Cybersecurity Trends and Attacks

(2017 Ransomware and Evil Russian Hacker edition)

Shannon McMurtrey, Ph.D. GPEN, GCIH, GWAPT
Assistant Professor of Management Information Systems
Drury University

DRURY UNIVERSITY

Shannon McMurtrey, Ph.D.

Assistant Professor of Management Information Systems

Drury University

smcmurtrey@drury.edu

@Shannonm

Education and Certifications

Ph.D. Computer Information Systems
Nova Southeastern University
MBA Missouri State University
B.S. Missouri State University
GPEN, GCIH, and GWAPT Certifications from GIAC
Cybersecurity Fundamentals Certificate from ISACA

Professional Experience

Co-founder, Cart32
Co-founder, Intuitive Medical Software
Founder, Digital River Information Security, LLC
Developer of Drury and Missouri State's Cybersecurity Graduate Programs
MSU College of Business research award winner

The game is changing…

National Security, Espionage

Nation-state actors
Stuxnet, Aurora, APT-1

Notoriety, Activism, Defamation

Hactivists
Lulzsec, Anonymous

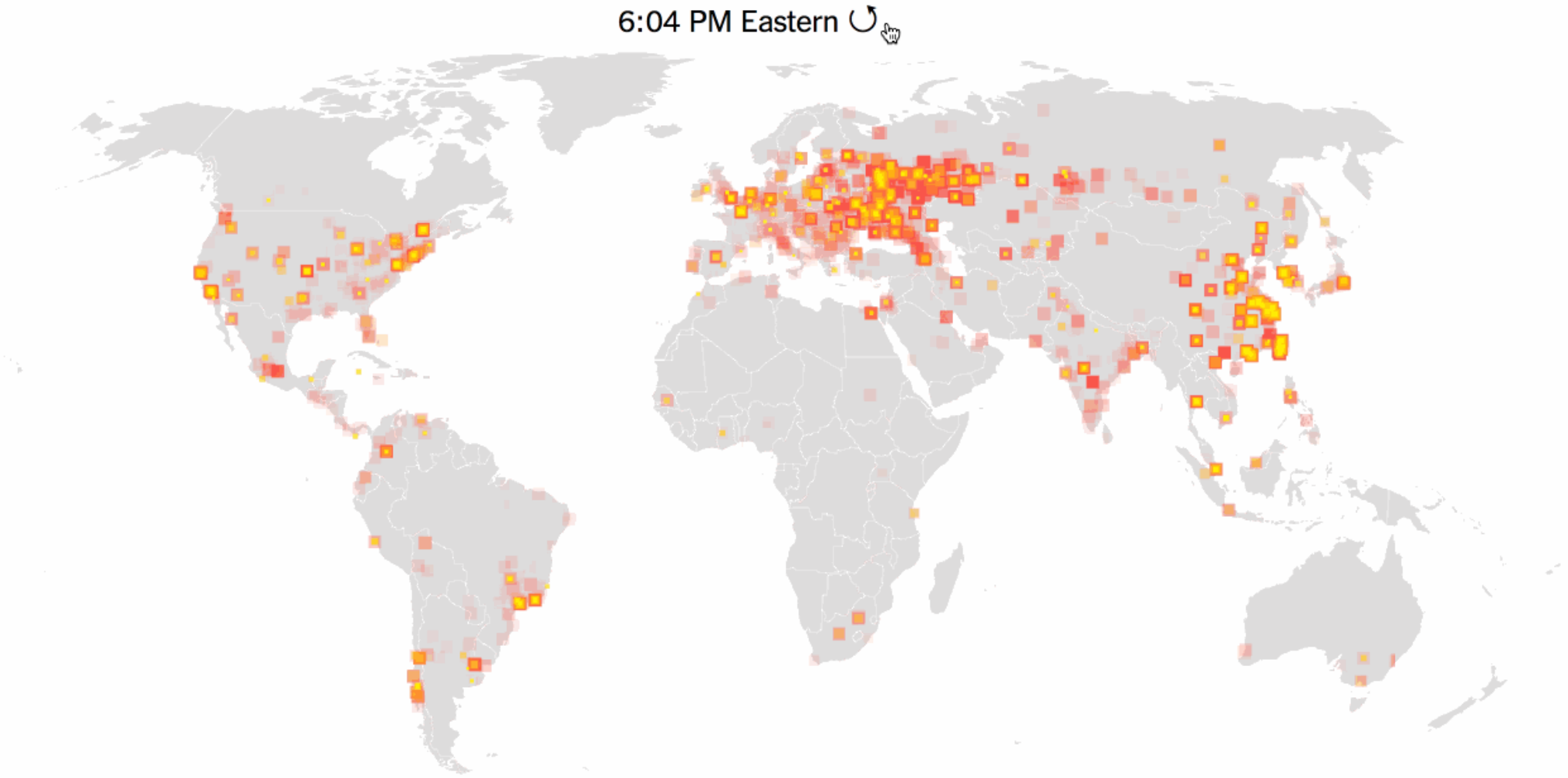
Monetary Gain

Organized crime
Zeus, ZeroAccess, Blackhole Exploit Pack

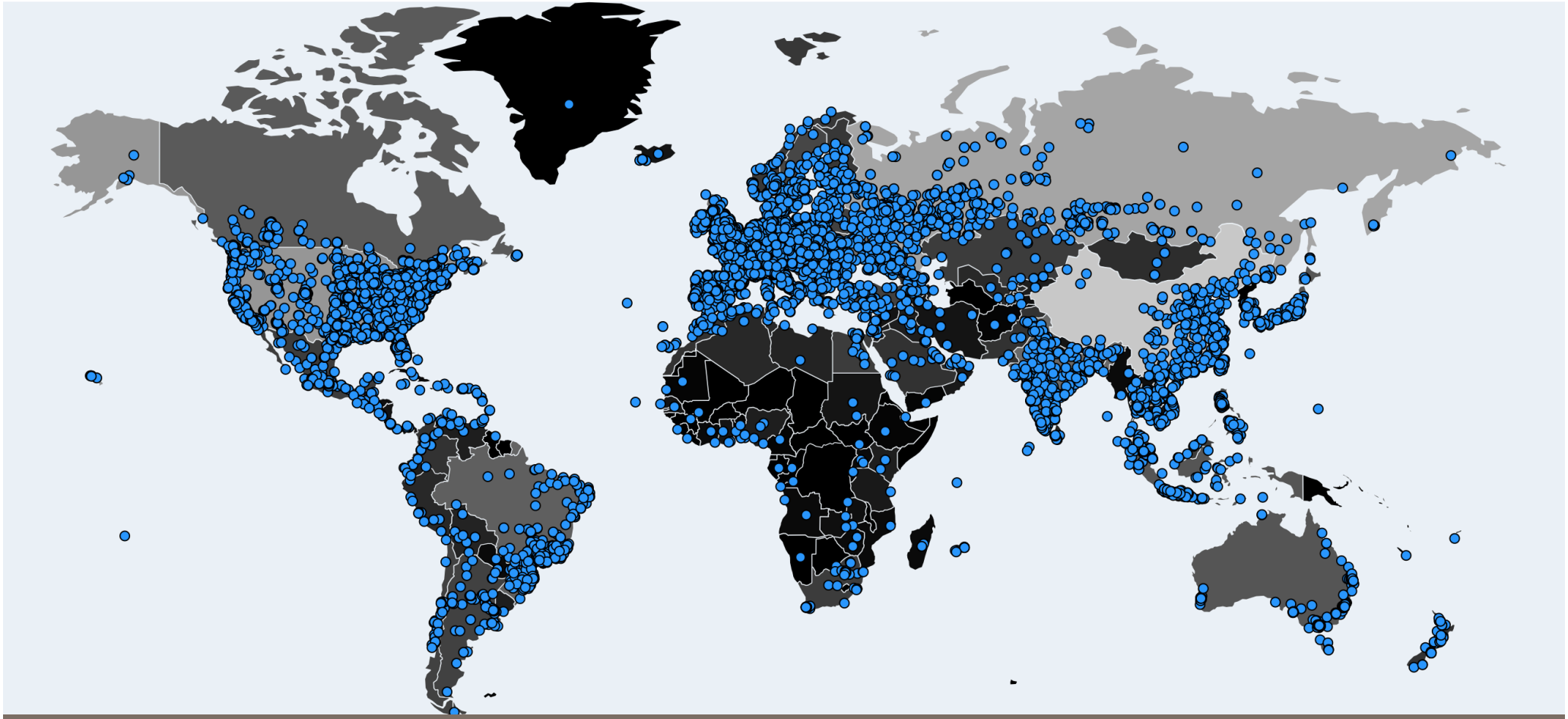
Nuisance, Curiosity

Insiders, Spam, Script-kiddies
Nigerian 419 Scams, Code Red

Global Ransomware outbreak May 12, 2017



Every blue dot represents a wannacry ransomware infection that occurred between 10:30am CST on 5/12 and 2:30 CST on 5/15/17.

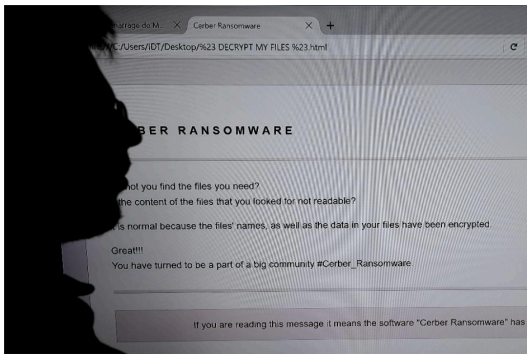


Security / #CyberSecurity

MAY 12, 2017 @ 12:10 PM 63,855

An NSA Cyber Weapon Might Be Be Ransomware Outbreak

Thomas Fox-Brewster, FORBES STAFF
I cover crime, privacy and security in digital and physical forms. FULL BIO



A huge ransomware outbreak has hit NHS hospitals, amongst many other targets. [+]

