They're Inside… Now What?

Eddie Schwartz
Chief Information Security Officer

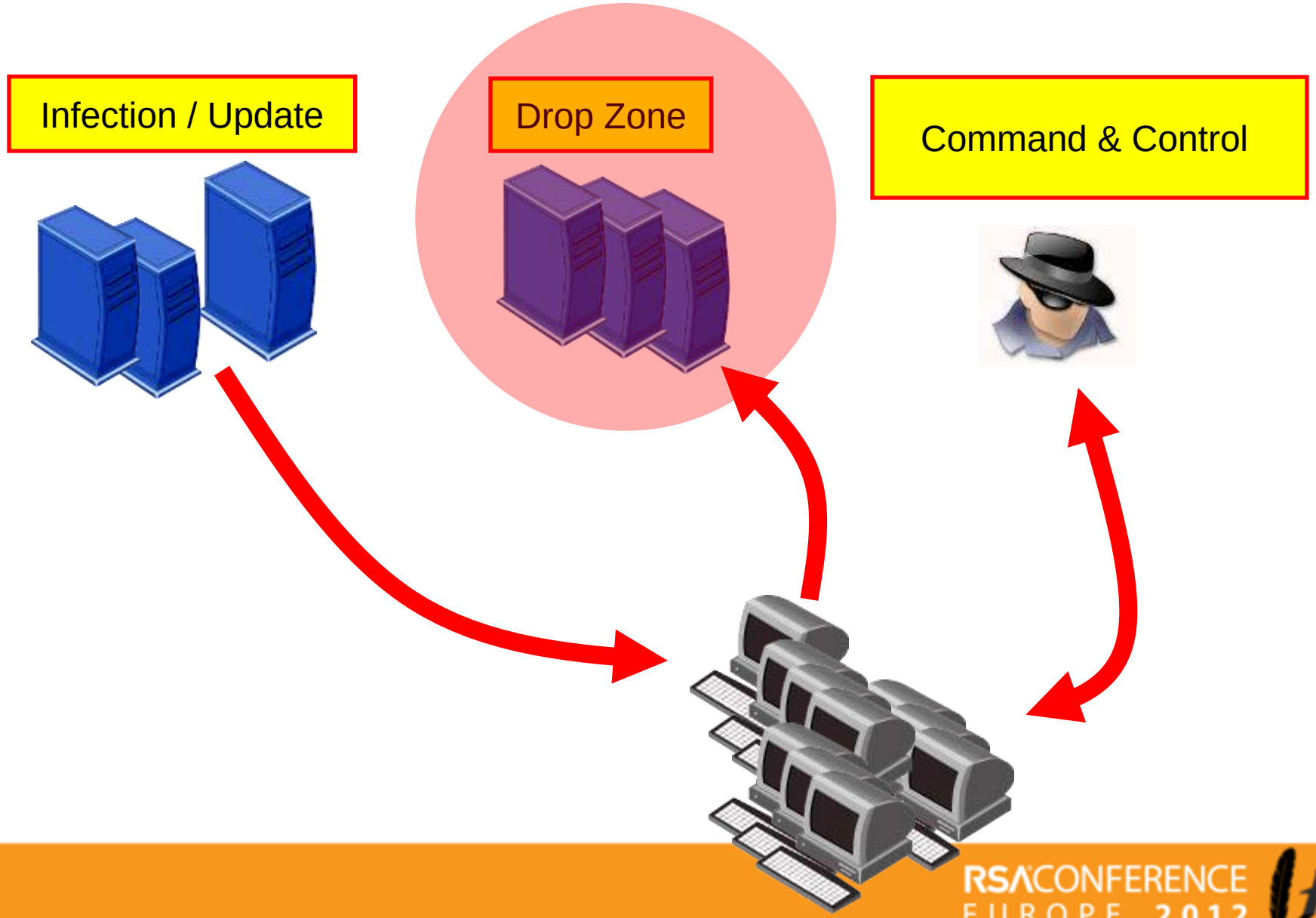
Uri Rivner
Head of Cyber Strategy

Session ID: HT-209
Session Classification: Intermediate

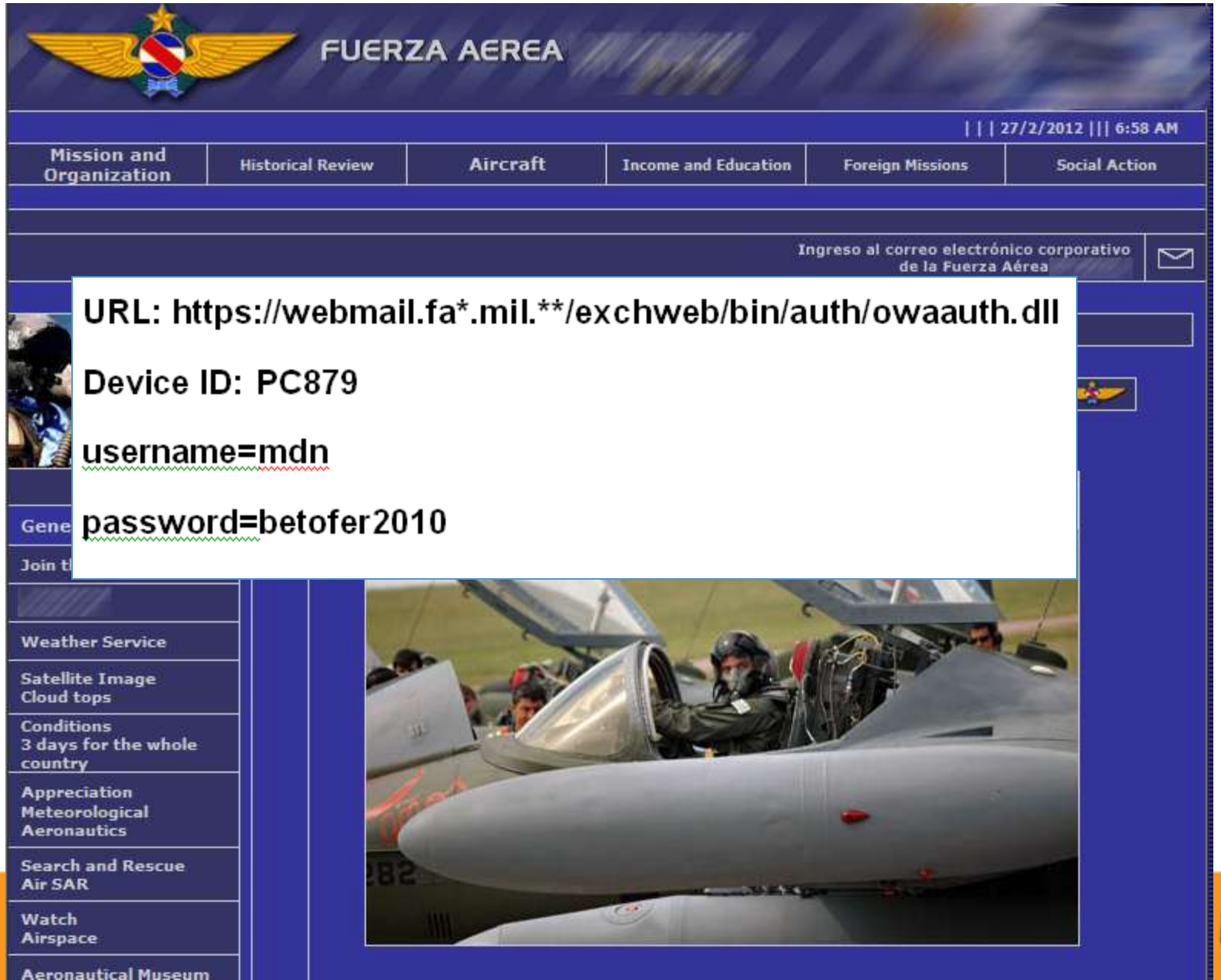
RSA CONFERENCE EUROPE 2012

If these are RANDOM attacks… We're screwed

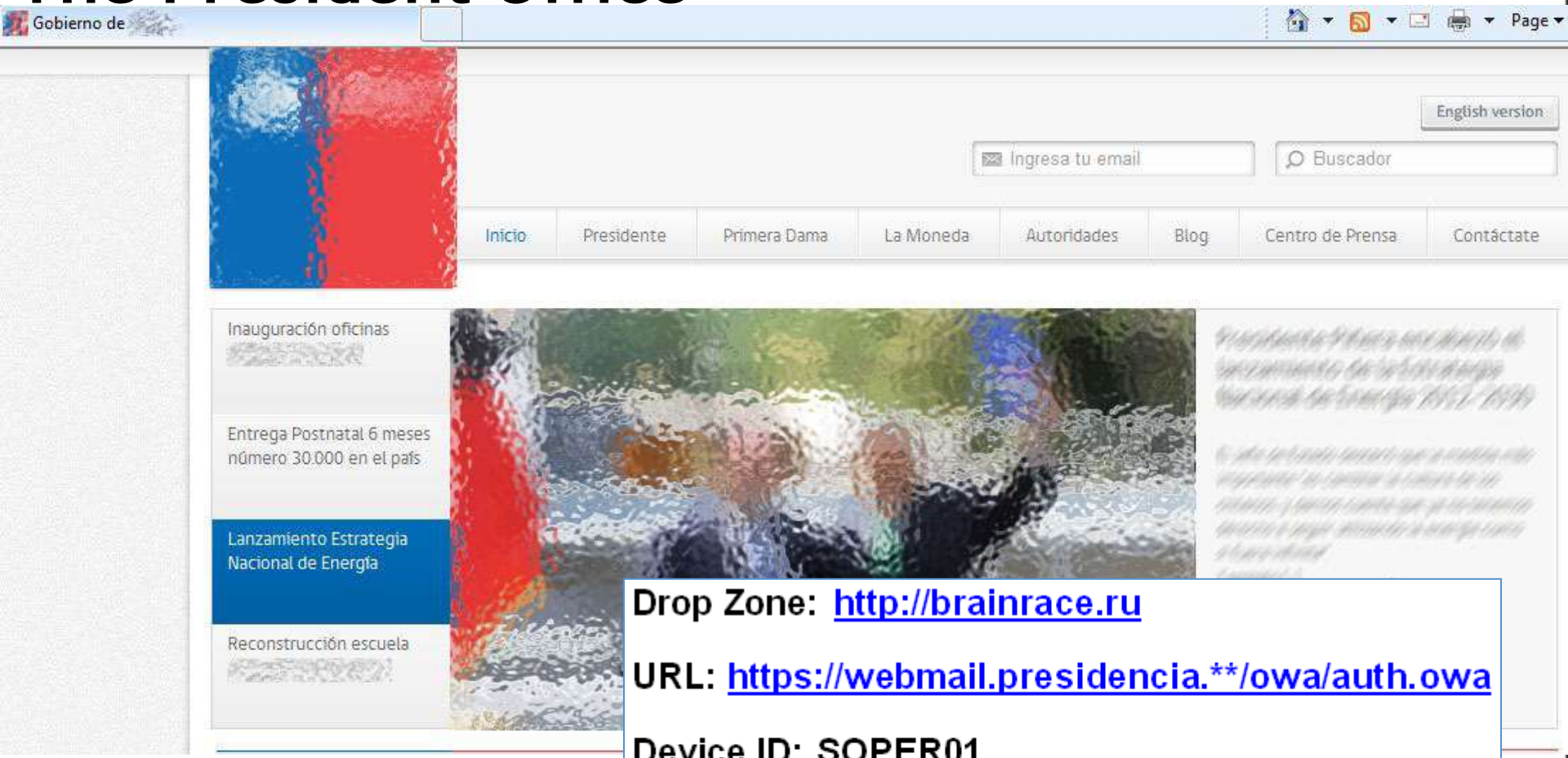
Trojan Infrastructure



Latin America Air Force



The President Office



Drop Zone: http://brainrace.ru

URL: https://webmail.presidencia.**/owa/auth.owa

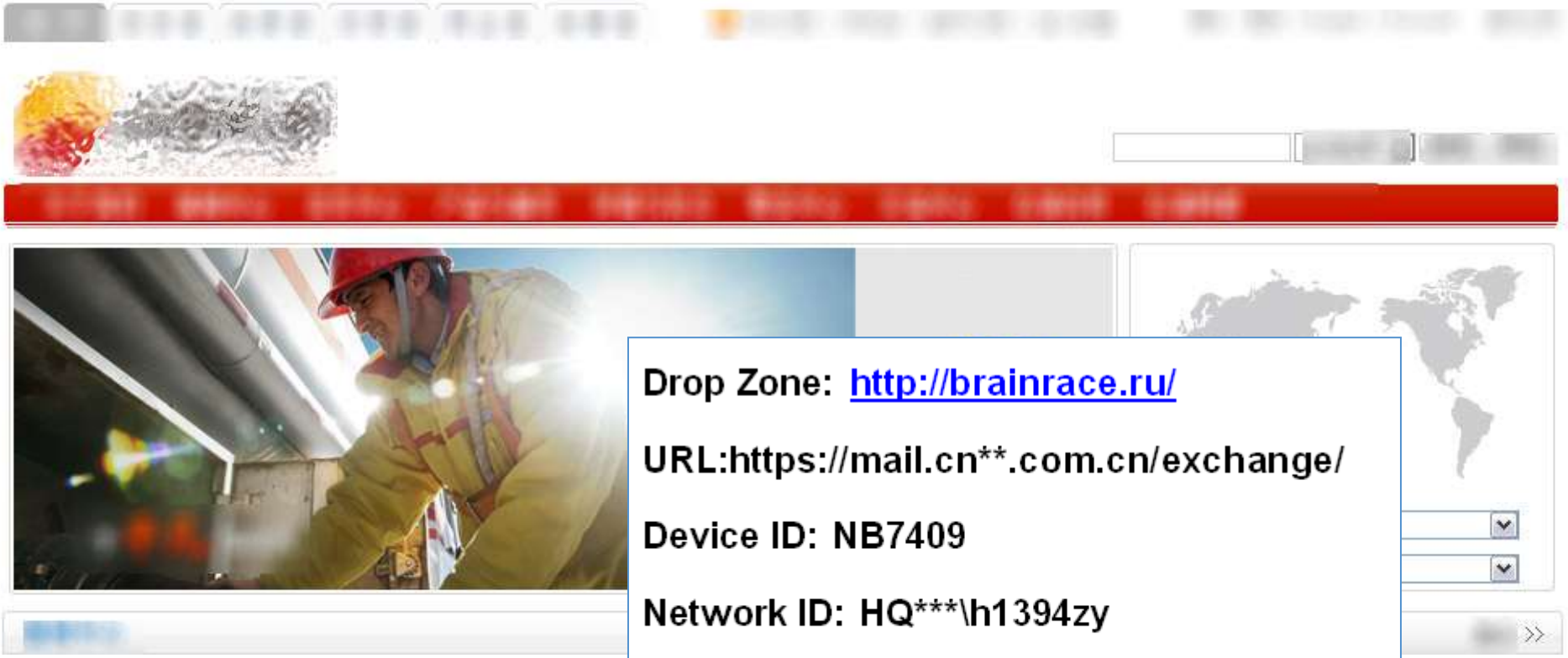
Device ID: SOPER01

Network Name: PR*****\monitores

User name=PR*****/SEGURIDAD

password=SEGURIDAD****

China Oil Giant



Drop Zone: http://brainrace.ru/

URL:https://mail.cn**.com.cn/exchange/

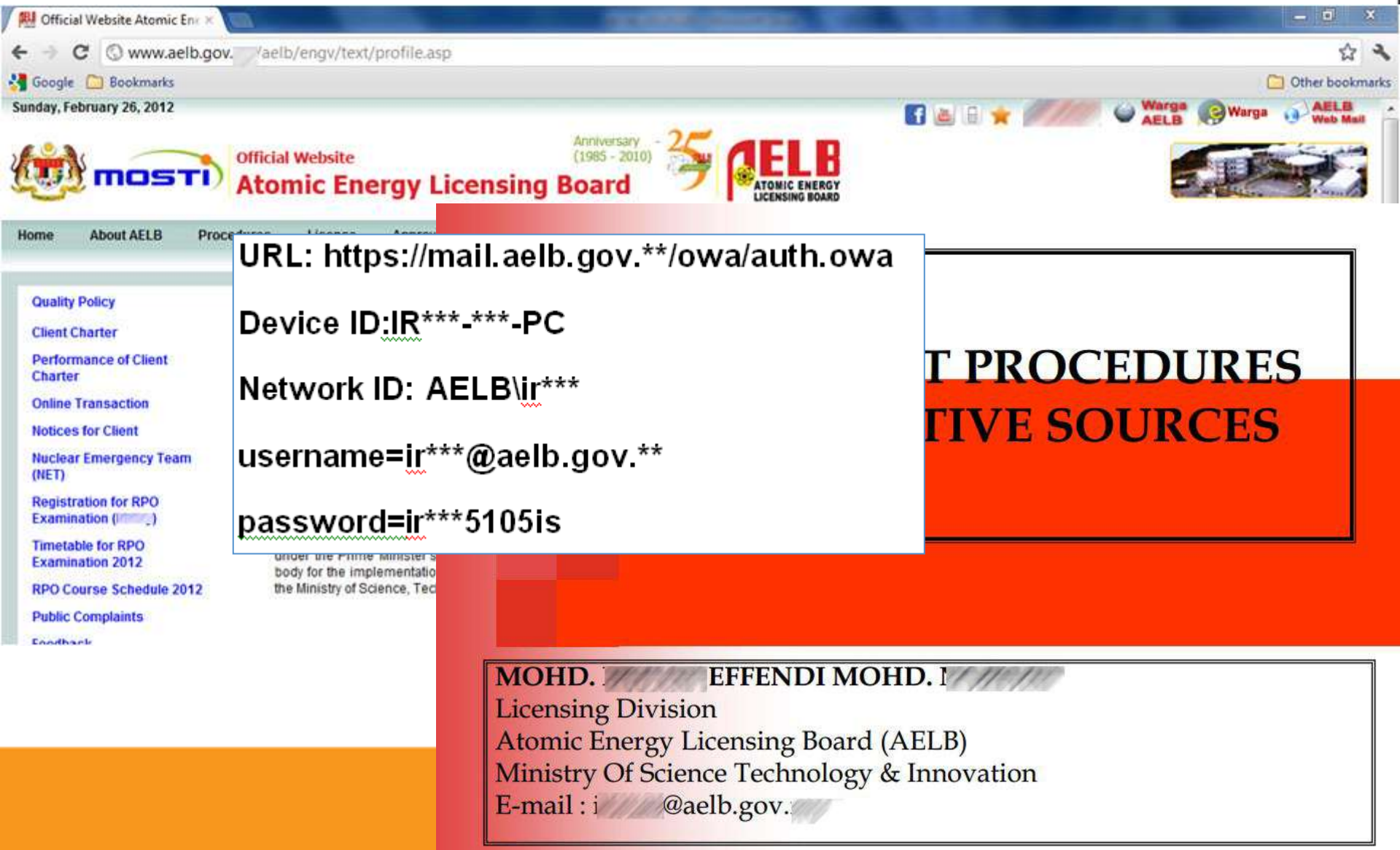
Device ID: NB7409

Network ID: HQ***\h1394zy

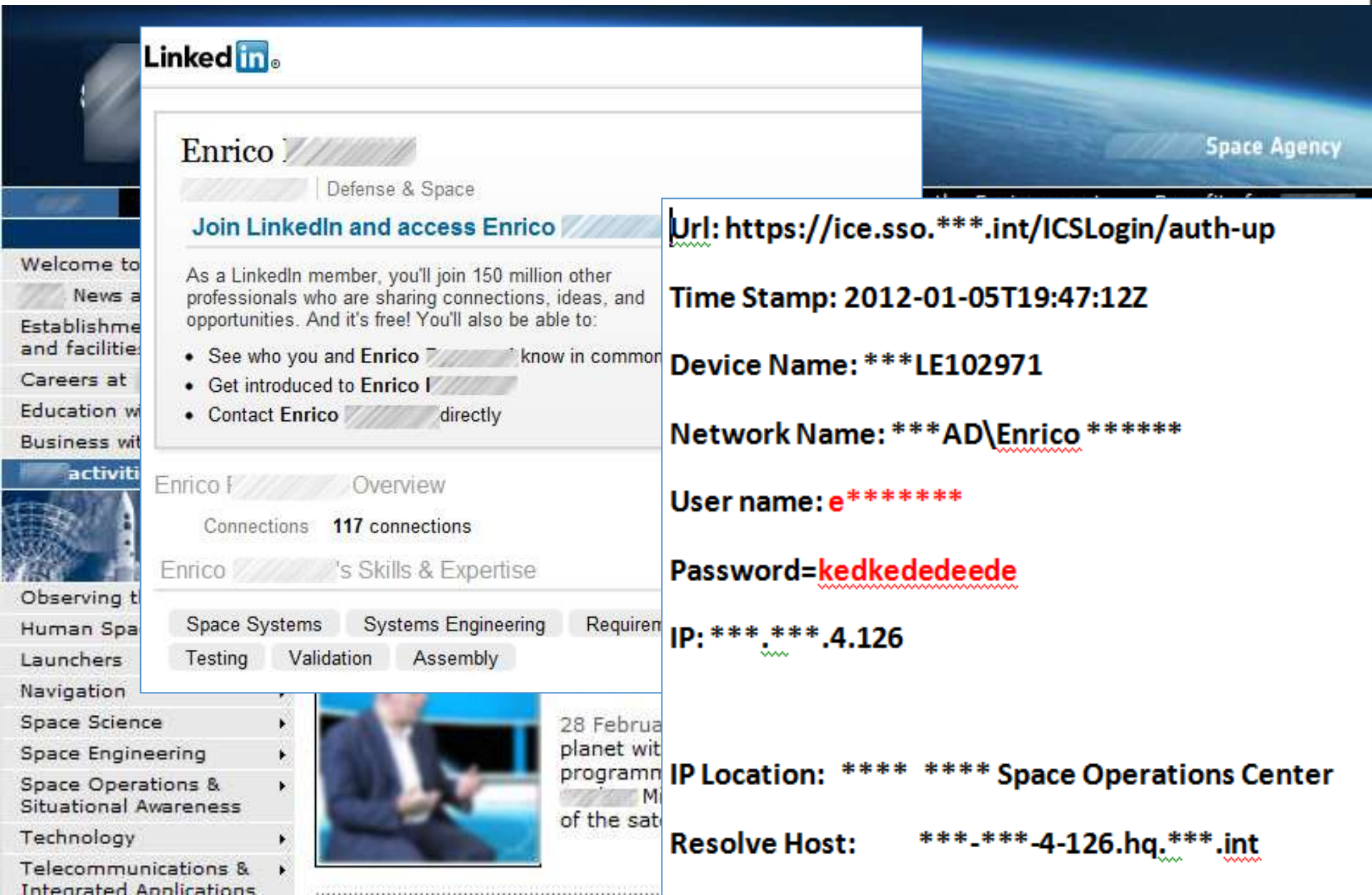
username=h1394zy

password=centrino

Atomic Energy in South East Asia



Foreign space agency



Particle Accelerator

IP Location: [redacted] Research And Academic Network

Device ID: PCENRI

Time Stamp: 2012-01-31T11:43:22Z

