Security Unveiled

How and Why People Hack

Agenda

- Me and Microsoft
- Vuln Economy
- Stuxnet
- Other interesting things
- Questions

Me

- David Seidman
- Microsoft Senior Security Program Manager
- Microsoft Security Response Center Software Security Incident Response Plan team
  - Aka MSRC SSIRP team

Microsoft®

How I got here

- Started at Dartmouth College
- Left to start a company – fail
- Boston University ‘05
  - Computer Science BA
  - Cognitive and Neural Systems MA
- Microsoft Office sustained engineering team
  - Patches
- Led to Office security response team
- Led to Microsoft’s response team

Microsoft Security Response Center

Investigate and Resolve Vulnerability Reports

- Staff public reporting alias
- Monitor security lists
- Single point of coordination and communications

Microsoft Security Response Process

- Own and coordinate company wide process
- Work to prevent issues through security engineering and development process changes

Building Relationships and Communications

- Work with law enforcement and industry influentials
- Create community with vulnerability finders

SSIRP

- Software Security Incident Response Plan
- React to the most high-impact security issues
  - Active attacks against unpatched vulnerabilities
  - Public disclosure of unpatched vulnerabilities
  - Miscellaneous other threats

My Job

- Evaluate the threat environment
- Build assessment of probable future developments
- Engineering decisions informed by threat environment and future developments
- Ensure correct actions are taken

Why my job is awesome

- Millions of dollars, and sometimes lives, are at stake
- Cloak and dagger
- I cause really bad days for really bad people
- It’s my call
- My team is full of cool geniuses
- Very interesting technically
- I mean, c’mon, it’s hacking, that’s awesome

Why Microsoft is awesome

- Everyone thinks they have the best job in the world
  - We already solved the easy problems
  - We don't pay you a lot of money to do dumb work
- Huge breadth and depth
  - If it involves software, we're doing it (and lots of hardware too)
  - We have experts in everything and you can be one
- Great culture and work environment
  - Identifying and fixing problems is rewarded. Feedback is rewarded.
  - All we care about is how good your work is, not how you dress, when you show up or other irrelevant things
  - Trying lots of things (job mobility) is encouraged
- Pay, benefits, career paths
- Seattle