It's been a matte
crew called Shad
tools believed to
Agency (NSA). It
tool, an exploit o
EternalBlue, is b
rapidly spreadin
WannaCry acros

The ransomware
multiple sources
wards, patients b
National Health
home. Barts Hea
advised patients to look for assistance elsewhere and said ambulanc
elsewhere, while another NHS organization said it had to turn away
radiology services. In the Essex town of Colchester, the hospital dec
department to accept only those in "critical or life-threatening situa

MICROSOFT | TECH

Microsoft has already patched the NSA's leaked Windows hacks

37

by Tom Warren | @tomwarren | Apr 15, 2017, 4:37am EDT

SHARE TWEET LINKEDIN

NOW TRENDING

Microsoft | TechNet

United States (English) Sign in

Security TechCenter

Search TechNet with Bing

Home Security Updates Tools Learn Library Support

Security Advisories and Bulletins > Security Bulletins > 2017

MS17-013
MS17-012
MS17-011
MS17-010
MS17-009
MS17-008
MS17-007
MS17-006
MS17-005
MS17-004
MS17-003

Microsoft Security Bulletin MS17-010 - Critical

Print
Share

Security Update for Microsoft Windows SMB Server (4013389)

Published: March 14, 2017

Version: 1.0

IN THIS ARTICLE
Executive Summary
Affected Software and Vulnerability Severity Ratings
Vulnerability Information
Security Update Deployment
Acknowledgments
Disclaimer
Revisions

Executive Summary

This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.

This security update is rated Critical for all supported releases of Microsoft Windows. For more information, see the **Affected Software and Vulnerability Severity Ratings** section.

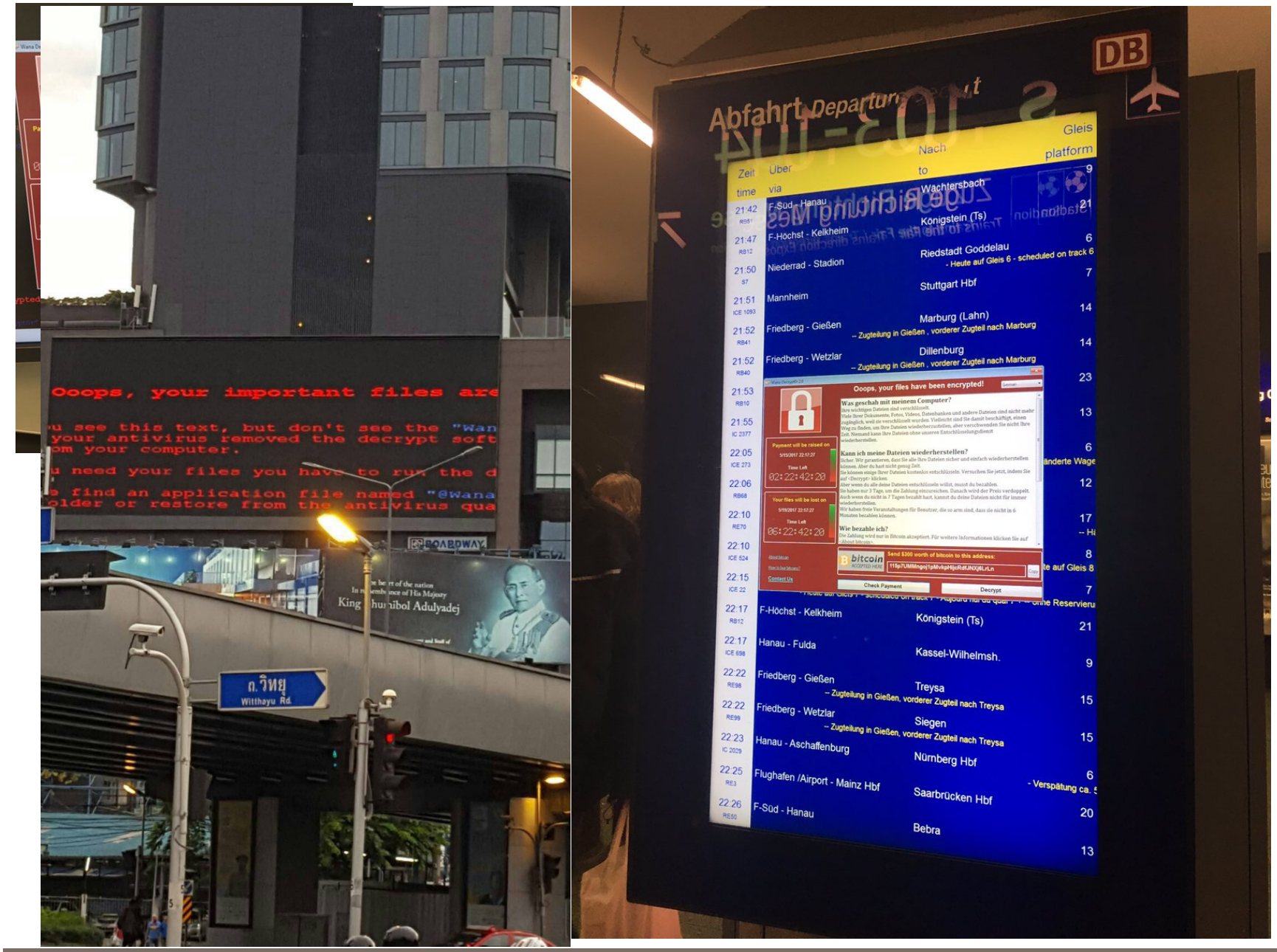
The security update addresses the vulnerabilities by correcting how SMBv1 handles specially crafted requests.

