Verisign® iDefense®
Cyber Security Trends

Rick Howard, iDefense General Manager
June 22, 2011
How Technical Are You?
Agenda

Operation Aurora Impact

Stuxnet Impact

Cyber Security Disruptors
Learning Points

Game Changer

Theory Fact

Data Loss Prevention Systems

Critical Infrastructure
Operation Aurora Impact
The Aurora Attacks – 5 Unprecedented Changes
The Aurora Attacks – 5 Unprecedented Changes
The Aurora Attacks – 5 Unprecedented Changes
The Aurora Attacks – 5 Unprecedented Changes
The Aurora Attacks – 5 Unprecedented Changes
The Aurora Attacks – 5 Unprecedented Changes

Moonlight Maze

Titan Rain

Operation Aurora

German Chancellor
Angela Merkel

US Sec of State
Mrs. Hillary Clinton
"We have been briefed by Google on these allegations, which raise very serious concerns and questions," she said. **We look to the Chinese government for an explanation.**

Source: Network World: 13 Jan 2010

"We look to Chinese authorities to conduct a thorough investigation of the cyber intrusions that led Google to make this announcement. We also look for that investigation and its results to be transparent."


"It was a very open and candid conversation. We agreed we would continue this conversation in the context of our ongoing dialogue."

Source: France 24: 28 Jan 2010

---

The Aurora Attacks – 5 Unprecedented Changes

---

Foreign Minister Yang Jiechi
The Aurora Attacks – 5 Unprecedented Changes
The Aurora Attacks – 5 Unprecedented Changes
The Aurora Attacks – 5 Unprecedented Changes

$100,000,000

Vulnerability Assessment

Capabilities Research

Critical Infrastructure

Raytheon

Operation Aurora

Perfect Citizen
The Aurora Attacks – 5 Unprecedented Changes
The Aurora Attacks – 5 Unprecedented Changes

Moonlight Maze
Byzantine Hades
Titan Rain

Operation Aurora
The Aurora Attacks – 5 Unprecedented Changes
The Aurora Attacks – 5 Unprecedented Changes
The Aurora Attacks – 5 Unprecedented Changes

CONFIDENCE IS HIGH

Is Hard …
But not Impossible

Operation Aurora
The Aurora Attacks – 5 Unprecedented Changes

CONFIDENCE IS HIGH

Is Hard …

But not Impossible

Operation Aurora
The Aurora Attacks – 5 Unprecedented Changes

1. Public Disclosure
2. Game Changer
3. NSA
4. Perfect Citizen
5. Operation Aurora

Cyber Espionage
Stuxnet Impact
The Stuxnet Attacks

Siemens
Industrial Control Systems (ICS)

Supervisory Control and Data Acquisition

Source: Vanity Fair Apr 2011
The Stuxnet Attacks

Source: Vanity Fair Apr 2011
The Stuxnet Attacks

Data from W 32.Stuxnet Dossier

Natanz Nuclear site
Stuxnet Timeline

Source: ISIS Feb 15 2011

2008

2009

First Strike

2010

2011
Stuxnet Timeline

P1 centrifuges at Natanz

Iranian President Mahmoud Ahmadinejad

Originally published by EurasiaNet.org: 2008

1000 Centrifuges Dismantled

Stuxnet Timeline

1000 Centrifuges Dismantled

2 Attacks

2008 2009 2010 2011

The Stuxnet Attacks

Speculation

Theory

Proof of Concept

2007

2008
The Stuxnet Attacks

Speculation

Theory

Proof of Concept

2007
The Stuxnet Attacks

Sophisticated

Real

Compared to What?
The Stuxnet Attacks – Why Sophisticated?

Well Financed

$400K – $1.5 Mil
The Stuxnet Attacks – Why Sophisticated?

Driver Signing
The Stuxnet Attacks – Why Sophisticated?

Realtek Semiconductor Corp. (瑞昱半導體股份有限公司)  
JMicron (智微有限公司)  
Innovation Road, Hsinchu Science Park, Hsinchu, Taiwan
The Stuxnet Attacks – Why Sophisticated?
The Stuxnet Attacks – Why Sophisticated?

New Trend in 2010
The Stuxnet Attacks – Why Sophisticated?

Enriched

Centrifuge

807 Hz and 1210 Hz

90%

SIEMENS

Industrial Control Systems (ICS)
The Stuxnet Attacks – Why Sophisticated?

Industrial Control Systems (ICS)

807 Hz and 1210 Hz

1400 Hz

Centrifuge

2 Hz

P1 Centrifuges at Natanz

Iranian President Mahmoud Ahmadinejad

Originally published by EurasiaNet.org: 2008

SIEMENS
The Stuxnet Attacks – Why Sophisticated?

