



## Advanced & Persistent Threat Analysis - II

Burak Ekici

ekcburak@hotmail.com

Department of Computer Engineering,  
Yaşar University,  
Turkey.

April 21, 2012

# Agenda

- 1 The Purpose
- 2 Cyberattack on F-35 Joint Strike Fighter Program
- 3 Titan Rain
- 4 CitiBank
- 5 Operation Aurora
- 6 Stuxnet
- 7 Summarization, Feedbacks & Questions

# The Purpose: Drawing Attention!!!

## Purpose

**Purpose of this presentation is examining the most well-known APTs performed against huge trade companies and some critical infrastructures.**

# Example I: Cyberattack on F-35 Joint Strike Fighter Program

## F-35 Joint Strike Fighter Lightning II Program

*The F-35 Lightning II Program (also known as the Joint Strike Fighter Program) is the U.S. Department of Defense's focal point for defining affordable next generation strike aircraft weapon systems for the Navy, Air Force, Marines, and other allies.*

*F-35 is the most affordable, lethal, supportable and survivable aircraft ever to be used by so many war-fighters across the globe manufactured by U.S. defence contractor Lockheed Martin and British defence and aerospace company BEA Systems.*

<http://www.jsf.mil/>

# Example I: Cyberattack on F-35 Joint Strike Fighter Program

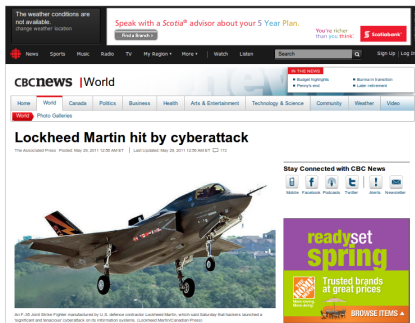
## F-35 Joint Strike Fighter Lightning II Program

*The F-35 Lightning II Program (also known as the Joint Strike Fighter Program) is the U.S. Department of Defense's focal point for defining affordable next generation strike aircraft weapon systems for the Navy, Air Force, Marines, and other allies.*

*F-35 is the most affordable, lethal, supportable and survivable aircraft ever to be used by so many war-fighters across the globe manufactured by U.S. defence contractor Lockheed Martin and British defence and aerospace company BEA Systems.*

<http://www.jsf.mil/>

# Example I: Cyberattack on F-35 Joint Strike Fighter Program



The screenshot shows the CBC News website interface. At the top, there are navigation links for News, Sports, Music, Radio, TV, My Region, and more. A search bar is visible. The main headline reads "Lockheed Martin hit by cyberattack" with a sub-headline "The Associated Press". Below the headline is a photograph of an F-35 Joint Strike Fighter in flight. To the right of the photo is a social media sharing section with icons for Twitter, Facebook, and YouTube. Below that is a "readyset spring" advertisement with the text "Trusted brands at great prices" and a "BROWSE ITEMS" button.

## F-35 Joint Strike Fighter Lightning II Program

*The **CBC News** announced, in 2009, that Hackers launched a "**significant and tenacious**" cyberattack on Lockheed Martin, a major U.S. defence contractor holding highly sensitive information, but its secrets remained safe.*

# Example I: Cyberattack on F-35 Joint Strike Fighter Program

The screenshot shows the top portion of a news website. At the top, there is a dark blue navigation bar with the text "THE AUSTRALIAN" on the left, and "LOGIN", "SIGN UP", "NEWS.COM.AU", "FOX SPORTS", "CAREERS", "CARSGUIDE", "REALESTATE", and "NEWS NETWORK" on the right. Below this is a large "NEWS" logo with a map of Australia. A secondary navigation bar contains categories like "NEWS", "OPINION", "NATIONAL AFFAIRS", "BUSINESS", "AUS IT", "HIGHER ED", "MEDIA", "SPORT", "ARTS", "MAGAZINES", and "CAREERS". Below that is a "BREAKING NEWS" section with links to "THE NATION", "THE WORLD", "FEATURES", "IN-DEPTH", "GALLERIES", "INVESTIGATIONS", "FOI", "HEALTH & SCIENCE", and "WEATHER". The main article area features a "THE TIMES LK" logo, a "0 tweets" button, a "Recommend" button, and font size controls. The article title is "Security experts admit China stole secret fighter jet plans". The byline is "The Australian March 12, 2012 12:00AM". The lead text reads: "CHINESE spies hacked into computers belonging to BAE Systems, Britain's biggest defence company, to steal details about the design, performance and electronic systems of the West's latest fighter jet, senior security figures have disclosed." To the right of the article is a sidebar with a profile picture of Henry Ergas and a quote: "Labor will remain between a pretense of democratic participation and a practice that reeks of its opposite".

THE AUSTRALIAN LOGIN SIGN UP NEWS.COM.AU FOX SPORTS CAREERS CARSGUIDE REALESTATE NEWS NETWORK

NEWS

NEWS OPINION NATIONAL AFFAIRS BUSINESS AUS IT HIGHER ED MEDIA SPORT ARTS MAGAZINES CAREERS

BREAKING NEWS THE NATION THE WORLD FEATURES IN-DEPTH GALLERIES INVESTIGATIONS FOI HEALTH & SCIENCE WEATHER

THE TIMES LK 0 tweets Recommend A+ A-

## Security experts admit China stole secret fighter jet plans

The Australian March 12, 2012 12:00AM

CHINESE spies hacked into computers belonging to BAE Systems, Britain's biggest defence company, to steal details about the design, performance and electronic systems of the West's latest fighter jet, senior security figures have disclosed.

HENRY ERGAS  
'Labor will remain between a pretense of democratic participation and a practice that reeks of its opposite'

## F-35 Joint Strike Fighter Lightning II Program

*The Australian* has announced, in March 2012, that: *China hacked BAE Systems to steal performance information on the F-35.*

# Example I: Cyberattack on F-35 Joint Strike Fighter Program

## Quotations from The Australian

*"Chinese spies hacked into computers belonging to BAE Systems, Britain's biggest defence company, to steal details about the design, performance and electronic systems of the West's latest fighter jet, senior security figures have disclosed."*

*"The Chinese exploited vulnerabilities in BAE's computer defences to steal vast amounts of data on the \$300 billion F-35 Joint Strike Fighter, a multinational project to create a plane that will give the West air supremacy for years to come, according to the sources."*



# Example I: Cyberattack on F-35 Joint Strike Fighter Program

## Quotations from The Australian

*"Chinese spies hacked into computers belonging to BAE Systems, Britain's biggest defence company, to steal details about the design, performance and electronic systems of the West's latest fighter jet, senior security figures have disclosed."*

*"The Chinese exploited vulnerabilities in BAE's computer defences to steal vast amounts of data on the \$300 billion F-35 Joint Strike Fighter, a multinational project to create a plane that will give the West air supremacy for years to come, according to the sources."*

# Example I: Cyberattack on F-35 Joint Strike Fighter Program

## Quotations from The Australian

*"Details of the attack on BAE have been a closely guarded secret within Britain's intelligence community since it was first uncovered nearly three years ago. **But they were disclosed by a senior BAE executive during a private dinner in London for cyber security experts late last year.**"*

*The BAE man said that for 18 months, Chinese cyber attacks had taken place against **BAE and had managed to get hold of plans of one of its latest fighters.***