Vulnerability Economy

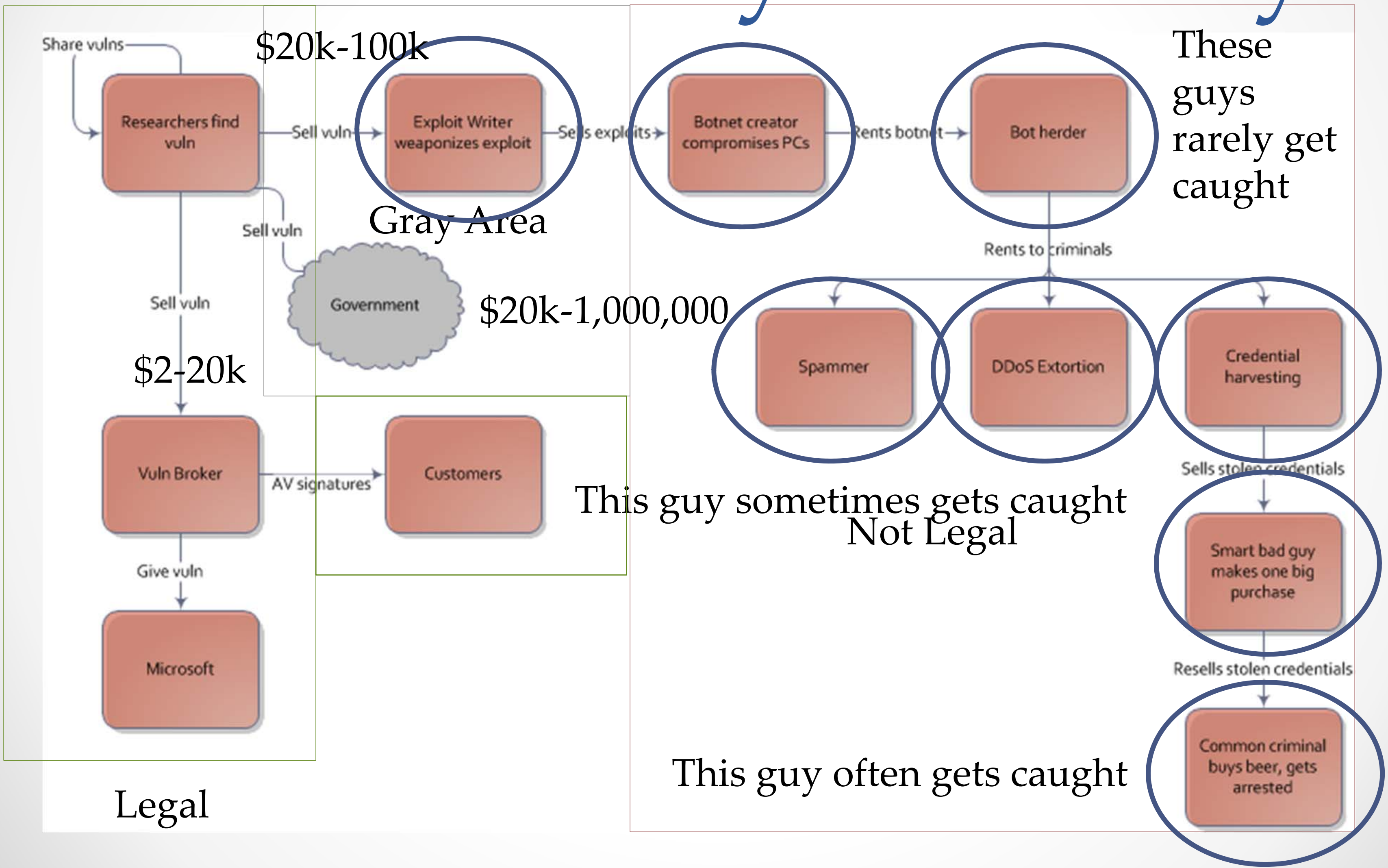
Definitions

- Hacker: Someone who's trying to do something they're not normally allowed to
  - There are many other definitions of "hacker"
  - This usage is a convenient shorthand
  - Hackers can be good, bad, or in between
- Bad guy: A hacker who harms others
  - Shades of gray do exist
- Security vulnerability: a software problem that allows someone to do something they're not allowed to
  - Typically run malicious code on the victim's computer

How To Compromise PCs

- Step 1: Get users to view your attack
  - Phishing
  - SQL Injection or Cross-Site Scripting (XSS) on a popular site
  - Malicious advertising
- Step 2: Compromise PC and/or credentials
  - Browse-and-own exploits
  - Social engineering ("dancing hamsters")
  - Phish for passwords
- Step 3: Profit!