1. Zero-Day Exploit
2. Driver Signing
3. Stuxnet

Sophisticated
Stuxnet Timeline

**SIEMENS**
Industrial Control Systems (ICS)

Supervisory Control and Data Acquisition

Source: Vanity Fair Apr 2011
Stuxnet Timeline

Source: Vanity Fair Apr 2011
Stuxnet Timeline

Source: Costin Raiu - Kaspersky, July 2010

Source: Vanity Fair Apr 2011
Stuxnet Timeline

Supervisory Control and Data Acquisition
Stuxnet Timeline

Source: Secure List Jul 21 2010
Stuxnet Timeline

30,000 Iranian Computers infected

½ of all Centrifuges are idle

Source: Washington Post Sep 28 2010
Source: The Economist Sep 2010
Stuxnet Timeline

2008 | 2009 | 2010 | 2011

Enriched

Source: NTI Nov 23 2010
Stuxnet Timeline

Enriched

Source: NTI Nov 23 2010
Stuxnet Timeline

Assassinated

Source: Crethi Plethi Blog

Assassination Attempt

Source: CNN

Dr. Majid Shahryari

Dr. Fereidun Abbasi

Source: NYT Nov 29 2010
Stuxnet Campaign

2008
Stuxnet Campaign Planning

2009
Stuxnet First Strike

2010
Stuxnet Second Strike

Public Discovery
Realtek Certificate Revoked

J Micron Certificate Revoked

Natanz Taken Offline
Natanz Back Online

Stuxnet J Micron Certificate Installed
DDOS Attack against SCADA Forums

Iranian Scientists Killed and Wounded

1000 Centrifuges Destroyed
Stuxnet Assessment

Nuclear Program Delayed until 2015

No Affect
The Stuxnet Attacks – What about Them?

Sophisticated

Driver Signing

Theory  Fact

Not

Not

REFRESHING

SCADA ATTACK

Stuxnet

ROOTKITS

Centrifuge

1 1 2 3

CYBER WARFARE

SCADA ATTACK
Cyber Security Disruptors
What is a Cyber Security Disruptor?

1997

Clayton Christensen

Theory

E=mc²
What is a Cyber Security Disruptor?

Clayton Christensen

Innovation

Business Failure
What is a Cyber Security Disruptor?
What is a Cyber Security Disruptor?

Innovation

Momentum
What is a Cyber Security Disruptor?
What is a Cyber Security Disruptor?
What is a Cyber Security Disruptor?
What is a Cyber Security Disruptor?

The Little Tramp

Clayton Christensen
What is a Cyber Security Disruptor?
What is a Cyber Security Disruptor?
What is a Cyber Security Disruptor?

Clayton Christensen

Shugart Associates
Micropolis
Priam
Quantum
What is a Cyber Security Disruptor?

Clayton Christensen

Micropolis
What is a Cyber Security Disruptor?

Clayton Christensen

Innovation
What is a Cyber Security Disruptor?
10 Cyber Security Disruptors

- DNSSEC
- IPv6
- Mobile Platform
- SCADA Attack
- Cloud Computing
- APT
- Developing Nations
- Cyber Terrorism
- Metaverse
- Top-Level Domain Extensions
- Internationalized Domains
- Application Store
Cyber Security Disruptor

Concept

Impact

Enterprise
Cyber Security Disruptor
## Cyber Security Disruptors Timeline

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Best Practices</th>
<th>Early Adopters</th>
<th>Predictions</th>
<th>Disruptors</th>
</tr>
</thead>
</table>

**Today**
Cyber Security Disruptors Timeline
Cyber Security Disruptors Timeline

Early Adopters  Predictions  Distruptors

Prime Time
Cyber Security Disruptors Review
**Disruptor: TLDS & IDNS**

**2010**

- **Concept**: Top-Level Domain Extensions + Internationalized Domains
- **Impact**: Blacklists become unmanageable at the Enterprise level

**2015**
IP Management just became very complex
Disruptors: APT

Intellectual Property is seriously at risk.
Cyber Security Disruptors Early Adopters


Best Practices | Early Adopters | Predictions | Disruptors

Today

MOBILE PLATFORM | ADVANCED PERSISTENT THREAT | APPLICATION STORE | TOP-LEVEL DOMAIN EXTENSIONS | INTERNATIONALIZED DOMAINS | METAVERSE
Cyber Security Disruptor
Conclusion

Operation Aurora Impact

Stuxnet Impact

Wikileaks Impact

Cyber Security Disruptors
Recap

Malware Analyst’s Cookbook

Cyber Security Essentials

Cyber Fraud

2011 Cyber Threats and Trends