Critical Infrastructure Protection from Terrorist Attacks

Candan BOLUKBAS

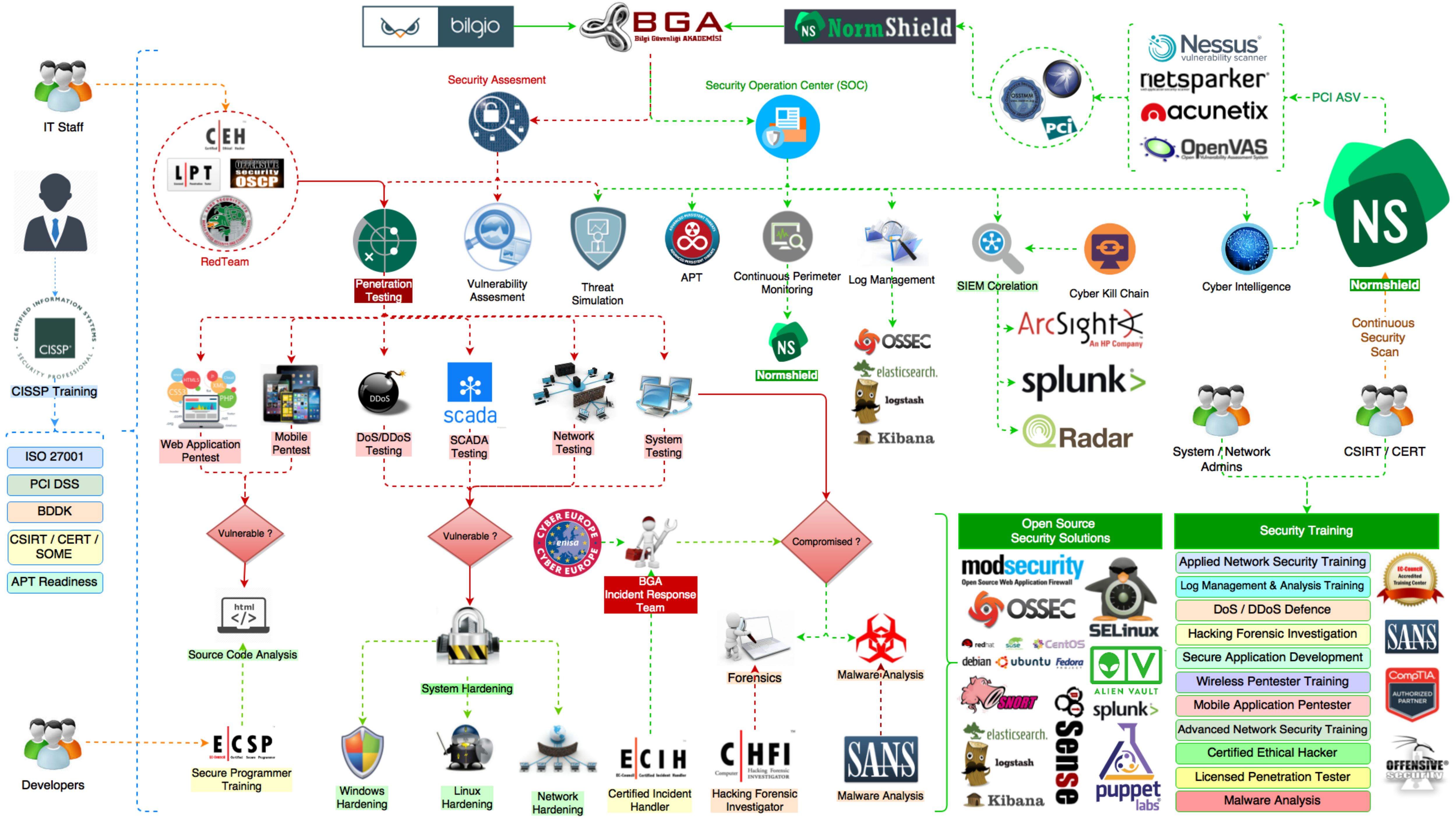
BGA Information Security & Consulting

NATO's Centre of Excellence Defense Against Terrorism (COE-DAT)

About me

Candan BÖLÜKBAŞ

- about.me/bolukbas
- METU Computer Eng.
- CCNA, CCNP, CEH, CAPT, ITIL, MCP, ECSP, ECIH, CHFI
- Enterprise Security Services Manager | Whitehat Hacker
- 7-year .Net & Obj-C Developer, 5-year Security Analysts
- ex Presidency of the Republic of Turkey Network & Security Admin
- candan.bolukbas@bga.com.tr
- @candanbolukbas



bilgio

BGA
Bilgi Güvenliği AKADEMİSİ

NormShield

Security Assesment

Security Operation Center (SOC)

Nessus vulnerability scanner
netsparker
acunetix
OpenVAS

PCI ASV

IT Staff

CEH
LPT
OFFENSIVE security OSCP
RedTeam

CISSP
CISSP Training

Penetration Testing
Vulnerability Assesment
Threat Simulation
APT
Continuous Perimeter Monitoring
Log Management
SIEM Corelation
Cyber Kill Chain
Cyber Intelligence
Normshield

Normshield
OSSEC
elasticsearch.
logstash
Kibana

ArcSight An HP Company
splunk>
Radar

Continuous Security Scan

System / Network Admins
CSIRT / CERT

ISO 27001
PCI DSS
BDDK
CSIRT / CERT / SOME
APT Readiness

Web Application Pentest
Mobile Pentest
DoS/DDoS Testing
scada
SCADA Testing
Network Testing
System Testing

Vulnerable ?
Vulnerable ?
CYBER EUROPE enisa
BGA Incident Response Team
Compromised ?

Source Code Analysis
System Hardening
Forensics
Malware Analysis

Developers
ECSP
Secure Programmer Training
Windows Hardening
Linux Hardening
Network Hardening
ECIH
Certified Incident Handler
CHFI
Hacking Forensic Investigator
SANS
Malware Analysis

Open Source Security Solutions

modsecurity Open Source Web Application Firewall
OSSEC
SELinux
redhat
suse
CentOS
debian
ubuntu
Fedora
SNORT
ALIEN VAULT
splunk>
elasticsearch.
logstash
Kibana
Sense
puppet labs

Security Training

Applied Network Security Training
Log Management & Analysis Training
DoS / DDoS Defence
Hacking Forensic Investigation
Secure Application Development
Wireless Pentester Training
Mobile Application Pentester
Advanced Network Security Training
Certified Ethical Hacker
Licensed Penetration Tester
Malware Analysis

EC-Council Accredited Training Center
SANS
CompTIA AUTHORIZED PARTNER
OFFENSIVE security

Supervisory Control and Data Acquisition (SCADA)

> Process control system (PCS), distributed control system (DCS), and supervisory control and data acquisition (SCADA) are names frequently applied to the systems that control, monitor, and manage large production systems. In 2008, the NIST applied SCADA as industry control systems (ICS), in its landmark publication of NIST 800-82

- Electric Power Generators,
- Transportation Systems,
- Dams,
- Chemical Facilities,
- Petrochemical Operations,
- Pipelines

Is Industrial Control System Security Different Than Regular IT Security?