Vulnerability Economy



$20k-100k

Gray Area

$20k-1,000,000

$2-20k

These guys rarely get caught

This guy sometimes gets caught

Not Legal

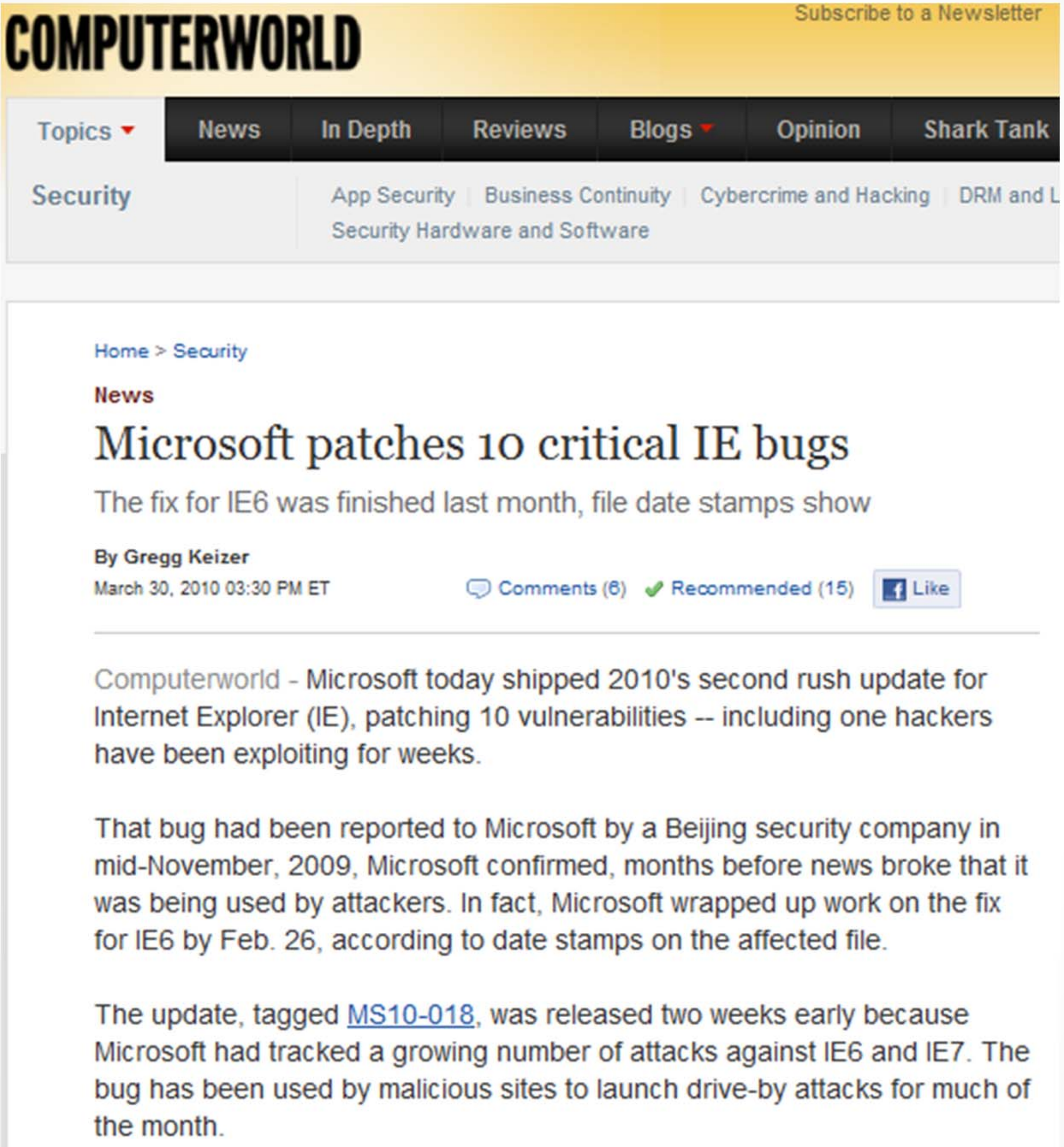
This guy often gets caught

Legal

Malware Value

- Vuln: up to $1M+ (typically ~$5k)
- Malware install: $0.30-$1.50 per installation
- Botnet rental: $50 - $50k+
  - Use of a compromised machine is worth < $30 a day
- Bank account info: $1-$1500 or 5-15% of balance
- Full PII: $5-30
- Spam: $1k for multiple millions of emails

http://www.viruslist.com/analysis?pubid=204792068



News

Microsoft patches 10 critical IE bugs

The fix for IE6 was finished last month, file date stamps show

By Gregg Keizer
March 30, 2010 03:30 PM ET

Computerworld - Microsoft today shipped 2010's second rush update for Internet Explorer (IE), patching 10 vulnerabilities -- including one hackers have been exploiting for weeks.

That bug had been reported to Microsoft by a Beijing security company in mid-November, 2009, Microsoft confirmed, months before news broke that it was being used by attackers. In fact, Microsoft wrapped up work on the fix for IE6 by Feb. 26, according to date stamps on the affected file.

The update, tagged MS10-018, was released two weeks early because Microsoft had tracked a growing number of attacks against IE6 and IE7. The bug has been used by malicious sites to launch drive-by attacks for much of the month.