For more information about the vulnerabilities, see the **Vulnerability Information** section.

For more information about this update, see Microsoft Knowledge Base Article 4013389.

On this page
Executive Summary
Affected Software and Vulnerability Severity Ratings
Vulnerability Information
Security Update Deployment
Acknowledgments
Disclaimer
Revisions

MS17-011	Uniscribe Information Disclosure Vulnerability	CVE-2017-0128	Mateusz Jurczyk of Google Project Zero
MS17-009	Microsoft PDF Memory Corruption Vulnerability	CVE-2017-0023	Henry Li (zenhumany) of Trend Micro
MS17-008	Hyper-V vSMB Remote Code Execution Vulnerability	CVE-2017-0021	Saruhan Karademir


Ooops, your important files are
u see this text, but don't see the "Wan
your antivirus removed the decrypt soft
om your computer.
u need your files you have to run the d
find an application file named "@wana
older or restore from the antivirus qua
ถ.วิทยุ
Witthayu Rd.
DB
Abfahrt Departure
Zeit time
Über via
Nach to
Gleis platform
21:42 F-Süd - Hanau Wachtersbach 9
21:47 F-Höchst - Kelkheim Königstein (Ts) 21
21:50 Niederrad - Stadion Riedstadt Goddelau 6
- Heute auf Gleis 6 - scheduled on track 6
21:51 Mannheim Stuttgart Hbf 7
21:52 Friedberg - Gießen Marburg (Lahn) 14
-- Zugteilung in Gießen , vorderer Zugteil nach Marburg
21:52 Friedberg - Wetzlar Dillenburg 14
-- Zugteilung in Gießen , vorderer Zugteil nach Marburg
Ooops, your files have been encrypted!
Was geschah mit meinem Computer?
Kann ich meine Dateien wiederherstellen?
Wie bezahle ich?
Payment will be raised on
Your files will be lost on
Time Left
bitcoin
Send $300 worth of bitcoin to this address:
Check Payment
Decrypt
22:10 RE70 22:10 ICE 524 22:15 ICE 22
22:17 F-Höchst - Kelkheim Königstein (Ts) 21
22:17 Hanau - Fulda Kassel-Wilhelmsh. 9
22:22 Friedberg - Gießen Treysa 15
-- Zugteilung in Gießen, vorderer Zugteil nach Treysa
22:22 Friedberg - Wetzlar Siegen 15
-- Zugteilung in Gießen, vorderer Zugteil nach Treysa
22:23 Hanau - Aschaffenburg Nürnberg Hbf 6
22:25 Flughafen /Airport - Mainz Hbf Saarbrücken Hbf 20
- Verspätung ca.
22:26 F-Süd - Hanau Bebra 13

Christian Borys ✓
@ItsBorys

Follow

Cyber attack in #Ukraine. Following known or allegedly hit so far...

Banks
Power grid
Postal
Gov't Ministry
Media
Airport
Cell providers

6:51 AM - 27 Jun 2017

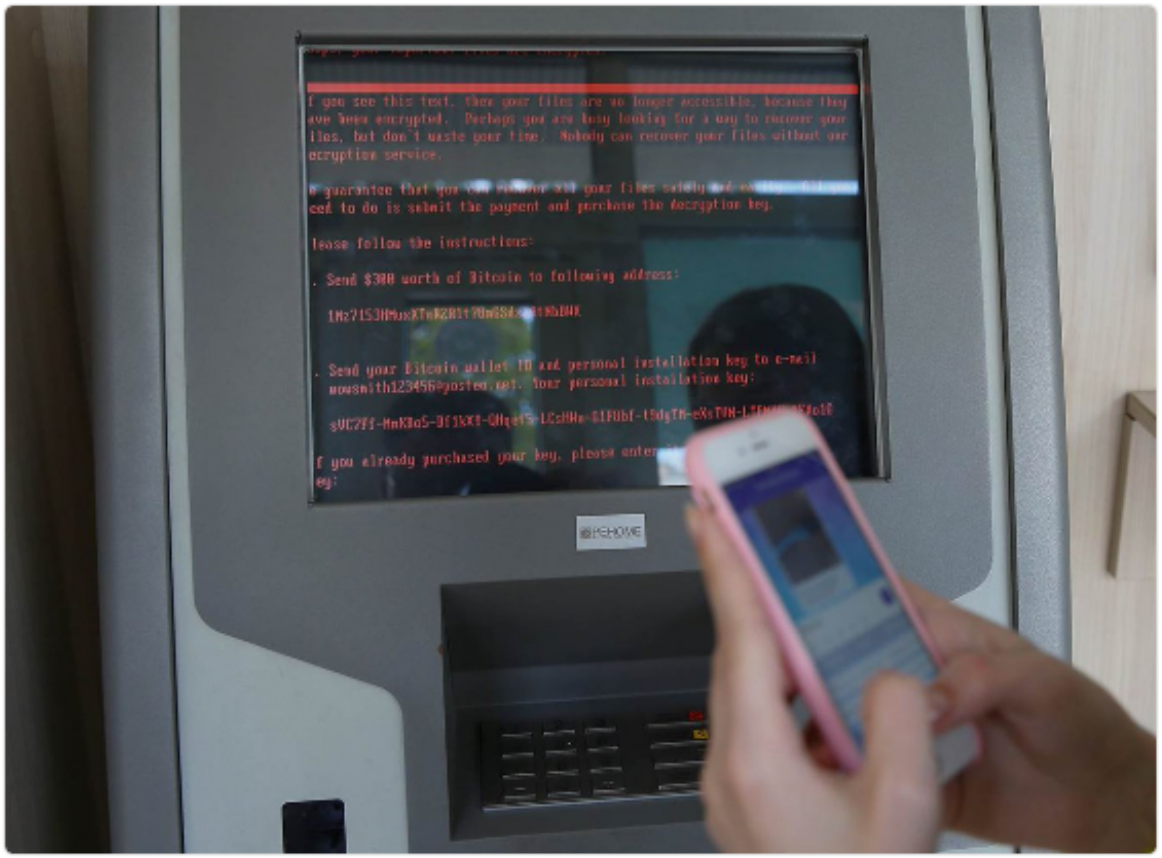
2,015 Retweets **1,341** Likes

102 2.0K 1.3K

Mikko Hypponen
@mikko

Following

Petya on an ATM. Photo by REUTERS.
pictures.reuters.com/archive/CYBER-…

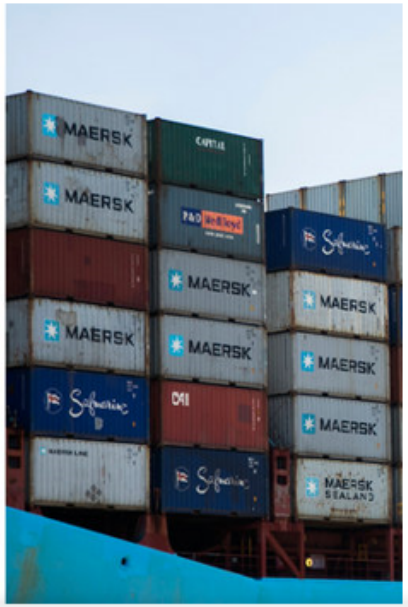


TECHNOLOGY

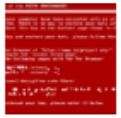
Cyberattack Hits Ukraine Then Spreads Internationally

