Threat Intelligence 2014
CERT-EU

Stavros Lingris

CERT-EU
Computer Emergency Response Team
for EU Institutions, Bodies, and Agencies

stavros.lingris@ec.europa.eu

About us

- EU Institutions’ own CERT
- Operational support for the internal IT teams
- Supports 60+ entities
- Defense against targeted cyber threats
- Single point of contact

Other EU “cyber bodies”

ENISA

- Europe-wide mandate in cyber security
- Supporting best practices, capacity building and awareness raising

EUROPOL EC3

- Europe-wide mandate in fight against cyber-crime
- Operational cooperation between police computer crime units

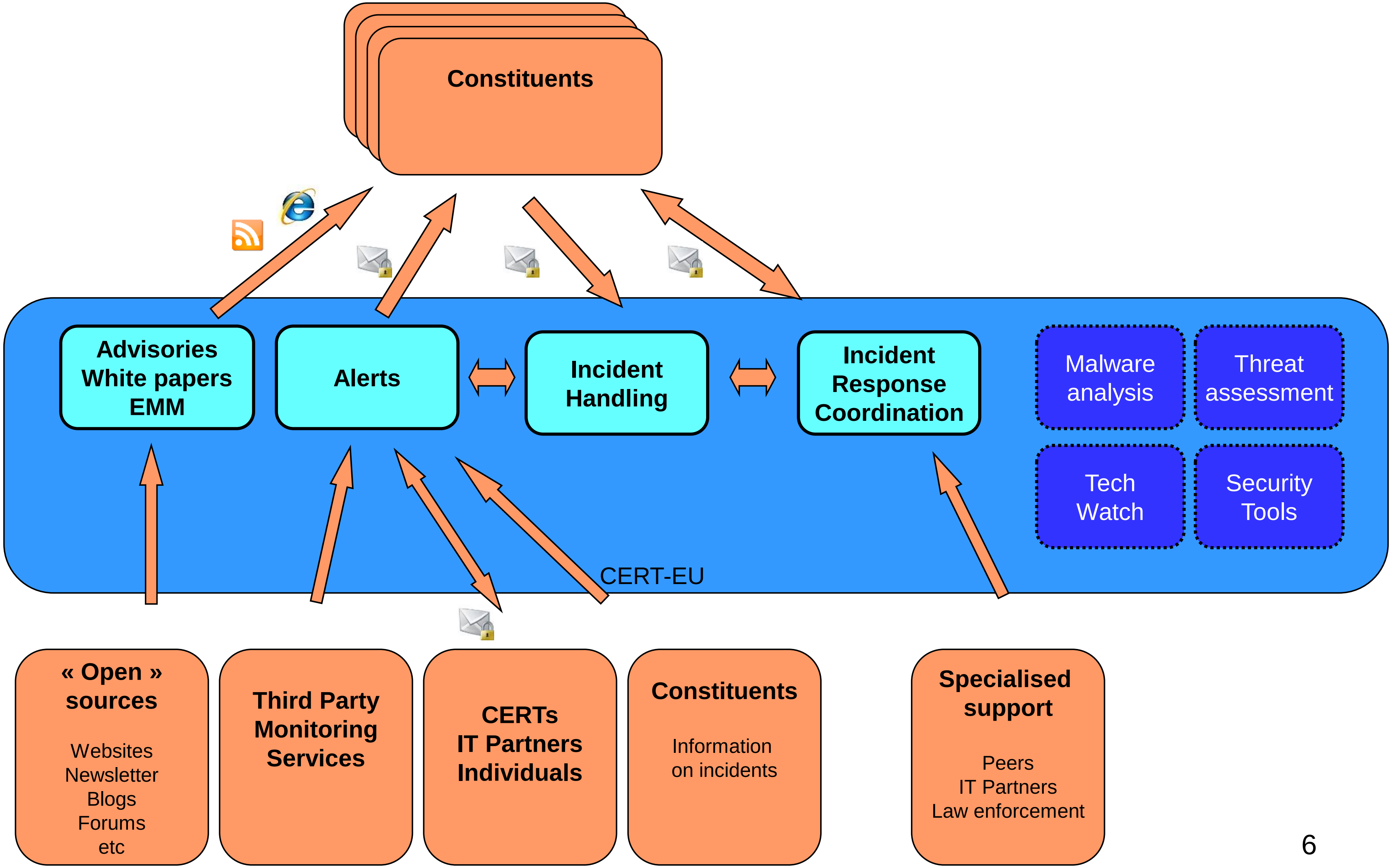
Institutional framework

- **Inter-institutional nature**
  - ✓ Mandate approved by EU Institions SGs
  - ✓ Staff secondment by main institutions
- **Commission decision 11/9/2012**
  - ✓ Permanent nature
  - ✓ Provision of infrastructure and services
  - ✓ Minimum staff contribution
- **Additional funding from SLAs**
  - ✓ Up-front flat rate funding for “Extended Services”
  - ✓ Additional capacity from income

Constituents

- Located in many different countries
- From 40 – 40.000 users
- Cross-sectoral
  - ✓ Government, foreign policy, embassies
  - ✓ Banking, energy, pharmaceutical, chemical, food, telecom
  - ✓ Maritime, rail and aviation safety
  - ✓ Law enforcement (EUROPOL, FRONTEX, EUPOL) and justice
  - ✓ Research, hi-tech, navigation (GALILEO), defence (EUMS, EDA)
- Heterogenous infrastructure
- Seperate legal entities
- High-value targets

Services


Constituents
Advisories
White papers
EMM
Alerts
Incident
Handling
Incident
Response
Coordination
Malware
analysis
Threat
assessment
Tech
Watch
Security
Tools
CERT-EU
« Open »
sources
Websites
Newsletter
Blogs
Forums
etc
Third Party
Monitoring
Services
CERTs
IT Partners
Individuals
Constituents
Information
on incidents
Specialised
support
Peers
IT Partners
Law enforcement

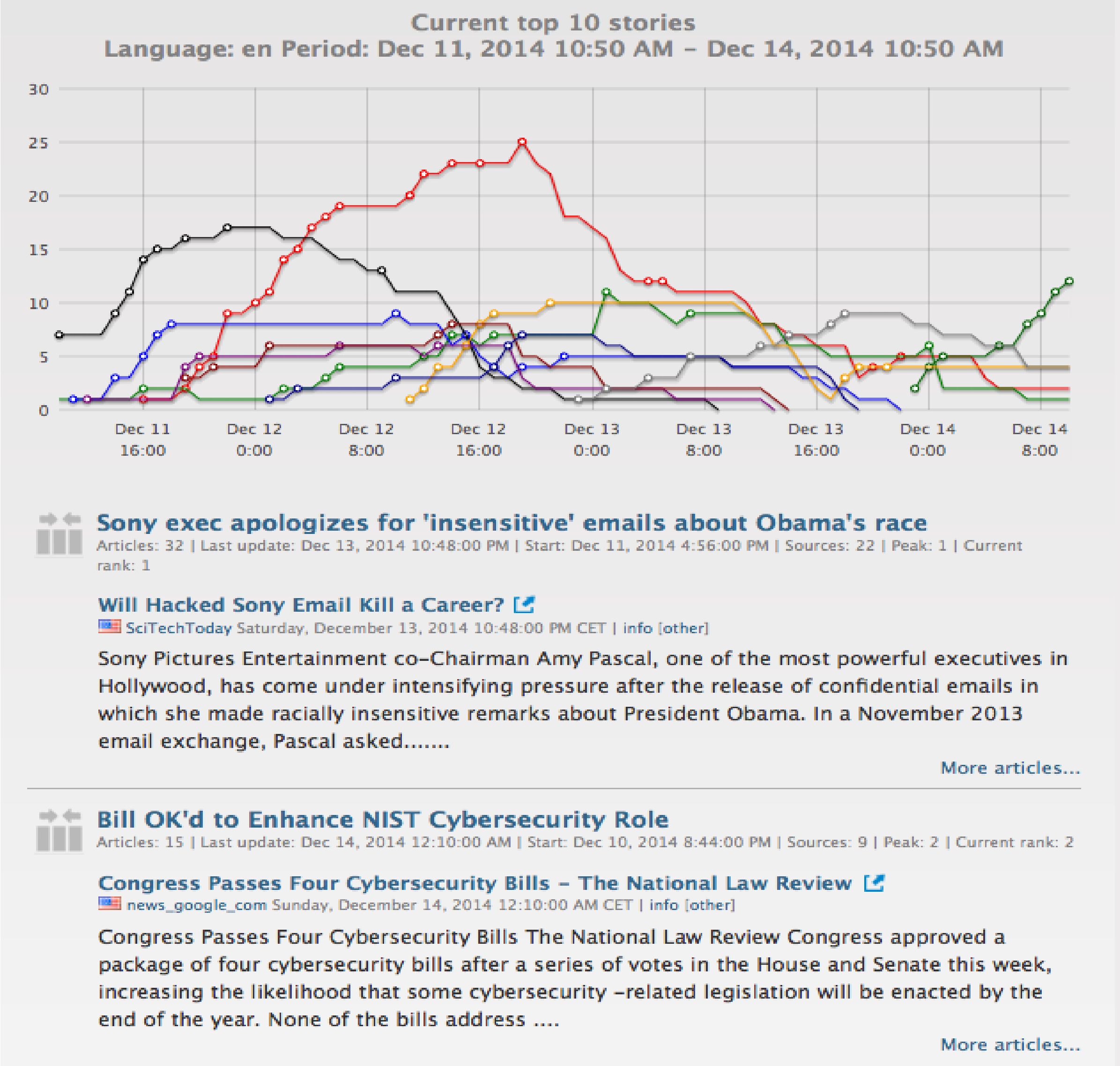
Announcements (News)

- **CERT-EU WebPortal**

  http://cert.europa.eu

  - ✓ 2500+ Sources
  - ✓ Automatic news scraping on threats and vulnerabilities
  - ✓ Clustering / RSS enabled
  - ✓ CERT-EU white papers
  - ✓ Private webportal emmp (1000 additional sources)
  - ✓ Cyber News interactive map
  - ✓ MobileApp on the Appstore (soon)

Announcements (News)



Current top 10 stories
Language: en Period: Dec 11, 2014 10:50 AM – Dec 14, 2014 10:50 AM

Sony exec apologizes for 'insensitive' emails about Obama's race
Articles: 32 | Last update: Dec 13, 2014 10:48:00 PM | Start: Dec 11, 2014 4:56:00 PM | Sources: 22 | Peak: 1 | Current rank: 1

Will Hacked Sony Email Kill a Career?
SciTechToday Saturday, December 13, 2014 10:48:00 PM CET | info [other]

Sony Pictures Entertainment co-Chairman Amy Pascal, one of the most powerful executives in Hollywood, has come under intensifying pressure after the release of confidential emails in which she made racially insensitive remarks about President Obama. In a November 2013 email exchange, Pascal asked.......