Case Study: Vuln Economy

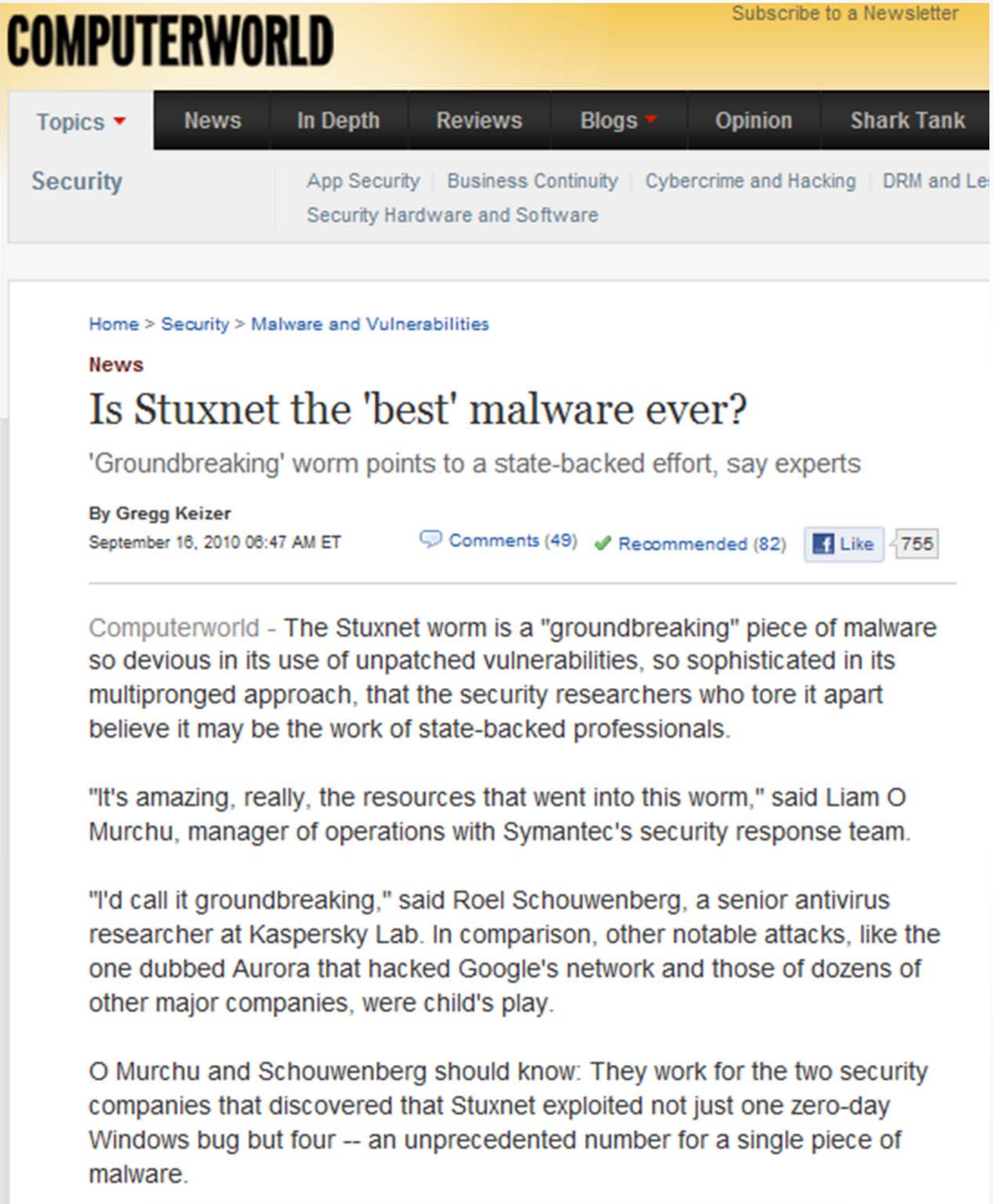
Stuxnet

Before we begin…

- Everything in this section of the presentation is derived from public knowledge
- Attackers have not been positively identified
  - Speculation in the media notwithstanding
- Purpose of the virus has not been positively identified
- Content on Siemens' systems comes from external parties
  - We don't know their code and didn't try to analyze it

Stuxnet: Outline

- A virus with multiple methods of propagation
- Targets Siemens industrial controllers (PLCs)
  - Appears to modify control of an industrial system (per 3rd parties)
- Epicenter of infection is Iran
- Uses multiple vulnerabilities, all 100% reliable
  - 1 0-day browse-and-own from USB keys and file shares (.lnk)
  - 1 0-day wormable vulnerability (Print Spooler)
  - 2 0-day Elevation of Privilege bugs (one for WinXP, one for Vista+7)
  - 2 stolen digital certificates
  - 1 patched wormable vulnerability (MS08-067) with targeted payloads
  - “Known issue” in Siemens system (static password)
- Multiple levels of rootkit
  - Can reside in the PLC and re-infect a PC that has been cleaned
- Limited spread by design



News

Is Stuxnet the 'best' malware ever?

'Groundbreaking' worm points to a state-backed effort, say experts

By Gregg Keizer
September 16, 2010 06:47 AM ET

Computerworld - The Stuxnet worm is a "groundbreaking" piece of malware so devious in its use of unpatched vulnerabilities, so sophisticated in its multipronged approach, that the security researchers who tore it apart believe it may be the work of state-backed professionals.

"It's amazing, really, the resources that went into this worm," said Liam O Murchu, manager of operations with Symantec's security response team.