By NICOLE PERLROTH, MARK SCOTT and SHEERA FRENKEL JUNE 27, 2017

494



RELATED COVERAGE



Global Ransomware Attack: What We Know and Don't Know JUNE 27, 2017

A Cyberattack 'the World Isn't Ready For' JUNE 22, 2017

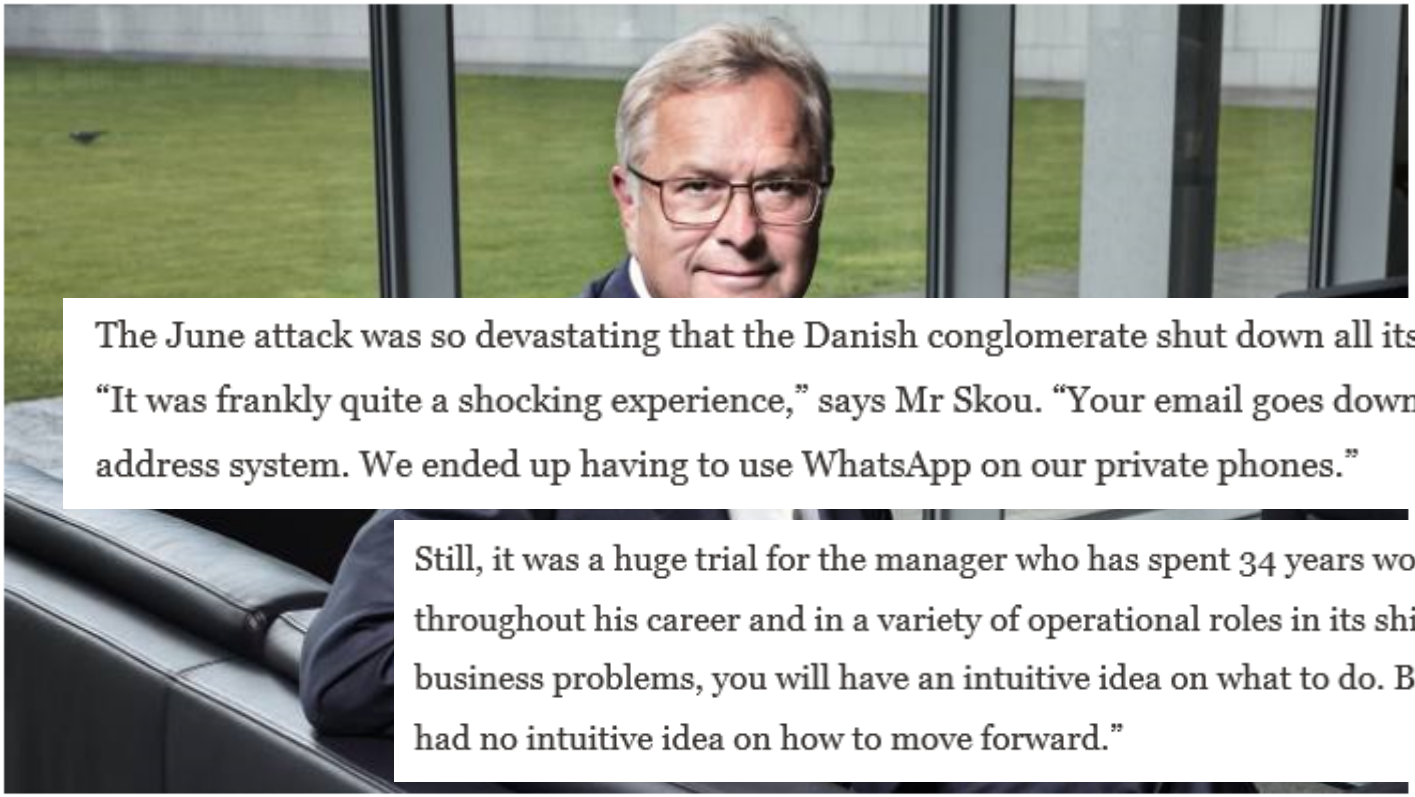
Ponzi Scheme Meets Ransomware for a Doubly Malicious Attack JUNE 6, 2017

Søren Skou

Maersk CEO Soren Skou on how to survive a cyber attack

After a stormy summer, the chief is shaking up the world's biggest shipping company

