around the world for the code names of American intelligence programs.

What gave the Russian hacking, detected more than two years ago, such global reach was its improvised search tool — antivirus software made by a Russian company, Kaspersky Lab, that is used by 400 million people worldwide, including by officials at some two dozen American government agencies.

The Israeli officials who had hacked into Kaspersky's own network alerted the United States to the broad Russian intrusion, which has not been previously reported, leading to a decision just last month to order Kaspersky software removed from government computers.

RELATED COVERAGE

Kaspersky Lab Antivirus Software Is Ordered Off U.S. Government Computers

Trove of Stolen Data Is Said to Include Top-Secret U.S. Hacking Tools

THE SATURDAY PROFILE
A Russian Cybersleuth Battles the 'Dark Ages' of the Internet

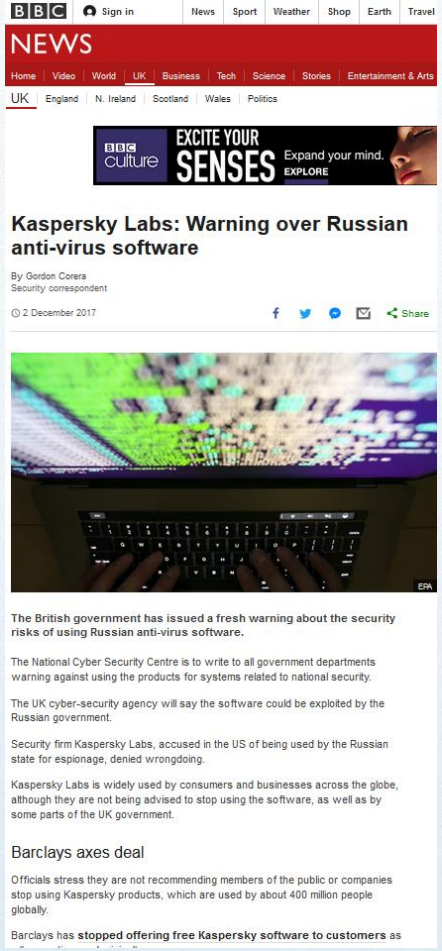
RECENT COMMENTS

Jim M October 12, 2017
If you think about at least 50 million Americans with Kaspersky cloudware/hybridware, routine comments, opinions, political views,...

Peter October 12, 2017
If the NSA knew in 2014 that the Kaspersky software was a threat, why did it take 3 years to ban it from all US federal agencies last month?...

Rodrian Roadeye October 12, 2017
So why don't we have the intelligence sources to find these things ourselves? We certainly PAY ENOUGH for them. And recently it came out...

SEE ALL COMMENTS



BBC NEWS

Home | Video | World | UK | Business | Tech | Science | Stories | Entertainment & Arts

UK | England | N. Ireland | Scotland | Wales | Politics

BBC culture EXCITE YOUR SENSES Expand your mind. EXPLORE

Kaspersky Labs: Warning over Russian anti-virus software

By Gordon Corera
Security correspondent

2 December 2017

The British government has issued a fresh warning about the security risks of using Russian anti-virus software.

The National Cyber Security Centre is to write to all government departments warning against using the products for systems related to national security.

The UK cyber-security agency will say the software could be exploited by the Russian government.

Security firm Kaspersky Labs, accused in the US of being used by the Russian state for espionage, denied wrongdoing.

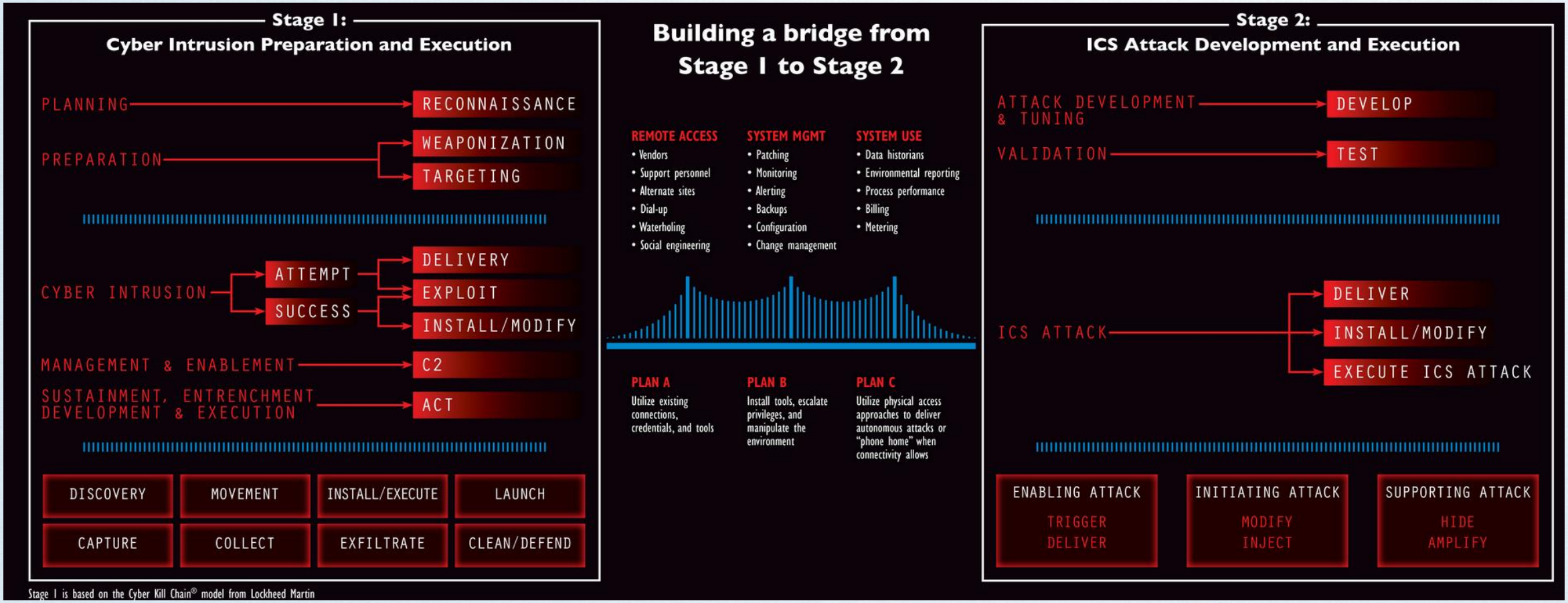
Kaspersky Labs is widely used by consumers and businesses across the globe, although they are not being advised to stop using the software, as well as by some parts of the UK government.

Barclays axes deal

Officials stress they are not recommending members of the public or companies stop using Kaspersky products, which are used by about 400 million people globally.