Comparing techniques, tools, and terminology, ICS security is not entirely different from current IT security. There are differences, however. These differences largely center around the following principles:

- ICS security failures impacts are frequently more severe and immediate.
- ICS security can be more difficult to manage: old systems that can’t be patched
- Cyber threats to an ICS include myriad additional threat vectors, including non-typical network protocols, commands that cannot be blocked due to safety or production issues
- Conventional protections such as antivirus or firewall that may not be able to be utilized
- No luxury of development and test environments.

ICS Compared to Safety Instrumented Systems

ICS includes safety instrumented systems (SIS), which are specifically hardened ICS elements built for high reliability and associated with failing safe. SIS have functional elements contributing substantially to operational safety and risk management, and often share technical architectures and features with more general purpose ICS.

SIS are generally designed with a single purpose in mind:
avoiding dangerous situations in the production system by stopping or shutting down processes if unsafe conditions develop.

What Has Changed in ICS That Raises New Vulnerabilities?

“Recent industrial history has demonstrated that the life cycle of a control system is now between 15 and 30 years. As little as even 15 years ago, network and software security was not a top priority in the control systems environment.”

161% increase in vulnerabilities over the prior year!

So what?

> "Some analysts estimated that 20% of all IP-enabled devices in existence today are ICS devices. This number of connected devices (versus people via PC and laptops) is expected to grow dramatically with a compound growth rate of 40% from 2015 to 2020—reaching as much 7 billion devices by that time and completely outnumbering people-oriented connections."

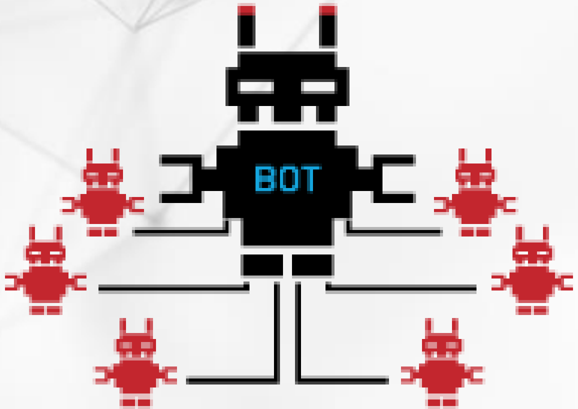
Distinct ICS Security Requirements and Sensitivity

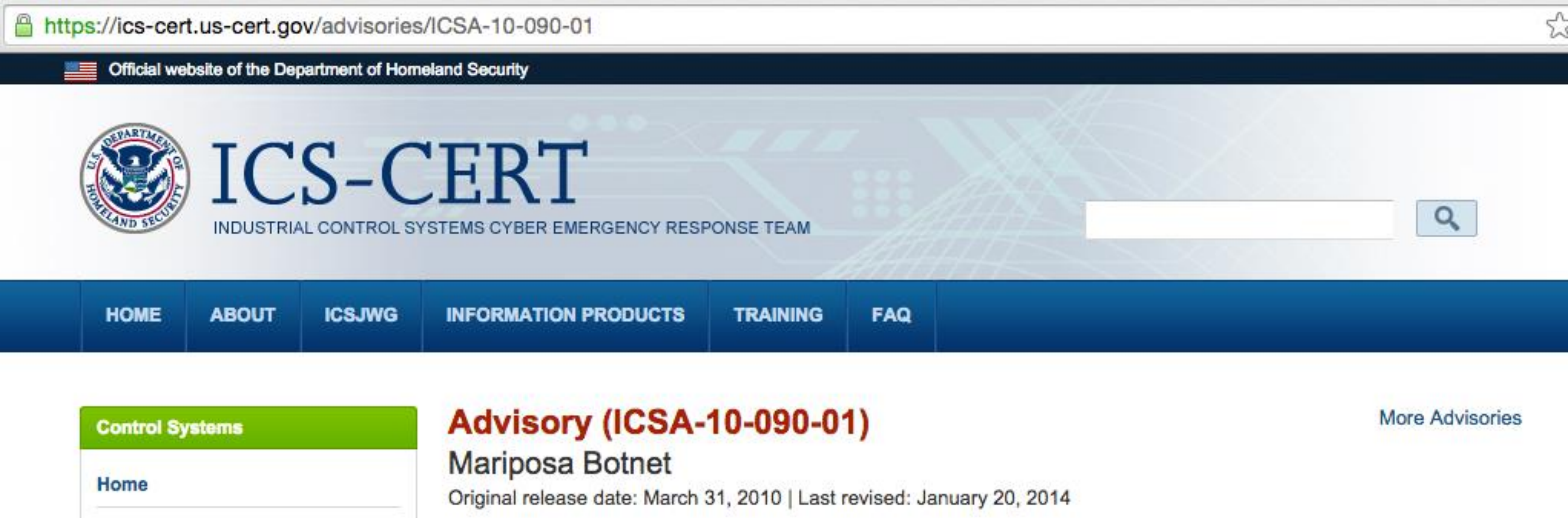
REQUIREMENT	DESCRIPTION
Performance	ICS are generally time critical; neither delay nor jitter is acceptable.
Availability	Unexpected outages of systems that control industrial processes are not acceptable.
Risk Management	For an ICS, human safety and fault tolerance are the primary concerns.
Architecture Security Focus	For ICS, edge clients need to be carefully protected since they are directly responsible for controlling the end processes.
Physical Interaction	All security functions integrated into the ICS must be tested to prove that they do not compromise normal ICS functionality.
Time-Critical Responses	For some ICS, automated response time or system response to human interaction is very critical
System Operation	Software and hardware applications are more difficult to upgrade in an operational control system network

ICS Threat Agents

THREAT AGENT	PROFILE	TARGETED ASSETS
Professional bot herders	Like malware wholesalers. They invest in the development and management of bot herds, and then rent them out to any of the other threat agents.	Seek to gain control of devices in order to repurpose them on demand and rent or sell the herd to any and all of the other agents

Last year, a family of malware known as BlackEnergy had infected unknown numbers of internet-facing ICS sites. Machines from Siemens, Advantech, and GE had all been compromised.




https://ics-cert.us-cert.gov/advisories/ICSA-10-090-01
Official website of the Department of Homeland Security
HOME
ABOUT
ICSJWG
INFORMATION PRODUCTS
TRAINING
FAQ
Control Systems
Home
More Advisories

ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Advisory (ICSA-10-090-01)