More articles...

Bill OK'd to Enhance NIST Cybersecurity Role
Articles: 15 | Last update: Dec 14, 2014 12:10:00 AM | Start: Dec 10, 2014 8:44:00 PM | Sources: 9 | Peak: 2 | Current rank: 2

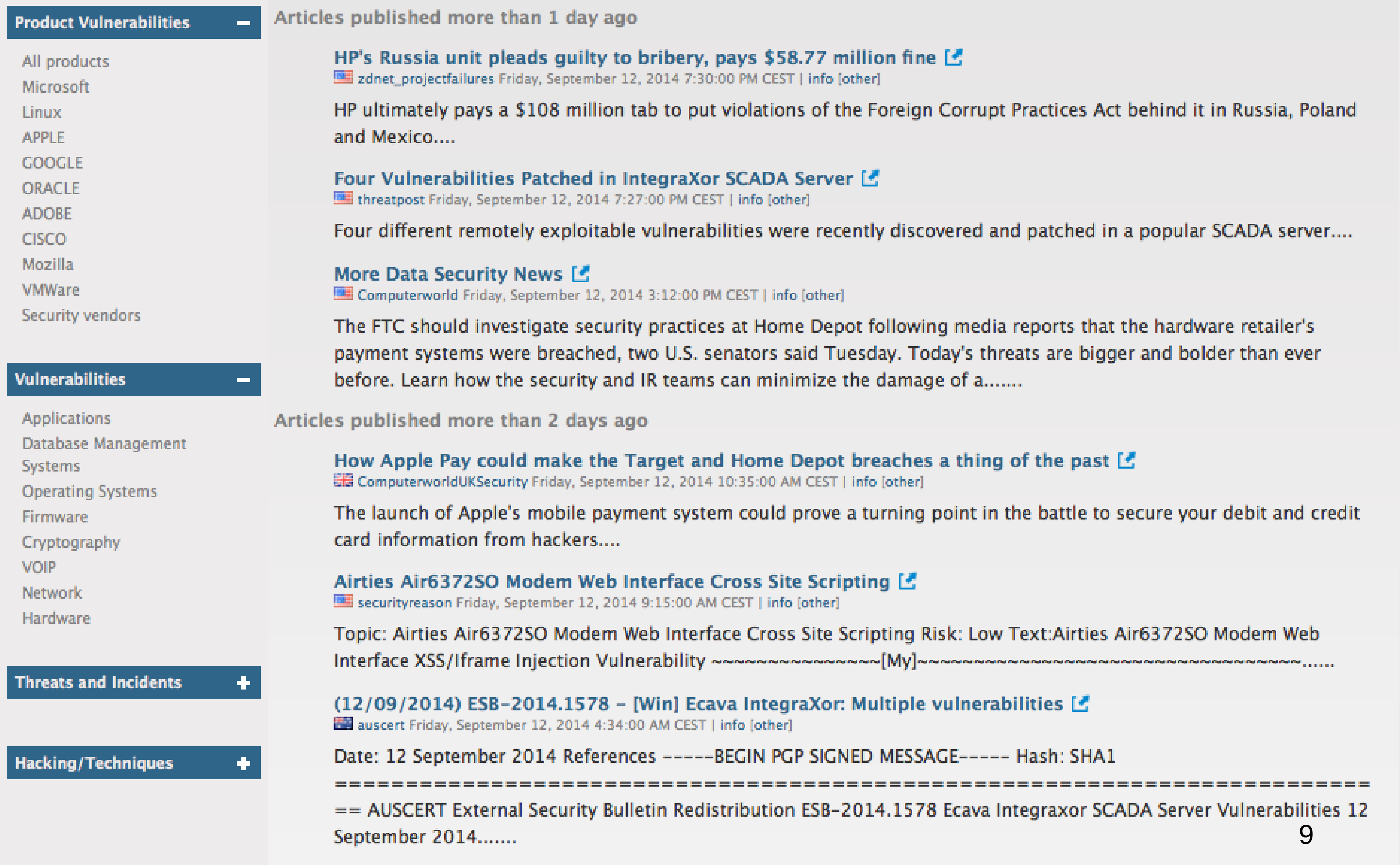
Congress Passes Four Cybersecurity Bills – The National Law Review
news_google_com Sunday, December 14, 2014 12:10:00 AM CET | info [other]

Congress Passes Four Cybersecurity Bills The National Law Review Congress approved a package of four cybersecurity bills after a series of votes in the House and Senate this week, increasing the likelihood that some cybersecurity –related legislation will be enacted by the end of the year. None of the bills address ....

More articles...

computer
emergency
response
team
CERT-EU
for the EU institutions, bodies
and agencies

Web Portal



Product Vulnerabilities –

- All products
- Microsoft
- Linux
- APPLE
- GOOGLE
- ORACLE
- ADOBE
- CISCO
- Mozilla
- VMWare
- Security vendors

Vulnerabilities –

- Applications
- Database Management Systems
- Operating Systems
- Firmware
- Cryptography
- VOIP
- Network
- Hardware

Threats and Incidents +

Hacking/Techniques +

Articles published more than 1 day ago

HP's Russia unit pleads guilty to bribery, pays $58.77 million fine
zdnet_projectfailures Friday, September 12, 2014 7:30:00 PM CEST | info [other]

HP ultimately pays a $108 million tab to put violations of the Foreign Corrupt Practices Act behind it in Russia, Poland and Mexico....

Four Vulnerabilities Patched in IntegraXor SCADA Server
threatpost Friday, September 12, 2014 7:27:00 PM CEST | info [other]

Four different remotely exploitable vulnerabilities were recently discovered and patched in a popular SCADA server....

More Data Security News
Computerworld Friday, September 12, 2014 3:12:00 PM CEST | info [other]

The FTC should investigate security practices at Home Depot following media reports that the hardware retailer's payment systems were breached, two U.S. senators said Tuesday. Today's threats are bigger and bolder than ever before. Learn how the security and IR teams can minimize the damage of a.......

Articles published more than 2 days ago

How Apple Pay could make the Target and Home Depot breaches a thing of the past
ComputerworldUKSecurity Friday, September 12, 2014 10:35:00 AM CEST | info [other]

The launch of Apple's mobile payment system could prove a turning point in the battle to secure your debit and credit card information from hackers....