Barclays has **stopped offering free Kaspersky software to customers** as

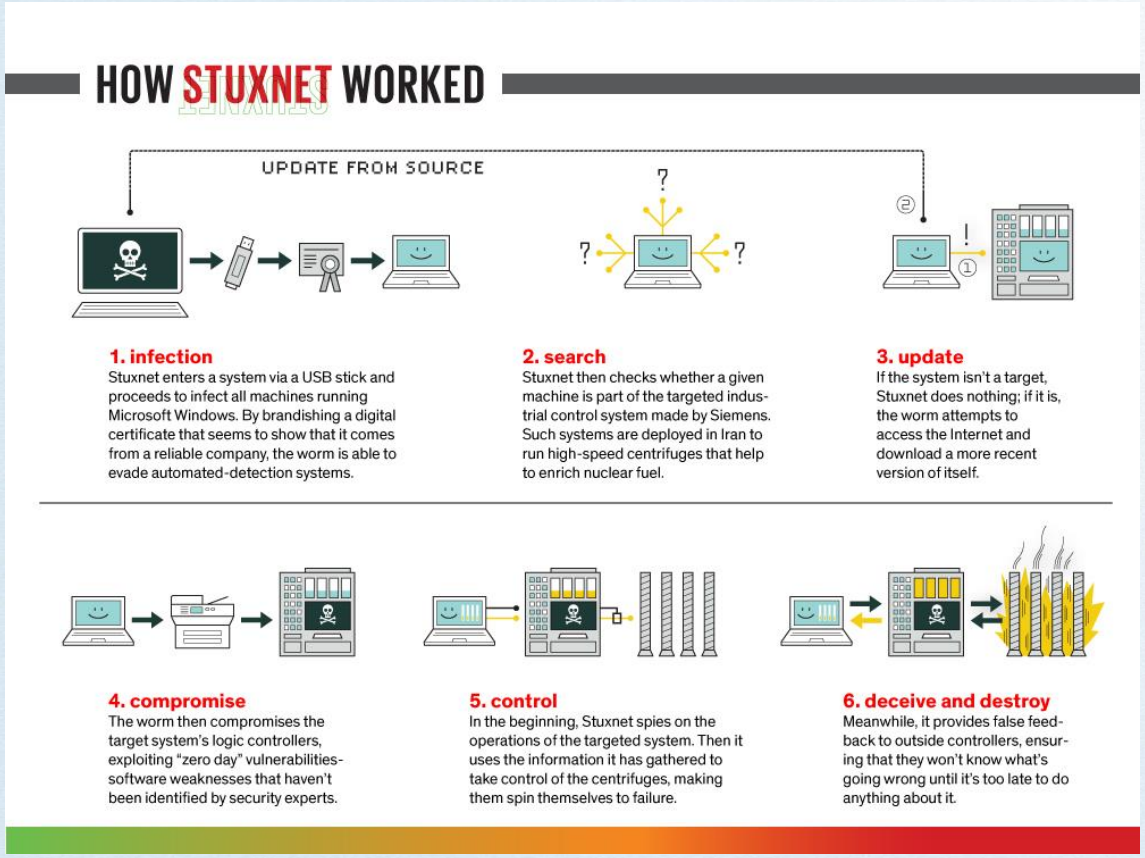
TILLBAKA TILL STYRSYSTEM



Fem, kända, malware mot styrsystem

STUXNET//HAVEX//BLACKENERGY2//CRASHOVERRIDE//TRISIS

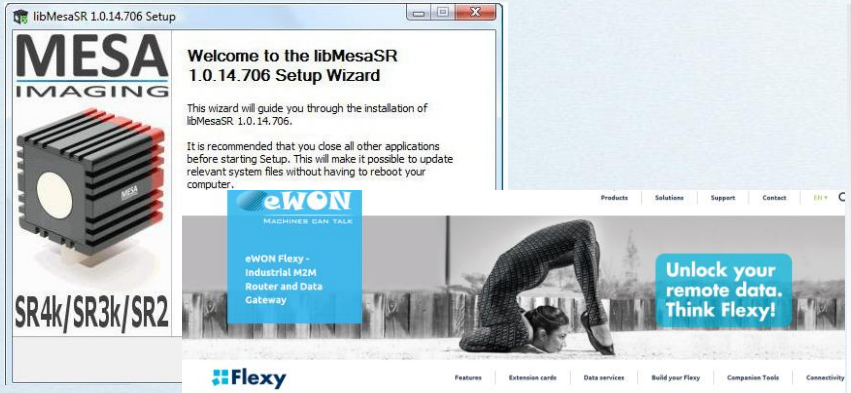
STUXNET

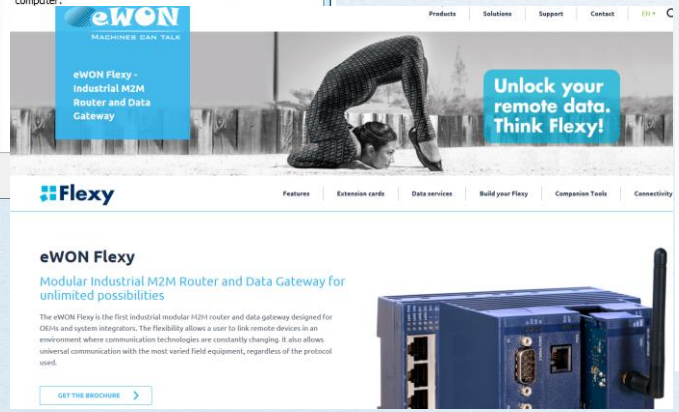

HOW STUXNET WORKED
UPDATE FROM SOURCE
1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.
2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.
3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.
4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.
5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.
6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

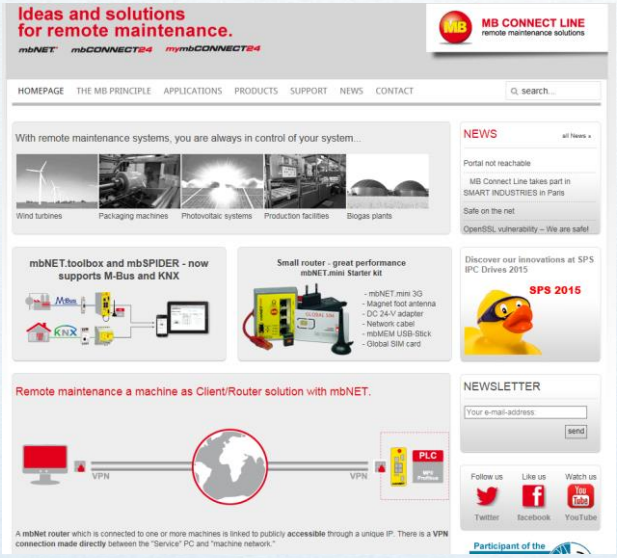
www.President.ir

HAVEX, ETT OPC-VIRUS!

Tre företags hemsidor blev hackade och malware blev instoppade i mjukvarupaketen!







MESA Imaging – Industriella kameror för avståndsmätning

eWON – Fjärruppkoppling mot styrsystem

MB Connect Line – Routrar och fjärruppkoppling mot styrsystem

U REDA'N

Skickat mail me
innehållande e

Inaktiverade U
kontrollrumme

Skriva sönder
operatörsstati
malware KillDis

MOTHERBOARD Watch Machines Discoveries Space Futures Gaming Earth

The Ukrainian Power Grid Was Hacked Again

January 10, 2017 // 10:07 AM EST

Written by
KIM ZETTER
CONTRIBUTOR

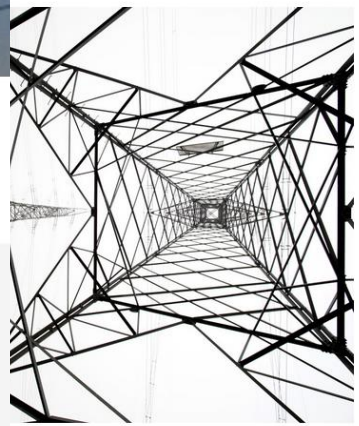
An investigation into a power outage that left customers in Ukraine without electricity for an hour last month has concluded that the cause was indeed a cyberattack, sources tell Motherboard. This would be the second such known hack of a Ukrainian power facility following a massive December 2015 power outage affecting about 230,000 people, which was later blamed on the Russian government.