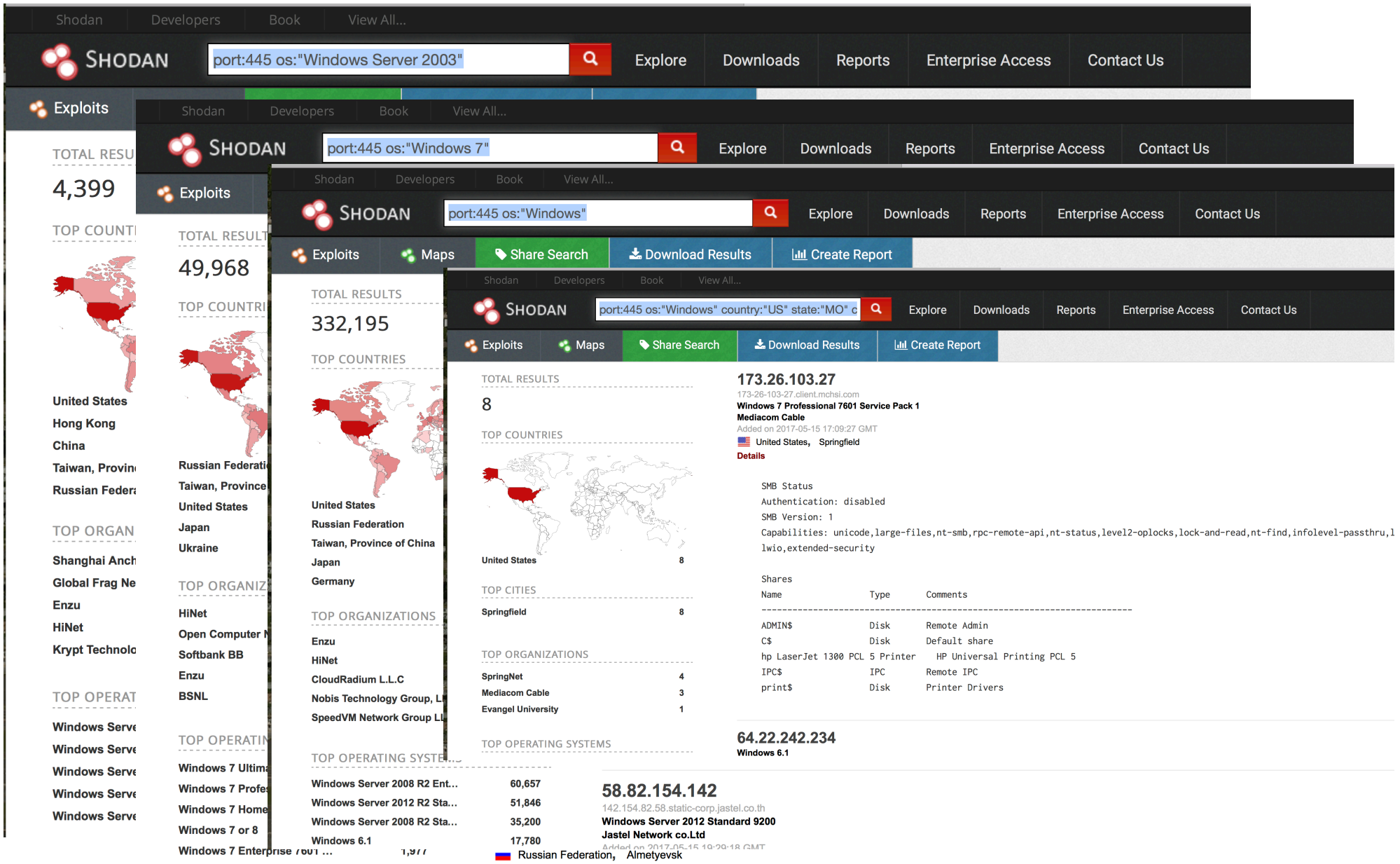
The Monday Interview



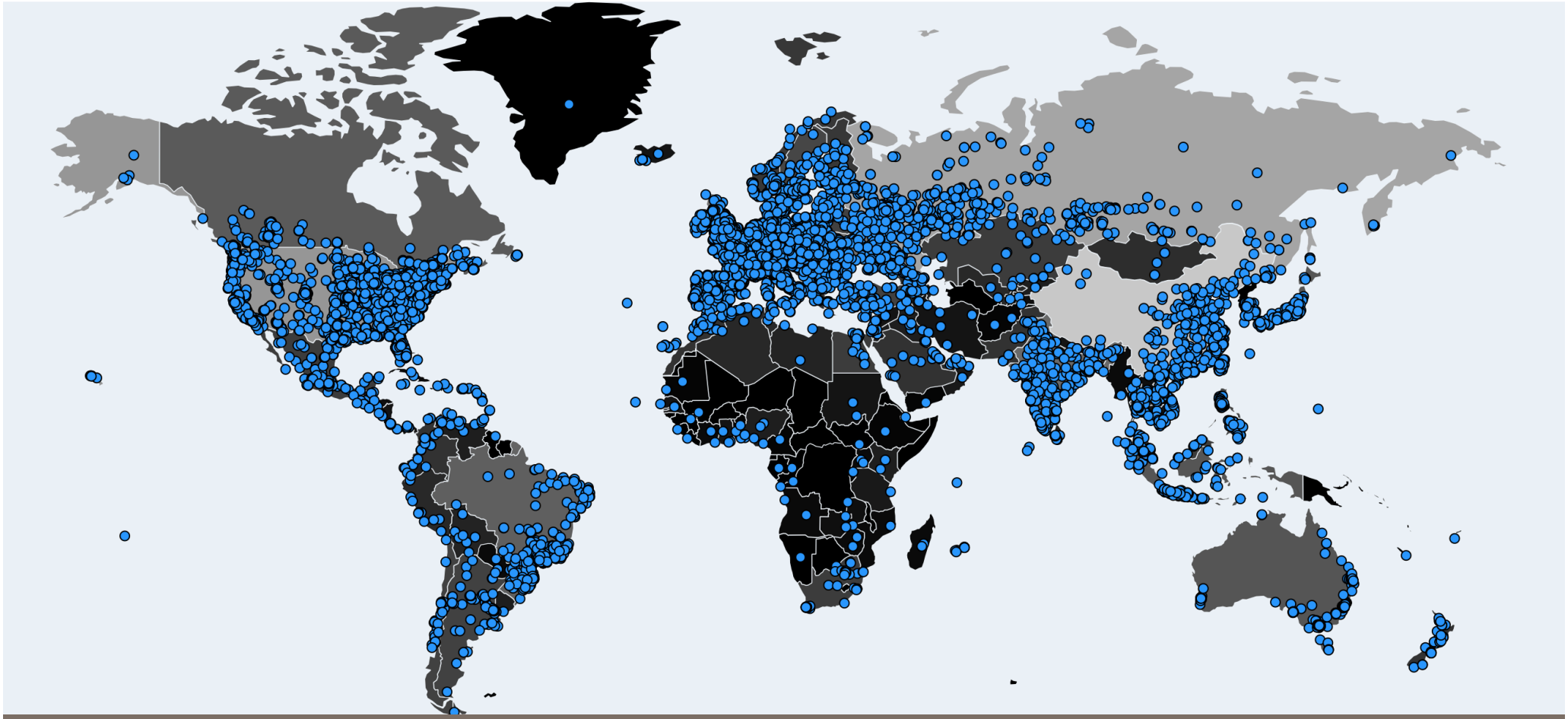
The June attack was so devastating that the Danish conglomerate shut down all its IT systems. "It was frankly quite a shocking experience," says Mr Skou. "Your email goes down, all your address system. We ended up having to use WhatsApp on our private phones."

Still, it was a huge trial for the manager who has spent 34 years working for the group throughout his career and in a variety of operational roles in its shipping businesses. "Most business problems, you will have an intuitive idea on what to do. But with this and my skills, I had no intuitive idea on how to move forward."

Søren Skou had only been in the job for 12 months when Maersk was hit by a cyber attack © Lars Bertelsen


Shodan
Developers
Book
View All...
SHODAN
port:445 os:"Windows Server 2003"
Explore
Downloads
Reports
Enterprise Access
Contact Us
Exploits
TOTAL RESU
4,399
TOP COUNT
United States
Hong Kong
China
Taiwan, Provin
Russian Federa
TOP ORGAN
Shanghai Anch
Global Frag Ne
Enzu
HiNet
Krypt Technolo
TOP OPERAT
Windows Serve
Windows Serve
Windows Serve
Windows Serve
Windows Serve
port:445 os:"Windows 7"
TOTAL RESULT
49,968
TOP COUNTRI
Russian Federati
Taiwan, Province
United States
Japan
Ukraine
TOP ORGANIZ
HiNet
Open Computer N
Softbank BB
Enzu
BSNL
TOP OPERATIN
Windows 7 Ultima
Windows 7 Profes
Windows 7 Home
Windows 7 or 8
Windows 7 Enterprise
port:445 os:"Windows"
Maps
Share Search
Download Results
Create Report
TOTAL RESULTS
332,195
TOP COUNTRIES
United States
Russian Federation
Taiwan, Province of China
Japan
Germany
TOP ORGANIZATIONS
Enzu
HiNet
CloudRadium L.L.C
Nobis Technology Group, L
SpeedVM Network Group L
TOP OPERATING SYSTE
Windows Server 2008 R2 Ent... 60,657
Windows Server 2012 R2 Sta... 51,846
Windows Server 2008 R2 Sta... 35,200
Windows 6.1 17,780
port:445 os:"Windows" country:"US" state:"MO" c
TOTAL RESULTS
8
TOP COUNTRIES
United States 8
TOP CITIES
Springfield 8
TOP ORGANIZATIONS
SpringNet 4
Mediacom Cable 3
Evangel University 1
TOP OPERATING SYSTEMS
173.26.103.27
173-26-103-27.client.mchsi.com
Windows 7 Professional 7601 Service Pack 1
Mediacom Cable
Added on 2017-05-15 17:09:27 GMT
United States, Springfield
Details
SMB Status
Authentication: disabled
SMB Version: 1
Capabilities: unicode,large-files,nt-smb,rpc-remote-api,nt-status,level2-oplocks,lock-and-read,nt-find,infolevel-passthru,l
lwio,extended-security
Shares
Name Type Comments
ADMIN$ Disk Remote Admin
C$ Disk Default share
hp LaserJet 1300 PCL 5 Printer HP Universal Printing PCL 5
IPC$ IPC Remote IPC
print$ Disk Printer Drivers
64.22.242.234
Windows 6.1
58.82.154.142
142.154.82.58.static-corp.jastel.co.th
Windows Server 2012 Standard 9200
Jastel Network co.Ltd
Russian Federation, Almetyevsk

Every blue dot represents a wannacry ransomware infection that occurred between 10:30am CST on 5/12 and 2:30 CST on 5/15/17.



The New York Times
@nytimes

Following

Hackers responsible for Ukraine's cyberattack didn't want to profit. They may have had a more sinister motive.