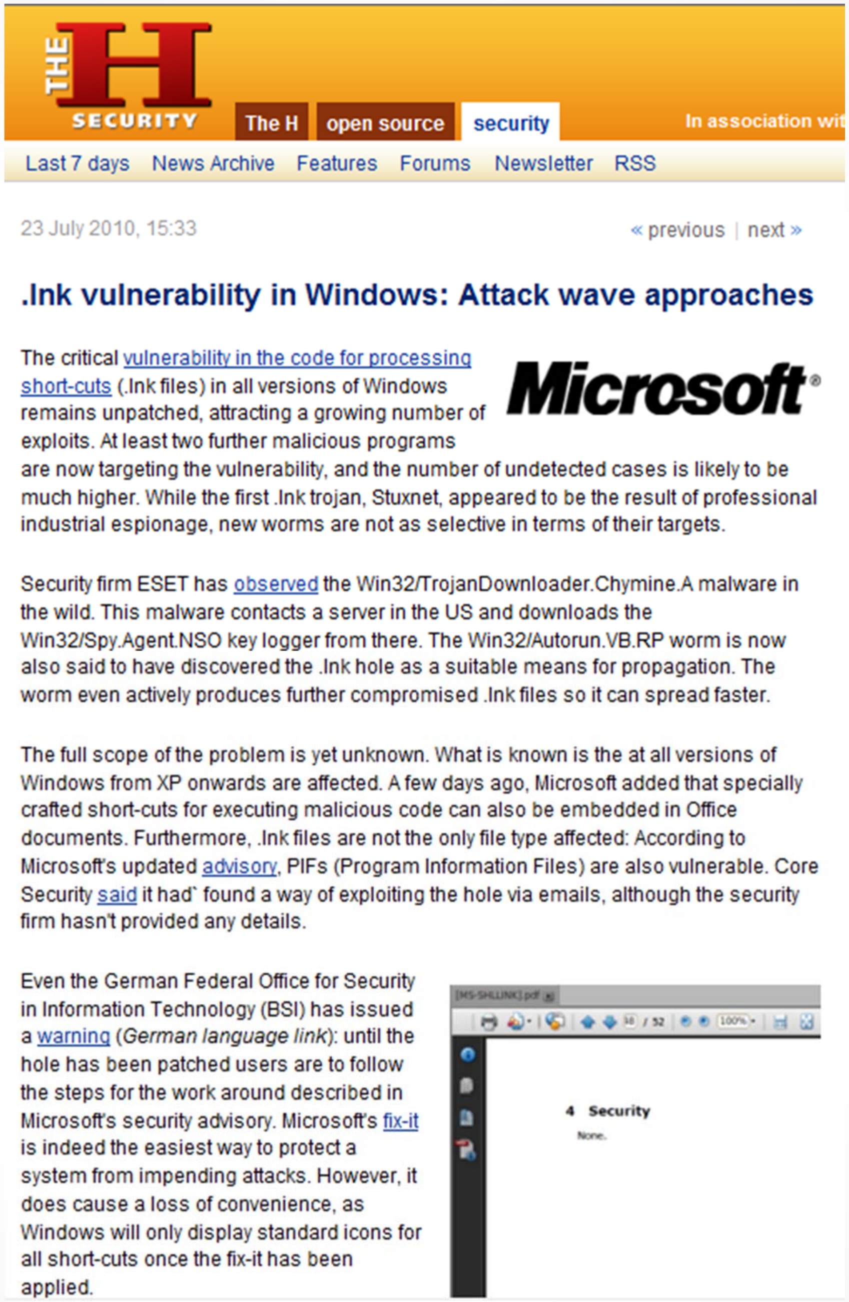
"I'd call it groundbreaking," said Roel Schouwenberg, a senior antivirus researcher at Kaspersky Lab. In comparison, other notable attacks, like the one dubbed Aurora that hacked Google's network and those of dozens of other major companies, were child's play.

O Murchu and Schouwenberg should know: They work for the two security companies that discovered that Stuxnet exploited not just one zero-day Windows bug but four -- an unprecedented number for a single piece of malware.

Case Study: Stuxnet

Stuxnet

- Small antivirus company announces discovery of new virus
  - Named “Stuxnet” by Microsoft – anagram of file name and a reg key
- Microsoft investigates, discovers .lnk vulnerability
  - So does everyone else…



23 July 2010, 15:33

.lnk vulnerability in Windows: Attack wave approaches

The critical vulnerability in the code for processing short-cuts (.lnk files) in all versions of Windows remains unpatched, attracting a growing number of exploits. At least two further malicious programs are now targeting the vulnerability, and the number of undetected cases is likely to be much higher. While the first .lnk trojan, Stuxnet, appeared to be the result of professional industrial espionage, new worms are not as selective in terms of their targets.

Security firm ESET has observed the Win32/TrojanDownloader.Chymine.A malware in the wild. This malware contacts a server in the US and downloads the Win32/Spy.Agent.NSO key logger from there. The Win32/Autorun.VB.RP worm is now also said to have discovered the .lnk hole as a suitable means for propagation. The worm even actively produces further compromised .lnk files so it can spread faster.

The full scope of the problem is yet unknown. What is known is the at all versions of Windows from XP onwards are affected. A few days ago, Microsoft added that specially crafted short-cuts for executing malicious code can also be embedded in Office documents. Furthermore, .lnk files are not the only file type affected: According to Microsoft's updated advisory, PIFs (Program Information Files) are also vulnerable. Core Security said it had` found a way of exploiting the hole via emails, although the security firm hasn't provided any details.

Even the German Federal Office for Security in Information Technology (BSI) has issued a warning (*German language link*): until the hole has been patched users are to follow the steps for the work around described in Microsoft's security advisory. Microsoft's fix-it is indeed the easiest way to protect a system from impending attacks. However, it does cause a loss of convenience, as Windows will only display standard icons for all short-cuts once the fix-it has been applied.