The more recent attack occurred at a transmission facility, as opposed to the 2015 attack that affected a distribution facility, and was not as far-reaching (although it could have been much worse—as disruptions to a transmission facility could impact a wider area than distribution facilities). But taken together, the implications of both attacks and a series of other breaches around Ukraine suggest that someone, or various individuals, may be using the country as a testbed for refining attacks on critical infrastructure that could be used across the world.

The attack last month, which occurred almost exactly one year after the previous outage, struck the Pivnichna substation outside the capital city Kiev, and cut power a

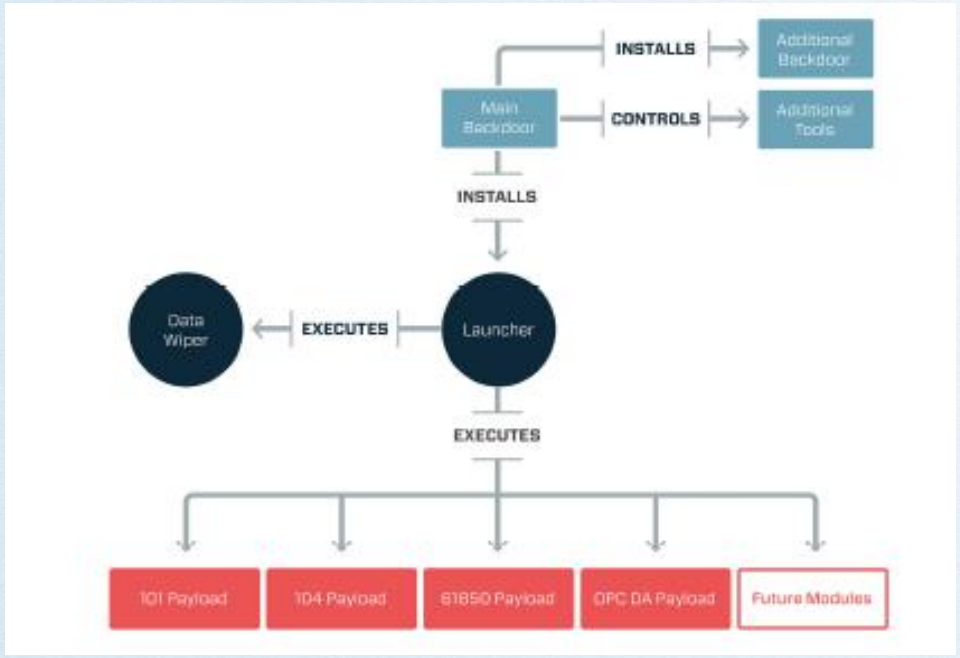
7:00 AM

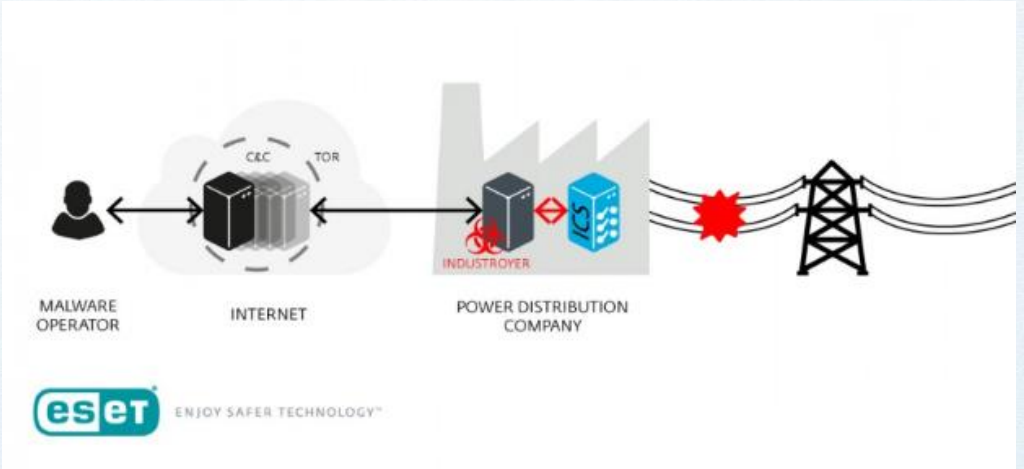
CUNNING,
NTED HACK OF
OWER GRID



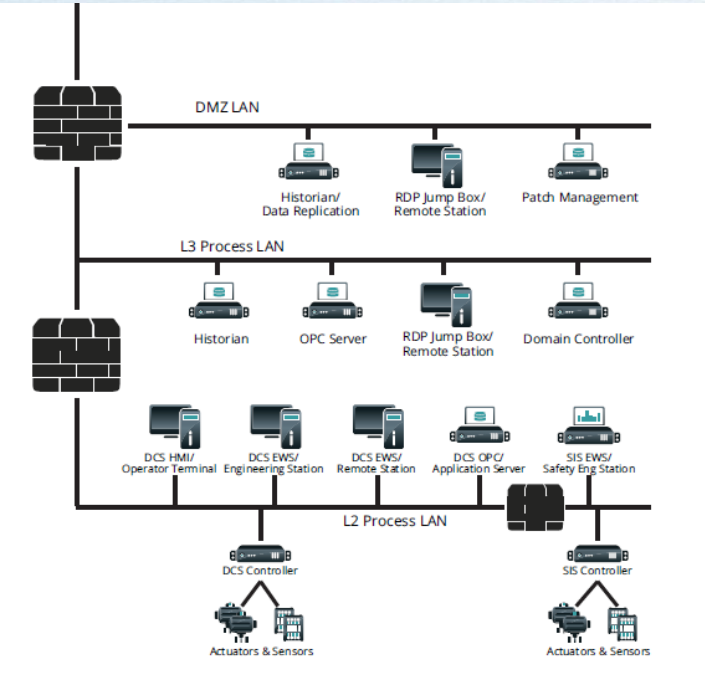
MAGES

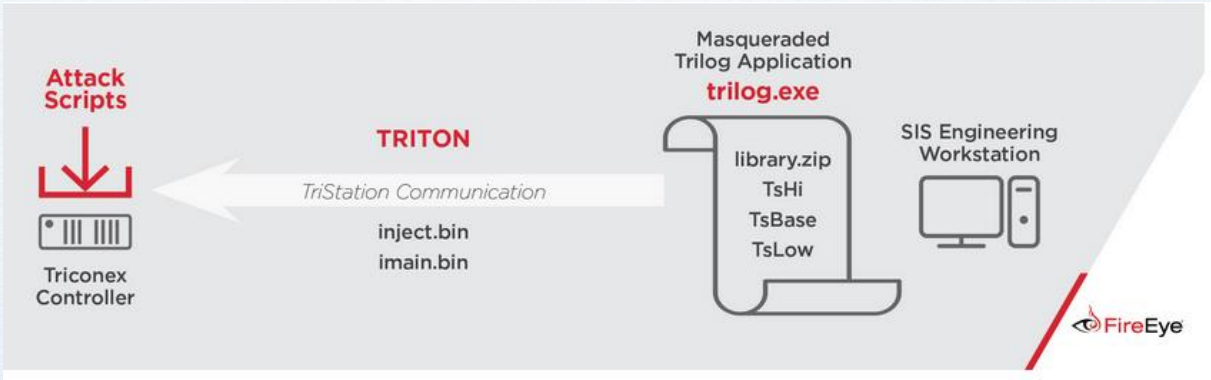
CRASHOVERRIDE



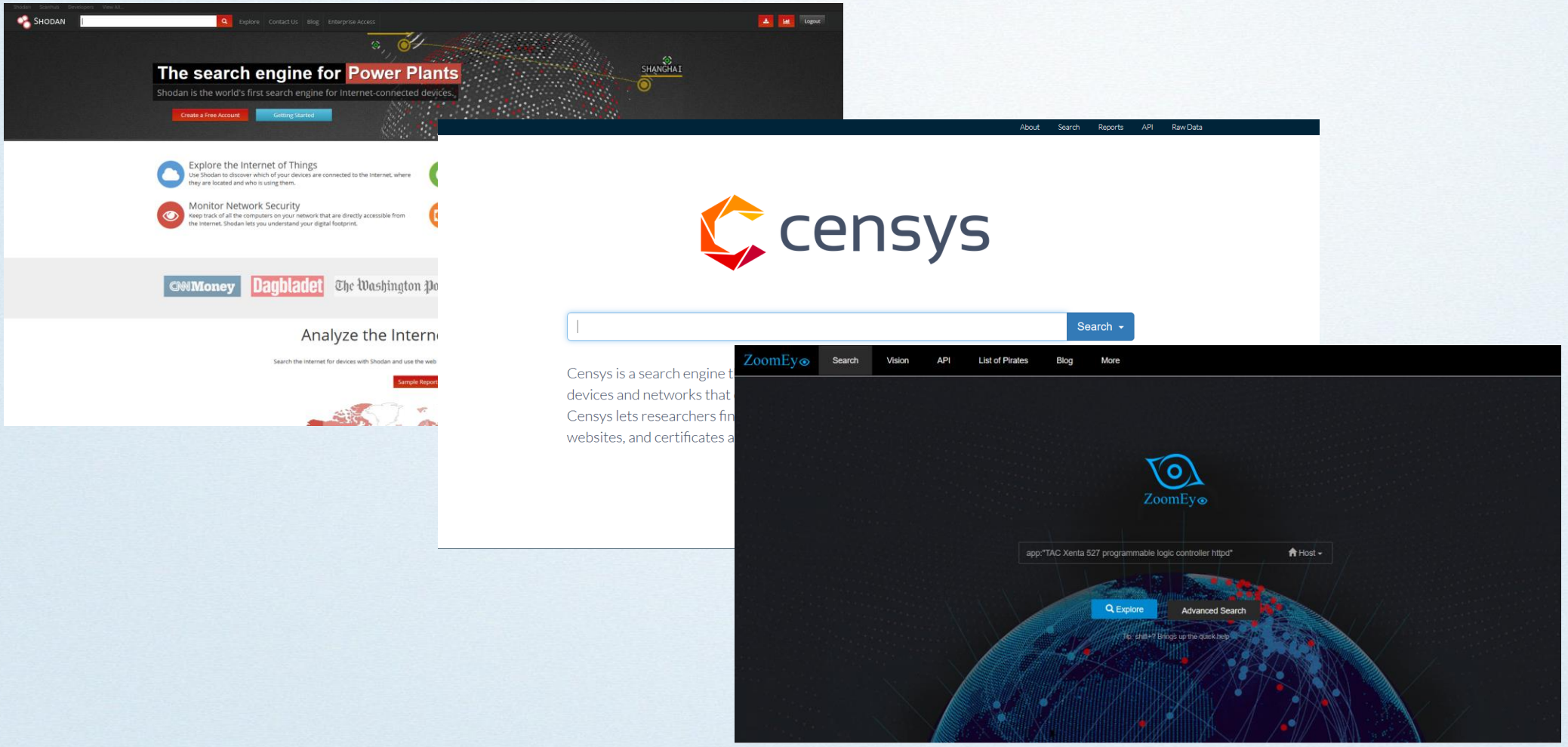


TRISIS

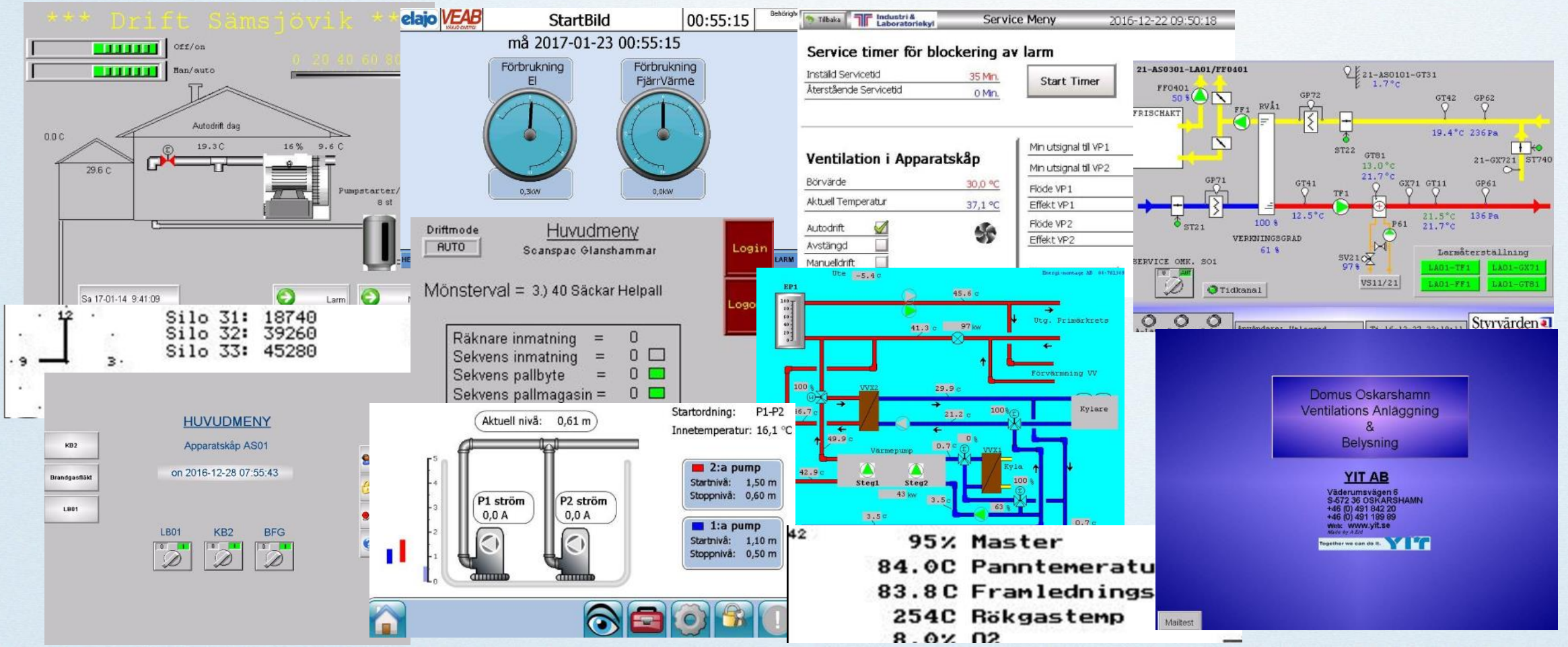

DMZ LAN
Historian/
Data Replication
RDP Jump Box/
Remote Station
Patch Management
L3 Process LAN
Historian
OPC Server
RDP Jump Box/
Remote Station
Domain Controller
DCS HMI/
Operator Terminal
DCS EWS/
Engineering Station
DCS EWS/
Remote Station
DCS OPC/
Application Server
SIS EWS/
Safety Eng Station
L2 Process LAN
DCS Controller
SIS Controller
Actuators & Sensors
Actuators & Sensors


Attack
Scripts
Triconex
Controller
TRITON
TriStation Communication
inject.bin
imain.bin
Masqueraded
Trilog Application
trilog.exe
library.zip
TsHi
TsBase
TsLow
SIS Engineering
Workstation
FireEye

HUR GÅR DET TILL?



MERA EXEMPEL PÅ SHODAN



HUR GÅR DET TILL?

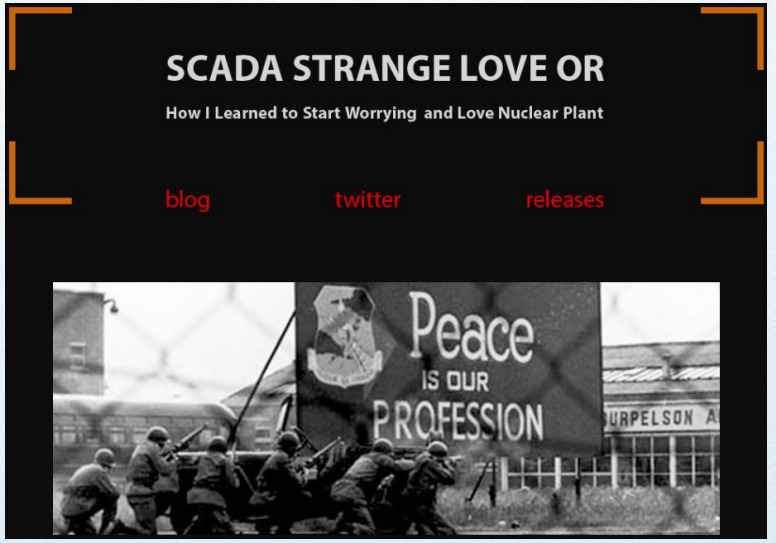
Rank	Password
1	123456
2	password
3	12345
4	12345678
5	football
6	qwerty
7	1234567890
8	1234567
9	princess
10	1234
11	login
12	welcome
13	solo
14	abc123
15	admin
16	121212
17	flower
18	passw0rd
19	dragon
20	sunshine
21	master
22	hottie
23	loveme
24	zaq1zaq1
25	password1

SplashData's annual "Worst Passwords" list 2016

Inte så lyckade lösenord inom automationsvärlden

default wdc westermo
edw100 root
basisk
bba wago
private manageronly
2WSXcder cisco
100 admin
.1q2w3e 1 deltav guest

https://github.com/scadastrangelove/SCADAPASS



HUR GÅR DET TILL?

sagitta>

sales@sagitta.pw

Home | Hardware | Software | Engineering | Support | Why Sagitta? | Company

High Performance ~~Computing~~ CRACKING

Sagitta is redefining HPC with high performance turnkey password cracking solutions tailored for . . .

Law Enforcement
Litigation Support
Military/Defense
Information Security
Forensics
eDiscovery

Enterprise Grade

Sagitta clusters are designed to provide years of reliable service under 24/7/365 operation and are built upon rock-solid enterprise technologies, including Intel Xeon processors, registered ECC memory, 80Plus Platinum certified power supplies, 10GbE & Infiniband, and top-of-the-line graphics processors.

Extreme Scalability

Whether you require three GPUs or three hundred, our Hashstack distributed cracking software enables us to deliver a solution that fits your precise needs – now, or at any time in the future. Hashstack also ensures last-generation hardware will always seamlessly integrate with next-generation hardware.

Empowering

