Global Information Assurance Certification Paper

TROJANS: Barbarians at the gate… again!!!
Jim Winburn
Senior Director of Technology
Inceutica
January 17, 2001

The following excerpt from an article on CNN's website " http://www.cnn.com/2000/WORLD/europe/10/27/usa.microsoft/" was repeated many times around the world on October 27, 2000.

Hackers attack Microsoft network

October 27, 2000
Web posted at: 5:06 PM EDT (2106 GMT)

SEATTLE -- Hackers have broken into Microsoft's computer network in what the company has described as "a deplorable act of industrial espionage."

The world's biggest computer software company confirmed the electronic break-in on Thursday night, saying it was working with law enforcement authorities to investigate the incident.

"We're still looking into it. We're still trying to figure out how it happened," Microsoft spokesman Rick Miller said. "We will work to protect our intellectual property."

The break-in was discovered on Wednesday by the software giant's security employees.

They discovered that passwords used to transfer the source code behind Microsoft's software were being sent from the company's computer network in Washington, to an e-mail account in St. Petersburg, Russia, the Wall Street Journal reported.

The unknown hackers are believed to have had access to the software codes for three months.

The hackers are believed to have accessed Microsoft's system by e-mailing software to the company's network and then opening a so-called back door -- known as a "Trojan" -- through the infected computer.

Analysis

This Microsoft attack illustrates several important security principals

applicable to any company using information technology as a key corporate asset. While Microsoft is a high-profile target for attack, similar means could be used in any organization that does not have at least a basic understanding of information security issues. This article reviews several key concepts of corporate information security and identifies three key actions that companies can readily take to greatly decrease their vulnerability to similar attacks.

The first issue at hand is to clarify this breach had nothing to do with Microsoft's website. It is well protected. If you executed as much as a ping against www.microsoft.comwww.microsoft.com"http://www.microsoft.com", their IDS would probably alert. At the very least your ISP would be notified and they would want to know what you're up to.

This is about Microsoft's internal network, which is similar to the infrastructure most companies provide. Microsoft is a bit different from most companies because they are a high-profile target for attack.

This attack did not succeed due to a "hole" in the security technology utilized by Microsoft. It probably succeeded due to a "hole" in the security policy and an unaware user.

This incident illuminates one of the most, if not the most important vunerability a company must deal with. A user without proper security awareness combined with an inadequate security policy and procedure represents a huge risk to any organization. **No amount of technology will protect a company's information assets if users are unaware of the potential threat and proper procedures are not applied.**

Imagine these three scenarios.

1. It's the holiday season and people are sending around e-mail attachments to their friends and family. You know those cute animations like the "Dancing Baby" or the "Frog in the Blender". The e-mail comes from a trusted person. Most people think nothing about double-clicking it.

   "After all, we have that virus "thingy" on exchange and on my desktop". "This is an animation not a word document, and aren't viruses spread through the macro functionality in word and excel, anyway"?

   Fact: Most if not all Trojan Servers can be encrypted and cloaked within other executables. This variation in

implementation is extremely challenging for virus scanners. If you execute "the Dancing Baby" program and a Trojan server is wrapped inside, you could be infected.

Fact: You can't absolutely rely only on firewalls and virus scanners as protection when it comes to defending your assets from Trojan software. A firewall configuration is somewhat static, while a Trojan can choose its configuration dynamically. The virus scanner may not detect a well-hidden Trojan, a new variant or strain of the Trojan or if the AV software signature file has not been updated or cannot recognize the attached file as infected.

2. An employee is busy at her workstation in a workspace located in an environment with lots of activity and traffic. She leaves her computer for a moment to get a quick cup of coffee; she'll only be away for two or three minutes. "No need to logout or lock my workstation, I'll only be gone for a moment".

   Fact: It only takes a few minutes to install a Trojan server from a floppy disk. It's very simple and requires very little technical knowledge. Once executed, it is difficult for a user to detect its existence.

3. My workstation is really slow today and I've got a lot of work to do. Maybe if I disable this auto start stuff on my toolbar perhaps my machine will run faster.

   Fact: Anti-virus scanners that monitor file activity should never be disabled. If a Trojan happens to circumvent the detection mechanism in the e-mail system, once executed accidentally from a well-hidden, embedded application, the AV scanner may be able to detect the Trojan in memory.

In the above three scenarios, the user was not aware of the potential threat. The security policy and procedure did not ensure user awareness and accountability.

The scenarios above are about basic user awareness. The main points are:

1. Never execute (double-click) an attachment. Save the file to a local or shared drive to ensure antivirus scanning of the file.

2. Always lock or logout when you physically leave your

workstation.

3. Never disable your AV software.

Fact: If applied, these three simple procedures greatly increase the effectiveness of a security system.

So, what is a Trojan?

Trojan or R.A.T. (Remote Administration Tool) software is similar to commercial remote administration software such as PC Anywhere. A Trojan in its simplest form consists of a client application and server application. The Trojan is named after the Trojan Horse in Greek mythology, where attacking soldiers hid in a hollow horse disguised as a gift in order to infiltrate the enemy defenses.

The basic idea is to execute the server application on a PC that you want to control (the victim) and the client application on the PC that will be the controller (the attacker). The connection between the two is the Internet.

