Anatomy of an Intrusion

Insider's look at a real, sustained attack against a major, multinational corporation

Shari Lawrence Pfleeger, RAND Corporation

IT Pro July/August 2010

Dr. Panayotis Kikiras
INFS 150
University of Thessaly

Oct 2015

Setting the Stage

- The company under attack has several thousand employees located around the world
- Its central server is located in the US
  - and supports thousands of end-user systems,
  - 200 to 300 other servers,
  - and two main Internet access points.
  - also supports customers and the general public

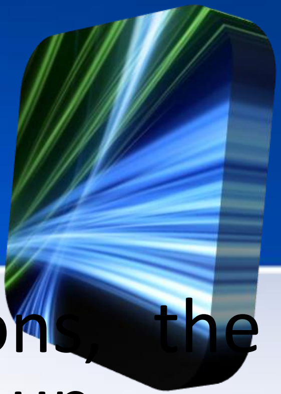
Setting the Stage

- Much of the company’s work involves databases of information that it must protect and separate from other parts of the network
- One portion of the network has substantial security requirements, including government classification of data.
- Other data sets aren’t classified but are sensitive
- and must be carefully protected

Setting the Stage

- The IT staff originally designed the network to support users’ and customers’ needs for functionality, with little regard for security except when explicitly required.
- All corporate staff have laptop or desktop computers with local administrator privileges.
- Many of the corporate employees and customers require remote access to the network

Setting the Stage



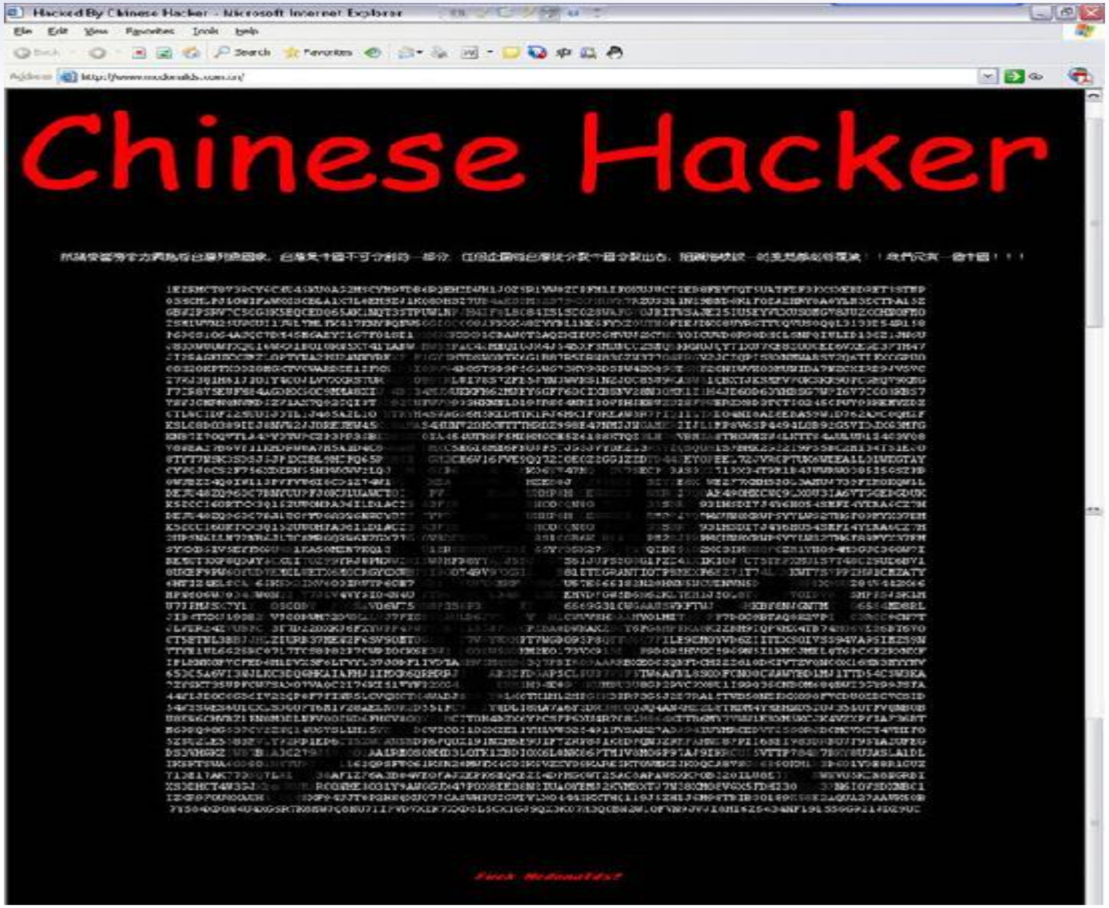
- Because of the diversity of work locations, the access ranges from highspeed linkage to dial-up.
- All remote offices send traffic to the central site.
- Ninety percent of the resources are at the central site, and only some remote offices provide IT support.
- Typically, traffic volume is high in the morning, drops mid-morning, and is up again at noon, often reflecting when the staff at remote sites gets to work and logs on to read email. There are major drops in volume over the weekend, but the volume is never zero.

Discovering the Attack

- The IT support staff was the first to notice something wrong.
- One domain controller, started acting strangely—restart itself for no apparent reason.
- Called Microsoft for help
- Luckily, they have a red –team exercise from an outside vendor
  - During the exercise, the participants discovered that real attackers were present on port 8080 an adversary was shipping rogue system files to an external destination.

The million dollar Question

- Can you imagine where?


Hacked By Chinese Hacker - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.mcdonalds.com.cn/
Go

Chinese Hacker

Fuck Mcdonalds!

Discovering the Attack

- These assaults were quite sophisticated

  —not the typical automated virus or denial of service.

- the attacks were targeted
  - were looking for specific information from people with expertise in particular areas
  - malicious software planted on corporate computers involved key loggers

First Reaction

- the company took steps to reduce unauthorized data leaving its systems
- the attackers responded with a massive effort to scan corporate networks for vulnerabilities.
- mandate that all employees reset their passwords to something that had not been used before
- increased the volume of help-desk calls to over
- 3,000

Handling the Attack

- Disconnect the system from the Internet
- observe background traffic for anomalous behavior (create own email, DNS directly out)
- Scan databases – (sun – solaris)
  - – an open source rootkit tool found

X-Raying the Attack

- What mechanisms enabled the attack?
  - Targeted, customized Trojans were used in the attackers' first strike.
- The Trojans arrived in several different ways,
- including
  - when staff opened a malicious email attachment, typically a Word file, PDF file, or spreadsheet;
  - when staff intentionally or inadvertently went to a malicious website;
  - when staff or a process opened a malicious file transmitted on a hard medium (such as a CD or thumb drive) or using a network protocol (such as FTP)
  - when a process accessed a company computer.

X-Raying the Attack

- Malware typically arrived in an email and, once enabled, sent and received data using a Domain Name System (DNS), HTTP, and HTTPS.
- **Malware's most telling symptom was the change in network traffic**
- The company uses three separate layers of antivirus protection from three separate vendors, **none** identified the Trojans.

Attack Enablers

- **Microsoft Word** was an important vector for the Trojans.
  - Even though all company computers had updated personal firewalls, antivirus software, spyware, and operating system patches, they didn’t have updated Microsoft Office patches.
  - because the attacks were persistent and changing, sometimes the adversary exploited a **vulnerability** for which **no patch was yet available.**

Attack Enablers

- A combination corporate of factors enabled the attacks' success:
  - Using the network for collaboration
  - Using email to share information
  - Employees moving frequently from one site to another
- many workers felt that the technology
- would protect them
- —so they focused more on getting their jobs done than on protecting their equipment and data.

Mitigating the Effects

- Mandating a proxy for Web browsing
- Requiring two-factor authentication
- Reducing update times
- Hardening operating systems and applications
- Investigating malware in attachments
- The company also hired staff with some forensic experience

Mitigating the Effects

- The short-term goal was twofold:
  - increase the work factor (that is, make the attackers work harder to compromise a machine) and
  - focus on behavior instead of signature- or rule-based discovery.
- Network-behavior monitoring tools support the search for unusual behavior

Addressing the Long-Term Threats

- When the company took the steps just described, the unauthorized flow of data from the corporate network was significantly reduced and **eventually eliminated**
- **the attackers fought back with a massive scan of vulnerabilities in the public-facing corporate systems.**

Addressing the Long-Term Threats

- Create new business and security Policies
- Resulting to a timeline and cost estimation
- Furthermore they decided to comply with the following strategy

Ten Steps Toward Security

- Run Red-Team Exercises
- Update the Security Plan
- Review Processes (Both business and Security)
- Develop Customized Tools
- Use Outside Experts.
- Increase Network Segmentation (create a “cold room” for extra – sensitive data)
- Continue System Hardening

Ten Steps Toward Security

- Enhance Security Awareness
- Remove Local Administrator Privileges
- Address Insider Threats (honeypots)

"Now there is more of a tilt toward security. The attack opened our eyes. Before the attack, we had never meditated deeply on where the balance between service and security should be."