You don't need to be an expert password cracker to harness the awesomeness of Sagitta's state-of-the-art hardware and software solutions. Regardless of your skill level, our solutions empower you to extract the most value from your organization's password cracking operations.

Brutalis

Brutalis is an eight-GPU monster, clawing its way through hashes at unprecedented speeds. Providing up to eight Nvidia GTX GPUs, two Intel Xeon E5-2600V3 CPUs, and up to 768 GB of registered ECC memory, the Brutalis is the fastest, meanest, most hardcore system money can buy. Ships with a 3-year warranty.

Base configuration price: 18,499 USD

HUR GÅR DET TILL?

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS
Subscribe (Free) | CISO Forum 20

Malware & Threats | Cybercrime | Mobile & Wireless | Risk & Compliance | Security Architecture | Manage
Cyberwarfare | Fraud & Identity Theft | Phishing | Malware | Tracking & Law Enforcement | Whitepapers

Home › Cybercrime

Teen Arrested for Cyberattack on 911 Emergency System

By Eduard Kovacs on October 28, 2016

Share 38 G+1 7 Tweet Rekommendera 2 RSS

An 18-year-old teen from Arizona was arrested this week after one of his iOS exploits caused serious disruption to 911 emergency systems.

According to the Maricopa County Sheriff's Office, Meetkumar Hiteshbhai Desai was booked on three counts of Computer Tampering, which in this case is a Class 2 felony, considered an extremely serious crime in Arizona and other states, due to the fact that it involved critical infrastructure.

The Maricopa County Sheriff's Office Cyber Crimes Unit launched an investigation after being notified of disruption to the 911 service in the Phoenix metro area and possibly in other states.