URL: https://login.**.**/adfs/ls/?wa=wsignin1.0&amp**

Login=*iani**

Password=Sisto***

Email: enrico.*iani@****.****

Premier League Club

Kazakhstan

The Treasurer

Trojan Family: Zeus Version 2.0

botId: ADMINISTRATOR

Path_source: https://remote.[redacted].gov/dana-na/auth/url_default/login.cgi

Network_id: ADMINISTRATOR\Home

Timestamp: 12 Jan 2011 01:12:32 GMT

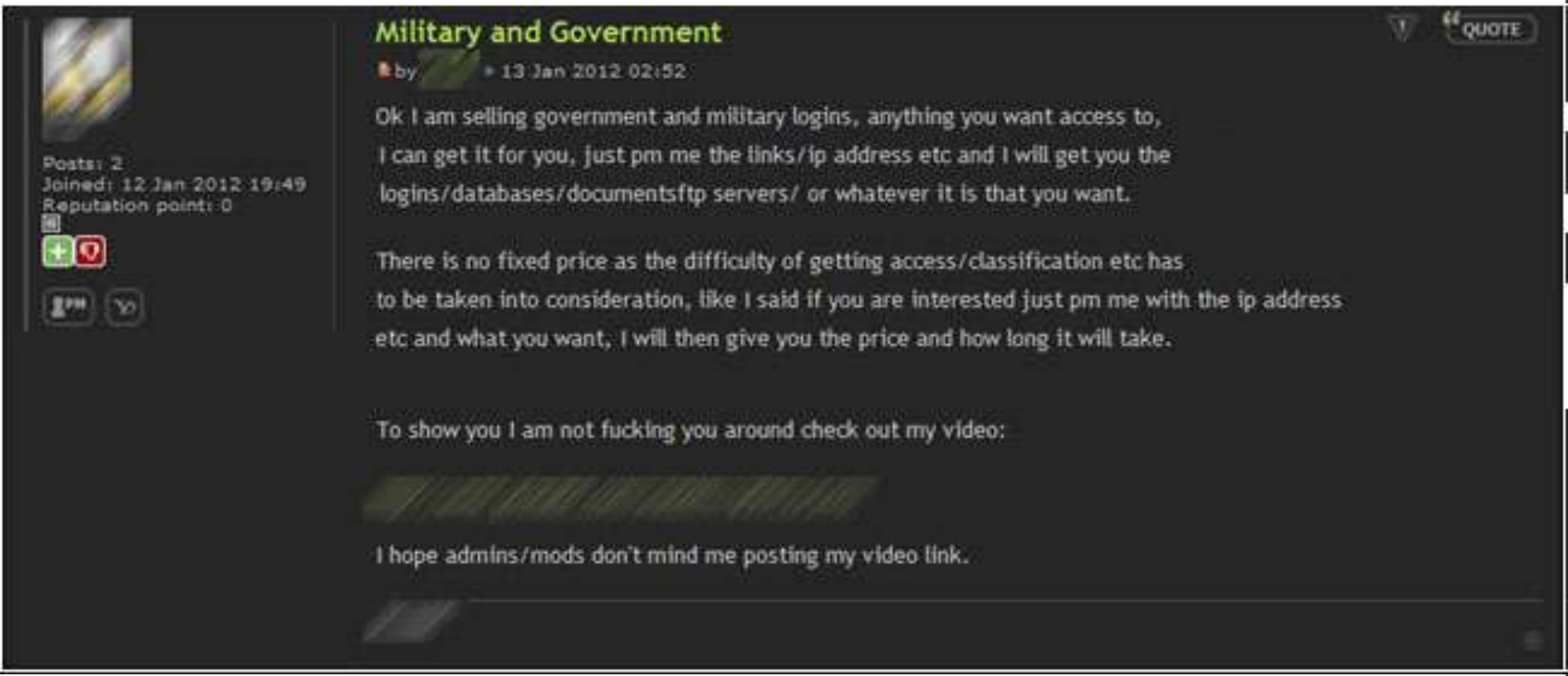
I would like to request that you remove [redacted] the current Treasurer from [redacted] tomorrow afternoon. The new Treasurer to be added is [redacted]. Please send me his log in and pass word

POST data:

username=[redacted]

password=summer[redacted]

Government, Military for Sale



Now lets talk about *Targeted* Attacks

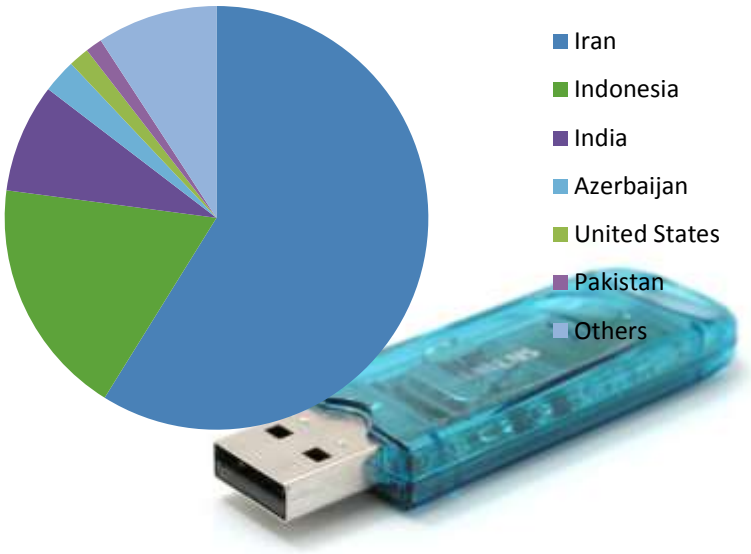
Advanced Persistent Threats
See anything in common?

Attack	Targets	Entry Vector	Going After
Ghostnet	Ministries, Embassies, Office of Dalai Lama	Spear Phishing	Sensitive documents
Aurora	34 companies: Google, Adobe, defense, internet, financial, critical infrastructure	Spear Phishing	Intellectual property
Night Dragon	Critical infrastructure	Spear Phishing	Intellectual property