*"A former U.S. official said the BAE Systems element of the **JSF program had "almost certainly" been penetrated.**"*

# Example I: Cyberattack on F-35 Joint Strike Fighter Program

## Quotations from The Australian

*"Details of the attack on BAE have been a closely guarded secret within Britain's intelligence community since it was first uncovered nearly three years ago. **But they were disclosed by a senior BAE executive during a private dinner in London for cyber security experts late last year.**"*

*The BAE man said that for 18 months, Chinese cyber attacks had taken place against **BAE and had managed to get hold of plans of one of its latest fighters.***

*"A former U.S. official said the BAE Systems element of the **JSF program had "almost certainly" been penetrated.**"*

# Example I: Cyberattack on F-35 Joint Strike Fighter Program

## Quotations from The Australian

*"Details of the attack on BAE have been a closely guarded secret within Britain's intelligence community since it was first uncovered nearly three years ago. **But they were disclosed by a senior BAE executive during a private dinner in London for cyber security experts late last year.**"*

*The BAE man said that for 18 months, Chinese cyber attacks had taken place against **BAE and had managed to get hold of plans of one of its latest fighters.***

*"A former U.S. official said the BAE Systems element of the **JSF program had "almost certainly" been penetrated.**"*

# Example I: Cyberattack on F-35 Joint Strike Fighter Program

## Quotations from The Australian

*The Chinese embassy in London described the claims as a “baseless allegation”.*

## Results of the Attack

The attack, defense and (if there is) counter-attack strategies were kept **SECRET!!!**

# Example I: Cyberattack on F-35 Joint Strike Fighter Program

## Quotations from The Australian

*The Chinese embassy in London described the claims as a “baseless allegation”.*

## Results of the Attack

The attack, defense and (if there is) counter-attack strategies were kept SECRET!!!

# Example I: Cyberattack on F-35 Joint Strike Fighter Program

## Quotations from The Australian

*The Chinese embassy in London described the claims as a “baseless allegation”.*

## Results of the Attack

**The attack, defense and (if there is) counter-attack strategies were kept SECRET!!!**

## Example II: Titan Rain

### Definition: Titan Rain

*Titan Rain* was the designation given by the federal government of the United States to **a series of coordinated attacks on American computer systems since 2003.**

The attacks were labeled as *Chinese in origin*, although their precise nature and aim is not known for sure; it is predicted as *state-sponsored espionage, corporate espionage, or random hacker attacks.*

Due to masking their real identities by *proxies and zombie computers*; they *remain unknown.*

The activity known as "Titan Rain" is believed to be *associated with an Advanced Persistent Threat.*

[http://en.wikipedia.org/wiki/Titan\\_Rain](http://en.wikipedia.org/wiki/Titan_Rain)



## Example II: Titan Rain

### Definition: Titan Rain

*Titan Rain* was the designation given by the federal government of the United States to **a series of coordinated attacks on American computer systems since 2003.**

The attacks were labeled as **Chinese in origin**, although their precise nature and aim is not known for sure; it is predicted as **state-sponsored espionage, corporate espionage, or random hacker attacks.**

Due to masking their real identities by **proxies and zombie computers**; they remain unknown.

The activity known as "Titan Rain" is believed to be **associated with an Advanced Persistent Threat.**

[http://en.wikipedia.org/wiki/Titan\\_Rain](http://en.wikipedia.org/wiki/Titan_Rain)

## Example II: Titan Rain

### Definition: Titan Rain

*Titan Rain* was the designation given by the federal government of the United States to **a series of coordinated attacks on American computer systems since 2003.**

The attacks were labeled as **Chinese in origin**, although their precise nature and aim is not known for sure; it is predicted as **state-sponsored espionage, corporate espionage, or random hacker attacks.**

Due to masking their real identities by **proxies and zombie computers; they remain unknown.**

The activity known as "Titan Rain" is believed to be **associated with an Advanced Persistent Threat.**

[http://en.wikipedia.org/wiki/Titan\\_Rain](http://en.wikipedia.org/wiki/Titan_Rain)

## Example II: Titan Rain

### Definition: Titan Rain

*Titan Rain* was the designation given by the federal government of the United States to **a series of coordinated attacks on American computer systems since 2003.**

The attacks were labeled as **Chinese in origin**, although their precise nature and aim is not known for sure; it is predicted as **state-sponsored espionage, corporate espionage, or random hacker attacks.**

Due to masking their real identities by **proxies and zombie computers; they remain unknown.**

The activity known as "Titan Rain" is believed to be **associated with an Advanced Persistent Threat.**

[http://en.wikipedia.org/wiki/Titan\\_Rain](http://en.wikipedia.org/wiki/Titan_Rain)

## Example II: Titan Rain

### The (Indefinite) Aim: Cyber Espionage

*Espionage or spying* involves a government or individual *obtaining information that is considered secret or confidential without the permission of the holder of the information.*

- 1 *Governmental Espionage: Governmental or Military issues.*
- 2 *Corporate Espionage: Industrial issues*

*Cyber Espionage or spying is a specific type of espionage performed on the Internet, networks or individual computers through the use of cracking techniques and malicious software including Trojan horses and spyware.*

<http://en.wikipedia.org/wiki/Espionage>

## Example II: Titan Rain

### The (Indefinite) Aim: Cyber Espionage

*Espionage or spying* involves a government or individual *obtaining information that is considered secret or confidential without the permission of the holder of the information.*

- 1 *Governmental Espionage*: Governmental or Military issues.
- 2 *Corporate Espionage*: Industrial issues

*Cyber Espionage or spying* is a *specific type of espionage performed on the Internet, networks or individual computers through the use of cracking techniques and malicious software including Trojan horses and spyware.*

<http://en.wikipedia.org/wiki/Espionage>

# Example II: Titan Rain

the **guardian**

News | Sport | Comment | Culture | Business | Money | London 2012 | Life & style | Travel | Em

News > Technology

## Titan Rain - how Chinese hackers targeted Whitehall

· Foreign Office among departments hit  
· Military involvement suspected

Richard Norton-Taylor  
The Guardian, Wednesday 5 September 2007 03.06 BST  
[Article history](#)



Whitehall departments including the Foreign Office have suffered cyber attacks.  
Photograph: Sandy Stockwell/Corbis

Tweet 4  
Share 1  
reddit this

larger | smaller

**Technology**  
Internet · Cybercrime · Hacking

**Politics**  
Civil service

**More news**

**Related**

27 Jul 2005  
Hacker 'left note on US army computer'

1 Nov 2011  
China 'targeted 48 chemical and military companies in hacking attack'

20 Nov 2011  
Cyber-attack claims at US

## Titan Rain: U.K. Extension

*The Guardian* announced at 5<sup>th</sup> of September 2007 that **Chinese hackers**, some believed to be from the **People's Liberation Army**, have been attacking the computer networks of British government departments.

## Example II: Titan Rain

### Quotations from The Guardian

The attackers have hit *the network at the Foreign Office* as well as those in other key departments, according to Whitehall officials.

Security and defence officials are coy about what they know of specific attacks. However, they say *several Whitehall departments have fallen victim to China's cyberwarriors*. One expert described it as a "constant ongoing problem".