Case Study: Stuxnet

Stuxnet

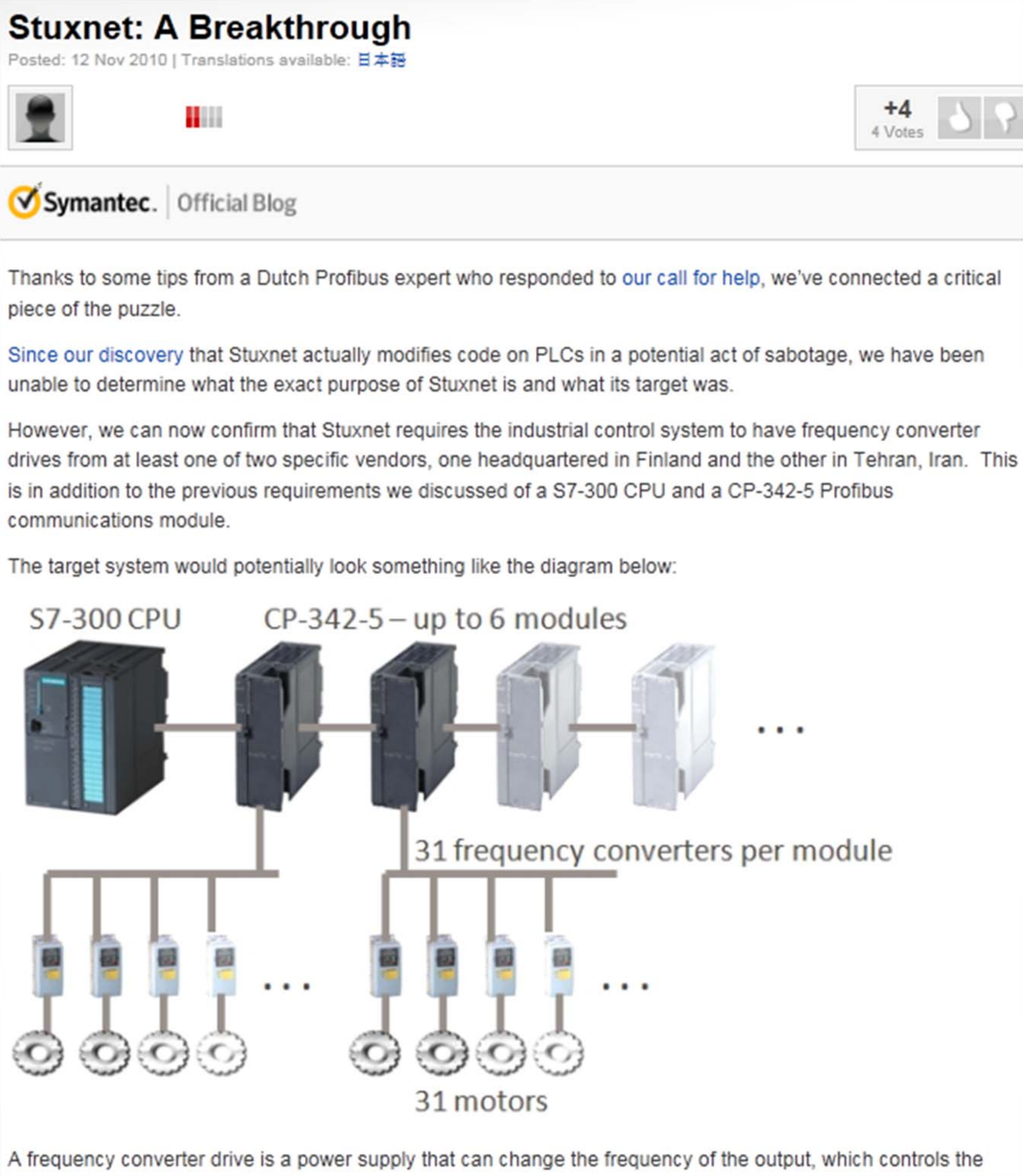
- Rootkit gets installed even from low rights
  - Elevation of Privilege (EOP) 1: Task Scheduler (Vista and Win7)
    - File describing scheduled tasks:
      - User-writeable
      - Contains identity to use when executing task
      - Protected by CRC32 hash => collisions are easy
    - Overwrite an existing task and pad it to match the hash
  - EOP 2: Keyboard Layout (WinXP)
    - Keyboard layout file loader in kernel has missing bounds check
- Bruce sets up a mini-network with an infected PC, goes to lunch
- Comes back to find other PC is infected

Stuxnet

- Wormable Print Spooler vulnerability
  - Print to a network printer
  - Print to file: C:\WINDOWS\System32\...
  - Write to a location that will be executed (trivial)
  - Only works on WinXP by default
- MS08-067 vulnerability
  - Wormable vulnerability used by Conficker
  - Stuxnet fingerprints target, delivers OS-specific payload
- Stolen certs
- Straightforward Command & Control
  - With FIPS-compliant peer-to-peer communication

Third Party Findings

- Uses hard-coded, unchangeable default password in Siemens SCADA system to gain access
- Modifies high-frequency processes with specific frequency changes
- Adjusts output values to read as normal
- Infects PLC microprocessor and will re-infect host from PLC



Stuxnet: A Breakthrough

Posted: 12 Nov 2010 | Translations available: 日本語

+4
4 Votes

Symantec. | Official Blog

Thanks to some tips from a Dutch Profibus expert who responded to our call for help, we've connected a critical piece of the puzzle.