Nitro	Oil and Gas companies	Spear Phishing	Intellectual property
Shady RAT	Defense, corporations, UN, Olympic Committee	Spear Phishing	Intellectual property and documents

Advanced Persistent Threats and Cyber Weapons

- Stuxnet
  - Discovered by Virus Block Ada June 2010
  - Sophisticated
  - Spread through Microsoft Windows systems initially indiscriminately
  - Targets vulnerable systems running Siemens industrial software and equipment
  - First to Contain PLC root kit
  - Infects PLCs by subverting the 7 step software application used in configuration

Computers Infected by Stuxnet by Country

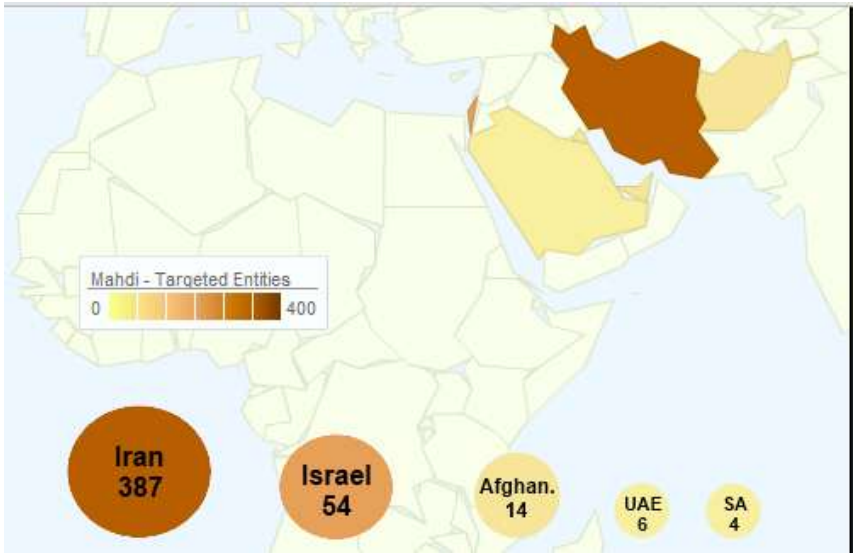


Advanced Persistent Threats and Cyber Weapons

- DuQu
  - Discovered by the CrySyS lab of Hungary
  - Stuxnet related code set
  - Noted on systems in the following nations:
    - France
    - India
    - Iran
    - Sudan
    - Vietnam
    - Hungary
    - Indonesia
    - United Kingdom
- Similar but different from Stuxnet
  - Focused more on exfiltrating data from the manufacturers of SCADA compliant PLC systems
  - ~50 systems affected as of November 2011 (confirmed)*
  - Uses complex, high level programming language known as “Duqu Framework”
  - Leverages the same installer exploit 0-day Windows kernel vulnerabilies
  - Components are signed with stolen keys
  - DuQu and Stuxnet are both highly targeted

Advanced Persistent Threats?

- Madhi
  - Discovered in February 2012 by Seculert
  - Kaspersky Labs and Seculert conducted analysis
    - Name derived from files seen during the analysis which reference the Muslim Messiah
  - Madhi may have been used since late 2011 for the purpose of targeted cyber espionage
  - Predominantly noted in Muslim nations and Iran
  - ~800 known infected machines



But there's more…

- Flame
  - Flamer
  - sKYWiper
  - Skywiper
- Discovered in May 2012
  - MAHER Center of Iranian National CERT
  - Kaspersky Labs
  - CrySysLab of Hungary
- Modular architecture
- Active within Microsoft Systems
- Promiscuous; transmitted via LAN or USB
- Exhibits attributes associated with other cyber espionage samples and campaigns such as Stuxnet and DuQu
- Ability to capture voice, video, data and encrypted message traffic (e.g. Skype)
- ~1000s of infected machines

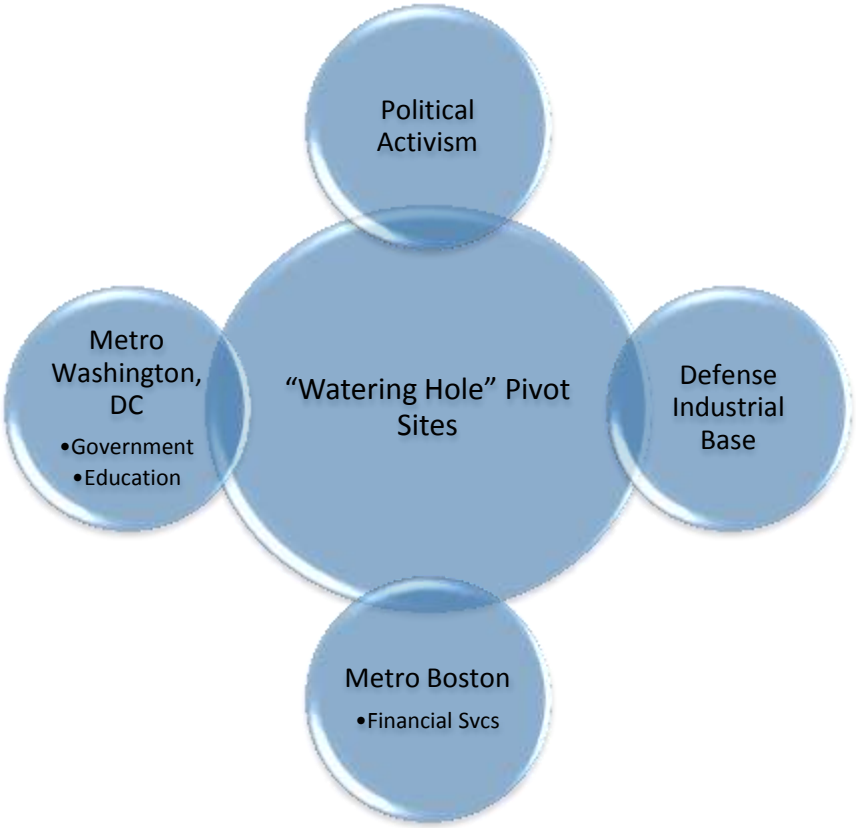
Name	Module Description
Flame	Modules that perform attack functions
Boost	Modules that perform reconnaissance & Intel harvesting functions
Flask	Module that performs attack function
Jimmy	Module that performs attack function
Munch	Module that controls installation and propagation
Snack	Module that controls local propagation
Spotter	Module that performs enumeration
Transport	Module that manages replication
Euphoria	Module that controls file exfiltration
Headache	Attack parameters & properties

One of the Latest -- VOHO

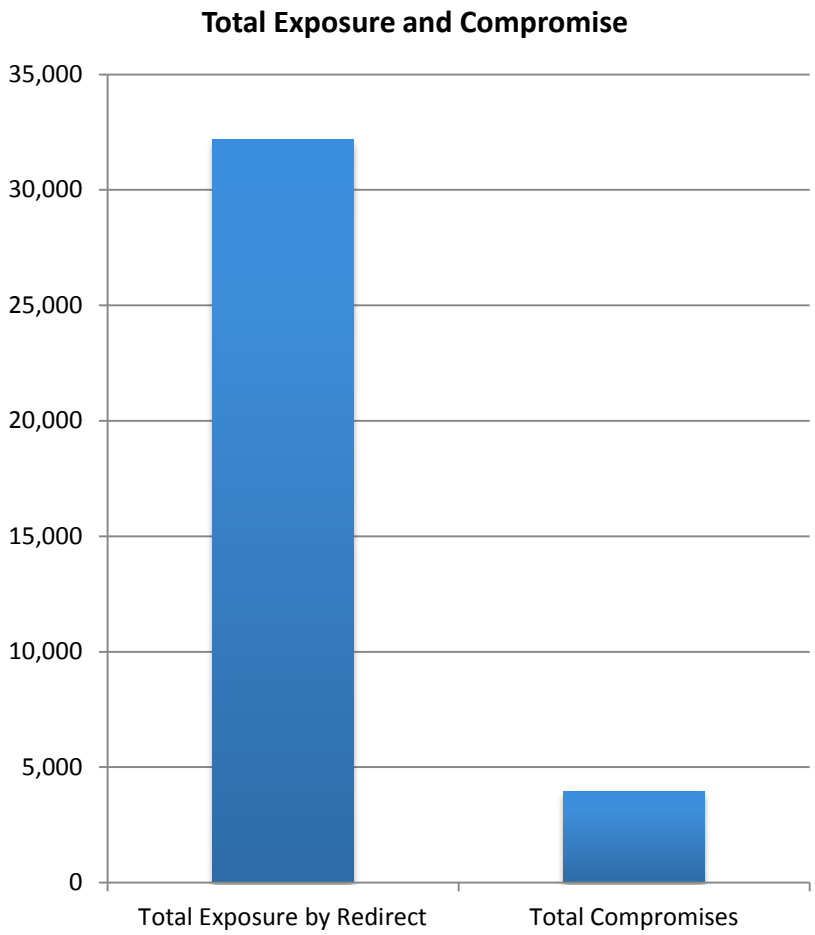
- VOHO
  - Discovered July 2012 by RSA FirstWatch
  - No aliases
- Multistage Campaign
  - Multiple stages
  - Redirection
    - Heavy dependency on JavaScript on two specific domains for majority of promulgation
- Leverages “Water Hole” technique heavily
  - TOO → TOI → Compromise → Exploitation → Enumeration → Exfiltration → Promulgation

- VOHO Campaign focused heavily on:
  - Geopolitical targets (especially useful in redirection / promulgation to exploit sites)
  - Defense Industrial Base (DIB)
  - High concentrations of activity noted from a geointelligence perspective in:
    - Boston, Massachusetts
    - Washington, D.C and NOVA
    - Northeastern New Jersey and New York City

Understanding VOHO

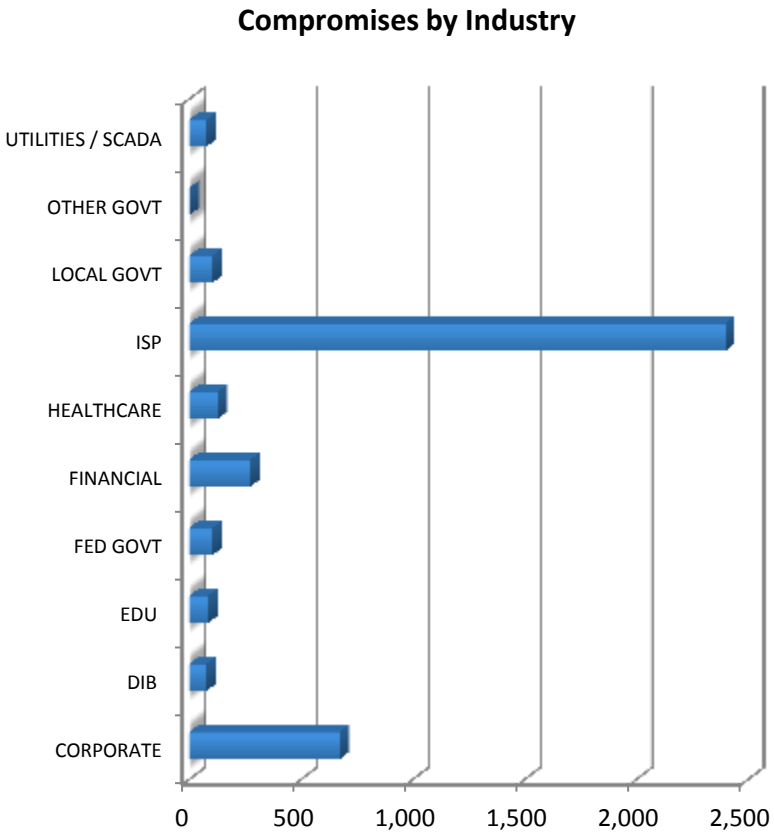


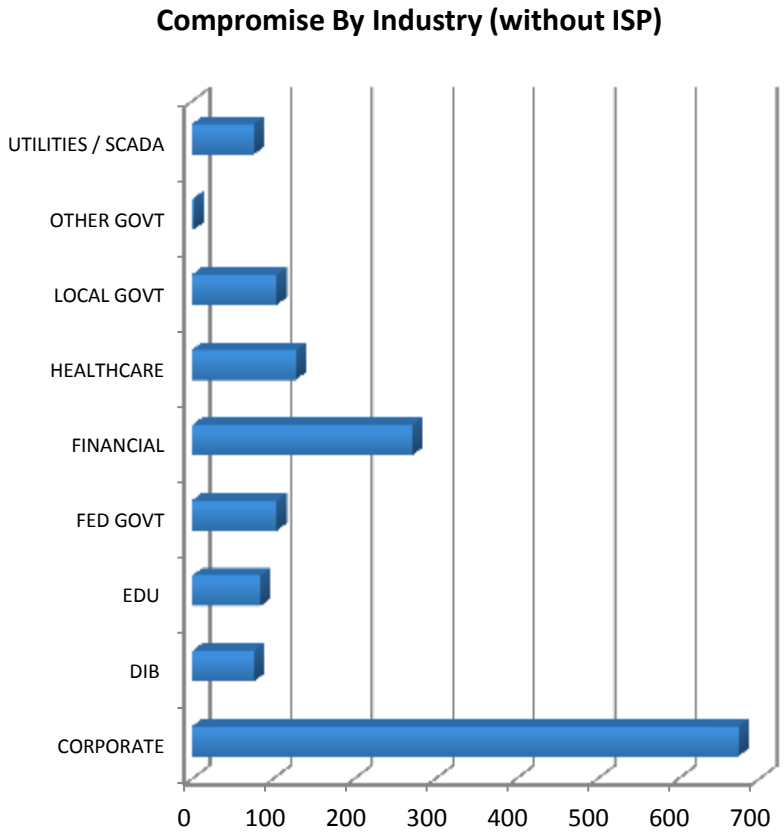
Casting a Vast Net



- Total of 32,160 unique hosts
- Representing 731 unique global organizations
- Redirected from compromised web servers injected with the redirect iframe to the exploit server
- Of these redirects, 3,934 hosts or 12% were seen to download the exploit CAB and JAR files (indicating a successful exploit/compromise of the visiting host)
- Based on our previous understanding of exploit campaigns, indicates a very successful campaign.