Desai apparently learned of an iOS bug that can be exploited to manipulate devices, including trigger pop-ups, open email, and abuse phone features. The teen created several exploits and published one of them on a website, linking to it from his Twitter account in an effort to prank his

While Desai claime
caused devices to r
iPads to continuall

According to police
followers and click
managed to shut d

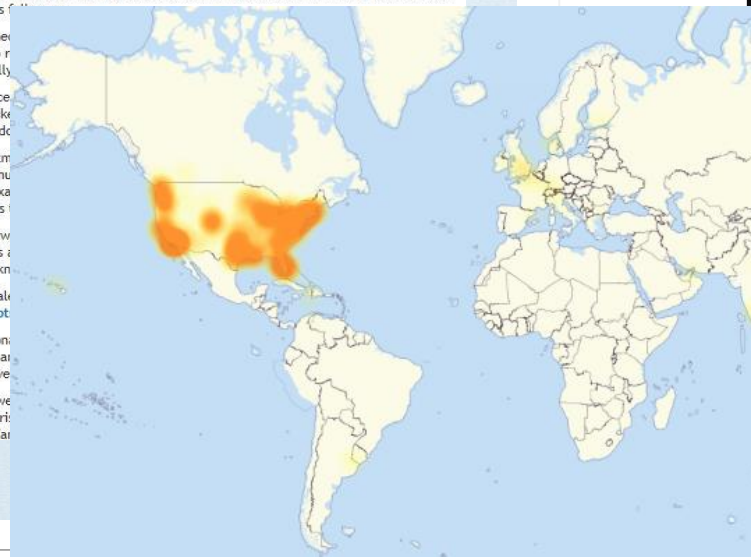
The police departm
service within minu
California and Texa
also received calls

Desai claimed he w
monetary rewards
to call 911 as he kn

Researchers reveal
disrupted by a bot

Security profession
services they are a
even convicted ove

One of the most we
to 41 months in pri
Levin, owner of Va



```
116    // Set up TCP he
117    tcph->dest = hto
118    tcph->source = s
119    tcph->doff = 5;
120    tcph->window = r
121    tcph->syn = TRUE
122
123    // Set up passwo
124    add_auth_entry("
125    add_auth_entry("
126    add_auth_entry("
127    add_auth_entry("
128    add_auth_entry("
129    add_auth_entry("
130    add_auth_entry("
131    add_auth_entry("
132    add_auth_entry("
133    add_auth_entry("
```

This Is Why Half the Internet Shut Down Today

William Turton
10/21/16 8:36am · Filed to: DNS

2.3M 1.1K 40

MYNDIGHETSSAJTER LÅG NERE EFTER ÖVERBELASTNINGSATTACK

G+1 Tweeta Dela 50 Gilla 144 personer gillar detta. Bli den första bland dina vänner.

Igår låg flertalet myndighetssajter nere såsom Krisinformation.se, Regeringen.se och MSB.se, men även flertalet internationella tjänster såsom Github, Spotify och Twitter. Anledningen till att de låg nere var en överbelastningsattack mot dess DNS-leverantör Dyn.

```
3511
zxv
min
min
8888
hdipc
fault
antech
3456
321
pport
one)
ssword
ot
345
er
one)
ss
min1234
11
cadmin
11
6666
ssword
34
v123
 // Administrator admin
rvice
 1); // supervisor supervisor
est
345
```

J
@_notJ
Följ

The following days attacks against the Swedish goverment and media spreading false propaganda will be targetted.

RETWEETS 104 GILLADE 101

12:15 - 19 mars 2016

Teknik

IT-attacker mot svenska medier

PUBLICERAD 2016-03-25

En ny överbelastningsattack, en så kallad ddos-attack, drabbade flera stora svenska mediers sajter under skärtorsdagens kväll och natten mot långfredagen.

Skriv ut Rätta artikel Bokmärk

Bland annat påverkades Expressen, Dagens Nyheter, Dagens industri, Sydsvenskan, Aftonbladet och Svenska Dagbladet men några av sajterna klarade sig med mindre störningar.

– Delar av expressen.se drabbades tidvis av störningar, men nyhetsförmedlingen fortsatte på olika andra plattformar och för nästan alla besökare fanns nästan hela expressen.se uppe även om vi inte kunde uppdatera så snabbt som vanligt, säger Expressens chefredaktör Thomas Mattsson på tidningens sajt sedan den började fungera som vanligt igen.

ANNONS

Telia
NU BLIR VI DUBBELT SÅ PERSONLIGA
LÄS MER

Tidigare på kvällen hade några av tidningarnas sajter kommit igång.

– Exakt vad som händer rent tekniskt vet vi inte, de undersöker. Men det stämmer att de har legat nere. Både Sydsvenskan och HD har legat nere i ungefär en halvtimme. Nu har vi sajterna uppe hjälpligt, sade Sydsvenskans chefredaktör Pia Rehnquist.

Förra helgen utsattes flera mediehus för IT-attacker som lamslog några av de största nyhetssajterna.

SEDAN HÄNDER DET I FINLAND

[redacted]

Country	Sweden
Organization	[redacted]
ISP	
Last Update	2016-01-05T13:40:13.488157
ASN	AS25176

Ports

1900 5900 8080

Services

1900 udp upnp

5900 tcp http-simple

217.208.162.180
Telia Sonera AB
Added on 2017-01-07 06:59:53 GMT
Sweden

220 Fidelix Fx2020 SMTP server at your service221 Fidelix Fx2020 SMTP server: Closing connection

game might attackers to

REAPER

CHECK POINT
RESEARCH
PUBLICATIONS
TOOLS
ABOUT US
CONTACT US
SUBSCRIBE
UNDER ATTACK?
Search IPS Protections, Malware Families, Applications and more...
A New IoT Botnet Storm is Coming
October 19, 2017
SHARE
Share
Tweet
Key Points:
• A massive Botnet is forming to create a cyber-storm that could take down the internet.
• An estimated million organizations have already been scanned with an unknown amount actually infected.
• The Botnet is recruiting IoT devices such as IP Wireless Cameras to carry out the attack.
New cyber-storm clouds are gathering. Check Point Researchers have discovered a brand new Botnet,
IPS ADVISORIES
vBulletin cacheTemplates Remote Code Execution (CVE-2017-17672)
vBulletin Routestring Remote Code Execution
ROBOT TLS_RSA Scanning Attempt (CVE-2017-6168; CVE-2017-17382; CVE-2017-17427; CVE-2017-17428; CVE-2017-12373; CVE-2017-13098; CVE-2017-1000385; CVE-2017-13099;