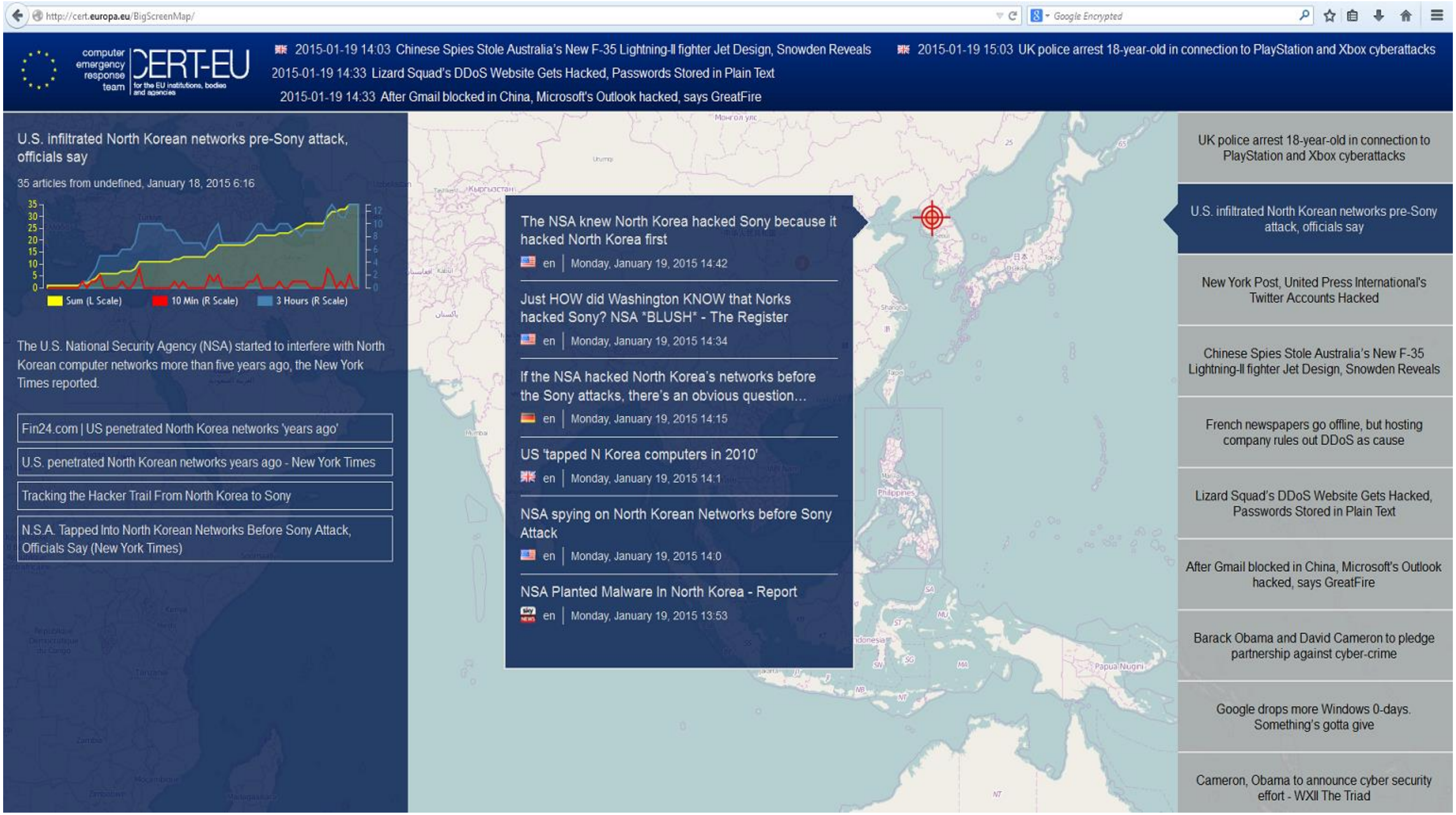
Airties Air6372SO Modem Web Interface Cross Site Scripting
securityreason Friday, September 12, 2014 9:15:00 AM CEST | info [other]

Topic: Airties Air6372SO Modem Web Interface Cross Site Scripting Risk: Low Text:Airties Air6372SO Modem Web Interface XSS/Iframe Injection Vulnerability ~~~~~~~~~~~~~~~~[My]~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~......

(12/09/2014) ESB-2014.1578 - [Win] Ecava IntegraXor: Multiple vulnerabilities
auscert Friday, September 12, 2014 4:34:00 AM CEST | info [other]

Date: 12 September 2014 References -----BEGIN PGP SIGNED MESSAGE----- Hash: SHA1 == AUSCERT External Security Bulletin Redistribution ESB-2014.1578 Ecava Integraxor SCADA Server Vulnerabilities 12 September 2014.......

Cyber News Map



http://cert.europa.eu/BigScreenMap/

computer emergency response team CERT-EU for the EU institutions, bodies and agencies

2015-01-19 14:03 Chinese Spies Stole Australia's New F-35 Lightning-II fighter Jet Design, Snowden Reveals

2015-01-19 15:03 UK police arrest 18-year-old in connection to PlayStation and Xbox cyberattacks

2015-01-19 14:33 Lizard Squad's DDoS Website Gets Hacked, Passwords Stored in Plain Text

2015-01-19 14:33 After Gmail blocked in China, Microsoft's Outlook hacked, says GreatFire

U.S. infiltrated North Korean networks pre-Sony attack, officials say

35 articles from undefined, January 18, 2015 6:16

The U.S. National Security Agency (NSA) started to interfere with North Korean computer networks more than five years ago, the New York Times reported.

- Fin24.com | US penetrated North Korea networks 'years ago'
- U.S. penetrated North Korean networks years ago - New York Times
- Tracking the Hacker Trail From North Korea to Sony
- N.S.A. Tapped Into North Korean Networks Before Sony Attack, Officials Say (New York Times)

The NSA knew North Korea hacked Sony because it hacked North Korea first
en | Monday, January 19, 2015 14:42

Just HOW did Washington KNOW that Norks hacked Sony? NSA *BLUSH* - The Register
en | Monday, January 19, 2015 14:34

If the NSA hacked North Korea's networks before the Sony attacks, there's an obvious question...
en | Monday, January 19, 2015 14:15

US 'tapped N Korea computers in 2010'
en | Monday, January 19, 2015 14:1

NSA spying on North Korean Networks before Sony Attack
en | Monday, January 19, 2015 14:0

NSA Planted Malware In North Korea - Report
en | Monday, January 19, 2015 13:53

- UK police arrest 18-year-old in connection to PlayStation and Xbox cyberattacks
- U.S. infiltrated North Korean networks pre-Sony attack, officials say
- New York Post, United Press International's Twitter Accounts Hacked
- Chinese Spies Stole Australia's New F-35 Lightning-II fighter Jet Design, Snowden Reveals
- French newspapers go offline, but hosting company rules out DDoS as cause
- Lizard Squad's DDoS Website Gets Hacked, Passwords Stored in Plain Text
- After Gmail blocked in China, Microsoft's Outlook hacked, says GreatFire
- Barack Obama and David Cameron to pledge partnership against cyber-crime
- Google drops more Windows 0-days. Something's gotta give
- Cameron, Obama to announce cyber security effort - WXII The Triad

http://cert.europa.eu/BigScreenMap/

Constituency - Prevention

- **Annual conference**
- **White papers** **(http://cert.europa.eu/cert/newsletter/en/latest_Publications%20and%20Newsletters_.html)**
  - ✓ Data protection guidance
  - ✓ DDOS mitigation
  - ✓ CISCO IOS risk mitigation
  - ✓ Golden Ticket
  - ✓ Handling of Potentially Malicious Emails
  - ✓ E-mail Sender Address Forgery
- **Green paper**
  - ✓ Detecting lateral movements in Windows
- **Awareness raising sessions**
  - ✓ Constituents
  - ✓ Peers and partners

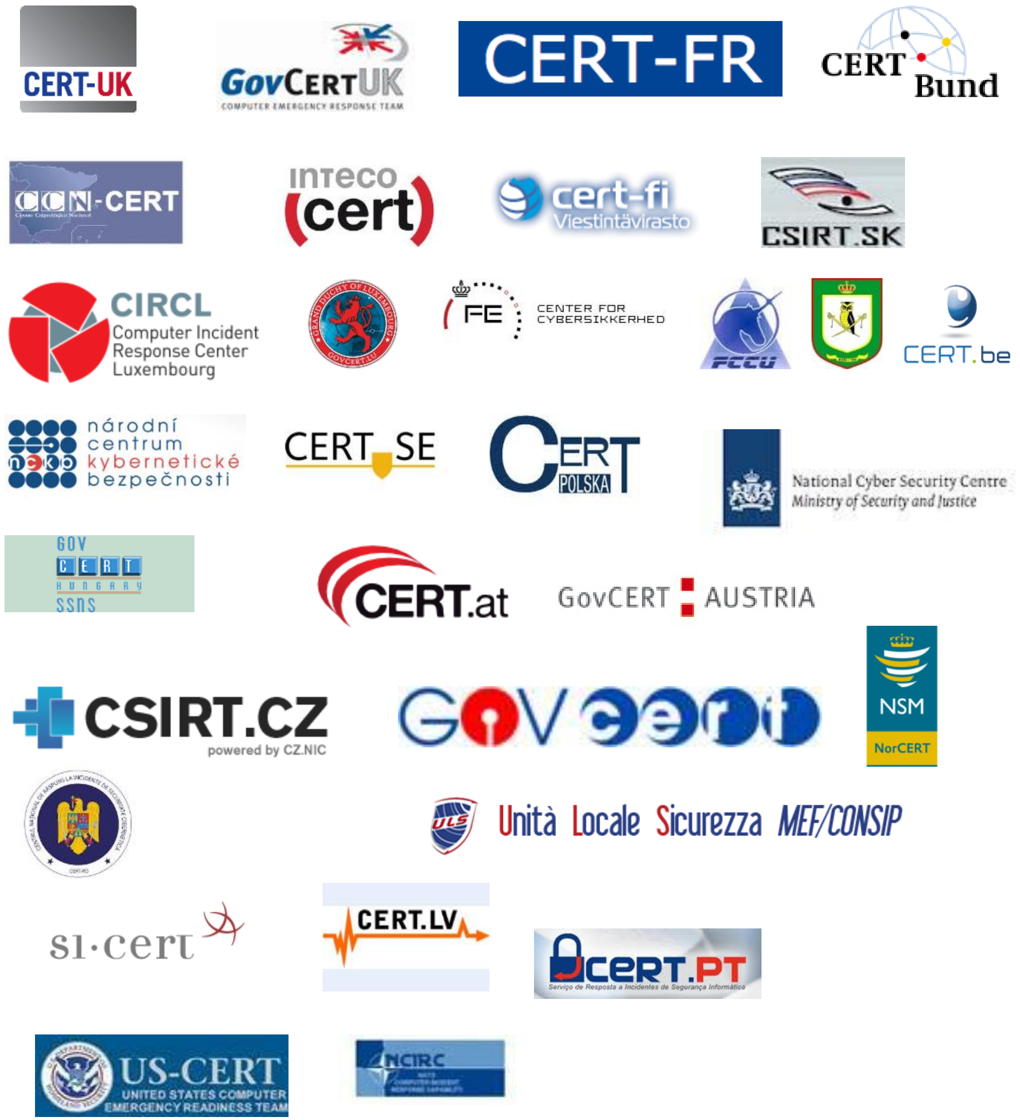
Alerts

- **Source of alerts**
  - ✓ Clients 30%
  - ✓ Other CERTs 20%
  - ✓ Automated sources 50%
- **Nature of alerts**
  - ✓ Malicious emails
  - ✓ Compromised systems
  - ✓ Vulnerable systems (SQL, XSS)
  - ✓ Leaked usernames / passwords
  - ✓ DDOS