Join the Club…



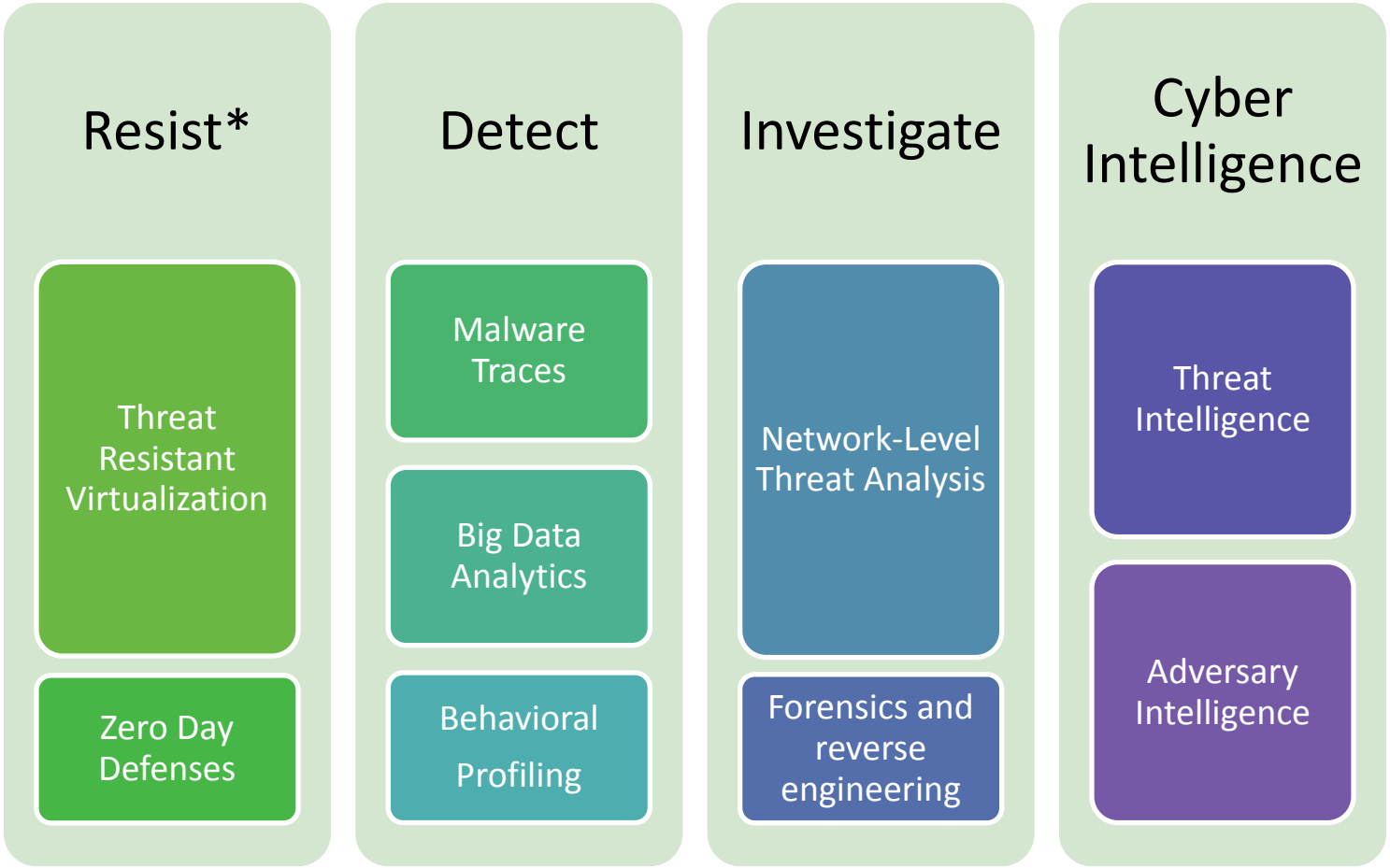


They’re inside… Do you have the right Cyber Intelligence?

OK, So You Were Hacked…Well, Join the Club

- So you got hacked, pwn3d, infiltrated, embarrassed, etc….
  - It happens in spite of all your hard work – that's why you need to reinvest
  - If it hasn't, it will
  - Learn from the event
  - Honest evaluation of faults and gaps should result in improvement

A New Defense Doctrine

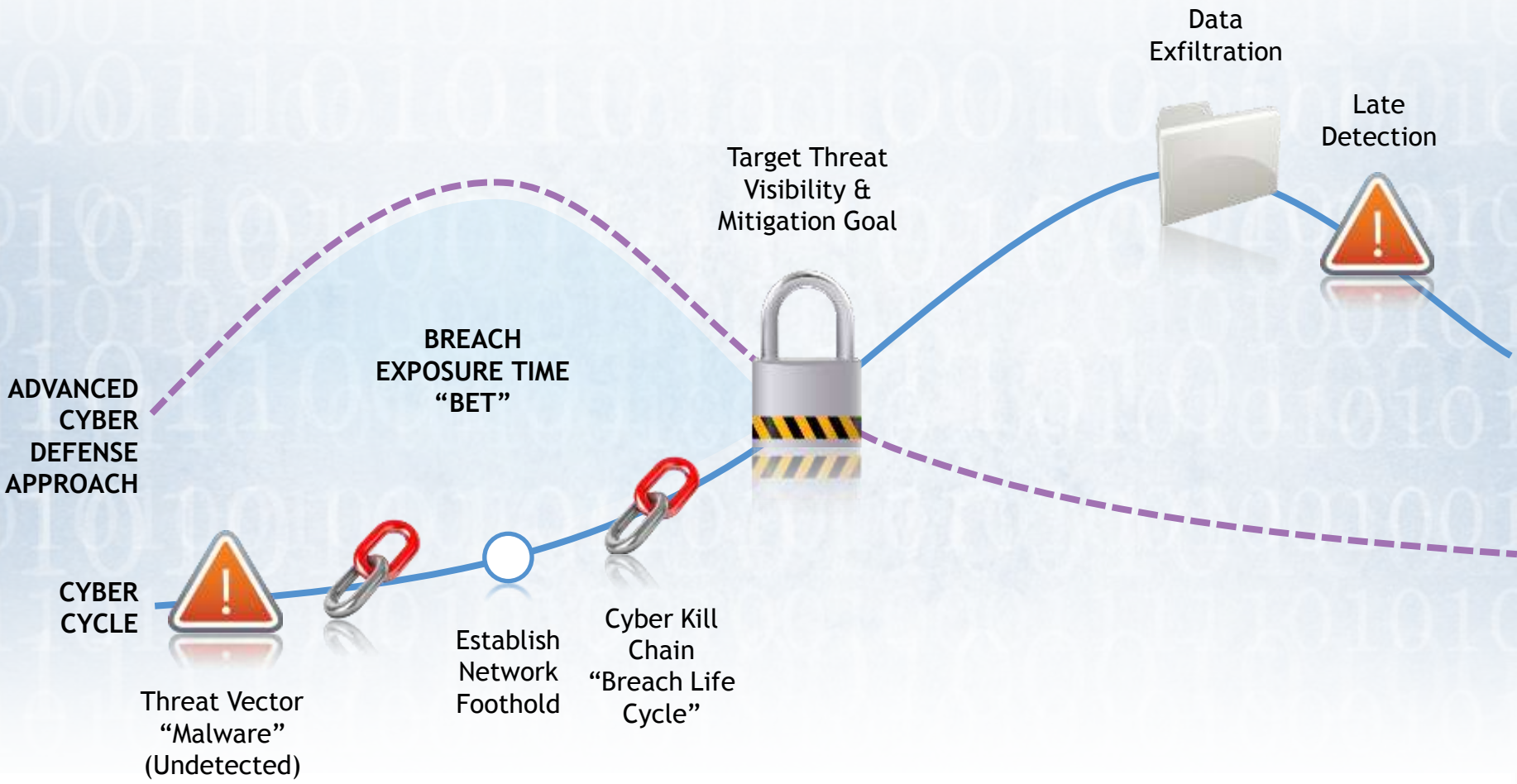


* You *will* fail to prevent

You Need Cyber Intelligence – What Is It?