Since our discovery that Stuxnet actually modifies code on PLCs in a potential act of sabotage, we have been unable to determine what the exact purpose of Stuxnet is and what its target was.

However, we can now confirm that Stuxnet requires the industrial control system to have frequency converter drives from at least one of two specific vendors, one headquartered in Finland and the other in Tehran, Iran. This is in addition to the previous requirements we discussed of a S7-300 CPU and a CP-342-5 Profibus communications module.

The target system would potentially look something like the diagram below:

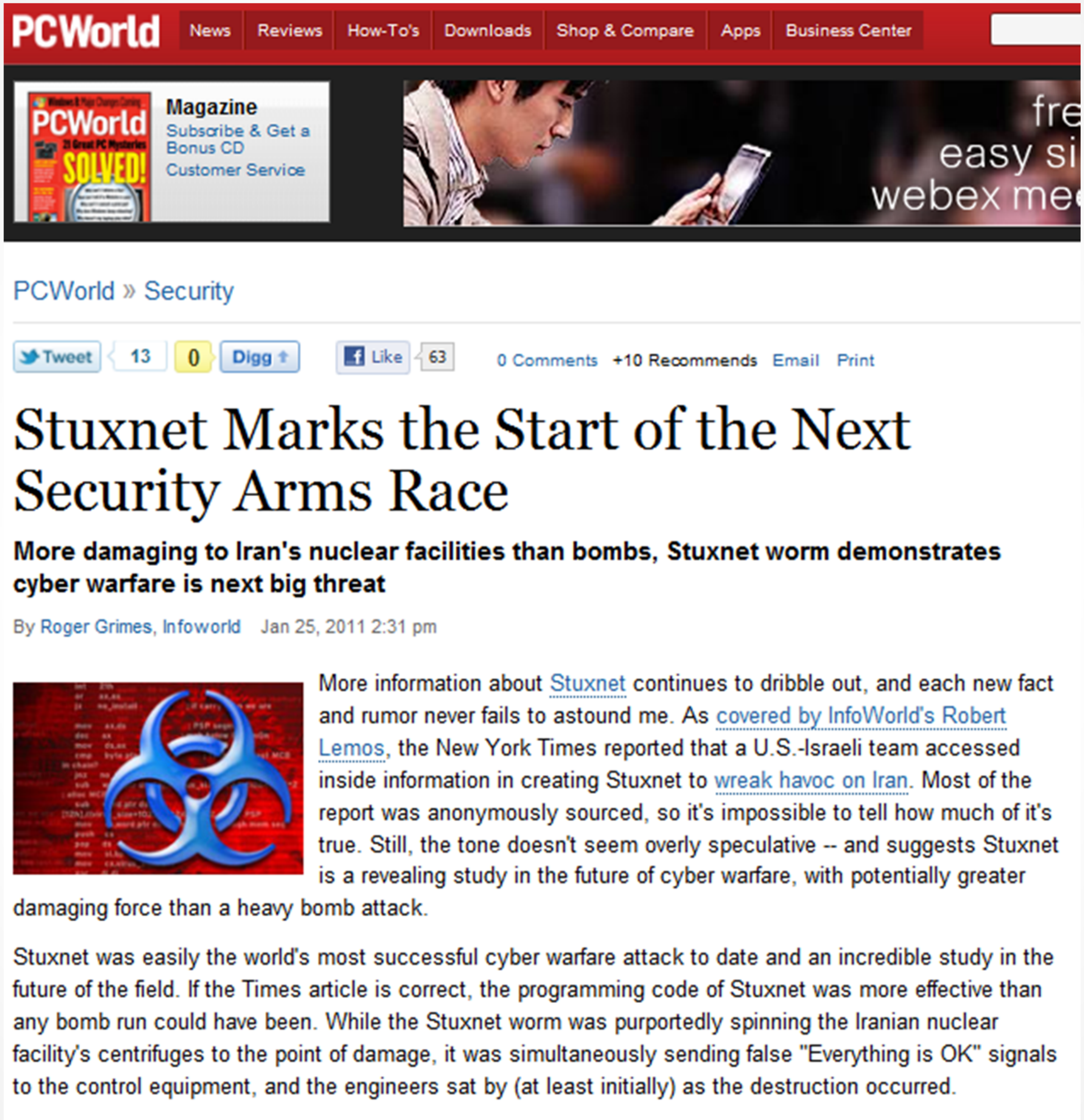
S7-300 CPU
CP-342-5 – up to 6 modules
. . .
31 frequency converters per module
. . .
. . .
31 motors