Incident response coordination

- Support for coordination in « critical » incidents
- Provision of "internal" expertise to the constituent
  - ✓ CERT-EU expertise and tools
  - ✓ « On call »expertise in the constituency
- Liaison and coordination with third parties
  - ✓ Other CERTs
  - ✓ Specialist IT companies
- On-site support if requested
- Constituent remains fully in charge

Peers

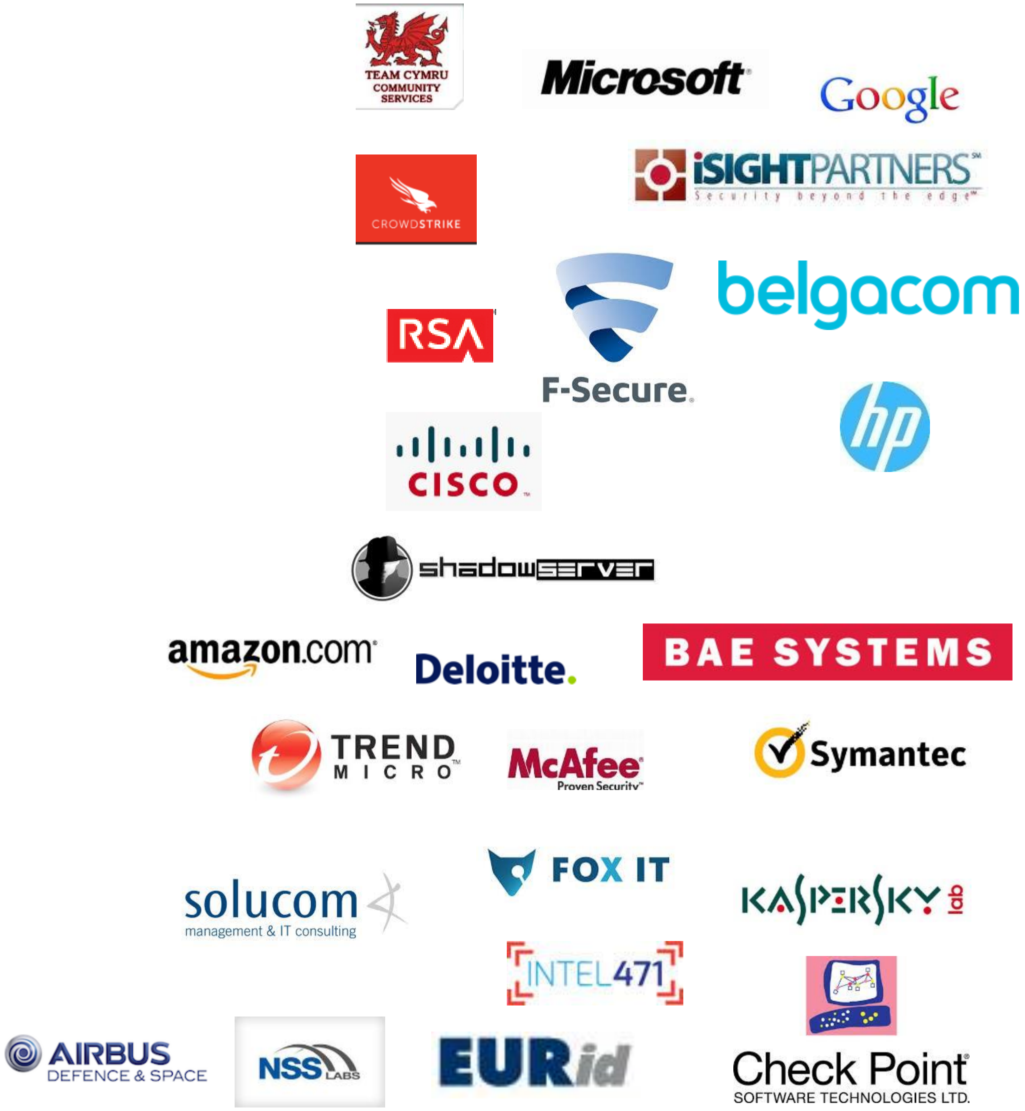

CERT-UK
GovCertUK
CERT-FR
CERT Bund
CCN-CERT
Inteco cert
cert-fi Viestintävirasto
CSIRT.SK
CIRCL Computer Incident Response Center Luxembourg
GOVCERT.LU
FE Center for Cybersikkerhed
FCCU
CERT.be
národní centrum kybernetické bezpečnosti
CERT SE
CERT Polska
National Cyber Security Centre Ministry of Security and Justice
GOV CERT Hungary SSNS
CERT.at
GovCERT AUSTRIA
CSIRT.CZ powered by CZ.NIC
GOVCERT
NSM NorCERT
Unità Locale Sicurezza MEF/CONSIP
si-cert
CERT.LV
CERT.PT
US-CERT United States Computer Emergency Readiness Team
NCIRC

- **Core group**
  - ✓ Very frequent contacts
  - ✓ Incident response and sharing
  - ✓ Automated feeds

- **Extended group**
  - ✓ Disemination IOCs
  - ✓ Specific cases

Partners

- Bilateral NDAs
- Access to privileged information
  - ✓ Campaign reports
  - ✓ Telemetry
  - ✓ Threat repositories
- Automated feeds
  - ✓ 100+ feeds
- Incident response



Targeted Attacks

- **Adversary's persistence**
  - ✓ They know what they want and they pursue their goal
  - ✓ They will repeatedly try to get in
  - ✓ Once they're in they try to stay
  - ✓ When you throw them out they will try to come back

- **Initial infection very difficult to avoid**
  - ✓ Spear-phishing e-mails
  - ✓ Social engineering to trick the user into running malware installers
  - ✓ Watering hole attacks using known exploits
  - ✓ Watering hole attacks that rely on social engineering

- Take control over the infrastructure: 10' -> 48hours

- **Detection**: average 229 days (**or never**)
- **Remediation:** 1-6 months

Motives

Traditional

- Geopolitical, Espionage
- Strategic / Military
- IPR theft

Upcoming

- Financial
  - ✓ Direct
  - ✓ Indirect
- Commercial
- Extortion
- Terrorism

Actors

Traditional

- ✓ Advanced nations' intelligence services

Upcoming

- ✓ Nations' subcontractors
- ✓ Rogue nations
- ✓ Traditional criminals
- ✓ Industrial Spies and Organized Crime Groups
- ✓ Hacktivists
- ✓ White collar criminals
- ✓ Terrorists
- ✓ Mafia

Methods

- **Open source research**
  - ✓ Passive collection
- **Spear-phishing e-mails using current themes as lures**
  - ✓ EP elections, new Commission
  - ✓ Ukraine, Russia (political developments, gas pipeline, EU sanctions)
  - ✓ Scottish referendum
  - ✓ “EU Restricted, releasable for internet transmission”
  - ✓ G20, meeting of central banks

Methods

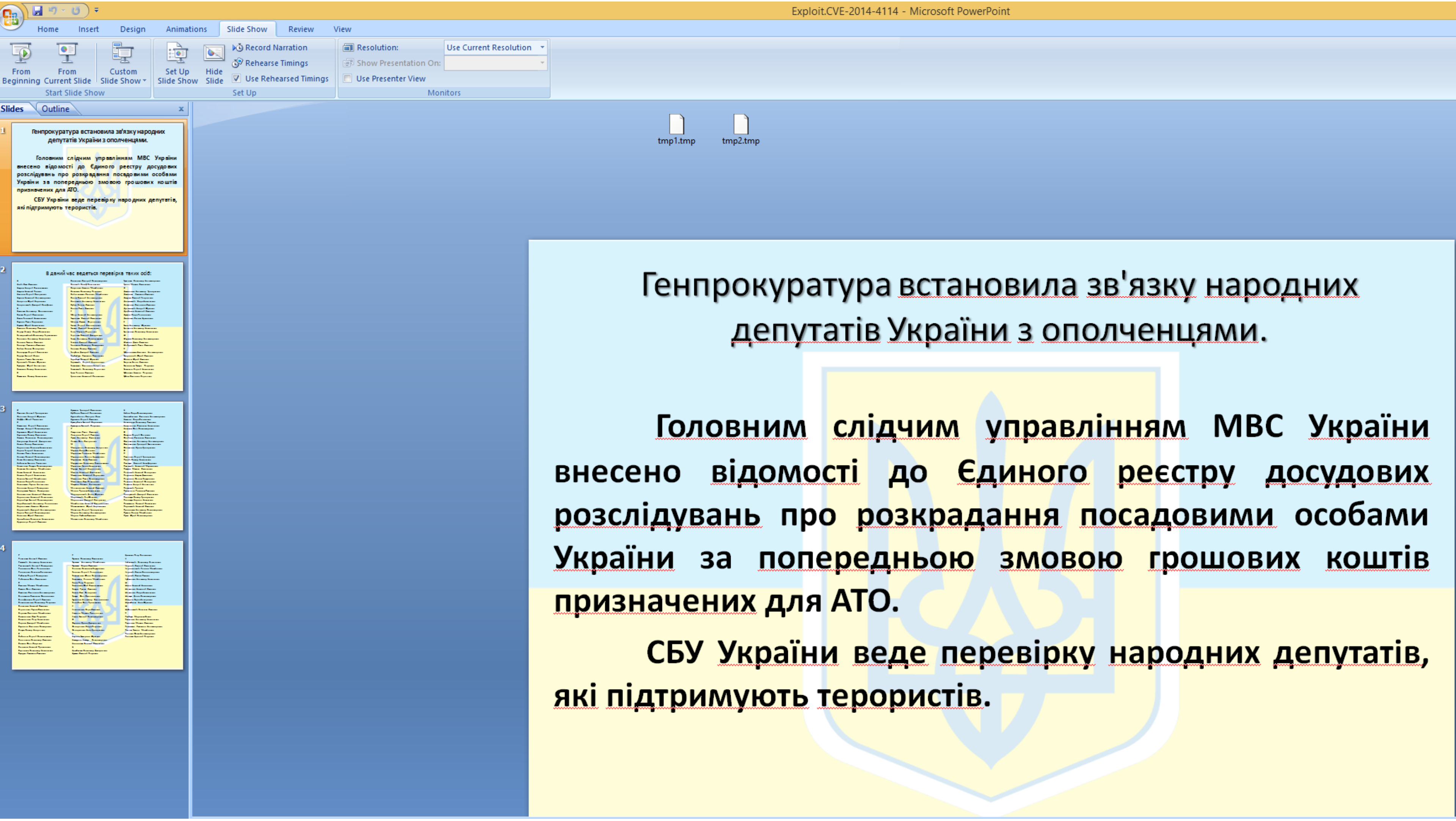
- **Open source research**
  - ✓ Passive collection
- **Spear-phishing e-mails using current themes as lures**
- **Vulnerabilities and exploits**
  - ✓ Unpatched vulnerabilities
  - ✓ 0-Day (Zero Day) application vulnerabilities
- **Credentials**
- **Exploitation of trusted relationships**
- **Social engineering to trick the user into running malware installers**
- **Watering hole attacks using known exploits**
- **Watering hole attacks that rely on social engineering**
- **Poor security practices / configurations**
- **Lack of end user education**
- **Lateral movements inside the infrastructure**