- Intelligence: The collection of information of military, economic and/or political value by nation state and/or other criminal actors.
- Counter-intelligence: efforts made by organizations to prevent cyber threat actors from successfully gathering and collecting intelligence against them for the purposes of targeted cyber attack

Attack Kill Chain Life Cycle



Basic Requirements - External Visibility

- Do I have external resources where I can go for intelligence?
  - Industry / Sector Working Groups
  - Government
  - Vendor (“pay per view”) Intelligence
  - Trusted Friends and Colleagues
- Can I quickly access this information?
  - Machine readable format
  - Database, text files, XML, wiki, whatever works!

Basic Requirements – Internal Visibility

- Do I have visibility in the places where it's needed?
  - Allowed Paths (HTTP, DNS, Email, etc.)
  - Critical / Sensitive Enclaves (Where are my "crown jewels"?)
- Do I have other sources of information besides logs?
  - What is the universe of internal data that is relevant to the security problem
  - Logs, full packet, asset, what else?

Using Intelligence Against the APT

- You must have access to same data as the APT
  - Friendly targeting vectors
  - Resources
  - Social networking profiles
- Cannot defend against the APT without building intelligence on them
  - Lines of communication (IRC channels, Bulletin Boards)
  - Logistics and supply chain (networking, encryption, Virus Total, etc.)

Beginning the Incident Analysis

- Can you connect the dots? Do you have the right tools and skills?
- You can never have enough data and analytics (logs, full packet, memory, etc..)
- Do you have anything conclusive that would be useful in establishing an attribution chain?
  - Compromises and threat actors have attributes unique to them
  - Have you identified anything that coincides with or ties to a known profile or indicator?
  - Do you have enough information from one or more systems and / or network elements to establish a pattern?
  - Telemetry? Geographic Intelligence?
  - Malware, lateral movement, etc..
- Once they're in, you have to be the hunter vs. the hunted

Adversary Campaign Analysis

- Malicious Code and Content Analysis
  - Vulnerability analysis
  - What's required (vulnerability) for the malicious code to execute and succeed in its goals?
- Observing the behavior of the malware in virtual machines and bare metal environments
- Do the attributes noted with the malware align with or match those seen in other campaigns?
- Is it part of a multi-stage campaign?
- How do the samples relate to the network telemetry?
  - C2
  - Pivot sites
  - Covert channels
- Botnet related?
- Other indicators?

The Path to Everything Flows Through NET…

- The Microsoft Windows Networking protocols support a large variety of lateral movement possibilities
- "Net" Commands
- With compromised credentials, authenticated access to most resources is trivial

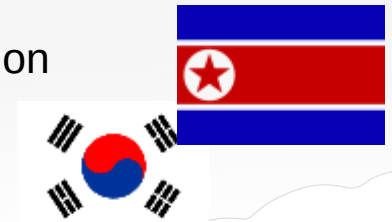
```
Net Use \\DomainControllerHost1 "complexpassword" /u:CORPDomain\DomAdmin.Account1
Net User Domdmin.Account1 /domain
Net Group "domain controllers" / domain
Net Group "domain admins" / domain
Net Time \\DomainControllerHost1 (Used in conjunction with the At command)
Net View \\DomainControllerHost1
Net View /domain | find "supersecrethost"
```

- Be on the lookout for scripts, PowerShell and WMIC (extremely powerful)

Attribution? Not So Simple…

Network Solutions' Back Online Following DDOS Attacks

North Korea in Attacks on South Korean Sites



LulzSec, Anonymous, Green rights,

Anonymous Hacks Murdoch's Sun Web Site

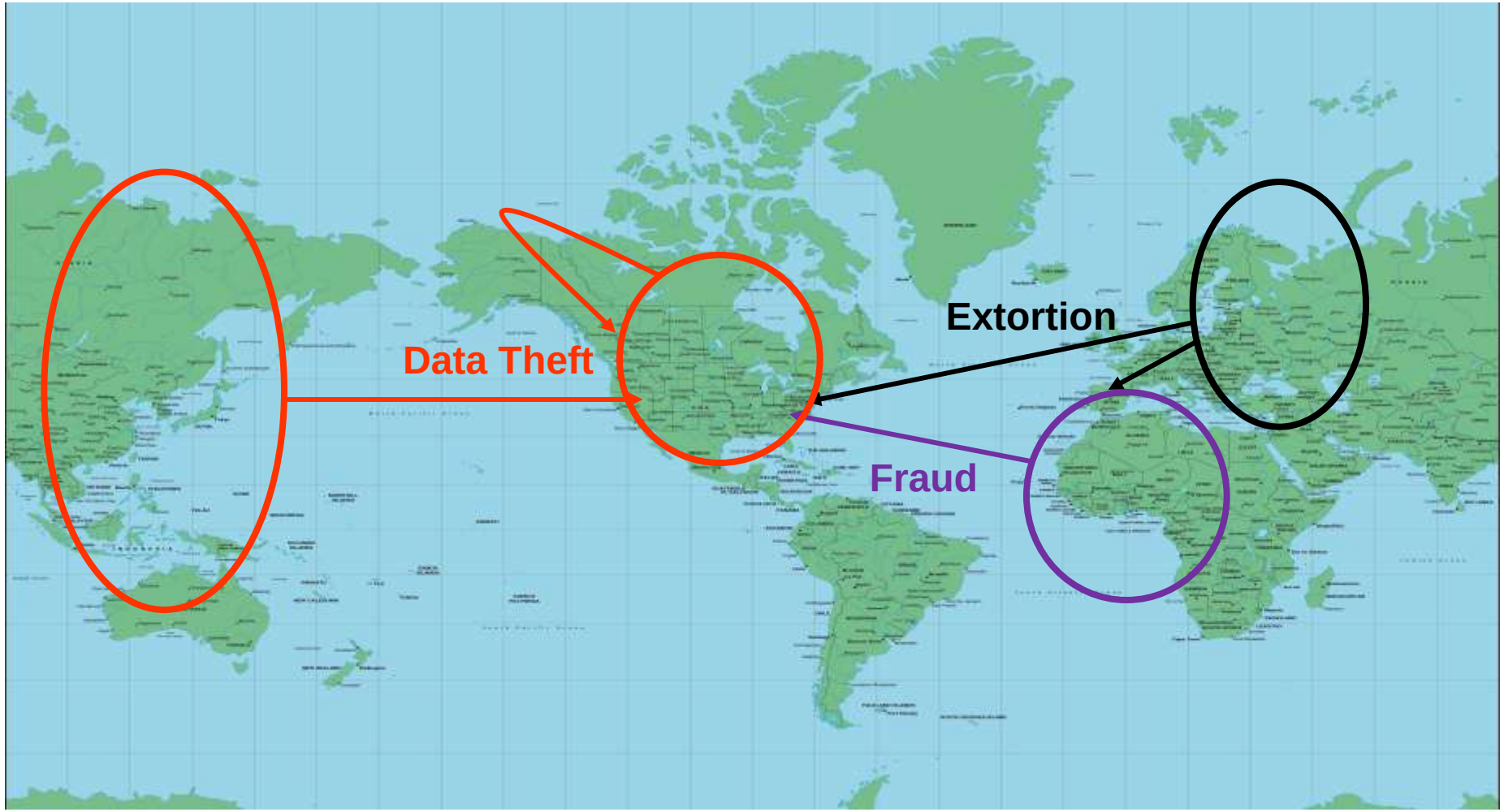
Romanian Duo Hacks MySql.com

DDoS attack strikes UltraDNS, affects Amazon, Wal-Mart[2]

Head of Russian Payment Processor ChronoPay Arrested

Blended Attacks

Advanced Threats



Exposing Lateral Movement with NetWitness

```
<token name="at" value="a&#x00;t&#x00;s&#x00;v&#x00;c&#x00;"/>
<token name="at" value="\PIPE\atsvc" />
```

- Learn how Windows talks to Windows (SMB, RPC, NetBIOS, etc.)
- Examples
  - Discovering Use of the Task Scheduler
  - Enumerating Named Pipes
- Follow Up on the NetWitness Community