KASPERSKY, INTERNET OCH STYRSYSTEM

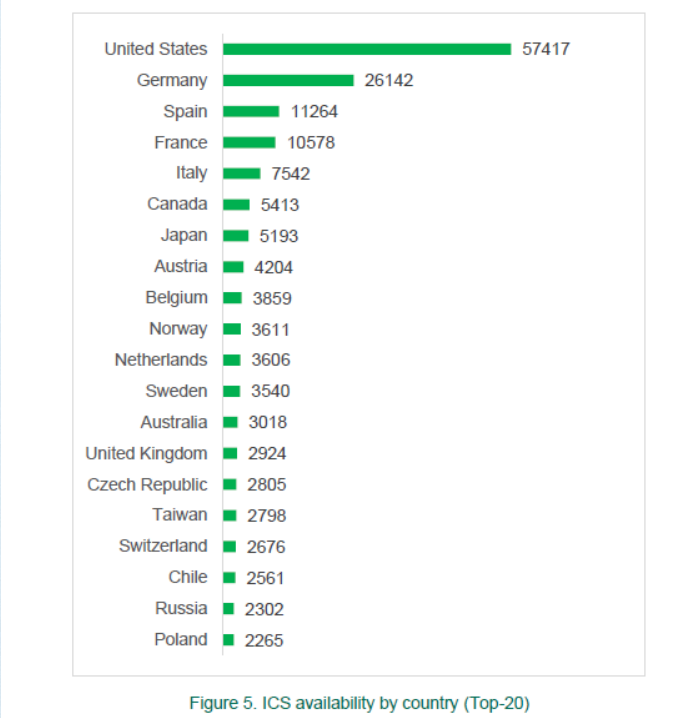
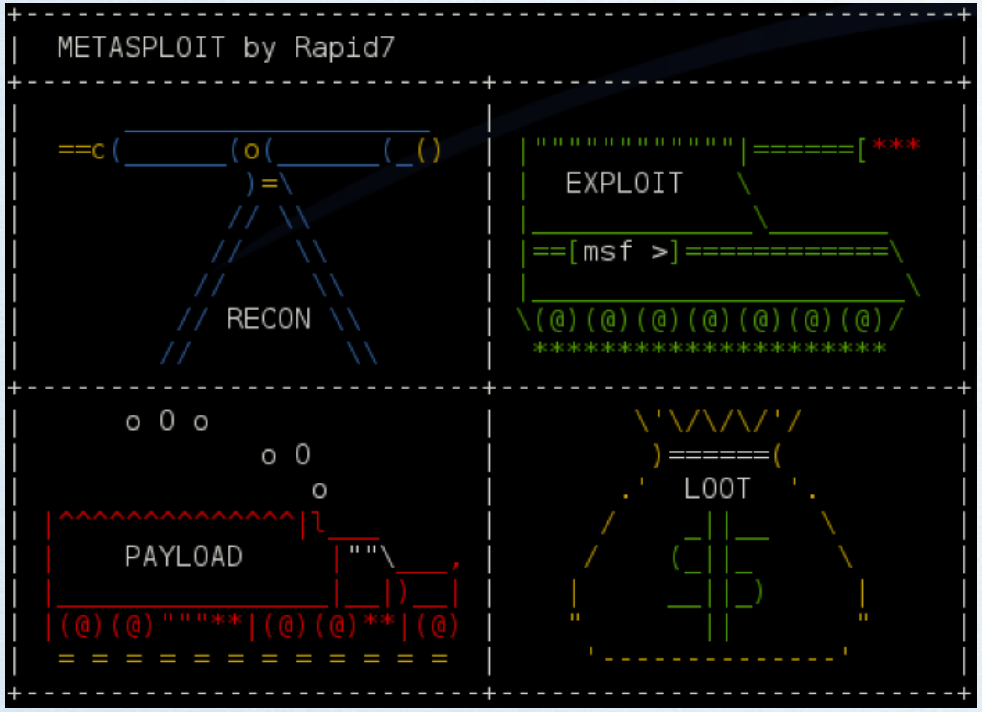
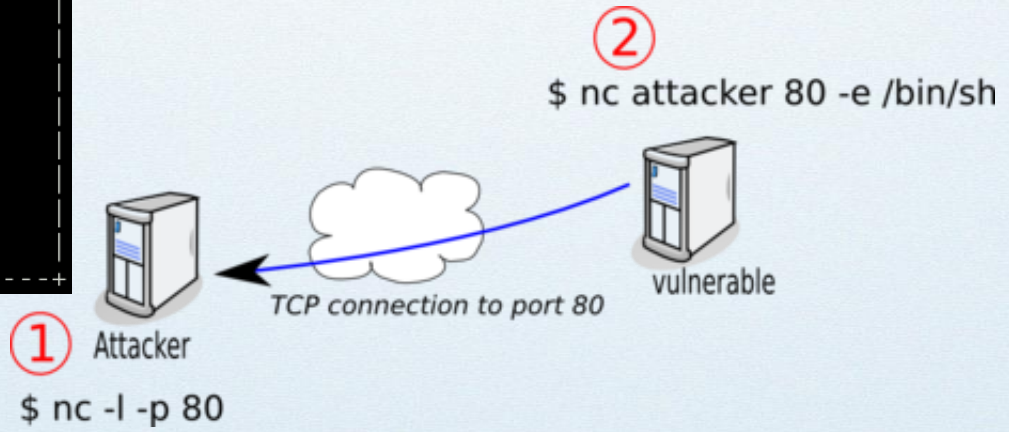


Figure 5. ICS availability by country (Top-20)

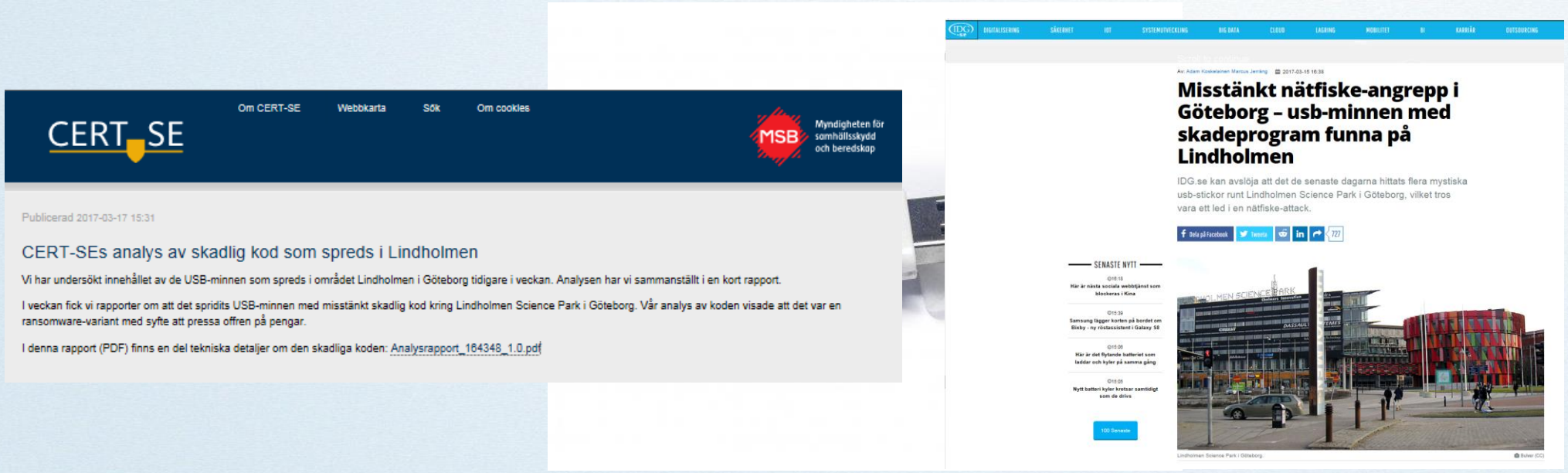
- 92% av enheterna har sårbarheter varav 87% har medelhöga risker och 7% kritiska
- Antal kända sårbarheter i styrsystemskomponenter har tiofaldigats de fem senaste åren
- 91,6% av styrsystemskomponenterna använder svaga protokoll som går att avlyssna och/eller manipulera

HUR GÅR DET TILL?





HUR GÅR DET TILL?



CERT SE

Om CERT-SE Webbkarta Sök Om cookies

MSB Myndigheten för samhällsskydd och beredskap

Publicerad 2017-03-17 15:31

CERT-SEs analys av skadlig kod som spreds i Lindholmen

Vi har undersökt innehållet av de USB-minnen som spreds i området Lindholmen i Göteborg tidigare i veckan. Analysen har vi sammanställt i en kort rapport.

I veckan fick vi rapporter om att det spridits USB-minnen med misstänkt skadlig kod kring Lindholmen Science Park i Göteborg. Vår analys av koden visade att det var en ransomware-variant med syfte att pressa offren på pengar.