The U.S. gave the codename "Titan Rain" to the growing number of Chinese attacks, notably directed at the Pentagon but also hitting different U.S. departments and other government departments, over the past few years.

## Example II: Titan Rain

### Quotations from The Guardian

The attackers have hit *the network at the Foreign Office* as well as those in other key departments, according to Whitehall officials.

Security and defence officials are coy about what they know of specific attacks. However, they say *several Whitehall departments have fallen victim to China's cyberwarriors*. One expert described it as a "*constant ongoing problem*".

The U.S. gave the codename "*Titan Rain*" to the growing number of Chinese attacks, notably directed at the Pentagon but also hitting different U.S. departments and other government departments, over the past few years.



## Example II: Titan Rain

### Quotations from The Guardian

The attackers have hit *the network at the Foreign Office* as well as those in other key departments, according to Whitehall officials.

Security and defence officials are coy about what they know of specific attacks. However, they say *several Whitehall departments have fallen victim to China's cyberwarriors*. One expert described it as a "*constant ongoing problem*".

The U.S. gave the codename "*Titan Rain*" to the growing number of Chinese attacks, notably directed at the Pentagon but also hitting *different U.S. departments and other government departments*, over the past few years.

## Example II: Titan Rain

### Quotations from The Guardian

*Angela Merkel, Germany's prime minister, is reported to have raised the issue of Chinese attacks on her government's computers during a visit to Beijing. Officials here declined to say whether the British government had raised the issue with the Chinese authorities.*

*Alex Neill, China expert and head of the Asia Security Programme at the Royal United Services Institute (RUSI), said cyber attacks by the Chinese had been going on for at least four years. He described the reported attack on the Pentagon as the "most flagrant and brazen to date".*

### Results of the Attack

The technical details of the attack and defense strategies were kept  
**SECRET!!!**

## Example II: Titan Rain

### Quotations from The Guardian

*Angela Merkel, Germany's prime minister, is reported to have raised the issue of Chinese attacks on her government's computers during a visit to Beijing. Officials here declined to say whether the British government had raised the issue with the Chinese authorities.*

*Alex Neill, China expert and head of the Asia Security Programme at the Royal United Services Institute (RUSI), said cyber attacks by the Chinese had been going on for at least four years. He described the reported attack on the Pentagon as the "most flagrant and brazen to date".*

### Results of the Attack

The technical details of the attack and defense strategies were kept  
**SECRET!!!**

## Example II: Titan Rain

### Quotations from The Guardian

*Angela Merkel, Germany's prime minister, is reported to have raised the issue of Chinese attacks on her government's computers during a visit to Beijing. Officials here declined to say whether the British government had raised the issue with the Chinese authorities.*

*Alex Neill, China expert and head of the Asia Security Programme at the Royal United Services Institute (RUSI), said cyber attacks by the Chinese had been going on for at least four years. He described the reported attack on the Pentagon as the "most flagrant and brazen to date".*

### Results of the Attack

**The technical details of the attack and defense strategies were kept SECRET!!!**

## Example III: CitiBank

### Citigroup

*Citigroup Inc. or Citi is an American multinational financial services corporation headquartered in Manhattan, New York, United States.*

*Citigroup was formed from one of the world's largest mergers in history by combining the banking giant Citicorp and financial conglomerate Travelers Group on April 7, 1998. The year 2012 marks Citi's 200<sup>th</sup> anniversary.*

<http://en.wikipedia.org/wiki/Citigroup>

# Example III: CitiBank

The screenshot shows a Reuters news article. At the top, the Reuters logo and navigation menu are visible. Below the navigation is a banner for Cisco with the text "SEE HOW CISCO CLOUDVERSE ENABLES THE WORLD OF MANY CLOUDS". The article title is "Citi says 360,000 accounts hacked in May cyber attack". The article text includes a "citi" logo and a photo of people in a store. Social media sharing options for Twitter, LinkedIn, Facebook, Email, and Print are visible on the right. The article is by Maria Azean, Kalvin Soh, and New York/Khong Kong, dated Thu Jun 16, 2011 3:37am EDT.

## Citibank Cyberattack

*According to Reuters; Citigroup Inc. said a cyber attack in May 2009 affected almost twice as many accounts as the bank's figures had initially suggested.*

### Results of the Attack

- ▶ *A total of 360,083 North American Citigroup credit card accounts were affected.*
- ▶ *Of those affected, some 217,657 customers were reissued with new cards along with a notification letter, while the remaining accounts were either inactive or had already received new cards earlier, the bank added.*
- ▶ *According to Bloomberg News, about 3,400 customers lost \$2.7 million when their credit-card information was breached by online hackers.*

# Example IV: Operation Aurora

## Operation Aurora

*Description of the attack:* A zero-day vulnerability of the Windows Internet Explorer was used as an entry point for the APT to get sensitive information from, around, 20 companies including Adobe and Google .

*The vulnerabilities could allow remote code execution when a*

- ▶ *user views a specially crafted Web page using Internet Explorer*
- ▶ *user opens a legitimate HTML file that loads a specially crafted library file*

*An attacker who successfully exploited any of these vulnerabilities could gain the same user rights as the local user.*



# Example IV: Operation Aurora

## Operation Aurora

*Description of the attack:* A zero-day vulnerability of the Windows Internet Explorer was used as an entry point for the APT to get sensitive information from, around, 20 companies including Adobe and Google . The vulnerabilities could allow remote code execution when a

- ▶ user views a specially crafted Web page using Internet Explorer
- ▶ user opens a legitimate HTML file that loads a specially crafted library file

*An attacker who successfully exploited any of these vulnerabilities could gain the same user rights as the local user.*

## Example IV: Operation Aurora

### Operation Aurora

*Description of the attack:* A zero-day vulnerability of the Windows Internet Explorer was used as an entry point for the APT to get sensitive information from, around, 20 companies including Adobe and Google . The vulnerabilities could allow remote code execution when a

- ▶ user views a specially crafted Web page using Internet Explorer
- ▶ user opens a legitimate HTML file that loads a specially crafted library file

*An attacker who successfully exploited any of these vulnerabilities could gain the same user rights as the local user.*

# Example IV: Operation Aurora



## Operation Aurora

### ► *Step by Step Operation Aurora:*

- 1 A targeted user received a link in email or instant message from a "trusted" source.
- 2 The user clicked on the link which caused them to visit a website hosted in Taiwan that also contained a malicious JavaScript payload.
- 3 The user's browser downloaded and executed the malicious JavaScript, which included a zero-day Internet Explorer exploit.

# Example IV: Operation Aurora



## Operation Aurora

- *Step by Step Operation Aurora:*
- 1 A targeted user received a link in email or instant message from a "trusted" source.
  - 2 The user clicked on the link which caused them to visit a website hosted in Taiwan that also contained a malicious JavaScript payload.
  - 3 The user's browser downloaded and executed the malicious JavaScript, which included a zero-day Internet Explorer exploit.

# Example IV: Operation Aurora



## Operation Aurora

- *Step by Step Operation Aurora:*
- 1 A targeted user received a link in email or instant message from a “trusted” source.
  - 2 The user clicked on the link which caused them to visit a website hosted in Taiwan that also contained a malicious JavaScript payload.
  - 3 The user’s browser downloaded and executed the malicious JavaScript, which included a zero-day Internet Explorer exploit.