Impact

- Extremely stealthy
- Difficult to detect (little to no footprint in the file system)
- Try to remain under detection radar
- Very little or Zero overhead to systems

Many organizations operate for years, without knowing they are breached!

Examples



Генпрокуратура встановила зв'язку народних депутатів України з ополченцями.

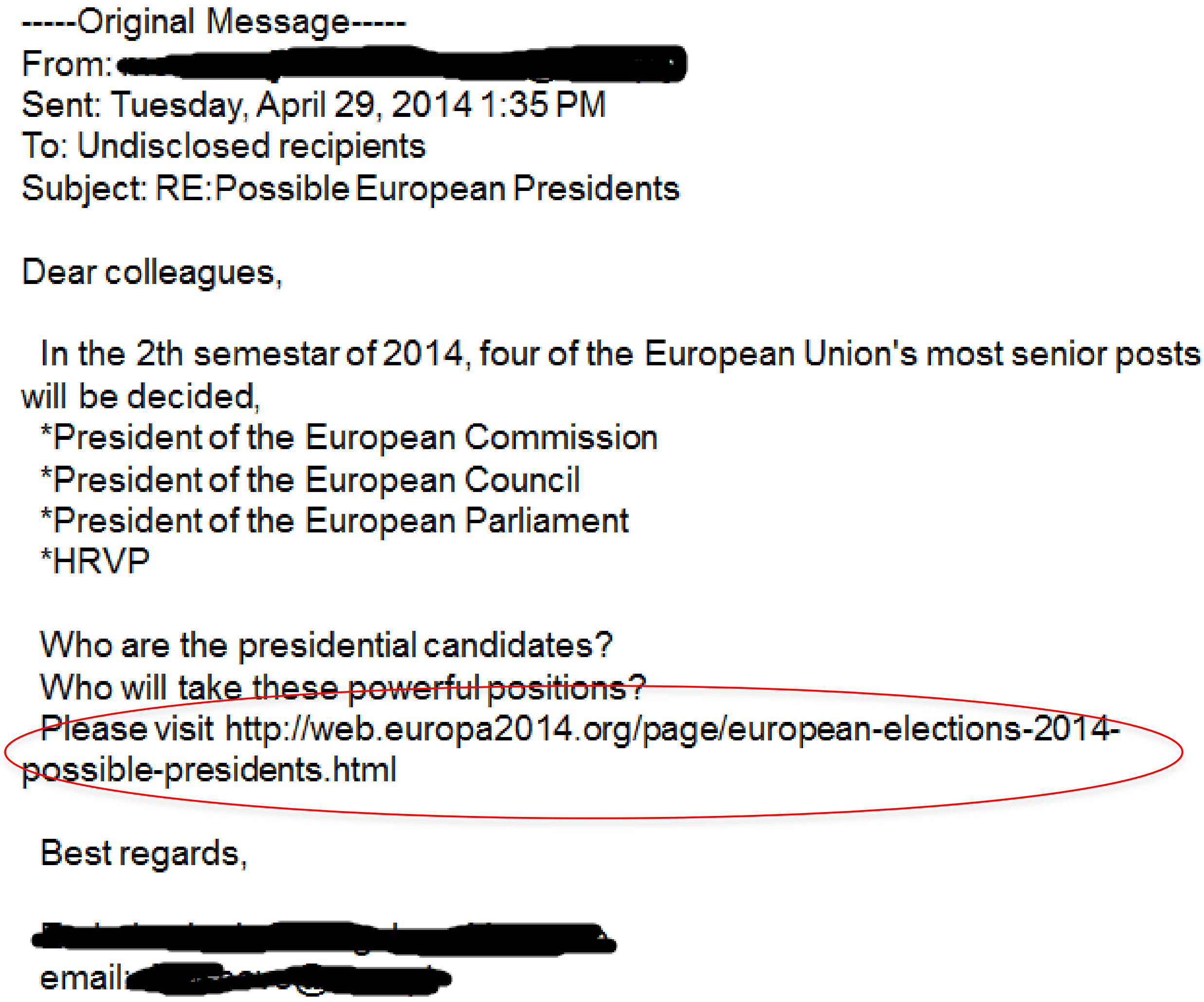
Головним слідчим управлінням МВС України внесено відомості до Єдиного реєстру досудових розслідувань про розкрадання посадовими особами України за попередньою змовою грошових коштів призначених для АТО.

СБУ України веде перевірку народних депутатів, які підтримують терористів.

В даний час ведеться перевірка таких осіб:

“Prosecutor’s General’s Office has established a connection with people’s deputies of Ukraine militias”

Examples



-----Original Message-----
From: [redacted]
Sent: Tuesday, April 29, 2014 1:35 PM
To: Undisclosed recipients
Subject: RE:Possible European Presidents

Dear colleagues,

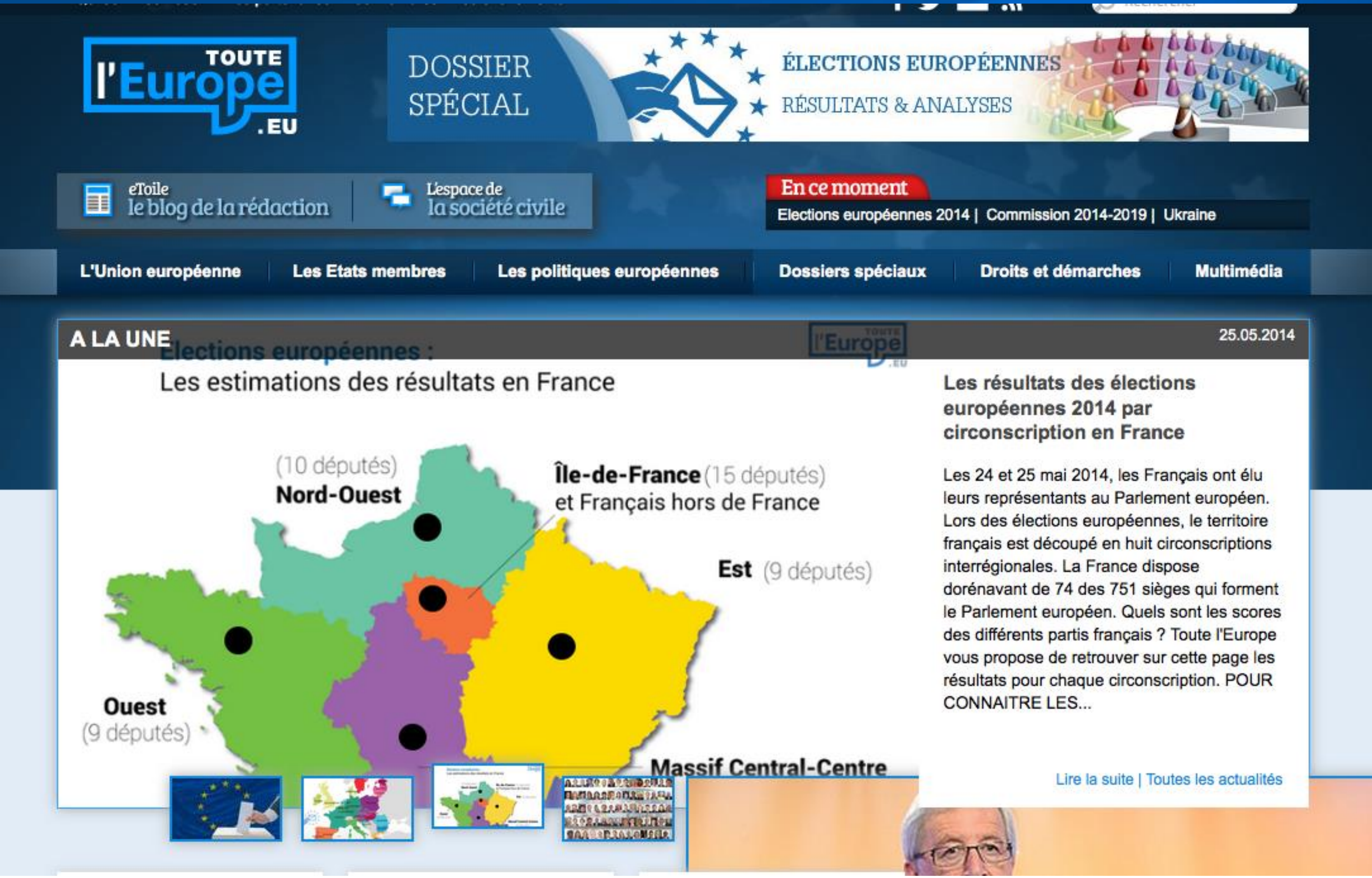
In the 2th semestar of 2014, four of the European Union's most senior posts will be decided,
*President of the European Commission
*President of the European Council
*President of the European Parliament
*HRVP