Mariposa Botnet

Original release date: March 31, 2010 | Last revised: January 20, 2014

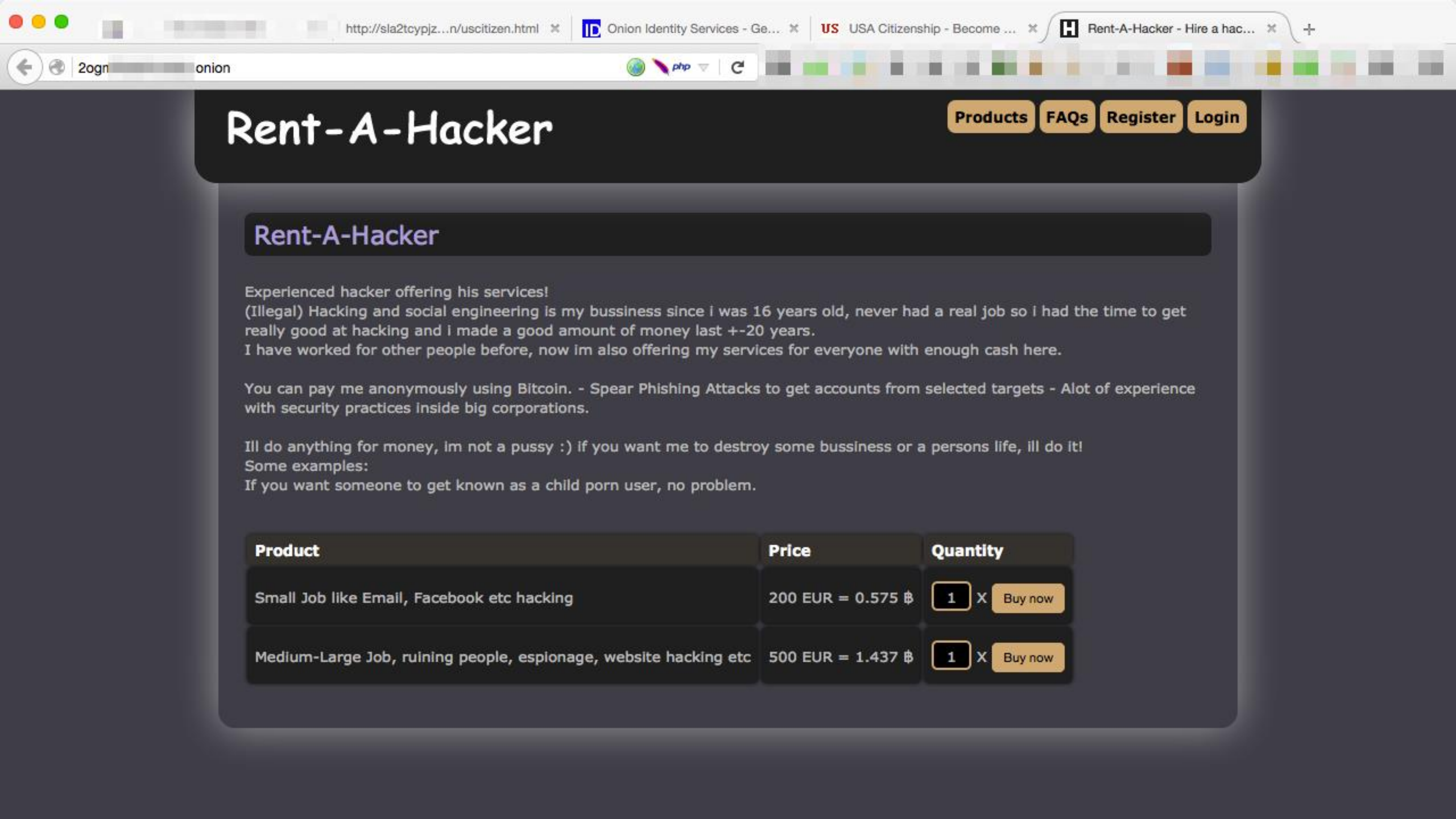
Details

In February 2010, a US utility company (USUTIL1) was notified by another US Utility partner company (USUTIL2) that a USUTIL1 employee had visited USUTIL2 with a Mariposa-infected laptop. There had been no indication from USUTIL1's computer network defense mechanisms (Anti-Virus, Intrusion Detection Systems, Firewalls etc.) that an infection had occurred and USUTIL2's notification was USUTIL1's first indication that there was an issue.

USUTIL1's investigation found that the initial infection vector may have been a USB drive shared at an industry conference. An instructor shared a USB drive among participants at a training event attended by USUTIL1's employee. It is believed that when the employee returned and connected his laptop to the corporate network, the malware spread to multiple business systems.

ICS Threat Agents

THREAT AGENT	PROFILE	TARGETED ASSETS
Organized Crime	Gangs and crime syndicates, engaged in debit and card fraud, now find that chip-based technology is forcing them online for better returns.	Personal identity information for identity theft and multiple forms of fraud.


http://sla2tcypjz...n/uscitizen.html
Onion Identity Services - Ge...
USA Citizenship - Become ...
Rent-A-Hacker - Hire a hac...
2ogm[redacted]onion
Rent-A-Hacker
Products
FAQs
Register
Login