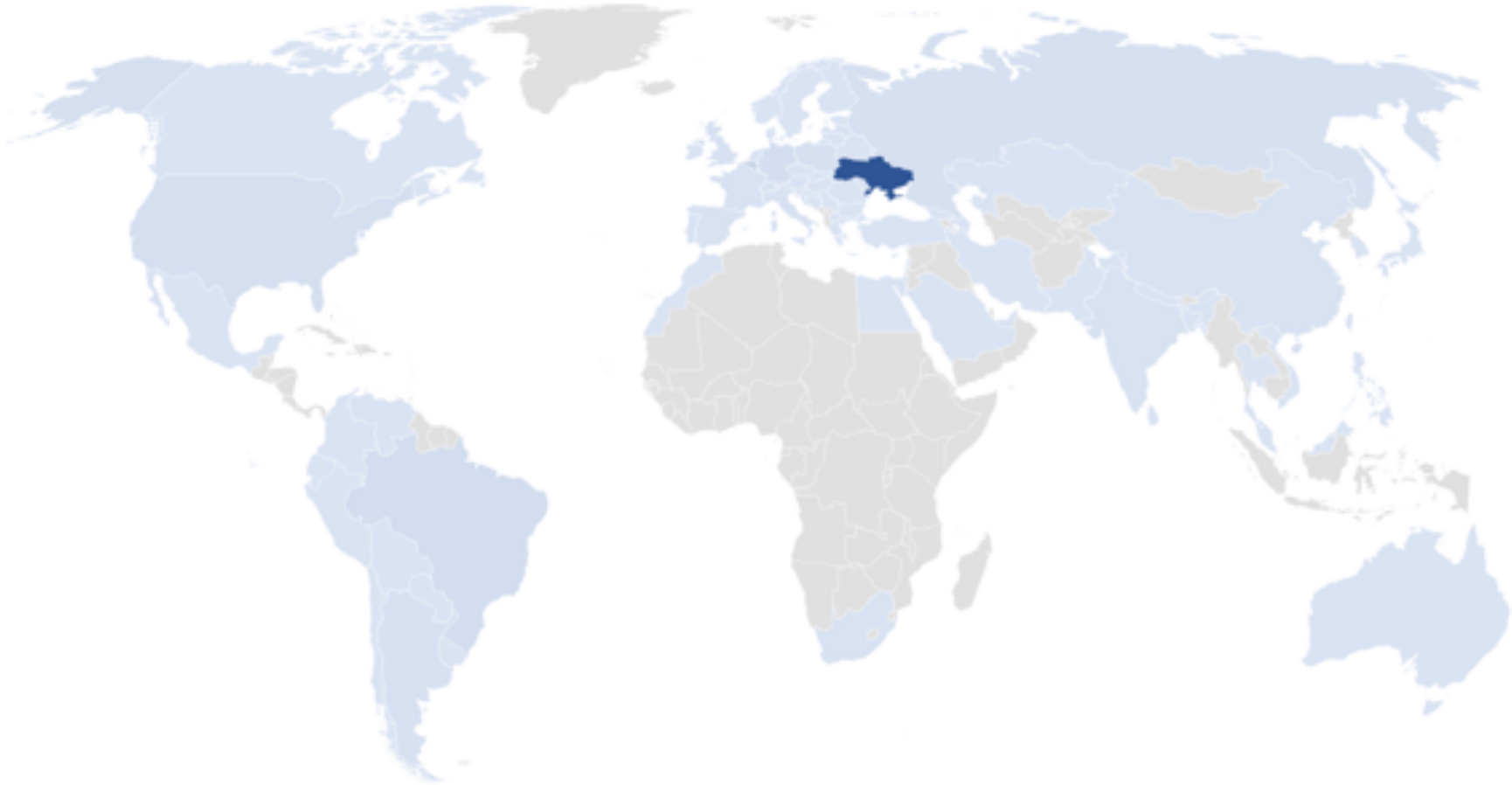
Ukraine Cyberattack Was Meant to Paralyze, not Profit, Evidence Shows

Pinpointing the initial targets of the assault — Ukrainian accountants who use a tax preparation software required by the government — was a major clue.

nytimes.com

6:40 PM - 28 Jun 2017

Geographic Distribution of Petya/NonPetya Outbreak



Forbes / Security

JAN 4, 2016 @ 12:15 PM 6,468 VIEWS

Ukraine Claims Hackers Caused Christmas Power Outage

Thomas Fox-Brewster

FORBES STAFF

I cover crime, privacy and security in digital and physical forms.

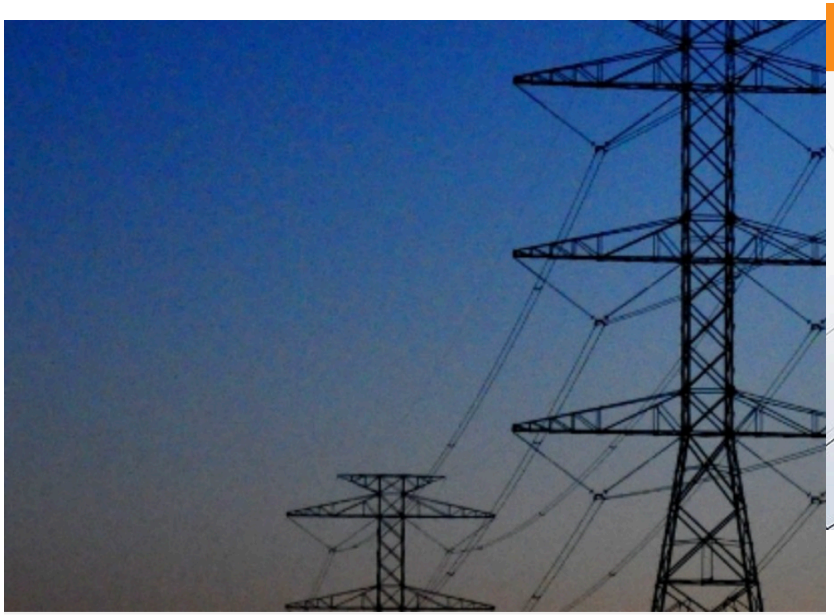
FOLLOW ON FORBES

FULL BIO >

Just before Christmas, power went out across western Ukraine. Soon after, the energy ministry confirmed it was exploring claims a cyber attack disrupted local energy provider Prykarpattyaoblenergo, causing blackouts across the Ivano-Frankivsk region on 23 December. The SBU state intelligence service said Russian attempts to disrupt the country's power grid had been deflected, but did not comment on any specific attack.

The details were patchy. But today, the Computer Emergency Response Team of Ukraine – CERT-UA – told FORBES the outages were caused by an attack. National CERTs are in charge of coordinating responses to and investigations into cyber attacks. Eugene Bryksin, a member of the government organization, said it was working with Prykarpattyaoblenergo on the investigation but could provide no information other than to confirm the accuracy of the reports.

If his information was accurate, the attack is a rare public example of hackers taking out critical infrastructure and another sign of the rising digitization of warfare. Neither Prykarpattyaoblenergo nor the SBU could be contacted at the time of publication.



The Ukrainian Power Gr
Hacked Again

January 10, 2017 // 10:07 AM EST

Someone, or various individua
usir
attac
"It was more like
capa

U.S. Grid in 'Imminent Danger' From Cyber-Attack, Study Says

by **Ari Natter** and **Mark Chediak**
January 6, 2017, 9:40 AM CST *Updated on* January 6, 2017, 2:37 PM CST

- Threats to U.S. electrical grid are more sophisticated
- Increase in smart grid technology increasing vulnerability

The U.S. Energy Department says the electricity system "faces imminent danger" from cyber-attacks, which are growing more frequent and sophisticated, but grid operators say they are already on top of the problem.