Who are the presidential candidates?
Who will take these powerful positions?
Please visit http://web.europa2014.org/page/european-elections-2014-possible-presidents.html

Best regards,

[redacted]
email: [redacted]

Examples



TOUTE l'Europe .EU

DOSSIER SPÉCIAL

ÉLECTIONS EUROPÉENNES

RÉSULTATS & ANALYSES

eToile le blog de la rédaction

L'espace de la société civile

En ce moment

Elections européennes 2014 | Commission 2014-2019 | Ukraine

L'Union européenne | Les Etats membres | Les politiques européennes | Dossiers spéciaux | Droits et démarches | Multimédia

A LA UNE

25.05.2014

Elections européennes :

Les estimations des résultats en France

Les résultats des élections européennes 2014 par circonscription en France

Les 24 et 25 mai 2014, les Français ont élu leurs représentants au Parlement européen. Lors des élections européennes, le territoire français est découpé en huit circonscriptions interrégionales. La France dispose dorénavant de 74 des 751 sièges qui forment le Parlement européen. Quels sont les scores des différents partis français ? Toute l'Europe vous propose de retrouver sur cette page les résultats pour chaque circonscription. POUR CONNAITRE LES...

Lire la suite | Toutes les actualités

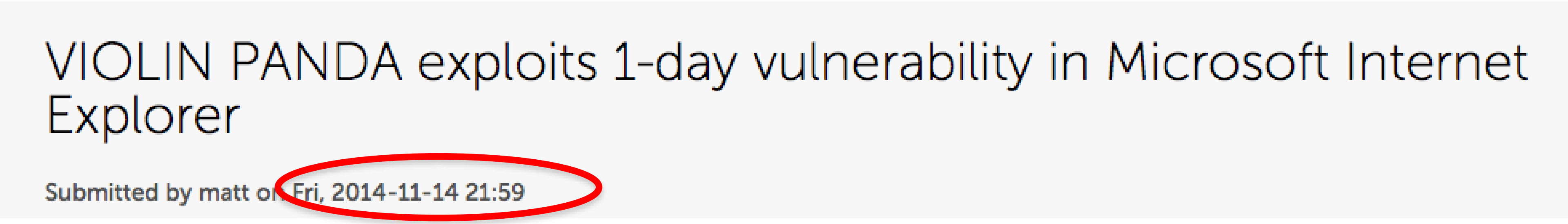
Vulnerabilities

Recent developments

- More advanced Automated discovery of vulnerabilities (fuzzers)
- Many critical vulnerabilities in OS and SSL since years
  - ✓ Heartbleed, Bash/Shellshock
  - ✓ MS14-064, MS14-066 and MS14-068
- Rapid development of exploits
- Market for vulnerabilities
  - ✓ Vupen, Endgame etc.
  - ✓ Community
- Involvement of nation states
  - ✓ Non-disclosure
  - ✓ Risk of disclosure

Unicorn bug

- CVE-2014-6332
- Windows OLE Automation Array Remote Code Execution vulnerability
- Disclosed publicly on **2014-11-11**

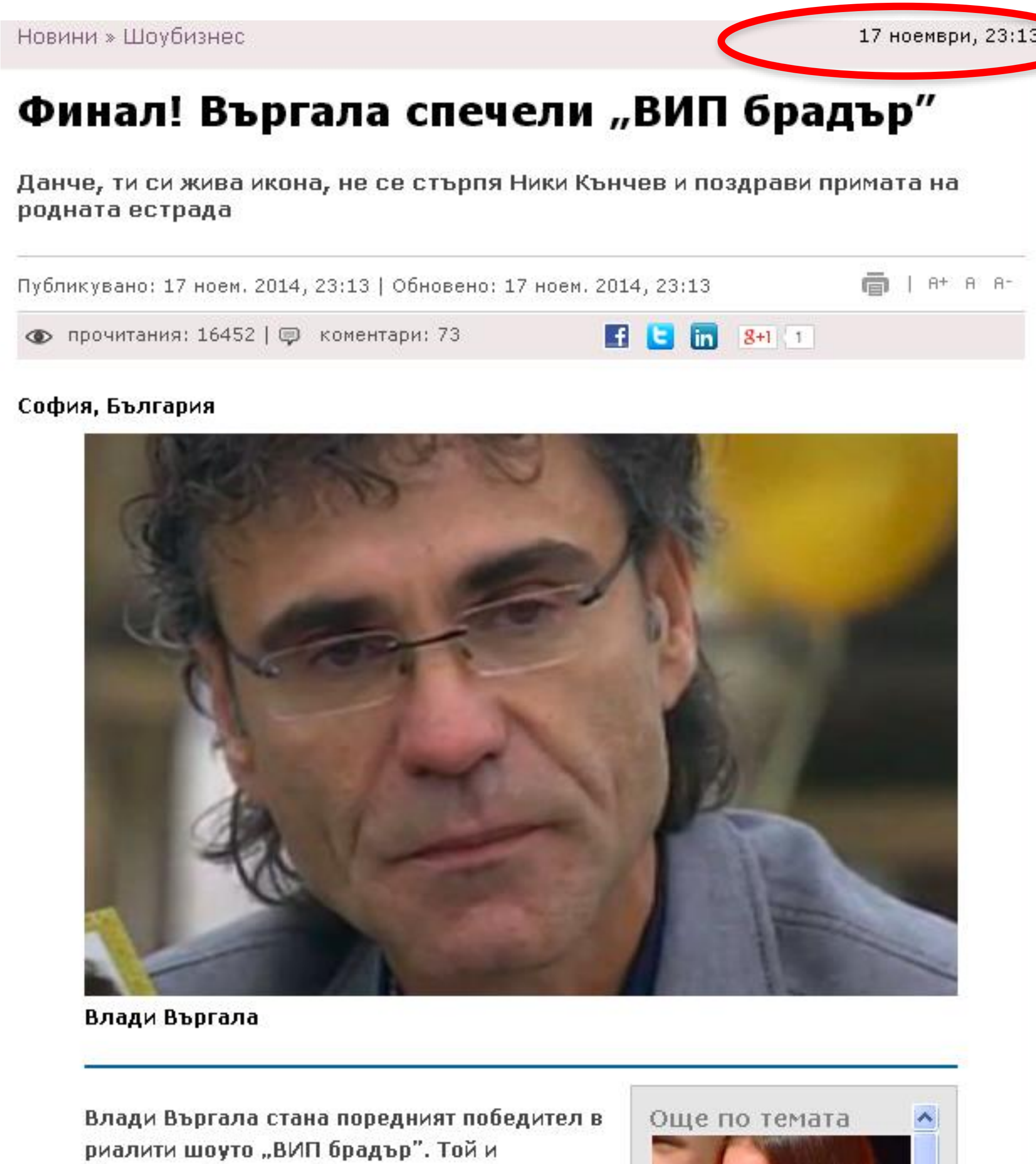


VIOLIN PANDA exploits 1-day vulnerability in Microsoft Internet Explorer

Submitted by matt on Fri, 2014-11-14 21:59

Unicorn bug

- CVE-2014-6332
- TOP 50 BG website
- One page infected
- Redirects to RU site with exploits



Новини » Шоубизнес 17 ноември, 23:13

Финал! Въргала спечели „ВИП брадър"

Данче, ти си жива икона, не се стърпя Ники Кънчев и поздрави примата на родната естрада