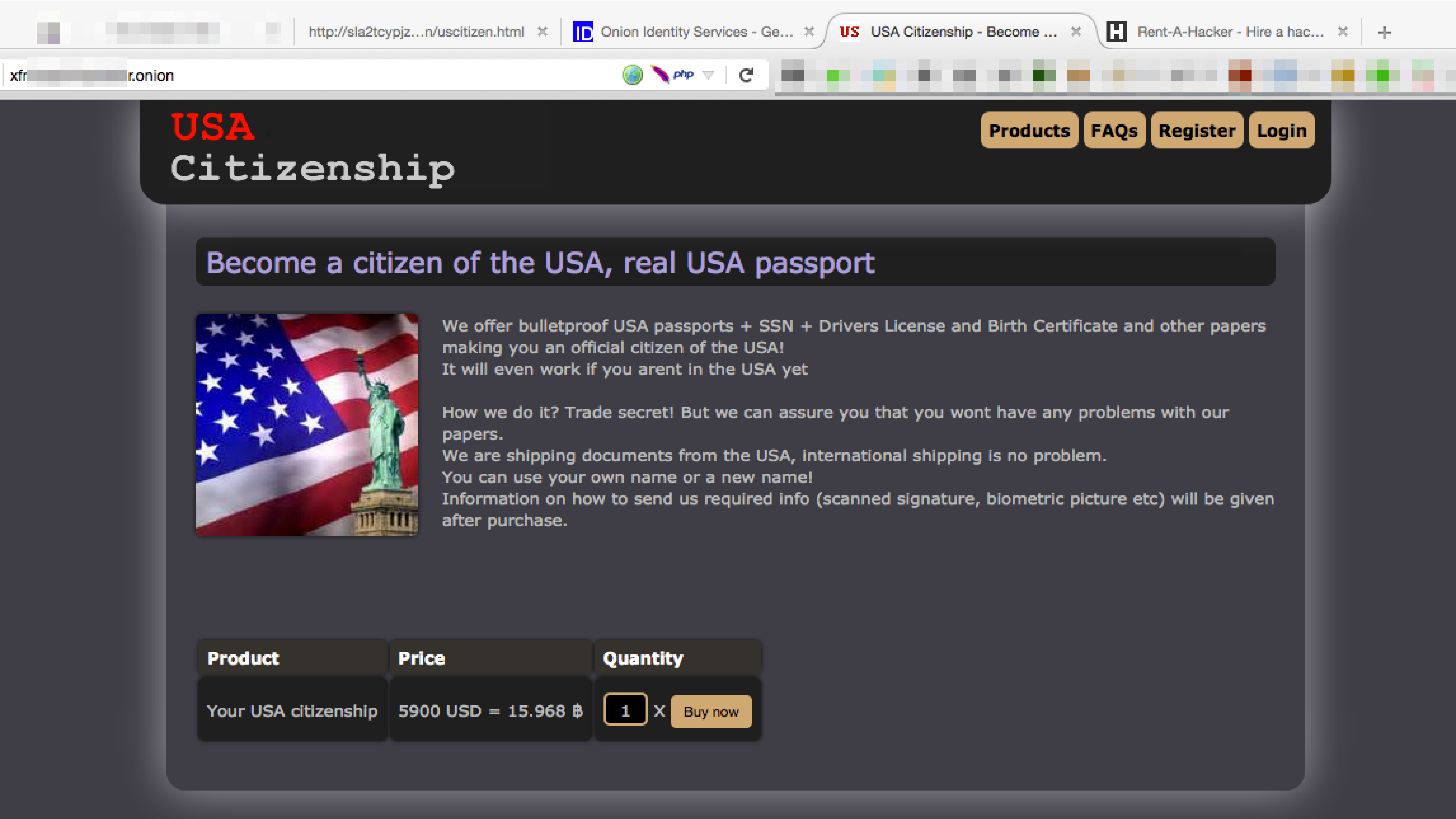
Rent-A-Hacker

Experienced hacker offering his services!
(Illegal) Hacking and social engineering is my bussiness since i was 16 years old, never had a real job so i had the time to get really good at hacking and i made a good amount of money last +-20 years.
I have worked for other people before, now im also offering my services for everyone with enough cash here.

You can pay me anonymously using Bitcoin. - Spear Phishing Attacks to get accounts from selected targets - Alot of experience with security practices inside big corporations.

Ill do anything for money, im not a pussy :) if you want me to destroy some bussiness or a persons life, ill do it!
Some examples:
If you want someone to get known as a child porn user, no problem.

Product	Price	Quantity
Small Job like Email, Facebook etc hacking	200 EUR = 0.575 ฿	1 X Buy now
Medium-Large Job, ruining people, espionage, website hacking etc	500 EUR = 1.437 ฿	1 X Buy now



[redacted]
http://sla2tcypjz....n/uscitizen.html
Onion Identity Services - Ge...
USA Citizenship - Become ...
Rent-A-Hacker - Hire a hac...
xfr[redacted]r.onion
[redacted]
Products
FAQs
Register
Login

USA Citizenship

Become a citizen of the USA, real USA passport

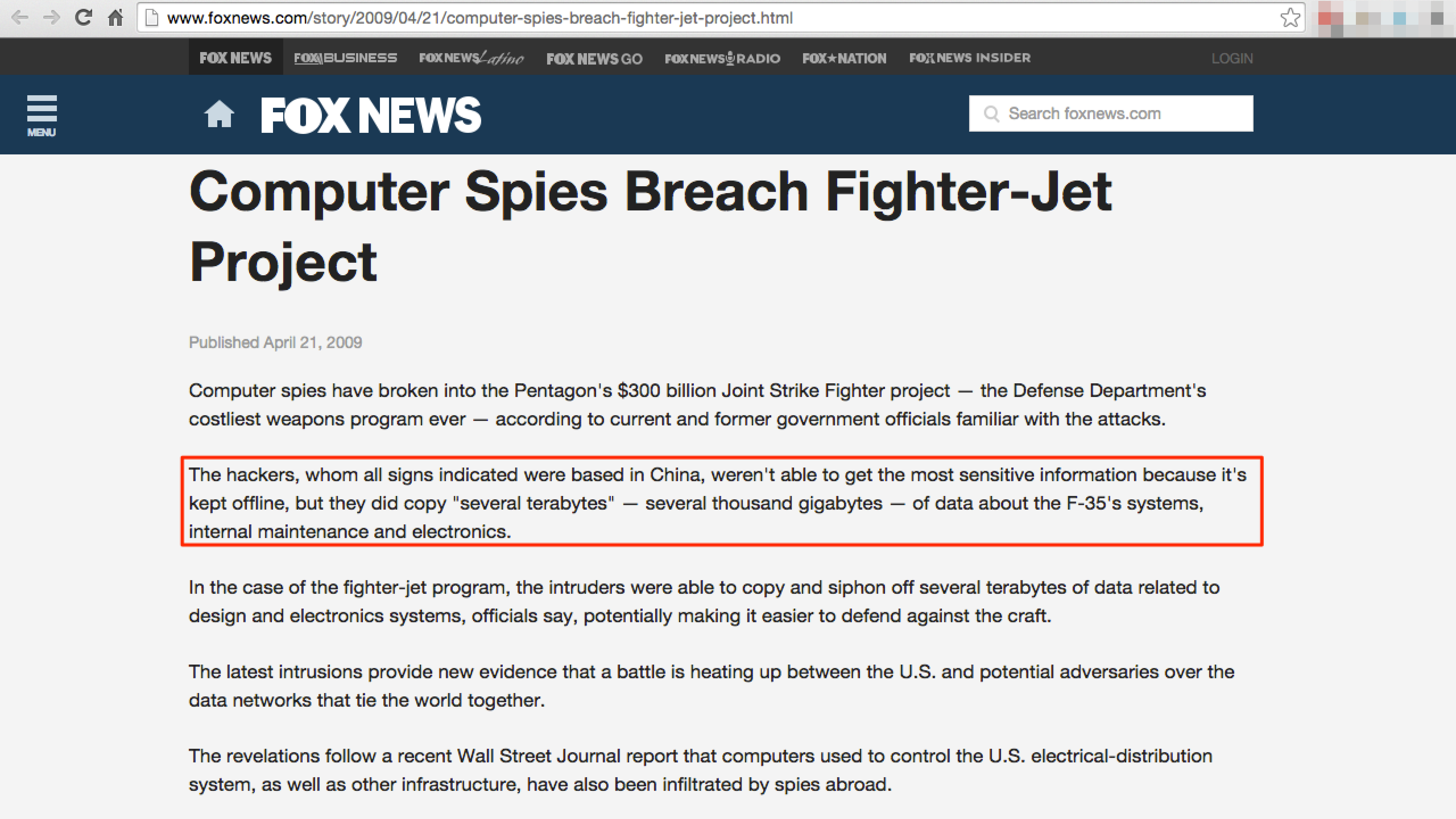
We offer bulletproof USA passports + SSN + Drivers License and Birth Certificate and other papers making you an official citizen of the USA!
It will even work if you arent in the USA yet

How we do it? Trade secret! But we can assure you that you wont have any problems with our papers.
We are shipping documents from the USA, international shipping is no problem.
You can use your own name or a new name!
Information on how to send us required info (scanned signature, biometric picture etc) will be given after purchase.

Product	Price	Quantity
Your USA citizenship	5900 USD = 15.968 ฿	1 X Buy now

ICS Threat Agents

THREAT AGENT	PROFILE	TARGETED ASSETS
Industrial espionage	Mercenary type entities hired to target specific corporate assets and industries.	Intellectual property, financial, and production information, plans, and strategies.



Computer Spies Breach Fighter-Jet Project

Published April 21, 2009

Computer spies have broken into the Pentagon's $300 billion Joint Strike Fighter project — the Defense Department's costliest weapons program ever — according to current and former government officials familiar with the attacks.