In the department's landmark Quadrennial Energy Review, it warned that a widespread power outage caused by a cyber-attack could undermine "critical defense infrastructure" as well as much of the economy and place at risk the health and safety of millions of citizens. The report comes amid increased concern over cybersecurity risks as U.S. intelligence agencies say Russian hacking was aimed at influencing the 2016 presidential election.

PRIVACY AND SECURITY FANATIC

By Ms. Smith, CSO |
AUG 22, 2017 8:14 AM PT

About

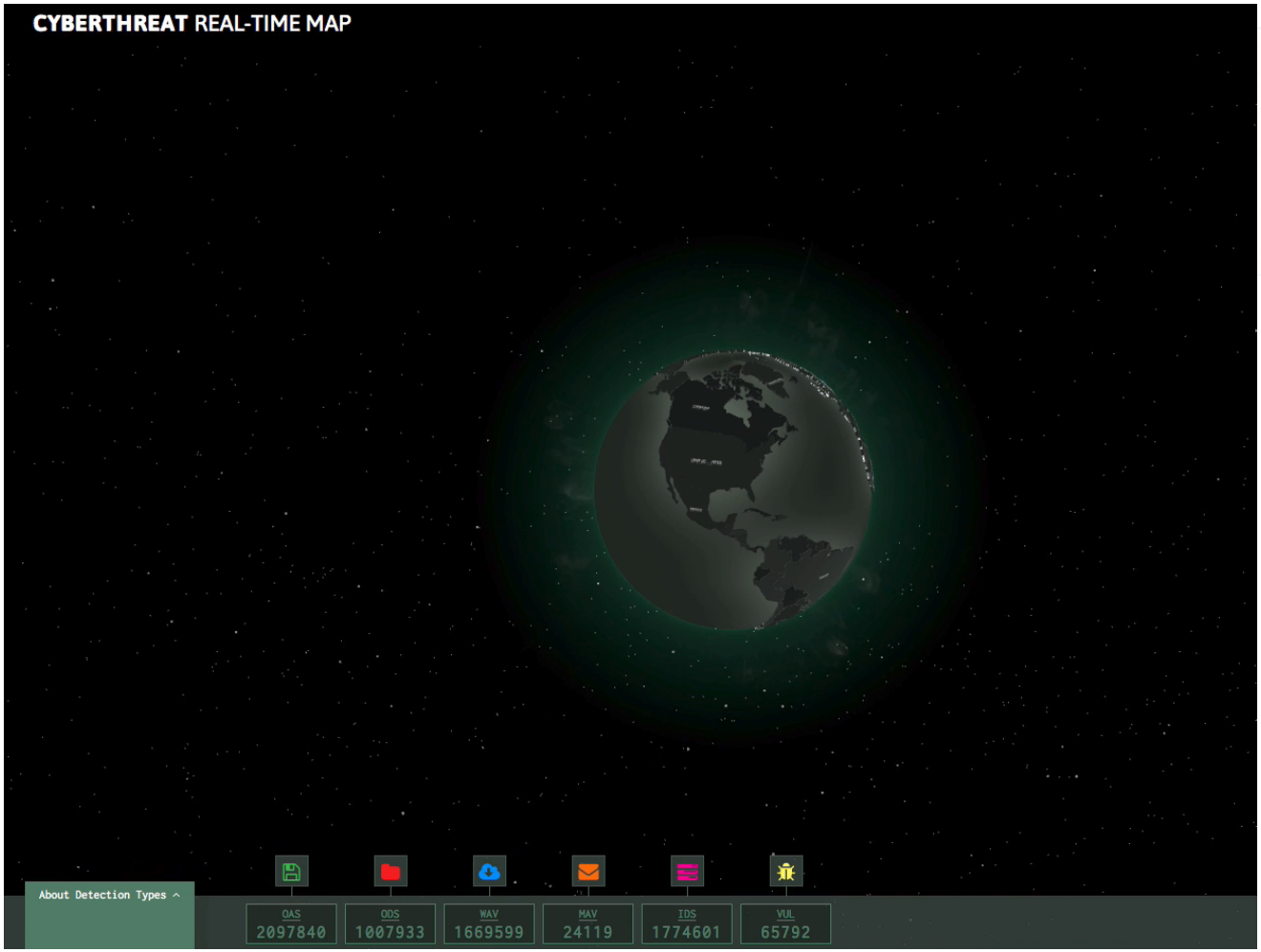
Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

NEWS

U.S. Navy considers possibility of cyber attack after another ship collision

U.S. Navy officials have gone on record to say hacking will be looked at as a possibility as the cause of the USS John S. McCain collision.

The game is changing…



Nation-state actors **Stuxnet**, **Aurora, APT-1**

LAW & DISORDER / CIVILIZATION & DISCONTENTS

Massive US-planned cyberattack against Iran went well beyond Stuxnet

"Nitro Zeus" reportedly targeted Iran's air defenses, communications, and power grid.

by **Dan Goodin** - Feb 16, 2016 7:26pm CST

Hackers made Iran's nuclear computers blast AC/DC

Baffled scientist says 'Thunderstruck' played in the middle

By Rich McCormick on August 7, 2014 04:20 am Email

(AC/DC)

THE LATEST

COMMENTS

Iran nuclear facilities hit by cyber attack that plays AC/DC's Thunderstruck at full volume

PUBLISHED: 08:43 EST, 25 July 2012 | **UPDATED:** 02:07 EST, 26 July 2012

Share

56 View comments

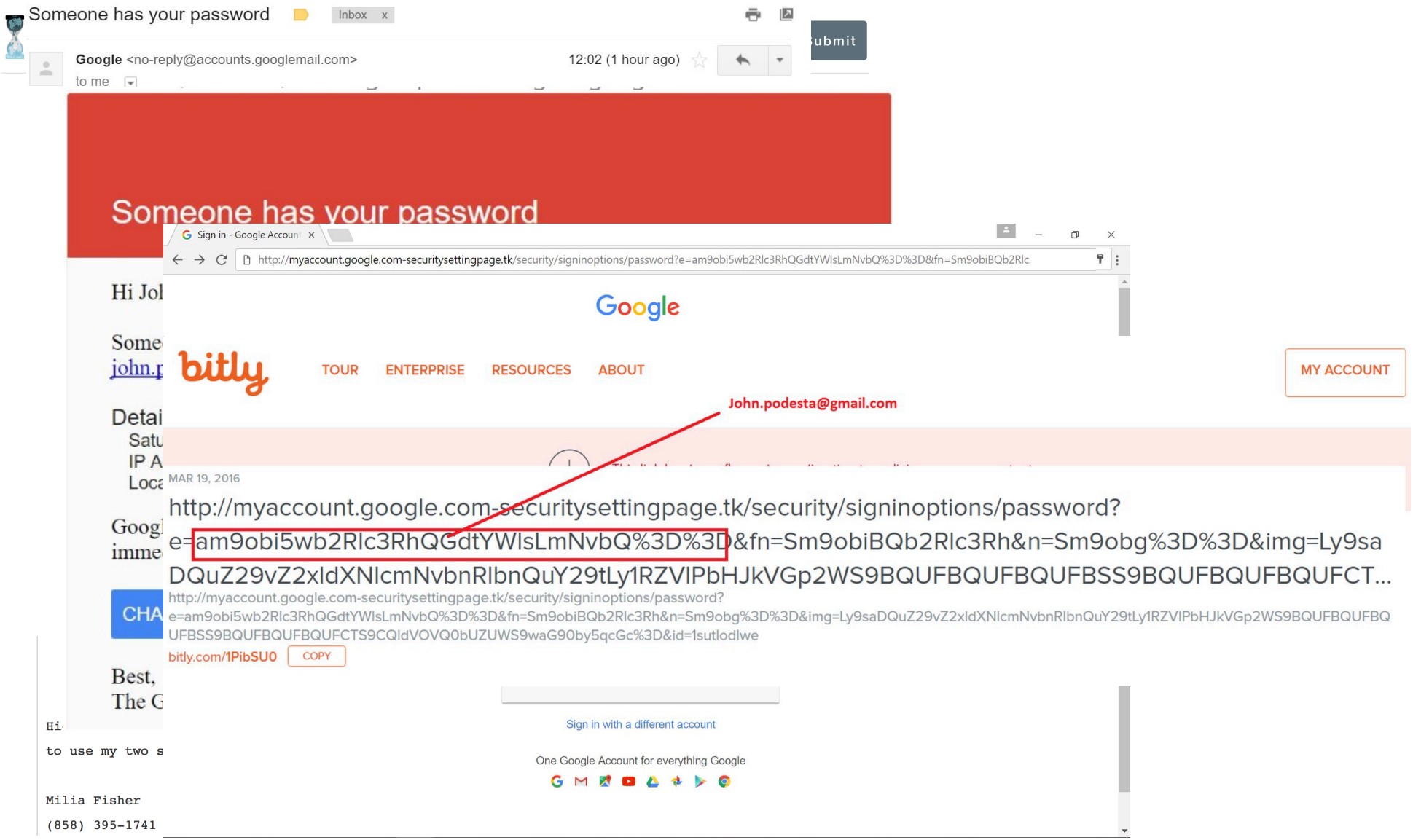
As far as malicious computer hacking is concerned, the most recent breach of security at Iran's nuclear facilities may not be very serious... unless you hate the music of Australian rock band AC/DC.