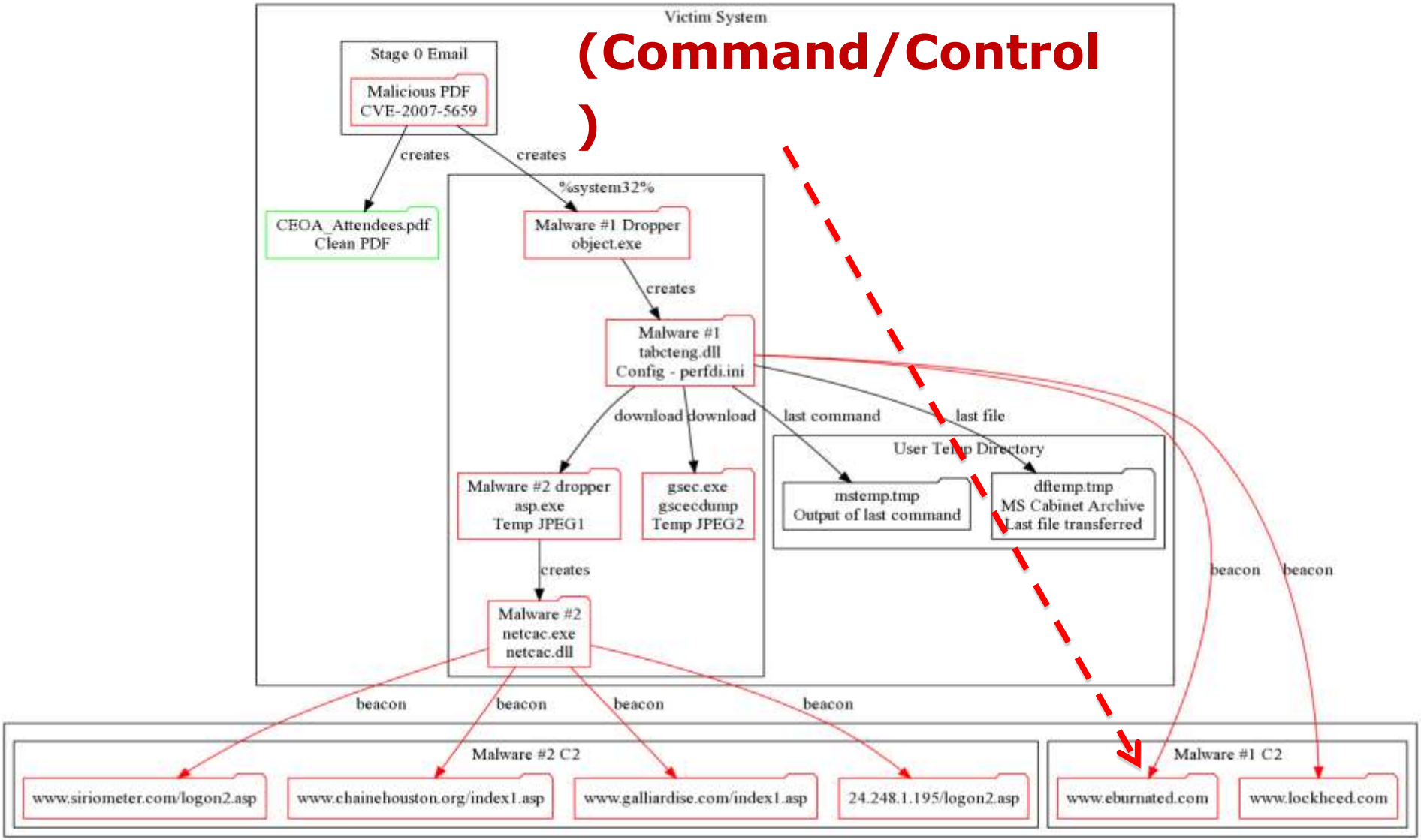
Getting the goods out - Obfuscated Exfiltration Commands

- WinRAR command line executable is renamed and does not even have a .exe extension, yet it runs just fine

```
temp.hlp a sec.bin "\\10.113.190.53\c$\security
log.csv" -hp1234!@#$qw
```

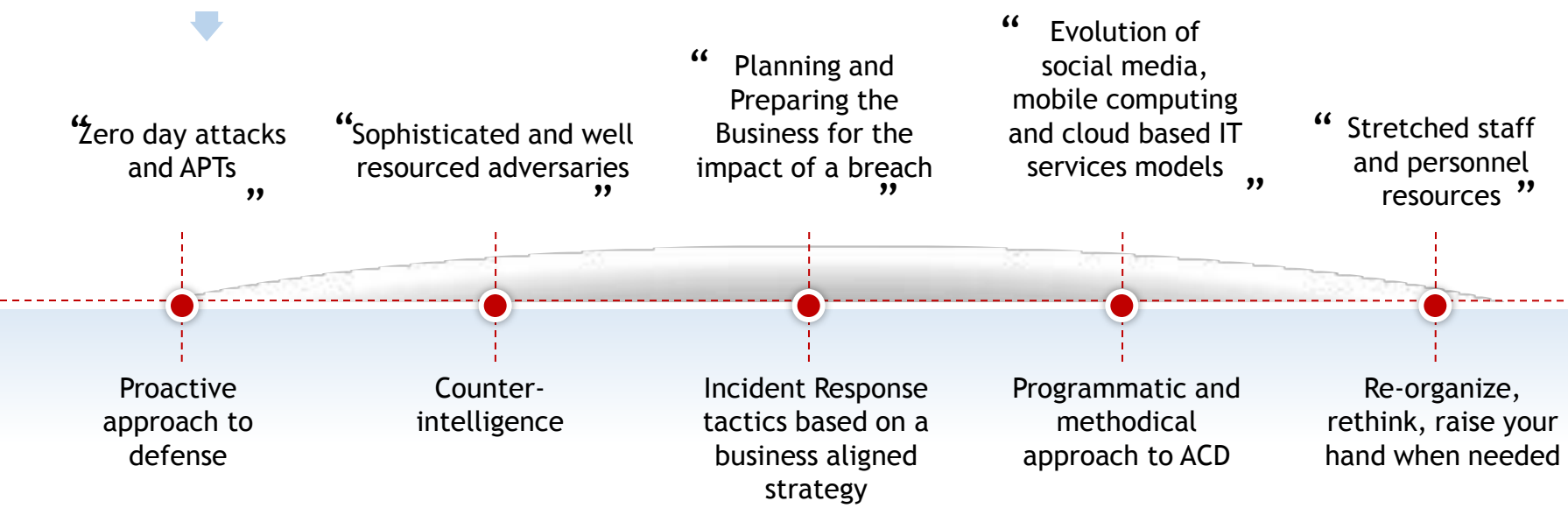
- No .rar file extension (.bin)
- Exfil file is created across the network via (Windows Protocols)
- Password creation methodology for Exfil files uses –hp switch for header encryption
  - Using -hp switch is actually a weakness
  - Can determine number of files in archive statically based on same salt
- Lazy one-handed left-to-right up-down naming conventions for passwords

Know Your Malware



Putting the Right Response Together

CHALLENGE



SOLUTION

A cyber defense strategy aligned with business objectives using cyber intelligence for a predictive approach to security

Recommendations

- Assume you are breached on a daily basis and focus on adversaries, TTPs and their targets
- Develop architecture and tools for internal and external intelligence for real-time and post-facto visibility into threats
- Understand current state of malware, attack trends, scenarios, and communications
- Adjust security team skills and incident management work flow
- Repeat and rinse

Apply Slide

- Within 3 months:
  - Evaluate your defense posture against APTs
    - Do you have access to relevant Cyber Intelligence?
    - Is your IT security framework geared towards APTs? You need to look at:
      - *Resistance*: do you use virtualization, sandboxing and other techniques to make sure sensitive applications are not run directly from Internet-connected devices?
      - *Detection*: what sort of detection capabilities do you have against advanced threats? Are you focused on looking for anomalies inside the network vs. attempting to prevent intrusion using perimeter security?
      - *Response*: if an advanced intrusion occurs, do you have fast, effective incident response tools and know-how?
  - Evaluate your exposure to random intrusions (data stealing Trojans)
    - Score your organization on: employee awareness, self-update patching, use of unmanaged devices
  - Look at the recommendations slide…

THANK YOU

Eddie Schwartz
eddie.schwartz@rsa.com
@eddieschwartz
community.emc.com/go/netwitness

Uri Rivner
Uri.rivner@biocatch.com
finextra.com/community/blogs.aspx?MemberID=39696