The "server" component is the key to a successful Trojan attack. If the "server" can be installed and executed on a "victims" machine, successful implementation or infection is possible.

There are many "Trojans" in existence. They however all function similarly. QAZ gained notoriety with the Microsoft breach but two of the most popular are Back Orifice 2000 and Sub Seven.

So, exactly what can a "Trojan" do?

As stated above, there are many known Trojans but all function similarly. Basically, whatever you can do from your keyboard and mouse, an attacker possibly could do remotely through the utilization of Trojan software.

Once the target machine is infected, the Trojan will contact (through e-mail, ICQ or possibly Yahoo or AIM) the person who originally configured the Trojan.

Your identity (TCP/IP address) is sent to the attacker along with other information that could enable the attacker to:

- Ping and query the Trojan server version
- Reboot the victim's machine
- Lock up the victim's system
- Retrieve list of passwords (yes, it works - passwords are retrieved from memory)
- Retrieve system information
- Log keyboard activities
- View and delete log files
- Open a message box with specified text and title on the victim's machine
- Map TCP ports to another IP, console application, HTTPfileserver, filename
- List mapped ports and send TCP files
- Add and remove network shares, list shares (including LAN), mapping of shared devices, listing of active connections
- Process control (works under NT as well): list, kill, start
- Gain full access to the Registry
- Play WAV files (looped playback is possible), capturing screen, AVI and video still
- Gain full disk access: list directories and files, finding, viewing, deleting, moving, copying files and folders, transfer list maintenance
- Remote compression and decompression of files
- Resolving full host name and IP address
- Flexible server control including plugin control and command

sockets manager

- Possibility to run plugins and to activate any functions within them with specified parameters. For example one plugin can initiate a video stream and 'highjack' a remote system

- Open/close your CD-rom drive

- QAZ, which was used in the Microsoft attack, automatically copies itself throughout shared folders on a LAN.

How do I know if a Trojan has infected my workstation?

You probably won't unless the attacker wants you to know. There is however a few things you can do. Please note, these are suggested starting points and are by no means absolutely conclusive nor define a complete defensive strategy.

1. If you use your workstation outside your company's premises, install a personal firewall that has the capability to alert and block any attempt to access TCP or UDP ports internally or externally.
   Note: this won't work within your company's network.

2. When a workstation is first installed:
   - The registry should be "dumped" and recorded.
   - Contents of the win.ini, system.ini and autoexec.bat (if it exist) should also be recorded.
   - Run Netstat to build a profile of normal TCP and UPD ports. (netstat -an 1>netstat.txt will write the output to a file)

   These documents can be used to compare the contents of the registry and configuration files in the event a breach is suspected or for auditing purposes.

3. Compare the original registry dump against the current registry:

   - RunServices and Run registry Keys for example:
     - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices or HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

- Compare the contents of the win.ini file and system.ini files noting any differences in the load and/or run parameters.
- Compare the contents of the original autoexec.bat file and the current autoexec.bat file noting any differences. Pay attention to lines that have the contents: WIN [path\][filename].
- Compare the original results of netstat with a current run to see if unidentifiable services have opened new ports

```
c:> netstat –an
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 10.10.30.33:137 0.0.0.0:0 LISTENING
TCP 10.10.30.33:138 0.0.0.0:0 LISTENING
TCP 10.10.30.33:139 0.0.0.0:0 LISTENING
UDP 0.0.0.0:135 *:*
UDP 10.10.30.33:137 *:*
UDP 10.10.30.33:138 *:*
```

```
c:> netstat –an
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP   0.0.0.0:54320   0.0.0.0:0   LISTENING
TCP 10.10.30.33:137 0.0.0.0:0 LISTENING
TCP 10.10.30.33:138 0.0.0.0:0 LISTENING
TCP 10.10.30.33:139 0.0.0.0:0 LISTENING
TCP 10.10.30.33:54320    0.0.0.0:0   LISTENING
UDP 0.0.0.0:135 *:*
UDP 10.10.30.33:137 *:*
UDP 10.10.30.33:138 *:*
```

- Examine the file size of notepad.exe (The QAZ Trojan)
  - If Notepad.exe has a length of 52,000 bytes (52KB), it is normal. If Notepad.exe has a length of 120,320 bytes you are infected with the QAZ Trojan.
- Verify every file in the windows startup folder.

Summary

One of the most effective tools in implementing a secure system is an aware user. The purpose of this document was to help the reader develop an understanding of the security threat that exist due to Trojan software and how one might detect the presents of a Trojan. Also, to offer a few suggestions as to how one might protect their system or workstation from attack.

References:

CERT® Advisory CA-1999-02 Trojan Horses. 8 March 1999. http://www.cert.org/advisories/CA-1999-02.html . (14 January 2001)

Roethlisberger, Daniel "Roe". BO2K_DOX.doc. 15 September 1999. http://www.datacomm.ch/roe (15 January 2001)

Green, Thomas C. How you hack into Microsoft: a step-by-step guide. 31 October 2000**. www.theregister.co.uk/content/1/14344.html** (15 January 2001)

Neo912. The Complete Idiots Guide to Subseven. http://www.sub7page.org/help/index.shtml. (16 January 2001)

McMillen Jr., Robert V..Back Orifice 2000. 2 August 2000. (14 January 2001)

Last Updated: July 22nd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor