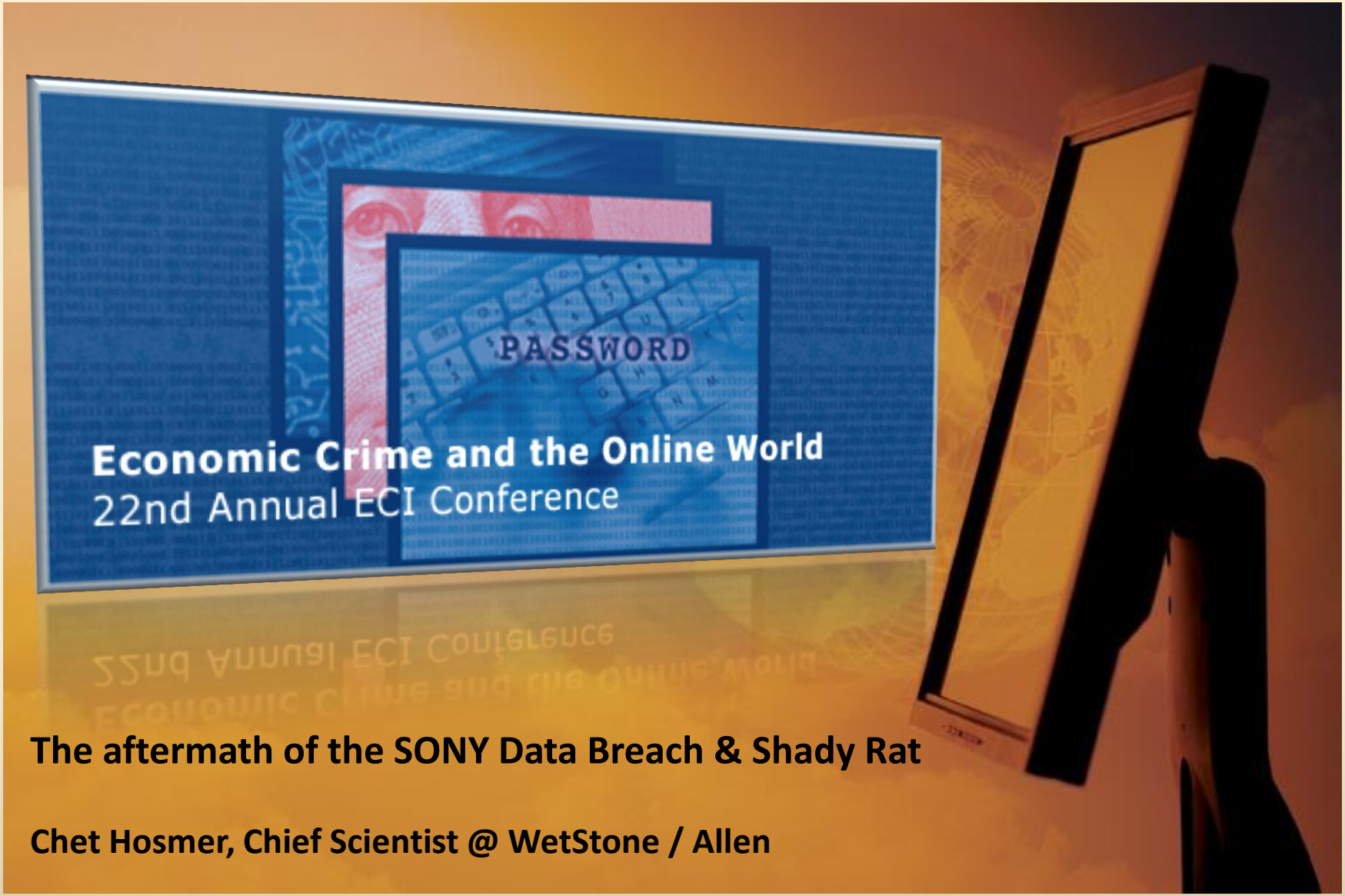


The aftermath of the SONY Data Breach & Shady Rat

Chet Hosmer, Chief Scientist @ WetStone / Allen

When things go wrong

Source Associated Press: *Sony CEO Kazuo Hirai, centre, bows in apology along with two other executives in Tokyo on May 1 regarding a security breach in April. Shizuo Kambayashi/Associated Press*

Statement from LulzSec

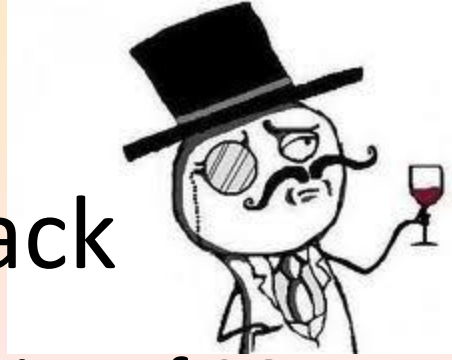
The group LulzSec posted a press release about the Sony breach on its website. Below are excerpts:

"We recently broke into SonyPictures.com and compromised over 1,000,000 users' personal information, including passwords, email addresses, home addresses, dates of birth, and all Sony opt-in data associated with their accounts. Among other things, we also compromised all admin details of Sony Pictures (including passwords) along with 75,000 'music codes' and 3.5 million 'music coupons.'...

"Our goal here is not to come across as master hackers, hence what we're about to reveal: SonyPictures.com was owned by a very simple SQL injection, one of the most primitive and common vulnerabilities, as we should all know by now. From a single injection, we accessed EVERYTHING. Why do you put such faith in a company that allows itself to become open to these simple attacks?"

Source cbcnews June 3, 2011

LulzSec Statement regarding SONY attack



- The LulzSec compromise of SONY claims to have breached
  - 1M+ user's Personal Identifiable Information
  - ALL admin details at SONY Pictures
  - 75,000 music codes
  - 3.5 Million music coupons
- The attack was "a simple SQL injection used against a well-known vulnerability"

Security Breach Missteps

What are you doing to make sure you aren't making the same $171 million mistakes?

April 20, 2011
PlayStation Network experiences beginning of network outage.

April 26, 2011 - 9:30 AM PT
PlayStation Network outage for 6 days and still no answers available for its customers.

April 26, 2011 - 1:00 PM PT
Later that same day, Sony says billing addresses, user names, passwords and possibly credit card info belonging to its PlayStation Network customers have been stolen.

April 28, 2011
A database of 2.2 million Sony customer credit cards is offered for sale on an underground Internet forum.

April 27, 2011
News about how unhappy users are with the lack of information from Sony continues to run rampant and Sony is sued.

April 29, 2011
Government officials question what Sony is doing and how they will make things right with customers.

April 30, 2011
PlayStation Network services announced they will be up and running later in the week and customers will get a free 30-day service and theft protection monitoring service.

May 2, 2011
PlayStation Network breach extends to Sony Online Entertainment.

May 4, 2011
Reports surface about Anonymous' potential involvement in the hack, but they deny it.

May 5, 2011
NY Attorney General subpoenas Sony and the same day the CEO offers the first apology and explanation for what may have happened.

May 6, 2011
According to reports, a security expert testifies to a House subcommittee that Sony knew it was in possession of outdated security software.

May 7, 2011
Sony says the PlayStation network might not be up and running as quickly as they thought due to more testing needed.

May 12, 2011
Sony announces "perks" post-breach.

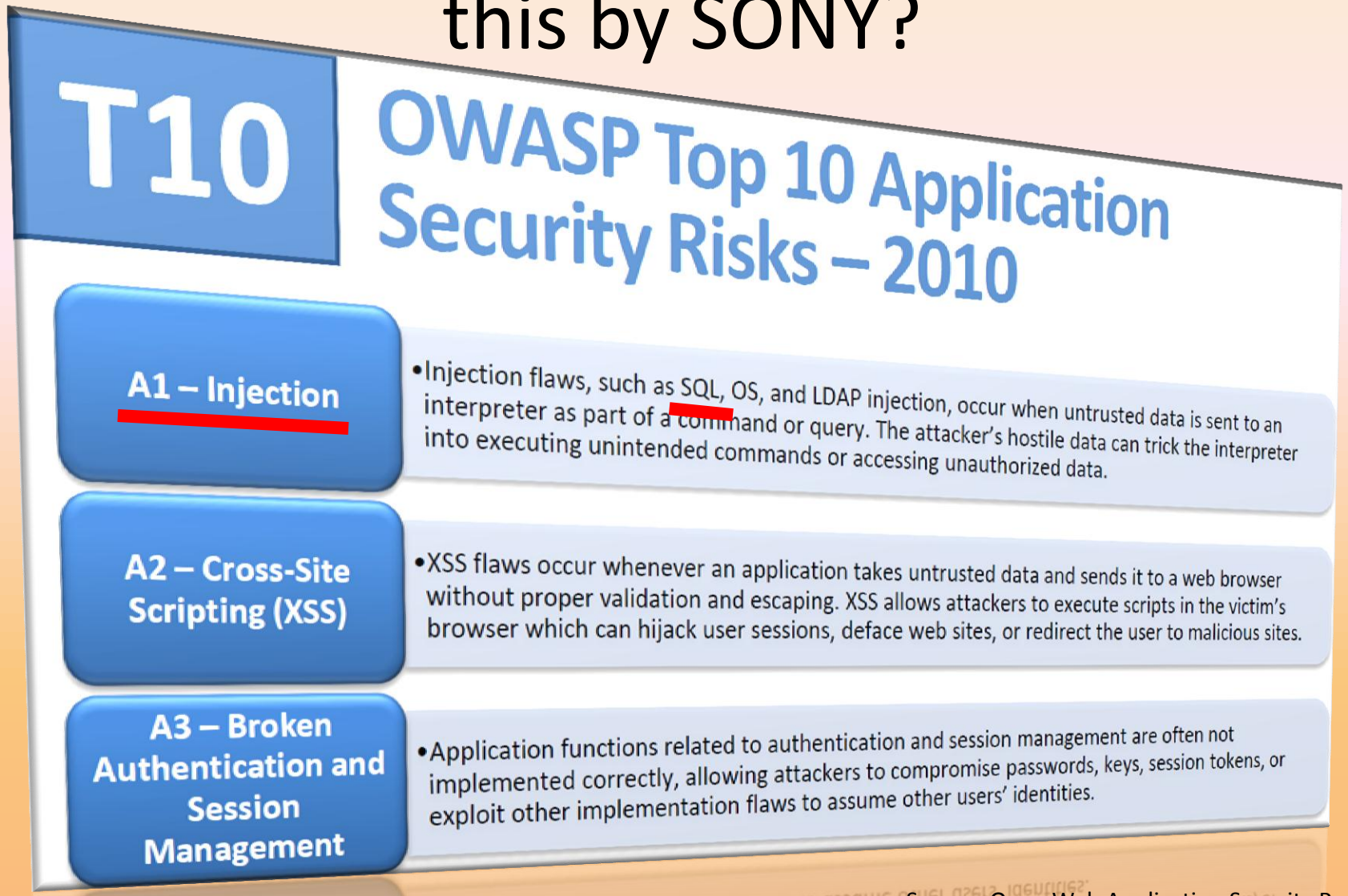
May 14, 2011
Sony begins relaunch of PlayStation Network in stages.

May 16, 2011
Japan's government announces they are waiting for better security measures from Sony.

May 17, 2011
Sony CEO Howard Stringer announces security has been restored and Sony is safe.

May 18, 2011
PlayStation Network experiences a vulnerability in its password reset interface and takes the site down "for maintenance."

How big of a blunder was this by SONY?

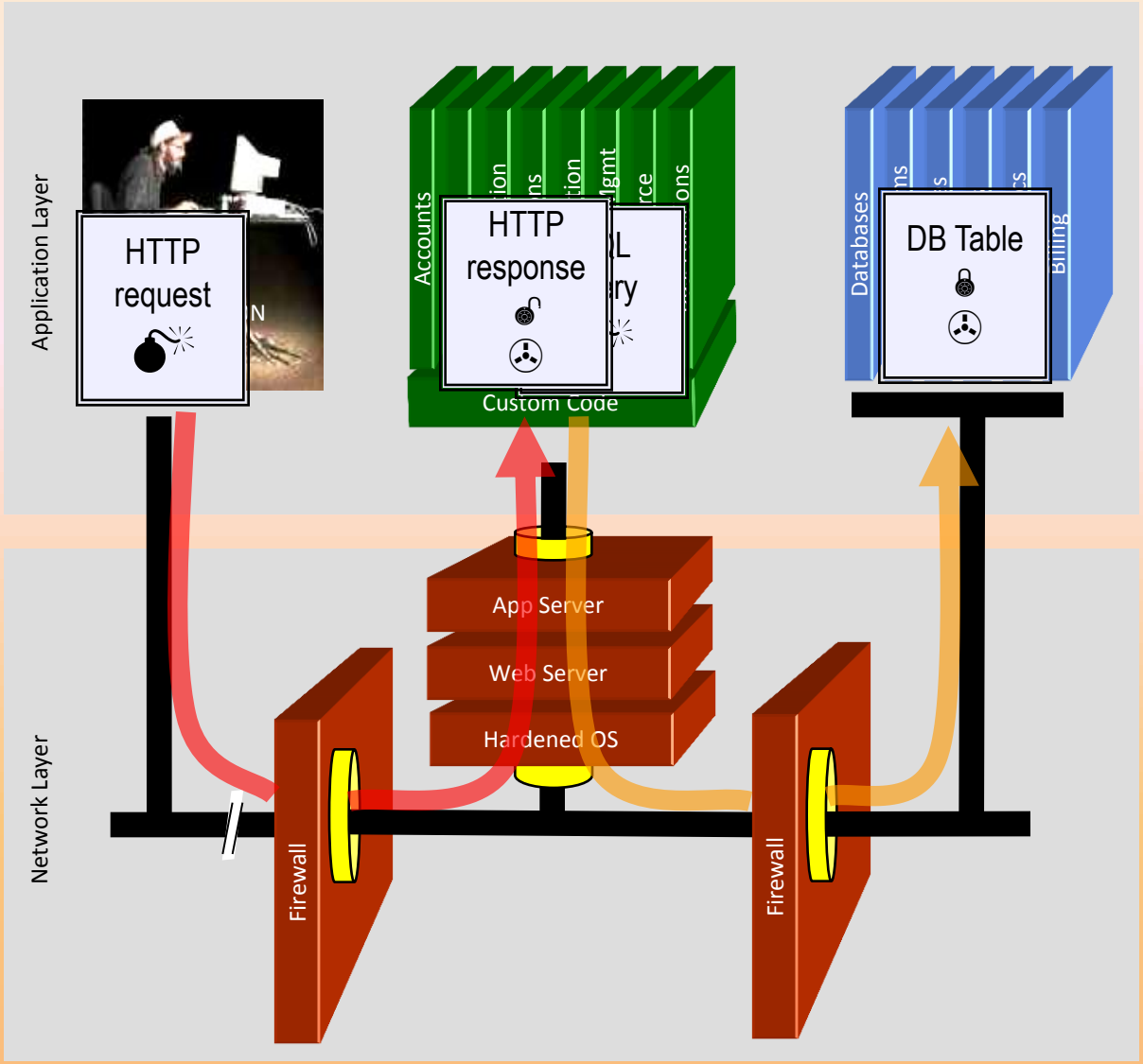


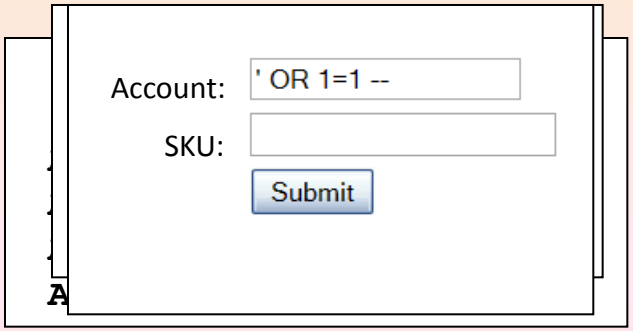
Source: Open Web Application Security Project
https://www.owasp.org/index.php/Top_10

How big of a blunder was this by SONY (continued)?

- OWASP **Number 1** Security Risk
- Flaws like this are fundamental and they indicate to hackers that the web infrastructure is poorly conceived and even sloppy, making additional attacks possible
- Basically, SQL Injection vulnerabilities violate multiple fundamental tenants of security
  - Lack of proper validation of untrusted input
  - Inadequate separation of roles and data
  - Improper application of least privilege access control
  - Poor protection of user PII

SQL Injection – Illustrated





1. Application presents a form to the attacker
2. Attacker sends an attack in the form data
3. Application forwards attack to the database in a SQL query
4. Database runs query containing attack and sends encrypted results back to application
5. Application decrypts data as normal and sends results to the user

Source OWASP 2010

So what have learned from the SONY Data Breach

- Actually not much!
  - The vulnerabilities and attack mechanisms are:
    - Well known
    - Easy to execute (you basically need a browser)
    - When successful they provide rich information to the attacker
  - It is estimated that over 75% of all commercial web sites are still vulnerable today to injection based attacks
  - Every web incident and vulnerability engagement we have executed (ever) has identified multiple injection vulnerabilities

Operation Shady Rat

A more sophisticated and potentially deadly endeavor

dark READING
Protect The Business Enable Access

CISO GUIDE: FISMA Compliance
Do more than just cursory scans. Dev
a holistic approach to app security.
Find out how!

Welcome Guest. | Log In | Register | Membership Benefits

ATTACKS / BREACHES | VULNERABILITIES | APPLICATION SEC
SECURITY MANAGEMENT | STORAGE SECURITY | ENCRYPTION | NAC

E-mail this page | Print this page | BOOKMARK

'Operation Shady RAT' Attackers Employed Steganography

Digital images hid commands controlling infected machines

Aug 11, 2011 | 02:42 PM | 6 Comments

By Kelly Jackson Higgins
Dark Reading

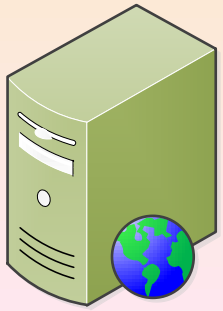
The attackers behind the "Operation Shady RAT" targeted cyberespionage hacks hid some of their activities behind digital images.

They used steganography, a relatively rarely deployed technique for hiding malicious code or data behind image files or other innocuous-looking files. In its analysis of Operation Shady RAT, Symantec found rigged images -- everything from images of a pastoral waterside scene to a suggestive photo of a woman in a hat -- that were masking commands ordering the infected machines to phone home to the command-and-control (C&C) server.

The commands are invisible to the human eye because the bits in the image are actually made up of those commands. They're "mathematically built into the data representing the image," according to Symantec researchers in a recent blog post that includes examples of the images its researchers found.

Jackson, Kelly
Dark Reading Retrieved on August 12, 2011
http://darkreading.eu/advanced-threats/167901091/security/attacks-breaches/231400084/operation-shady-rat-attackers-employed-steganography.html

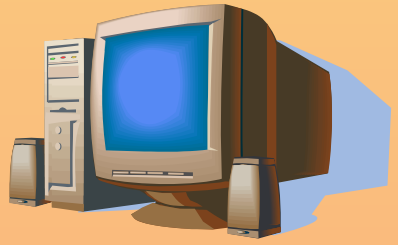
Operation Shady RAT



Based upon the target organization, custom tailored email messages containing Microsoft Office based attachments are sent out

Upon opening the attachment, a trojan horse is installed on the victim computer along with a clean copy of the Microsoft Office file to simulate proper function

Once the trojan is installed, it attempts to connect to a number of hard coded URLs to download images. These images have the commands to be executed by the trojan horse hidden in them via steganography, thus protecting them from end users and investigators



Symantac Official Blog
Retrieved on September 24, 2011
http://www.symantec.com/connect/blogs/truth-behind-shady-rat

Sample Images Reportedly Used by Operation Shady RAT

Symantac Official Blog
Retrieved on September 24, 2011
http://www.symantec.com/connect/blogs/truth-behind-shady-rat

Operation Shady RAT Impact (to-date)

Organization

- 71 companies, governments, and non-profit organizations
- 27 of the 71 were US federal and state government agencies and defense contractors

Geographic

- 14 different countries including USA, India, Germany, Hong Kong, Singapore, Canada, Japan, South Korea, and UK
- 49 of the 71 victims were in the USA
- Command and Control Centers have been traced back to China and Shanghai

Microsoft Malware Protection Center
Retrieved on September 26, 2012
http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

Unfortunately, that isn't the bad news

So what have we learned from Operation Shady Rat?

- We are still learning
  - It may be the first large scale example of Advanced Persistent Threat (APT)
  - Some argue that it is not a true APT due to some of the technical mistakes that finally led to the discovery.
    - *I would suggest that Shady Rat result was much worse. It was an SPT, a Successful Persistent Threat*
  - The integration of advanced data hiding and covert communication raises the stakes

In summary

- ✓Attack vectors can be simple or sophisticated
- ✓The impacts on individual privacy, state secrets and intellectual property are real and the stakes are high
- ✓The expansion of technology (smart mobile devices and cloud infrastructure) are evolving rapidly
  - ✓Intel/McAfee predict 20 Billion connected devices by the year 2020 … What do we do then?

Thank you

Chet Hosmer, Chief Scientist
WetStone/Allen
c h e t @ w e t s t o n e t e c h . c o m