A frequency converter drive is a power supply that can change the frequency of the output, which controls the

Case Study: Stuxnet

Stuxnet Speculation

- PLC code varies frequency of high-frequency drives
  - Like the ones used for uranium centrifuges… and nothing else.
- Was it created by a nation-state? Evidence:
  - Multiple 100% reliable 0-days. Each one is worth $50-100k+.
  - Stolen certificates
  - Infected systems were probably not on the internet
  - Multiple types of expertise required
    - Symantec claims >30 programmers wrote the code
- Epicenter in Iran?
  - Secondary epicenters in India and Indonesia?
  - Iran announced a “setback” in their nuclear program and confirmed that Stuxnet had infected its nuclear facilities (separately).
- Who’s behind it? We did not investigate and have no opinion.



Stuxnet Marks the Start of the Next Security Arms Race

More damaging to Iran's nuclear facilities than bombs, Stuxnet worm demonstrates cyber warfare is next big threat

By Roger Grimes, Infoworld Jan 25, 2011 2:31 pm

More information about Stuxnet continues to dribble out, and each new fact and rumor never fails to astound me. As covered by InfoWorld's Robert Lemos, the New York Times reported that a U.S.-Israeli team accessed inside information in creating Stuxnet to wreak havoc on Iran. Most of the report was anonymously sourced, so it's impossible to tell how much of it's true. Still, the tone doesn't seem overly speculative -- and suggests Stuxnet is a revealing study in the future of cyber warfare, with potentially greater damaging force than a heavy bomb attack.

Stuxnet was easily the world's most successful cyber warfare attack to date and an incredible study in the future of the field. If the Times article is correct, the programming code of Stuxnet was more effective than any bomb run could have been. While the Stuxnet worm was purportedly spinning the Iranian nuclear facility's centrifuges to the point of damage, it was simultaneously sending false "Everything is OK" signals to the control equipment, and the engineers sat by (at least initially) as the destruction occurred.

Case Study: Stuxnet

Microsoft Response to Vulns

- Hundreds of person-hours of work
- 4 patches (1 out-of-band)
- 1 advisory
- Conference presentations
  - Virus Bulletin
  - Chaos Communication Congress (CCC)
    - Search for "Bruce Dang" on YouTube
    - Use headphones: Bruce uses some course language

Other Interesting Things

Malware Compatibility Test Lab

…Surely no one would hook into the kernel like that

- MS10-015 Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege
- Fix included changes to kernel registers
- Rootkit had used said registers to hook into the kernel
- The change caused BSOD on infected machines

Bug trends

- Simple code bugs are largely a thing of the past
- In their place are…
  - Blended threats
  - Shared libraries and industry-wide releases
  - Architectural issues
  - Problems in protocols and standards
- Shift from OS to:
  - Applications, especially non-Microsoft
  - Web vulnerabilities

Bug trends continued

- Number of bugs is up
  - More people looking for them
  - Increased value of finding them
- Severity of bugs is way down
  - Critical bugs at lowest level since 2005
- Impact is down
  - No out-of-cycle updates between September 2010 and December 2011, and no client-side out-of-cycle updates in 2 years
- Emphasis shifting away from bugs altogether
  - Social engineering, phishing

Coordinated Disclosure

- Report suspected vulnerabilities to secure@microsoft.com
  - If it’s something a bad person could do to a victim, and it’s “interesting” (a bad guy might actually bother to do it), we want to know about it
  - If in doubt, get a hold of us.
  - A real person reads 100% of these emails, including the spam.
- We will work with you to fix it.
- Please keep it private until you talk to us.
  - Once it’s public, bad guys can use it, and they will.
  - If you need to publish a paper or give a talk, we’ll work with you on that.
- Resolve issues without risking real damage

BlueHat Prize

- **First BlueHat Prize Challenge:**

For More Info

- **Entry Period:** Aug 3, 2011 – Apr 1, 2012

http://www.microsoft.com/security/bluehatprize/

for Microsoft to use the technology

Grand Prize:	• **$200,000** in cash
Second Prize:	• **$50,000** in cash
Third Prize:	• MSDN subscription ($10,000 value)

Resources

Report vulnerabilities and free security tools

www.microsoft.com/security/msrc

Free guidance and tools for secure development

www.microsoft.com/sdl

Security updates, advisories, best practices for IT

www.microsoft.com/technet/security

Attack, exploit, vulnerability data

www.microsoft.com/sir

Internet health

www.microsoft.com/security/internethealth

Careers

- www.microsoft.com/university

Questions?

Microsoft®

The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.
MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.