# Example IV: Operation Aurora



## Operation Aurora

- *Step by Step Operation Aurora:*
- 1 A targeted user received a link in email or instant message from a "trusted" source.
  - 2 The user clicked on the link which caused them to visit a website hosted in Taiwan that also contained a malicious JavaScript payload.
  - 3 The user's browser downloaded and executed the malicious JavaScript, which included a zero-day Internet Explorer exploit.

# Example IV: Operation Aurora

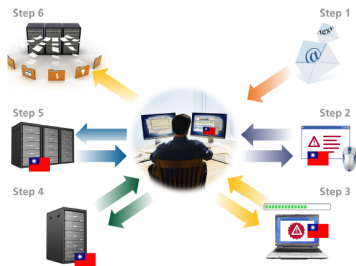


## Operation Aurora

### ► *Step by Step Operation Aurora:*

- 1 The exploit downloaded a binary disguised as an image from Taiwan servers and executed the malicious payload.
- 2 The payload set up a backdoor and connected to command and control servers in Taiwan.

# Example IV: Operation Aurora



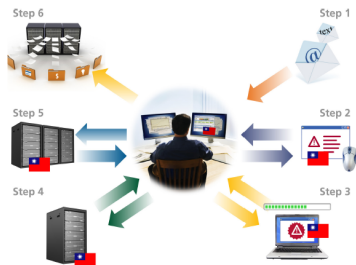
## Operation Aurora

### ► *Step by Step Operation Aurora:*

- 4 The exploit downloaded a binary disguised as an image from Taiwan servers and executed the malicious payload.
- 5 The payload set up a backdoor and connected to command and control servers in Taiwan.



# Example IV: Operation Aurora



## Operation Aurora

### ► *Step by Step Operation Aurora:*

- 4 The exploit downloaded a binary disguised as an image from Taiwan servers and executed the malicious payload.
- 5 The payload set up a backdoor and connected to command and control servers in Taiwan.

# Example IV: Operation Aurora



## Operation Aurora

### ► *Step by Step Operation Aurora:*

- As a result, attackers had complete access to internal systems. They targeted sources of intellectual property, including software configuration management (SCM) systems accessible by the compromised system. The compromised system could also be leveraged to further penetrate the network.

# Example IV: Operation Aurora



## Operation Aurora

### ► *Step by Step Operation Aurora:*

- 6 As a result, attackers had complete access to internal systems. They targeted sources of intellectual property, including software configuration management (SCM) systems accessible by the compromised system. The compromised system could also be leveraged to further penetrate the network.

# Example IV: Operation Aurora

## The “Operation Aurora” incident

- How Aurora operated:

- FW & IPS Failed** → • Attacks began in 2009 using a zero-day IE 6.0 vulnerability
- Web Gateway Failed** → • Lured users to click a link, directing them to a malicious Web site
- Antivirus Failed** → • Once system was compromised, a Trojan was installed
- FW & IDS Failed** → • Once installed, the Trojan would communicate with the command & control for variety of commands
- Antivirus Failed** → • New payloads would allow for further compromise of the companies systems

Figure: Operation Aurora Incident

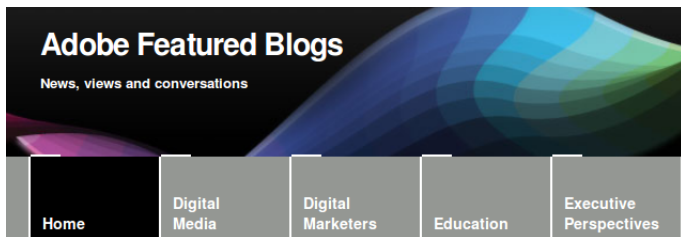
Source: Advanced Persistent Threats (September 30, 2010) by Ali Golshan

# Results of Operational Aurora: Comments of Hillary Clinton



The screenshot shows the U.S. Department of State website. At the top left is the Department of State seal. The main header reads "U.S. DEPARTMENT OF STATE" and "DIPLOMACY IN ACTION". A red navigation bar contains "SECRETARY CLINTON", "MEDIA CENTER", and "TRAVEL". Below this is a white navigation bar with links for "ABOUT STATE", "POLICY ISSUES", "COUNTRIES & REGIONS", "ECONOMICS & ENERGY", "ARMS CONTROL & SECURITY", "DEMOCRACY & GLOBAL AFFAIRS", and "PL &". The main content area has a blue background with a world map. The breadcrumb trail reads: "Home » Secretary of State Hillary Rodham Clinton » Secretary's Comments » 2010 Secretary Clinton's Remarks » Remarks by Secretary Clinton: January 2010 » Statement on Google Operations in China". The title of the page is "Statement on Google Operations in China" in red. Below the title is the name "Hillary Rodham Clinton", her title "Secretary of State", the location "Washington, DC", and the date "January 12, 2010". The text of the statement begins: "We have been briefed by Google on these allegations, which raise very serious concerns and questions. We look to the Chinese government for an explanation. The ability to operate with confidence in cyberspace is critical in a modern society and economy. I will be giving an address next week on the centrality of internet freedom in the 21st century, and we will have further comment on this matter as the facts become clear."

# Results of Operational Aurora: Official Statement by Adobe



## Adobe Investigates Corporate Network Security Issue

POSTED BY POOJA PRASAD ON [JANUARY 12, 2010 3:16 PM](#) IN [UNCATEGORIZED](#)

Adobe became aware on January 2, 2010 of a computer security incident involving a sophisticated, coordinated attack against corporate network systems managed by Adobe and other companies. We are currently in contact with other companies and are investigating the incident. At this time, we have no evidence to indicate that any sensitive information—including customer, financial, employee or any other sensitive data—has been compromised. We anticipate the full investigation will take quite some time to complete. We have and will continue to use information gained from this attack to make infrastructure improvements to enhance security for Adobe, our customers and our partners.

# Results of Operational Aurora: Official Statement by



Google™ Official Blog

## A new approach to China

January 13, 2010 at 1:00 AM

+1 38

Like many other well-known organizations, we face cyber attacks of varying degrees on a regular basis. In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google. However, it soon became clear that what at first appeared to be solely a security incident--albeit a significant one--was something quite different.

First, this attack was not just on Google. As part of our investigation we have discovered that at least twenty other large companies from a wide range of businesses--including the Internet, finance, technology, media and chemical sectors--have been similarly targeted. We are currently in the process of notifying those companies, and we are also working with the relevant U.S. authorities.

Second, we have evidence to suggest that a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists. Based on our investigation to date we believe their attack did not achieve that objective. Only two Gmail accounts appear to have been accessed, and that activity was limited to account information (such as the date the account was created) and subject line, rather than the content of emails themselves.

Third, as part of this investigation but independent of the attack on Google, we have discovered that the accounts of dozens of U.S.-, China- and Europe-based Gmail users who are advocates of human rights in China appear to have been routinely accessed by third parties. These accounts have not been accessed through any security breach at Google, but most likely via phishing scams or malware placed on the users' computers.