It has been alleged that unidentified computer hackers have forced workers at two of the country's controversial nuclear facilities to endure AC/DC's hit song Thunderstruck repeatedly - and at full volume - sometimes in the middle of the night.

Of course, there has been no confirmation of the attack from Iran - the evidence stems from a series of e-mails purporting to be from the Atomic Energy Organisation of Iran.

Affected: The nuclear enrichment plant at Natanz in central Iran has been hit with a worm that affects automated systems... and plays AC/DC's Thunderstruck

Here's how evil Russian hackers hacked John Podesta (and more importantly how they would probably hack you.



Many of the accounts in the 2015 campaign belonged to individuals in

Russ

forme

indivi

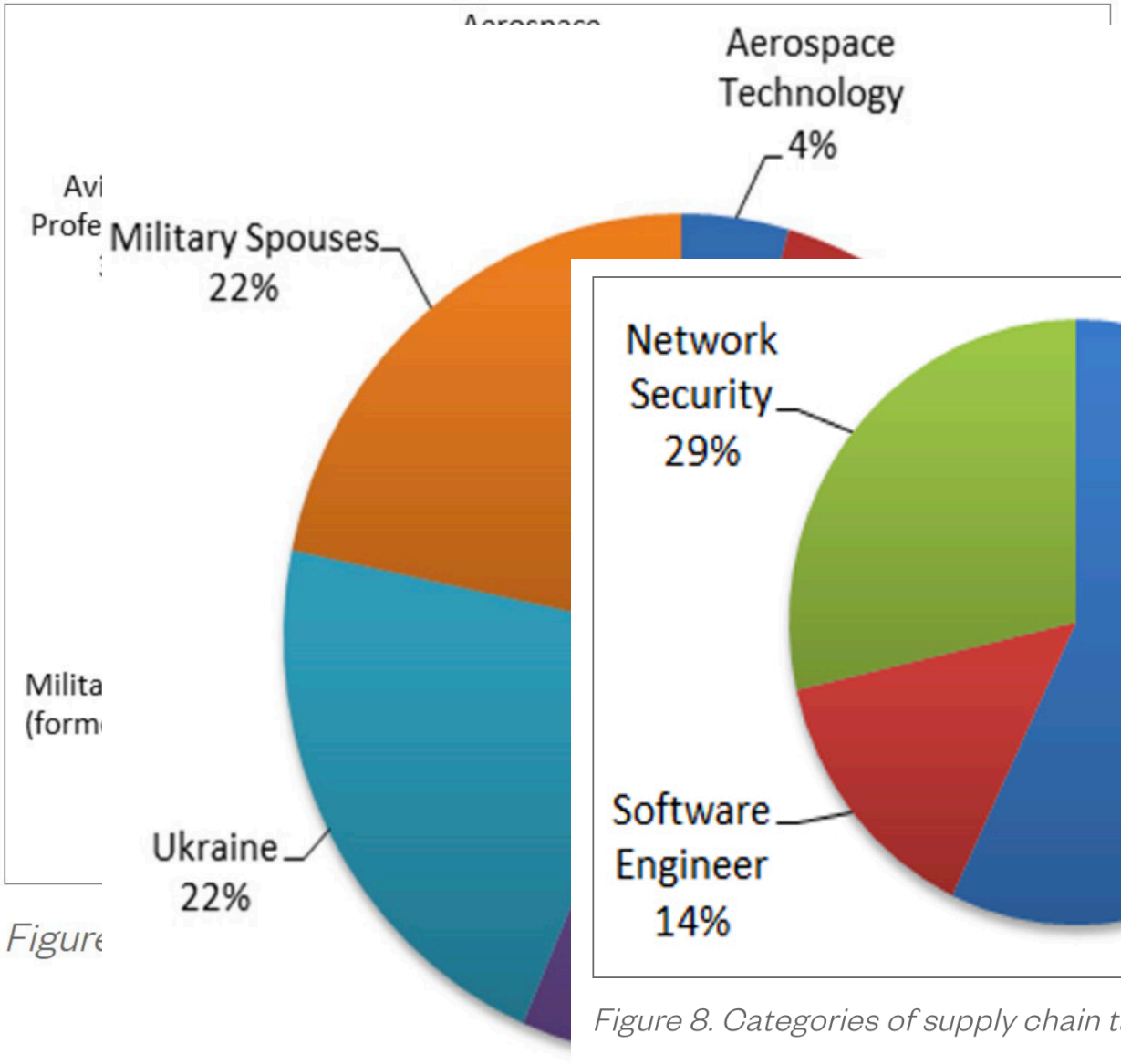
autho

range

to inc

and i

whos



Figure

Figure 8. Categories of supply chain targets. (Source: SecureWorks)

Office of Personnel Management

CNN politics

Search CNN

2016 Washington Nation World Our Team

First on CNN: U.S. data hack may be 4 times larger than the government originally said

By Evan Perez and Shimon Prokupecz, CNN

Updated 10:59 PM ET, Tue June 23, 2015

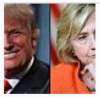
Source: CNN

U.S.: Hack of 18 million Americans came from China 01:13

More Top Stories


ESPN pulls analyst after tweet


O'Donnell's daughter leaves


Poll has big news for Biden


Killer's mom apologizes to victims


White House jumper killed in courthouse


Trump's new Twitter tirade against Kelly

Report: 'Failure of OPM's leadership' led to historic data breaches

"The government of the United States of Americ
never before been more vulnerable to cyberattac
241-page report reads.

By *Chris Bing*
SEPTEMBER 7, 2016 12:30 PM

BIO

*Office of Personnel Management in Washington, D.C. in 2012 / Photo Cred
Believer via CC 3.0*

A 2014 data breach at the Office of Personnel Management was the result of failed leadership and consistent cybersecurity ignorance, according to an investigative report released Wednesday by members of the House

Shannon McMurtrey, PhD
Drury University

smcmurtrey@drury.edu
@shannonm on Twitter
417-861-8884