The hackers, whom all signs indicated were based in China, weren't able to get the most sensitive information because it's kept offline, but they did copy "several terabytes" — several thousand gigabytes — of data about the F-35's systems, internal maintenance and electronics.

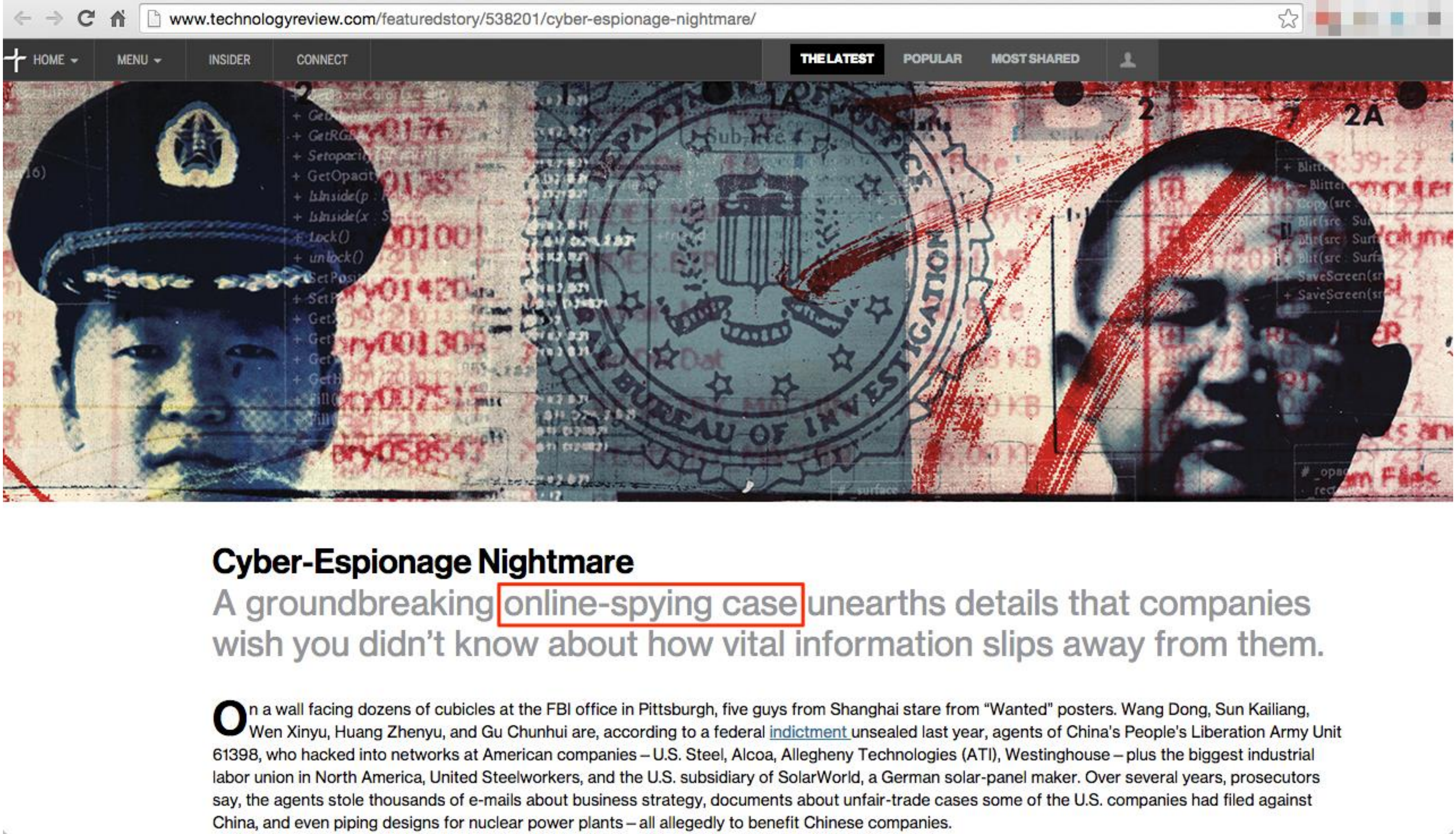
In the case of the fighter-jet program, the intruders were able to copy and siphon off several terabytes of data related to design and electronics systems, officials say, potentially making it easier to defend against the craft.

The latest intrusions provide new evidence that a battle is heating up between the U.S. and potential adversaries over the data networks that tie the world together.

The revelations follow a recent Wall Street Journal report that computers used to control the U.S. electrical-distribution system, as well as other infrastructure, have also been infiltrated by spies abroad.

ICS Threat Agents

THREAT AGENT	PROFILE	TARGETED ASSETS
Foreign intelligence services / nation-states	State-sponsored entities, possibly paramilitary, usually operating from identifiable networks or geographic regions, if you can trace them.	National secrets, plans, and strategies, and industrial secrets, plans and strategies.


www.technologyreview.com/featuredstory/538201/cyber-espionage-nightmare/
HOME
MENU
INSIDER
CONNECT
THE LATEST
POPULAR
MOST SHARED

Cyber-Espionage Nightmare

A groundbreaking online-spying case unearths details that companies wish you didn't know about how vital information slips away from them.