# Results of Operational Aurora: Official Statement by



---

We have already used information gained from this attack to make infrastructure and architectural improvements that enhance security for Google and for our users. In terms of individual users, we would advise people to deploy reputable anti-virus and anti-spyware programs on their computers, to install patches for their operating systems and to update their web browsers. Always be cautious when clicking on links appearing in instant messages and emails, or when asked to share personal information like passwords online. You can read more [here](#) about our cyber-security recommendations. People wanting to learn more about these kinds of attacks can read this [Report to Congress](#) (PDF) by the U.S.-China Economic and Security Review Commission (see p. 163-), as well as a related [analysis](#) (PDF) prepared for the Commission, [Nart Villeneuve's blog](#) and [this](#) presentation on the GhostNet spying incident.

We have taken the unusual step of sharing information about these attacks with a broad audience not just because of the security and human rights implications of what we have unearthed, but also because this information goes to the heart of a much bigger global debate about freedom of speech. In the last two decades, China's economic reform programs and its citizens' entrepreneurial flair have lifted hundreds of millions of Chinese people out of poverty. Indeed, this great nation is at the heart of much economic progress and development in the world today.



# Results of Operational Aurora: Official Statement by



We launched Google.cn in January 2006 in the belief that the benefits of increased access to information for people in China and a more open Internet outweighed our discomfort in agreeing to censor some results. At the time [we made clear](#) that "we will carefully monitor conditions in China, including new laws and other restrictions on our services. If we determine that we are unable to achieve the objectives outlined we will not hesitate to reconsider our approach to China."

These attacks and the surveillance they have uncovered--combined with the attempts over the past year to further limit free speech on the web--have led us to conclude that we should review the feasibility of our business operations in China. We have decided we are no longer willing to continue censoring our results on Google.cn, and so over the next few weeks we will be discussing with the Chinese government the basis on which we could operate an unfiltered search engine within the law, if at all. We recognize that this may well mean having to shut down Google.cn, and potentially our offices in China.

The decision to review our business operations in China has been incredibly hard, and we know that it will have potentially far-reaching consequences. We want to make clear that this move was driven by our executives in the United States, without the knowledge or involvement of our employees in China who have worked incredibly hard to make Google.cn the success it is today. We are committed to working responsibly to resolve the very difficult issues raised.

**Update:** Added a link to another referenced report in paragraph 5.

Posted by David Drummond, SVP, Corporate Development and Chief Legal Officer

# Example V: Stuxnet

## What is Stuxnet?

### Stuxnet;

- ▶ *is very complicated and sophisticated computer worm,*
- ▶ *first discovered* by the security company VirusBlokAda in June 2010,
- ▶ *targeting* PLCs used in **Supervisory Control and Data Acquisition (SCADA) Systems**
- ▶ *via a malware which is capable of*
  - ▶ *detecting specific SCADA software*
  - ▶ *injecting itself into the PLCs*

**to subvert them!**

**Industrial Sabotage !!!**

## What is Stuxnet?

### Stuxnet;

- ▶ *is very complicated and sophisticated computer worm,*
- ▶ *first **discovered** by the security company VirusBlokAda in June 2010,*
- ▶ *targeting PLCs used in Supervisory Control and Data Acquisition (SCADA) Systems*
- ▶ *via a **malware** which is **capable of***
  - ▶ *detecting specific SCADA software*
  - ▶ *injecting itself into the PLCs*

**to subvert them!**

**Industrial Sabotage !!!**

## What is Stuxnet?

### Stuxnet;

- ▶ *is very complicated and sophisticated computer worm,*
- ▶ *first **discovered** by the security company VirusBlokAda in June 2010,*
- ▶ **targeting PLCs used in Supervisory Control and Data Acquisition (SCADA) Systems**
- ▶ *via a **malware** which is **capable of***
  - ▶ *detecting specific SCADA software*
  - ▶ *injecting itself into the PLCs***to subvert them!**

**Industrial Sabotage !!!**

## What is Stuxnet?

### Stuxnet;

- ▶ *is very complicated and sophisticated computer worm,*
- ▶ *first discovered* by the security company VirusBlokAda in June 2010,
- ▶ *targeting* PLCs used in **Supervisory Control and Data Acquisition (SCADA) Systems**
- ▶ *via a malware which is capable of*
  - ▶ *detecting specific SCADA software*
  - ▶ *injecting itself into the PLCs*

**to subvert them!**

Industrial Sabotage !!!

## What is Stuxnet?

### Stuxnet;

- ▶ *is very complicated and sophisticated computer worm,*
- ▶ *first discovered* by the security company VirusBlokAda in June 2010,
- ▶ *targeting* PLCs used in **Supervisory Control and Data Acquisition (SCADA) Systems**
- ▶ *via a malware which is capable of*
  - ▶ *detecting specific SCADA software*
  - ▶ *injecting itself into the PLCs*

**to subvert them!**

**Industrial Sabotage !!!**

# Example V: Stuxnet

## Vulnerabilities Exploited by Stuxnet

- 1 **MS08-067 RPC Vulnerability**
- 2 MS10-046 LNK Vulnerability
- 3 MS10-061 Spool Server Vulnerability
- 4 MS10-073 Win32k.sys Vulnerability
- 5 CVE-2010-2772: Siemens SIMATIC WinCC Default Password Vulnerability

# Example V: Stuxnet

## Vulnerabilities Exploited by Stuxnet

- 1 **MS08-067 RPC Vulnerability**
- 2 **MS10-046 LNK Vulnerability**
- 3 MS10-061 Spool Server Vulnerability
- 4 MS10-073 Win32k.sys Vulnerability
- 5 CVE-2010-2772: Siemens SIMATIC WinCC Default Password Vulnerability



# Example V: Stuxnet

## Vulnerabilities Exploited by Stuxnet

- 1 **MS08-067 RPC Vulnerability**
- 2 **MS10-046 LNK Vulnerability**
- 3 **MS10-061 Spool Server Vulnerability**
- 4 MS10-073 Win32k.sys Vulnerability
- 5 CVE-2010-2772: Siemens SIMATIC WinCC Default Password Vulnerability

# Example V: Stuxnet

## Vulnerabilities Exploited by Stuxnet

- 1 **MS08-067 RPC Vulnerability**
- 2 **MS10-046 LNK Vulnerability**
- 3 **MS10-061 Spool Server Vulnerability**
- 4 **MS10-073 Win32k.sys Vulnerability**
- 5 **CVE-2010-2772: Siemens SIMATIC WinCC Default Password Vulnerability**

## Vulnerabilities Exploited by Stuxnet

- 1 MS08-067 RPC Vulnerability
- 2 MS10-046 LNK Vulnerability
- 3 MS10-061 Spool Server Vulnerability
- 4 MS10-073 Win32k.sys Vulnerability
- 5 CVE-2010-2772: Siemens SIMATIC WinCC Default Password Vulnerability

## Definition: Remote Procedure Call

In computer science, *a remote procedure call (RPC)* is an *inter-process communication* that lets any computer program to call a subroutine or procedure to execute in another address space (commonly on another computer on a shared network) without requiring programmer explicitly coding the details for this remote interaction.