I denna rapport (PDF) finns en del tekniska detaljer om den skadliga koden: Analysrapport_184348_1.0.pdf

IDG

Misstänkt nätfiske-angrepp i Göteborg – usb-minnen med skadeprogram funna på Lindholmen

IDG.se kan avslöja att det de senaste dagarna hittats flera mystiska usb-stickor runt Lindholmen Science Park i Göteborg, vilket tros vara ett led i en nätfiske-attack.

SENASTE NYTT

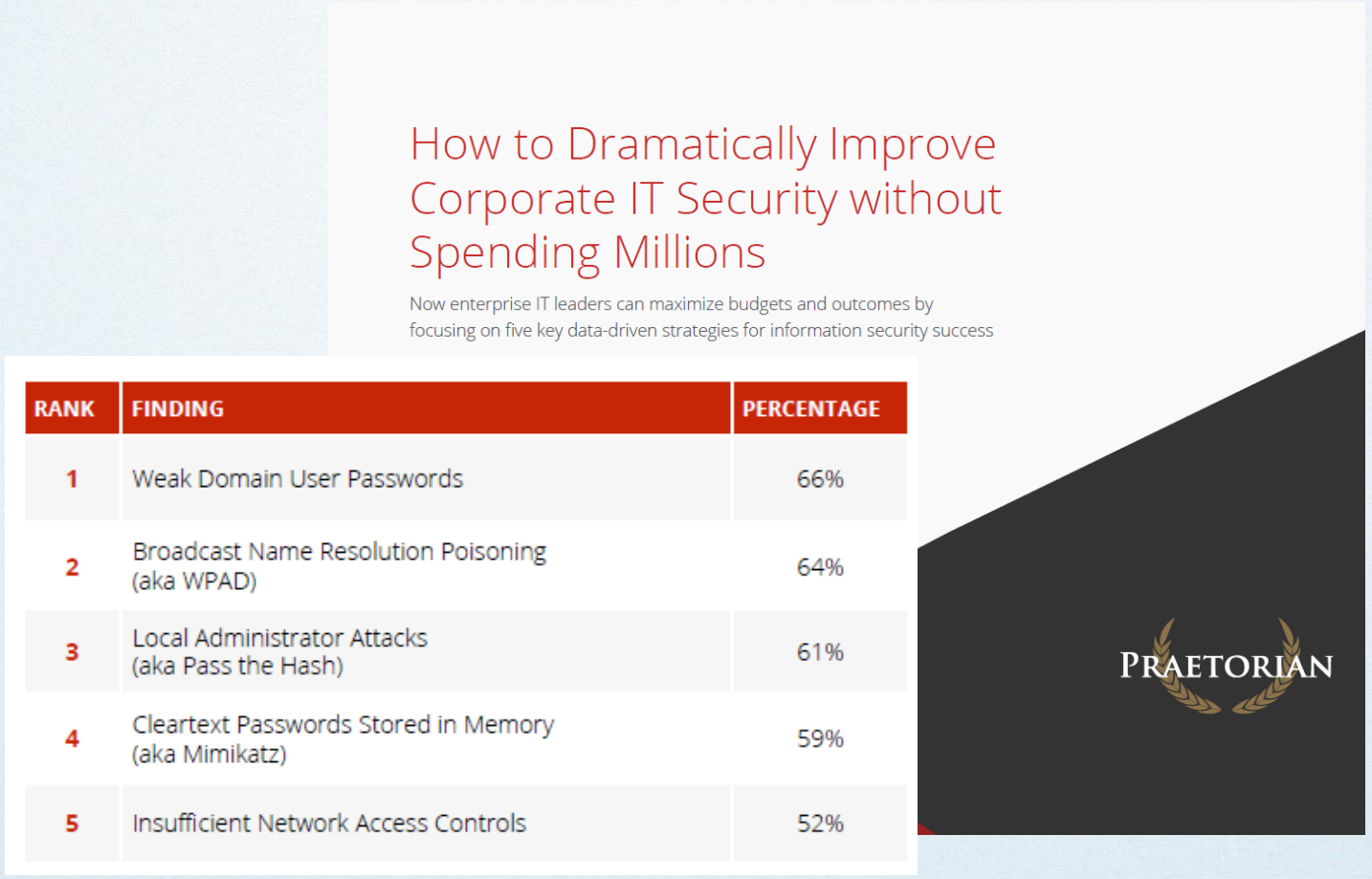
HUR GÅR DET TILL?

VAD GÖR VI NU?

> *The three golden rules to ensure computer security are: do not own a computer; do not power it on; and do not use it.*
>
> *- Robert Morris*

VAD GÖR VI NU?

- Autentisering
- Behörighet
- Segmentering



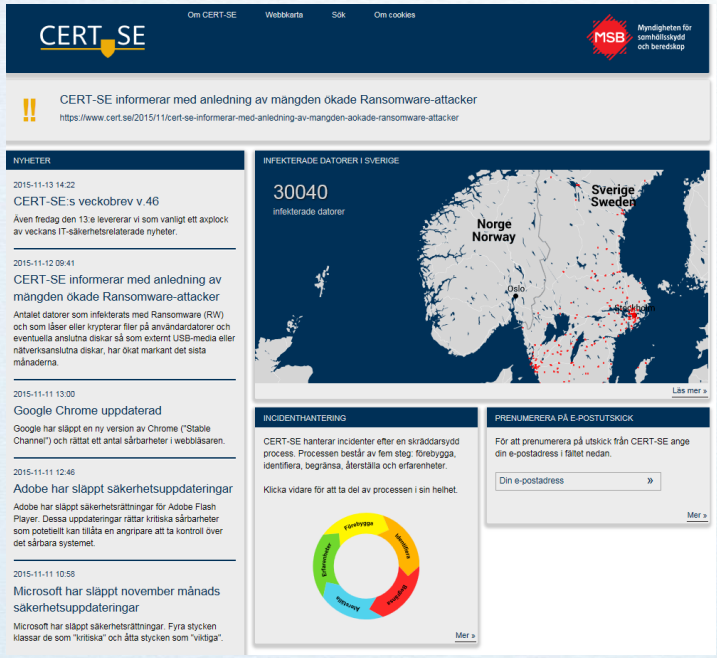
How to Dramatically Improve Corporate IT Security without Spending Millions

Now enterprise IT leaders can maximize budgets and outcomes by focusing on five key data-driven strategies for information security success

RANK	FINDING	PERCENTAGE
1	Weak Domain User Passwords	66%
2	Broadcast Name Resolution Poisoning (aka WPAD)	64%
3	Local Administrator Attacks (aka Pass the Hash)	61%
4	Cleartext Passwords Stored in Memory (aka Mimikatz)	59%
5	Insufficient Network Access Controls	52%

PRAETORIAN

ANDRA TIPS PÅ INFORMATION



https://www.msb.se/ics

TACK FÖR MIG!
FRÅGOR, TANKAR OCH FUNDERINGAR?

Nicklas Keijser

Götalandsvägen 230, Hus 23

125 45 Älvsjö

Mail: nicklas.keijser@rejlers.se

Tel: 072-7104928

…eller så kan ni hitta mig på LinkedIn

REJLERS