Публикувано: 17 ноем. 2014, 23:13 | Обновено: 17 ноем. 2014, 23:13 | A+ A A-

прочитания: 16452 | коментари: 73

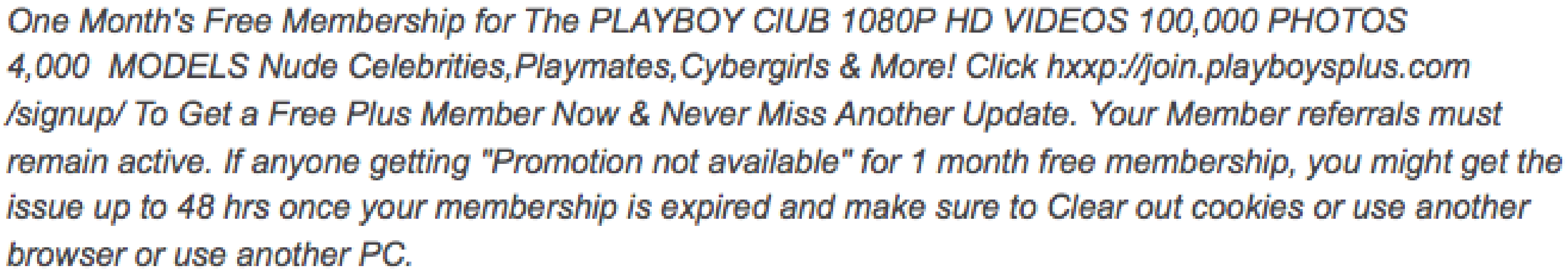
София, България

Влади Въргала

Влади Въргала стана поредният победител в риалити шоуто „ВИП брадър". Той и

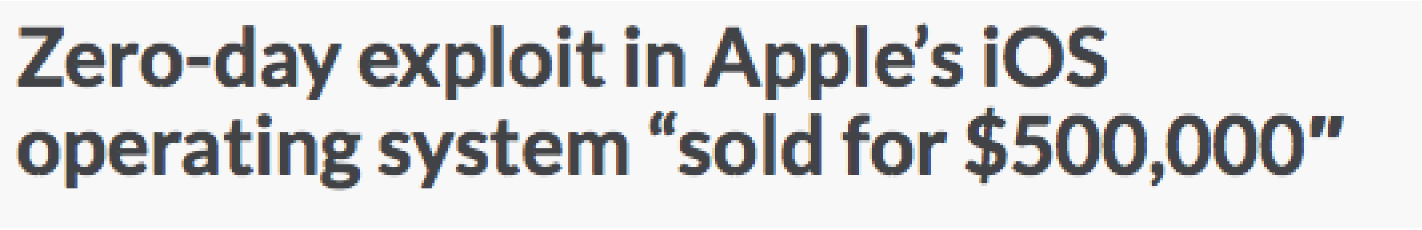
Unicorn bug

“APT3 has quietly continued to send waves of spear phishing messages over the past few months. This actor initiated their most recent campaign on **November 19, 2014** targeting multiple organizations. The attacker leveraged multiple exploits, targeting both **CVE-2014-6332**
and CVE-2014-4113.

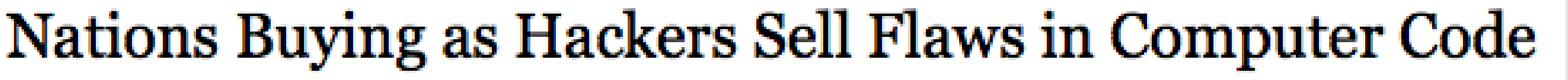


One Month's Free Membership for The PLAYBOY CIUB 1080P HD VIDEOS 100,000 PHOTOS 4,000 MODELS Nude Celebrities,Playmates,Cybergirls & More! Click hxxp://join.playboysplus.com /signup/ To Get a Free Plus Member Now & Never Miss Another Update. Your Member referrals must remain active. If anyone getting "Promotion not available" for 1 month free membership, you might get the issue up to 48 hrs once your membership is expired and make sure to Clear out cookies or use another browser or use another PC.

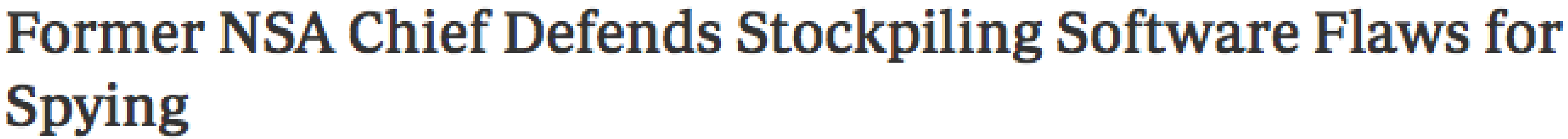
Vulnerabilities



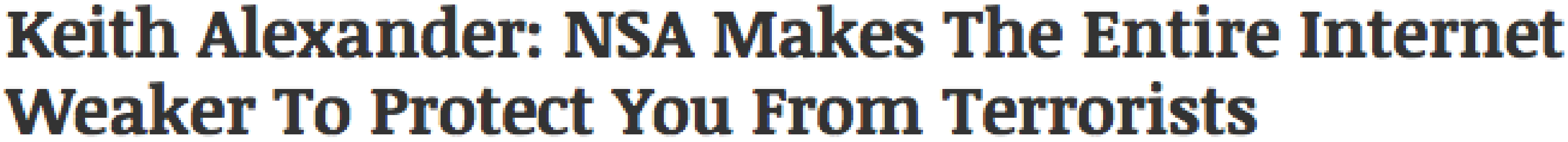
Zero-day exploit in Apple's iOS operating system "sold for $500,000"



Nations Buying as Hackers Sell Flaws in Computer Code

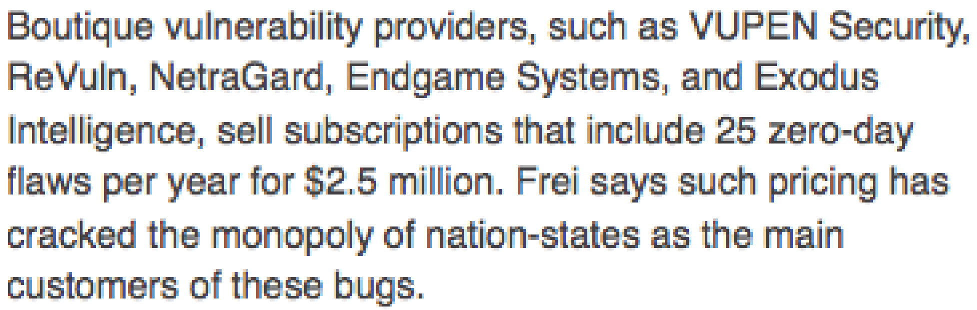


Former NSA Chief Defends Stockpiling Software Flaws for Spying



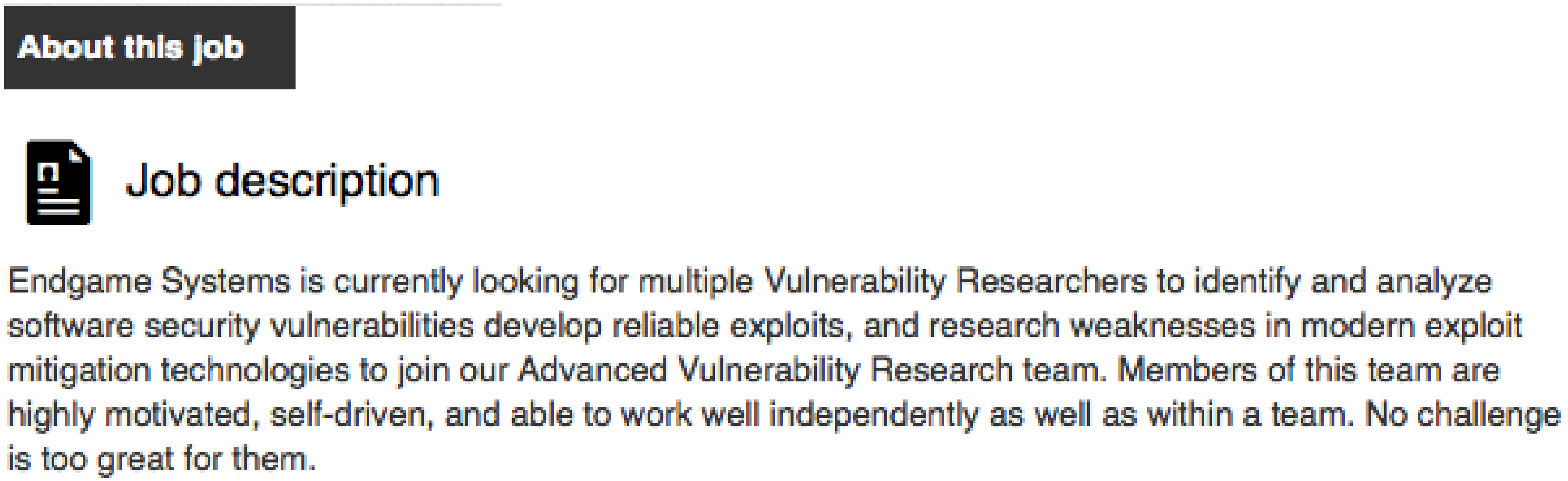
Keith Alexander: NSA Makes The Entire Internet Weaker To Protect You From Terrorists

Vulnerabilities Market



Boutique vulnerability providers, such as VUPEN Security, ReVuln, NetraGard, Endgame Systems, and Exodus Intelligence, sell subscriptions that include 25 zero-day flaws per year for $2.5 million. Frei says such pricing has cracked the monopoly of nation-states as the main customers of these bugs.