## MS08-067 RPC Vulnerability

- ▶ *Vulnerability in WordPad Text Converters could allow remote code execution, when a user opens a specially crafted file using WordPad.*
- ▶ *An attacker who successfully exploited this vulnerability could gain the same user rights as the local user.*

## Definition: Remote Procedure Call

*In computer science, **a remote procedure call (RPC)** is an **inter-process communication** that lets any computer program to call a subroutine or procedure to execute in another address space (commonly on another computer on a shared network) without requiring programmer explicitly coding the details for this remote interaction.*

## MS08-067 RPC Vulnerability

- ▶ *Vulnerability in WordPad Text Converters could allow remote code execution, when a user opens a specially crafted file using WordPad.*
- ▶ *An attacker who successfully exploited this vulnerability could gain the same user rights as the local user.*

## Definition: Remote Procedure Call

*In computer science, a **remote procedure call (RPC)** is an **inter-process communication** that lets any computer program to call a subroutine or procedure to execute in another address space (commonly on another computer on a shared network) without requiring programmer explicitly coding the details for this remote interaction.*

## MS08-067 RPC Vulnerability

- ▶ *Vulnerability in WordPad Text Converters could allow remote code execution, when a user opens a specially crafted file using WordPad.*
- ▶ *An attacker who successfully exploited this vulnerability could gain the same user rights as the local user.*

## MS08-067 RPC Vulnerability: Recommendation

- ▶ *In order to understand; whether your versions or editions are affected or not; visit the web-site and perform required tests:*

*<http://technet.microsoft.com/en-us/security/bulletin/MS10-067>*

- ▶ *Microsoft's Claim: Problem is solved upon the installation of the related update; if your versions are affected, for sure.*

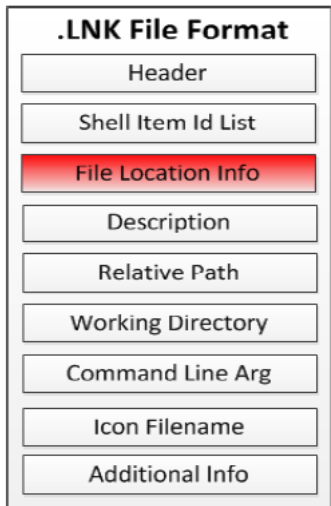
## MS08-067 RPC Vulnerability: Recommendation

- ▶ *In order to understand; whether your versions or editions are affected or not; visit the web-site and perform required tests:*

*<http://technet.microsoft.com/en-us/security/bulletin/MS10-067>*

- ▶ **Microsoft's Claim:** *Problem is solved upon the installation of the related update; if your versions are affected, for sure.*

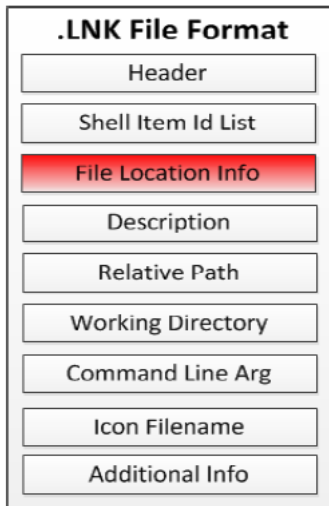




## MS08-067 LNK Vulnerability

- ▶ *In the File Location Info field there is a path to the file that contains the payload that should be executed.*
- ▶ *The vulnerability could allow remote or local code execution if the path of a specially crafted malware is fed into the file location info part.*
- ▶ *An attacker who successfully exploited this vulnerability could gain the same user rights as the local user.*

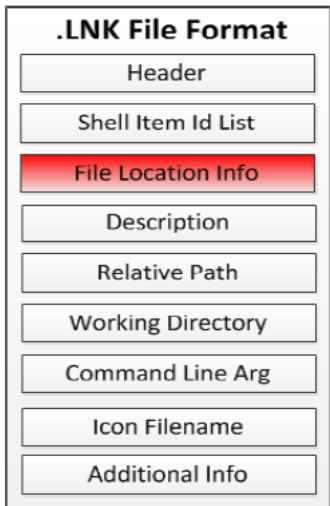
Figure: .LNK File Format



## MS08-067 LNK Vulnerability

- ▶ *In the File Location Info field there is a path to the file that contains the payload that should be executed.*
- ▶ *The vulnerability could allow remote or local code execution if the path of a specially crafted malware is fed into the file location info part.*
- ▶ *An attacker who successfully exploited this vulnerability could gain the same user rights as the local user.*

Figure: .LNK File Format



## MS08-067 LNK Vulnerability

- ▶ *In the File Location Info field there is a path to the file that contains the payload that should be executed.*
- ▶ *The vulnerability could allow remote or local code execution if the path of a specially crafted malware is fed into the file location info part.*
- ▶ *An attacker who successfully exploited this vulnerability could gain the same user rights as the local user.*

Figure: .LNK File Format

## MS08-067 LNK Vulnerability: Recommendation

- ▶ *In order to understand; whether your versions or editions are affected or not; visit the web-site and perform required tests:*

*<http://technet.microsoft.com/en-us/security/bulletin/MS10-046>*

- ▶ *Microsoft's Claim: Problem is solved upon the installation of the related update; if your versions are affected, for sure.*

## MS08-067 LNK Vulnerability: Recommendation

- ▶ *In order to understand; whether your versions or editions are affected or not; visit the web-site and perform required tests:*

*<http://technet.microsoft.com/en-us/security/bulletin/MS10-046>*

- ▶ **Microsoft's Claim:** *Problem is solved upon the installation of the related update; if your versions are affected, for sure.*

# MS10-061 Spool Server Vulnerability

## MS10-061 Spooler

*Print spooler manages the printing process, which includes retrieving the location of the correct printer driver, loading the driver, spooling high-level function calls into a print job, scheduling the print job for printing.*

## MS10-061 Spool Server Vulnerability

- ▶ *The vulnerability arises due to the Windows Print Spooler insufficiently restricting where a user has permissions to print to a file. A remote attacker could exploit this issue by sending a malicious print request to a vulnerable server. Successful exploitation of this vulnerability could allow the attacker to take complete control of an affected system.*
- ▶ *An open source computer security program called **metasploit** could be used to define if your system has this kind of a vulnerability or not. Additionally; this program helps you to exploit it.*

# MS10-061 Spool Server Vulnerability

## MS10-061 Spooler

*Print spooler manages the printing process, which includes retrieving the location of the correct printer driver, loading the driver, spooling high-level function calls into a print job, scheduling the print job for printing.*

## MS10-061 Spool Server Vulnerability

- ▶ *The vulnerability arises due to the Windows Print Spooler insufficiently restricting where a user has permissions to print to a file. A remote attacker could exploit this issue by sending a malicious print request to a vulnerable server. Successful exploitation of this vulnerability could allow the attacker to take complete control of an affected system.*
- ▶ *An open source computer security program called **metasploit** could be used to define if your system has this kind of a vulnerability or not. Additionally; this program helps you to exploit it.*

# MS10-061 Spool Server Vulnerability

## MS10-061 Spooler

*Print spooler manages the printing process, which includes retrieving the location of the correct printer driver, loading the driver, spooling high-level function calls into a print job, scheduling the print job for printing.*

## MS10-061 Spool Server Vulnerability

- ▶ *The vulnerability arises due to the Windows Print Spooler insufficiently restricting where a user has permissions to print to a file. A remote attacker could exploit this issue by sending a malicious print request to a vulnerable server. Successful exploitation of this vulnerability could allow the attacker to take complete control of an affected system.*
- ▶ *An open source computer security program called **metasploit** could be used to define if your system has this kind of a vulnerability or not. Additionally; this program helps you to exploit it.*