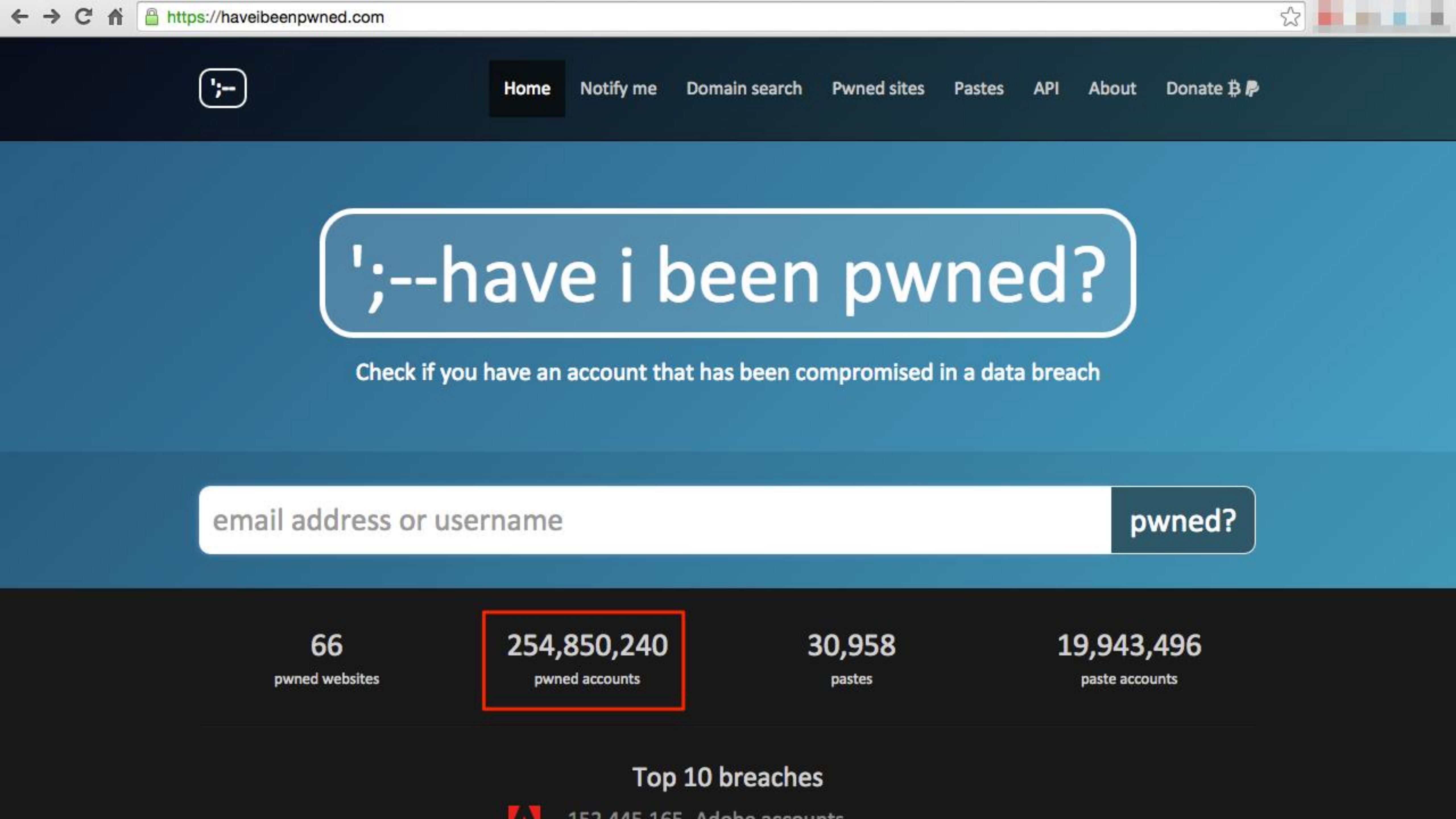
On a wall facing dozens of cubicles at the FBI office in Pittsburgh, five guys from Shanghai stare from "Wanted" posters. Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui are, according to a federal indictment unsealed last year, agents of China's People's Liberation Army Unit 61398, who hacked into networks at American companies – U.S. Steel, Alcoa, Allegheny Technologies (ATI), Westinghouse – plus the biggest industrial labor union in North America, United Steelworkers, and the U.S. subsidiary of SolarWorld, a German solar-panel maker. Over several years, prosecutors say, the agents stole thousands of e-mails about business strategy, documents about unfair-trade cases some of the U.S. companies had filed against China, and even piping designs for nuclear power plants – all allegedly to benefit Chinese companies.

ICS Threat Agents

THREAT AGENT	PROFILE	TARGETED ASSETS
Spammers	Specialize in harvesting legitimate e-mail addresses from sources such as Web sites, blogs, social networks, Web mail providers, and any other possible source. Generate massive lists of addresses, both real and randomized/guessed to send junk e-mail (spam).	Individuals who will either buy (semi)legitimate products, submit to fraudulent transactions, identity theft, or pyramid schemes, or fence stolen goods.

ICS Threat Agents

THREAT AGENT	PROFILE	TARGETED ASSETS
Phishers	In close effort with spammers, phishers attempt to attract individual users to Web sites loaded with malicious software in order to compromise the user devices once they connect to a Web site, and gain access to contents or make them into bots.	Individual fraud and identity theft, industrial espionage as described above, and public sector entities for national security assets.



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

66
pwned websites

254,850,240
pwned accounts

30,958
pastes

19,943,496
paste accounts

Top 10 breaches

152,445,165 Adobe accounts

ICS Threat Agents

THREAT AGENT	PROFILE	TARGETED ASSETS
Activists and terrorists	Ideologically motivated entities typically without the resources to develop exploits independently but with enough resources to hire compromised devices from herders or leverage off-the-shelf exploit “kits.”	Industrial sabotage of assets (physical or logical), public sector entities, and government and military for planning, strategic, or national security secrets.

www.computerworld.com/article/2471318/healthcare-it/brace-for--son-of-stuxnet-----duqu-spies-on-scada.html

NEWS ANALYSIS

Brace for "son of Stuxnet" -- Duqu spies on SCADA

By Richi Jennings (@richi) - October 19, 2011.

A supposed "precursor" to the next Stuxnet has been discovered. The Duqu Trojan aims to reconnoiter critical SCADA infrastructure in advance of future attacks. In IT Blogwatch, bloggers watch closely.

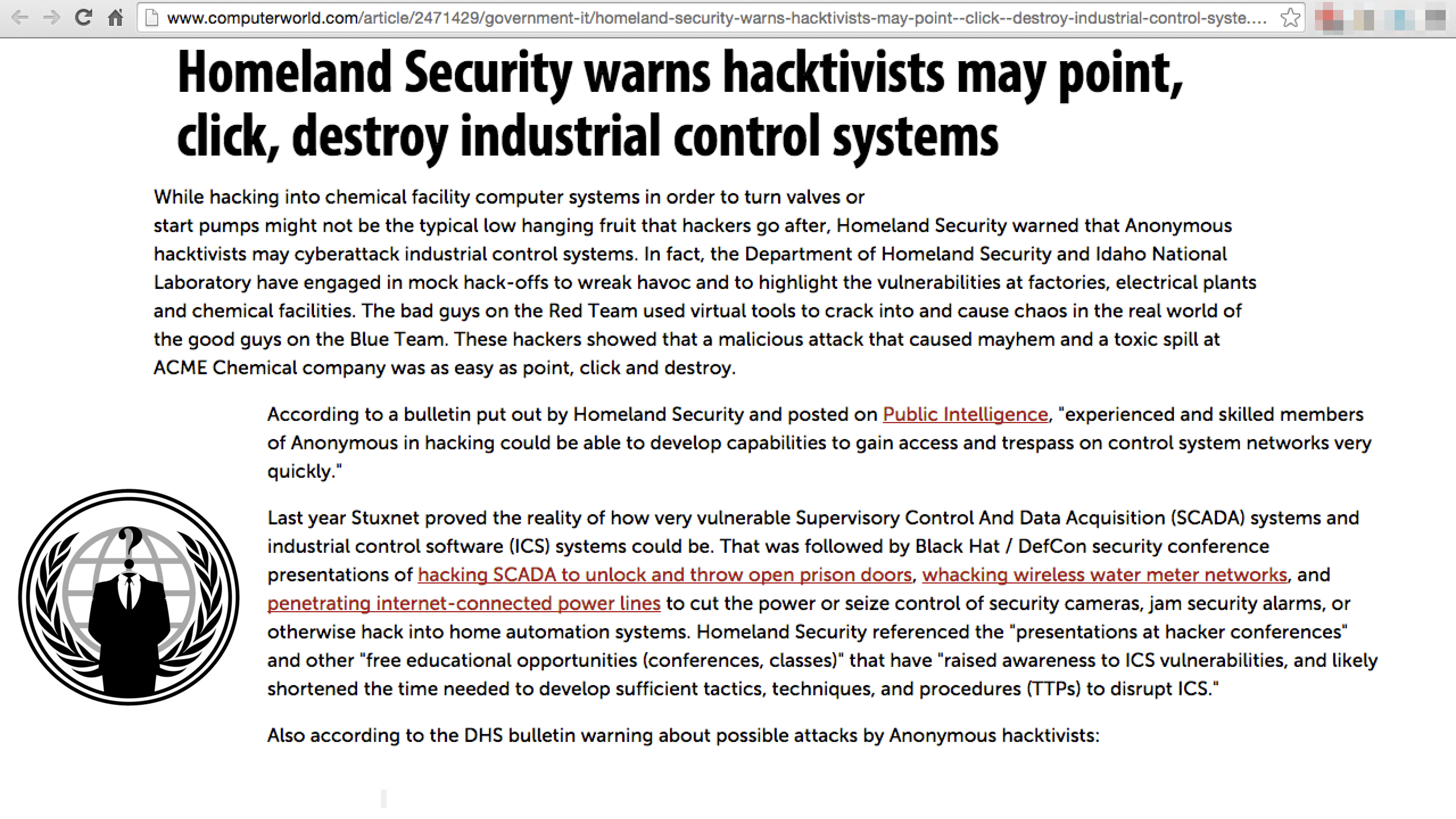
Your humble blogwatcher curated these bloggy bits for your entertainment.