NSSLABS 2013



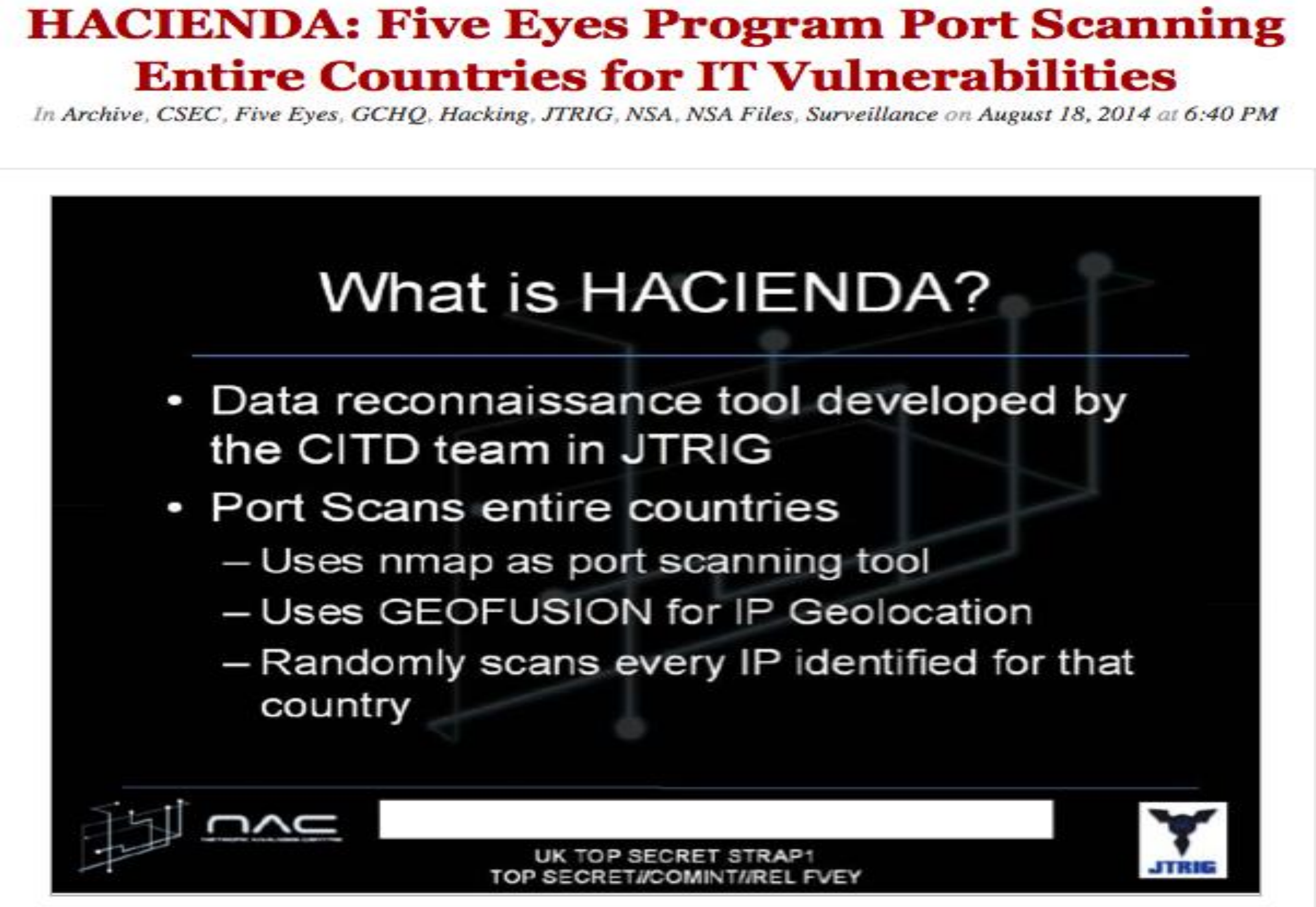
About this job

Job description

Endgame Systems is currently looking for multiple Vulnerability Researchers to identify and analyze software security vulnerabilities develop reliable exploits, and research weaknesses in modern exploit mitigation technologies to join our Advanced Vulnerability Research team. Members of this team are highly motivated, self-driven, and able to work well independently as well as within a team. No challenge is too great for them.

LinkedIn

Scanning for vulnerabilities



HACIENDA: Five Eyes Program Port Scanning Entire Countries for IT Vulnerabilities

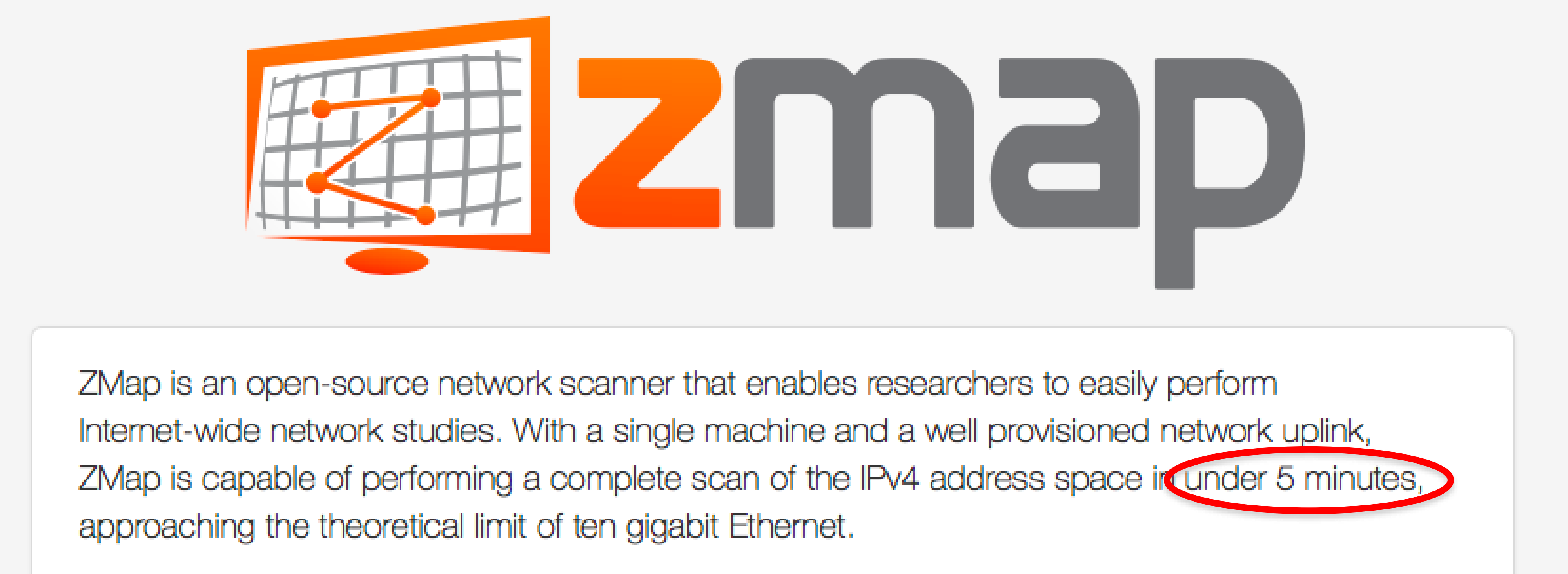
In Archive, CSEC, Five Eyes, GCHQ, Hacking, JTRIG, NSA, NSA Files, Surveillance on August 18, 2014 at 6:40 PM

What is HACIENDA?

- Data reconnaissance tool developed by the CITD team in JTRIG
- Port Scans entire countries
  - Uses nmap as port scanning tool
  - Uses GEOFUSION for IP Geolocation
  - Randomly scans every IP identified for that country

UK TOP SECRET STRAP1
TOP SECRET//COMINT//REL FVEY

Scanning for vulnerabilities



ZMap is an open-source network scanner that enables researchers to easily perform Internet-wide network studies. With a single machine and a well provisioned network uplink, ZMap is capable of performing a complete scan of the IPv4 address space in under 5 minutes, approaching the theoretical limit of ten gigabit Ethernet.

Download : https://zmap.io/download.html

Internet-Wide Scan Data Repository : https://scans.io/

Campaigns

Group	Compromised organisations include
Ke3Chang/Vixen Panda/	Metushy waves of attack 2014. Spear phishing email attacks in relation to the G20 meeting and central bank meetings in the context of G20. Part of a broader, continuous campaign.
Cybercrime	Target, Home Depot, K-Mart and more than 1000 other businesses in US, some in Europe as well. POS malware.
APT18-CN	Community Health Systems, data of more than 5mio patients in the US was stolen, linked to Heartbleed.
Darkhotel	Targeted attacks on visitors of international hotels, using the hotel Wi-Fi infrastructure.
Regin	High profile victims, telecom operators, international organisations, research

Campaigns

Group	Compromised organisations include
Snake / Turla	Ministeries of Foreign Affairs, Defence, Embassies. Banks, travel agencies. Defence, aviation and electronics industry.
Miniduke / Cosmic Duke/ Onion Duke	Governments of multiple countries, research foundations, think-tanks, healthcare providers.
Energetic Bear / DragonFly	20.000 victim IP addresses. Energy and manufacturing sector, research organisations, public sector, industrial control systems. Gathers information about connected controls systems (OPC).
Sofacy/APT28	Governments of multiple countries, think-tanks, opposition groups.
Black Energy/ Sandworm	Ukrainian regional government departments, European government agencies, NATO, 0-day, ICS.

Recent developments

- Cybercrime becomes more sophisticated
  - ✓ First APT against banks (https://www.fox-it.com/en/files/2014/12/Anunak_APT-against-financial-institutions2.pdf)
  - ✓ Citadel -> password stealing
- Mobile Malwares are a reality
- Emergence of attacks against ICS
- Threats are Increasing
- Threats become more sophisticated

Final Words

- Threats increase and become more sophisticated
- Inherent vulnerabilities are systematically exploited
- Pace is increasingly challenging
- Early detection and rapid incident response
- Cooperation in post-Snowden era

Thank You

http://cert.europa.eu/