## MS10-061 Spool Server Vulnerability: Recommendation

- ▶ *In order to understand; whether your versions or editions are affected or not; visit the web-site and perform required tests:*

*<http://technet.microsoft.com/en-us/security/bulletin/MS10-061>*

- ▶ *Microsoft's Claim: Problem is solved upon the installation of the related update; if your versions are affected, for sure.*

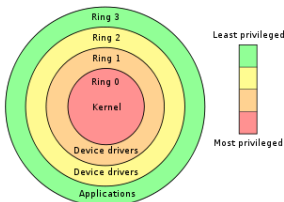
## MS10-061 Spool Server Vulnerability: Recommendation

- ▶ *In order to understand; whether your versions or editions are affected or not; visit the web-site and perform required tests:*

*<http://technet.microsoft.com/en-us/security/bulletin/MS10-061>*

- ▶ **Microsoft's Claim:** *Problem is solved upon the installation of the related update; if your versions are affected, for sure.*

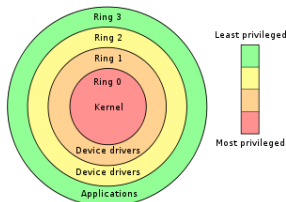
# MS10-073 Win32k.sys Vulnerability



## MS10-073 Win32k.sys Vulnerability

- ▶ *Win32k.sys* → *Windows kernel mode driver*
- ▶ *The specific vulnerability exists within the "win32k.sys" that does not properly index a table of function pointers when loading a keyboard layout from disk via the function LoadKeyboardLayout().*
- ▶ *Once a crafted file is loaded by the Win32K kernel driver, the malware sends an event to the keyboard input stream to effectively trigger the vulnerability. If an attacker exploits the vulnerability he may achieve code execution right with kernel privileges.*

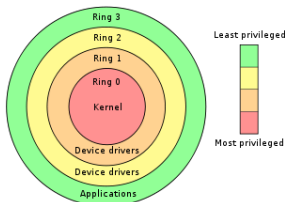
# MS10-073 Win32k.sys Vulnerability



## MS10-073 Win32k.sys Vulnerability

- ▶ *Win32k.sys* → Windows kernel mode driver
- ▶ The specific vulnerability exists within the "win32k.sys" that does not properly index a table of function pointers when loading a keyboard layout from disk via the function `LoadKeyboardLayout()`.
- ▶ Once a crafted file is loaded by the Win32K kernel driver, the malware sends an event to the keyboard input stream to effectively trigger the vulnerability. If an attacker exploits the vulnerability he may achieve code execution right with kernel privileges.

# MS10-073 Win32k.sys Vulnerability



## MS10-073 Win32k.sys Vulnerability

- ▶ *Win32k.sys* → *Windows kernel mode driver*
- ▶ *The specific vulnerability exists within the "win32k.sys" that does not properly index a table of function pointers when loading a keyboard layout from disk via the function LoadKeyboardLayout().*
- ▶ *Once a crafted file is loaded by the Win32K kernel driver, the malware sends an event to the keyboard input stream to effectively trigger the vulnerability. If an attacker exploit the vulnerability he may achieve code execution right with kernel privileges.*

## MS10-073 Win32k.sys Vulnerability: Recommendation

- ▶ *In order to understand; whether your versions or editions are affected or not; visit the web-site and perform required tests:*

*<http://technet.microsoft.com/en-us/security/bulletin/MS10-073>*

- ▶ *Microsoft's Claim: Problem is solved upon the installation of the related update; if your versions are affected, for sure.*

## MS10-073 Win32k.sys Vulnerability: Recommendation

- ▶ *In order to understand; whether your versions or editions are affected or not; visit the web-site and perform required tests:*

*<http://technet.microsoft.com/en-us/security/bulletin/MS10-073>*

- ▶ **Microsoft's Claim:** *Problem is solved upon the installation of the related update; if your versions are affected, for sure.*

# CVE-2010-2772 Siemens SIMATIC WinCC Default Password Vulnerability

## CVE-2010-2772 Siemens SIMATIC WinCC Default Password Vulnerability

*Siemens Simatic WinCC and PCS 7 SCADA system uses a **hard-coded password**, which allows local users to access a **back-end database** and gain privileges.*

*By default, Siemens SIMATIC installs with a default password. The 'WinCCConnect' and 'WinCCAdmin' accounts have a password of '2WSXcder' which is publicly known and documented. This allows attackers to trivially access the program or system.*



# CVE-2010-2772 Siemens SIMATIC WinCC Default Password Vulnerability

## CVE-2010-2772 Siemens SIMATIC WinCC Default Password Vulnerability

*Siemens Simatic WinCC and PCS 7 SCADA system uses a **hard-coded password**, which allows local users to access a **back-end database** and gain privileges.*

*By default, Siemens SIMATIC installs with a default password. The 'WinCCConnect' and 'WinCCAdmin' accounts have a password of '2WSXcder' which is publicly known and documented. This allows attackers to trivially access the program or system.*

## How Stuxnet Spreads?

- 1 *Removable Storage Devices (USBs)*
  - ▶ *.LNK extended files*
  - ▶ *autorun.inf*
- 2 *Local Area Network Communications*
  - ▶ *Network shares*
  - ▶ *Printer Spooler vulnerability*
- 3 *Infected Application Data Files*
  - ▶ *Copies into Siemens STEP7 Project files*
  - ▶ *Installs in Siemens WinCC SQL Server database via known credentials*

## How Stuxnet Spreads?

- 1 *Removable Storage Devices (USBs)*
  - ▶ *.LNK extended files*
  - ▶ *autorun.inf*
- 2 *Local Area Network Communications*
  - ▶ *Network shares*
  - ▶ *Printer Spooler vulnerability*
- 3 *Infected Application Data Files*
  - ▶ *Copies into Siemens STEP7 Project files*
  - ▶ *Installs in Siemens WinCC SQL Server database via known credentials*

## How Stuxnet Spreads?

- 1 *Removable Storage Devices (USBs)*
  - ▶ *.LNK extended files*
  - ▶ *autorun.inf*
- 2 *Local Area Network Communications*
  - ▶ *Network shares*
  - ▶ *Printer Spooler vulnerability*
- 3 *Infected Application Data Files*
  - ▶ *Copies into Siemens STEP7 Project files*
  - ▶ *Installs in Siemens WinCC SQL Server database via known credentials*

# Example V: Stuxnet



**Figure:** Bushehr Nuclear Power Plant, Iran

## Affected Countries

According to Symantec researchers;

- 1 **Iran: 58.85%**
- 2 *Indonesia: 18.22%*
- 3 *India: 8.31%*
- 4 *Azerbaijan: 2.57%*
- 5 *USA: 1.56%*
- 6 *Pakistan: 1.28%*
- 7 *Others: 9.21%*

## A Comment

*This was a good idea, alright? But I also admit this was a big idea, too!*

**Mike Hayden (Former NSA and CIA Director)**

# Example V: Stuxnet



**Figure:** Bushehr Nuclear Power Plant, Iran

## Affected Countries

According to Symantec researchers;