Jaikumar Vijayan reports:

> [It] appears to have been written by the authors of Stuxnet, or at least by someone who has access to Stuxnet source code. ... Duqu's purpose is to steal data from manufactures of industrial control systems that can then be used to craft attacks.
>
> [T]he Trojan is "highly targeted" at a limited number of organizations. ... News of the new Trojan is sure to reinforce concerns about...the industrial control systems used in critical infrastructures. ... The Stuxnet worm...has affected industrial control systems in many countries...especially Iran.

Dan Goodin adds:

> *Dubbed Duqu, the remote access trojan has been detected in a handful of organizations, where it...gathered keystrokes and system information that can be used to attack a third party.*
>
> *[The] sample was recovered from computer systems located in Europe, from a limited number of organizations, including those involved in making...SCADA, or supervisory control and data acquisition systems.*



www.computerworld.com/article/2471429/government-it/homeland-security-warns-hacktivists-may-point--click--destroy-industrial-control-syste....

Homeland Security warns hacktivists may point, click, destroy industrial control systems

While hacking into chemical facility computer systems in order to turn valves or start pumps might not be the typical low hanging fruit that hackers go after, Homeland Security warned that Anonymous hacktivists may cyberattack industrial control systems. In fact, the Department of Homeland Security and Idaho National Laboratory have engaged in mock hack-offs to wreak havoc and to highlight the vulnerabilities at factories, electrical plants and chemical facilities. The bad guys on the Red Team used virtual tools to crack into and cause chaos in the real world of the good guys on the Blue Team. These hackers showed that a malicious attack that caused mayhem and a toxic spill at ACME Chemical company was as easy as point, click and destroy.

According to a bulletin put out by Homeland Security and posted on Public Intelligence, "experienced and skilled members of Anonymous in hacking could be able to develop capabilities to gain access and trespass on control system networks very quickly."

Last year Stuxnet proved the reality of how very vulnerable Supervisory Control And Data Acquisition (SCADA) systems and industrial control software (ICS) systems could be. That was followed by Black Hat / DefCon security conference presentations of hacking SCADA to unlock and throw open prison doors, whacking wireless water meter networks, and penetrating internet-connected power lines to cut the power or seize control of security cameras, jam security alarms, or otherwise hack into home automation systems. Homeland Security referenced the "presentations at hacker conferences" and other "free educational opportunities (conferences, classes)" that have "raised awareness to ICS vulnerabilities, and likely shortened the time needed to develop sufficient tactics, techniques, and procedures (TTPs) to disrupt ICS."

Also according to the DHS bulletin warning about possible attacks by Anonymous hacktivists:

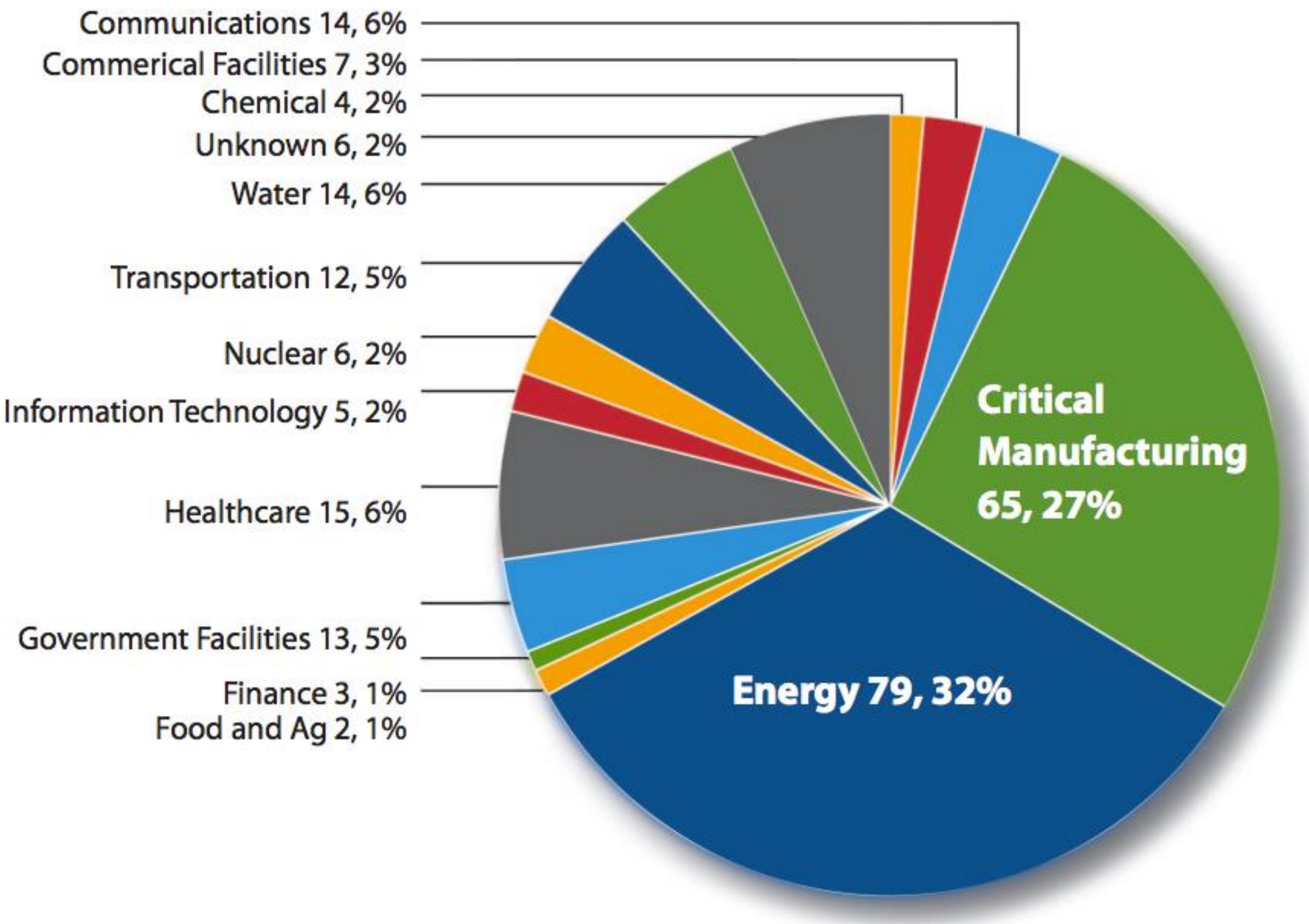


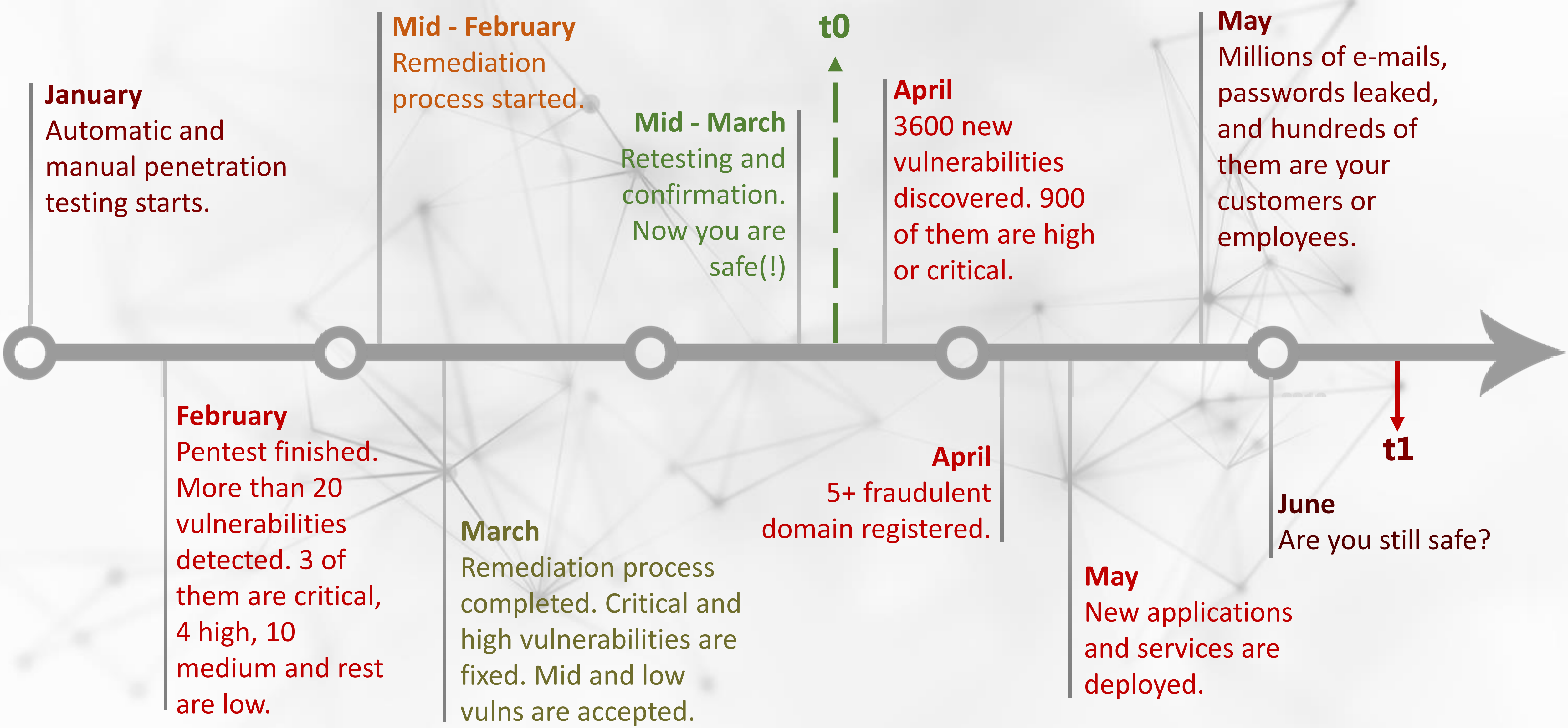
Figure 1. FY 2014 incidents reported by sector (245 total).

INCIDENT RESPONSE/VULNERABILITY COORDINATION IN 2014

Collateral Damage

The largest generalized threat to ICS security is related to collateral damage from systems that have been hi-jacked for the illicit purposes of organized crime and foreign intelligence.

Why Continuous Security Scan (CSS)



January
Automatic and manual penetration testing starts.

February
Pentest finished. More than 20 vulnerabilities detected. 3 of them are critical, 4 high, 10 medium and rest are low.

Mid - February
Remediation process started.

March
Remediation process completed. Critical and high vulnerabilities are fixed. Mid and low vulns are accepted.

Mid - March
Retesting and confirmation. Now you are safe(!)

April
3600 new vulnerabilities discovered. 900 of them are high or critical.

April
5+ fraudulent domain registered.

May
Millions of e-mails, passwords leaked, and hundreds of them are your customers or employees.

May
New applications and services are deployed.

June
Are you still safe?

> Network breaches are no longer a matter of “if,” but “when.”

References

https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf
http://www.escortsproject.eu
European Committee for Standardization (Comité Européen de Normalisation);
https://espace.cern.ch/EuroSCSIE/default.aspx
http://sta.jrc.ec.europa.eu/index.php/cip-action-menu?start=10
http://www.first.org
http://www.us-cert.gov/GFIRST
http://www.us-cert.gov/control_systems/pdf/ICS_CERT Factsheet.pdf
http://www.us-cert.gov/control_systems/icsjwg
http://www.iee.org
http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf
http://ieeexplore.ieee.org/iel5/4453837/4453852/04453853.pdf?arnumber=4453853
http://www.qualitylogic.com/Contents/Smart-Grid/Technology/IEEE-1686-2007.aspx
http://grouper.ieee.org/groups/sub/wgc6/documents/drafts/P1711%2020Draft%20203%20202008-08-16.pdf
http://www.thei3p.org
http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

рахмат
danke
謝謝
ngiyabonga
Баярлалаа
spas
teşekkür ederim
mersi
kia ora
barka
welalin
tack
tapadh leat
mahalo
спасибо
faafetai lava
vinaka
blagodaram
dank je
misaotra
paldies
grazzi
спасибі
matondo
kiitos
dankie
nanni
nandri
dhanyavad
mauruuru
thank you
gracias
хвала
asante
manana
köszönöm
bedankt
bayarlalaa
gràçie
hvala
aciū
dankon
akun
obrigada
tenki
murakoze
enkosi
djiere dieuf
tau
mochchakkeram
дякую
mamnun
dziękuję
chnorakaloutioun
gratias ago
gràcies
sulpáy
go raibh maith agat
chokrane
sobodi
děkuji
sagolun
sukriya
kop khun krap
taiku
arigatô
takk
dakujem
trugarez
obrigado
mèsi
didi madloba
najis tuke
ありがとう
tanemirt
grazie
terima kasih
rahmet
ευχαριστώ
diolch
dhanyavadagalu
shukriya
mercé
мерси
kam sah hamnida
rahmat
তোমাকে ধন্যবাদ
감사합니다
xièxie
merci