- 1 Iran: 58.85%
- 2 Indonesia: 18.22%
- 3 India: 8.31%
- 4 Azerbaijan: 2.57%
- 5 USA: 1.56%
- 6 Pakistan: 1.28%
- 7 Others: 9.21%

## A Comment

*This was a good idea, alright? But I also admit this was a big idea, too!*

**Mike Hayden (Former NSA and CIA Director)**

# Example V: Stuxnet



**Figure:** Bushehr Nuclear Power Plant, Iran

## Affected Countries

*According to Symantec researchers;*

- 1 *Iran: 58.85%*
- 2 *Indonesia: 18.22%*
- 3 *India: 8.31%*
- 4 *Azerbaijan: 2.57%*
- 5 *USA: 1.56%*
- 6 *Pakistan: 1.28%*
- 7 *Others: 9.21%*

## A Comment

*This was a good idea, alright? But I also admit this was a big idea, too!*

**Mike Hayden (Former NSA and CIA Director)**

## Example V: Stuxnet

### Some Excerpts

*It's amazing, really, the resources that went into this worm!*

**Liam O. Murchu (Manager of Symantec's Security Response Team)**

*I'd call it groundbreaking!*

**Roel Schouwenberg (A Senior Anti-virus Researcher at Kaspersky Labs)**

*In comparison, other notable attacks, like the one dubbed Aurora that hacked Google's network and those of dozens of other major companies, were child's play.*

**Gregg Keizer**





# An Iranian News Reporter: Fars News Agency



## According to Fars

According to Fars News report; Iran's telecommunications minister said that *it had not caused "serious damage to government systems"*.

## According to Reuters

The Head Manager of the Bushehr Nuclear Power Plant told Reuters that *only the personal computers of staff at the plant had been infected by Stuxnet*.

# An Iranian News Reporter: Fars News Agency



## According to Fars

According to Fars News report; Iran's telecommunications minister said that *it had not caused "serious damage to government systems"*.

## According to Reuters

The Head Manager of the Bushehr Nuclear Power Plant told Reuters that *only the personal computers of staff at the plant had been infected by Stuxnet*.

# The Reminder: General Defense Strategy Against APTs

## The General Picture of Defense Against APTs

- 1 **Tools:** Focus on logging and monitoring efforts
- 2 **Baselines:** Be aware of what the environment should look like
- 3 **Testing:** Test security measures like an attacker
- 4 **Defense-in-Depth:** Close up the gaps
- 5 **Security Awareness:** Foster the security mindset

Despite everything, sometimes there is nothing to do against an APT which has still not been disclosed!!!

# The Reminder: General Defense Strategy Against APTs

## The General Picture of Defense Against APTs

- 1 **Tools:** Focus on logging and monitoring efforts
- 2 **Baselines:** Be aware of what the environment should look like
- 3 **Testing:** Test security measures like an attacker
- 4 **Defense-in-Depth:** Close up the gaps
- 5 **Security Awareness:** Foster the security mindset

Despite everything, sometimes there is nothing to do against an APT which has still not been disclosed!!!

# The Reminder: General Defense Strategy Against APTs

## The General Picture of Defense Against APTs

- 1 **Tools:** Focus on logging and monitoring efforts
- 2 **Baselines:** Be aware of what the environment should look like
- 3 **Testing:** Test security measures like an attacker
- 4 **Defense-in-Depth:** Close up the gaps
- 5 **Security Awareness:** Foster the security mindset

Despite everything, sometimes there is nothing to do against an APT which has still not been disclosed!!!

# The Reminder: General Defense Strategy Against APTs

## The General Picture of Defense Against APTs

- 1 **Tools:** Focus on logging and monitoring efforts
- 2 **Baselines:** Be aware of what the environment should look like
- 3 **Testing:** Test security measures like an attacker
- 4 **Defense-in-Depth:** Close up the gaps
- 5 **Security Awareness:** Foster the security mindset

Despite everything, sometimes there is nothing to do against an APT which has still not been disclosed!!!

# The Reminder: General Defense Strategy Against APTs

## The General Picture of Defense Against APTs

- 1 **Tools:** Focus on logging and monitoring efforts
- 2 **Baselines:** Be aware of what the environment should look like
- 3 **Testing:** Test security measures like an attacker
- 4 **Defense-in-Depth:** Close up the gaps
- 5 **Security Awareness:** Foster the security mindset

Despite everything, sometimes there is nothing to do against an APT which has still not been disclosed!!!



# The Reminder: General Defense Strategy Against APTs

## The General Picture of Defense Against APTs

- 1 **Tools:** Focus on logging and monitoring efforts
- 2 **Baselines:** Be aware of what the environment should look like
- 3 **Testing:** Test security measures like an attacker
- 4 **Defense-in-Depth:** Close up the gaps
- 5 **Security Awareness:** Foster the security mindset

**Despite everything, sometimes there is nothing to do against an APT which has still not been disclosed!!!**

## Summarization

- 1 *General definitions of known advanced and persistent threats via public declarations of their sufferers.*
- 2 *Overall defense strategies together with the awareness that indicates that APTs will be the new cyberwarfare strategies for the nation-states or the other organizations to gather critical and sensitive information.*

## Summarization

- 1 *General definitions of known advanced and persistent threats via public declarations of their sufferers.*
- 2 *Overall defense strategies together with the awareness that indicates that APTs will be the new cyberwarfare strategies for the nation-states or the other organizations to gather critical and sensitive information.*

# Feedback

## Contact Information

**Çok Teşekkürler!**

**Efcharistó Polý!**

**Muito Obrigado!**

**Danke Schön!**

**Bedankt!**

**Labai Ačiu!**

**Thanks a Lot!**

Burak Ekici

ekcburak@hotmail.com

# Feedback

## Bugs, Comments, Suggestions and Questions

Please let me know, if you have;

- ▶ seen any **Bugs** in the presentation.

Please share, if you have;

- ▶ any **Comments** and **Suggestions**.

QUESTIONS?

# Feedback

## Bugs, Comments, Suggestions and Questions

Please let me know, if you have;

- ▶ seen any **Bugs** in the presentation.

Please share, if you have;

- ▶ any **Comments** and **Suggestions**.

QUESTIONS?

# Bibliography



[Websense2011] White Paper

Protecting Your Critical Assets Lessons - Learned from “Operation Aurora” .

*McAfee Labs and McAfee Foundstone Professional Services.*



[Websense2011] Websense

ADVANCED PERSISTENT THREATS AND OTHER ADVANCED ATTACKS.

*THREAT ANALYSIS AND DEFENSE STRATEGIES FOR SMB, MID-SIZE, AND ENTERPRISE ORGANIZATIONS.*



[Golshan2010] Ali Golshan

Advanced Persistent Threats

*PRICEWATERHOUSECOOPERS.*

# Bibliography

-  [McAfeeSolutionBriefs]  
Advanced Persistent Threats  
*Fight large-scale threats with unified solutions and advanced intelligence from McAfee.*
-  [Ruf2011] Lukas Ruf  
Advanced Persistent Threat  
*Information Security Society - Switzerland.*
-  [Matrosov] Aleksandr Matrosov et al.  
Advanced Persistent Threat: Attacker Sophistication Continues to Grow?  
*ISSA Journal, June 2011.*
-  [Andress2011] Jason Andress  
Stuxnet Under the Microscope  
*ISSA Journal, June 2011.*