iDEFENSE
A VeriSign Company

VeriSign

// THE POWER OF INTELLIGENCE

Targeted Attacks and Their Impact

iDefense Intelligence Operations

Nov. 4, 2005

TABLE OF CONTENTS

1 Executive Summary

Recent news stories about a report from the UK National Infrastructure Security Coordination Centre (NISCC), followed by a similar but separate CERT advisory, have generated much concern about targeted attacks, including their likelihood and potential impact. This report overviews targeted attacks, select examples to date, exploits and code utilized in targeted attacks, likelihood and impact, and mitigation measures.

A targeted attack focuses on a specific sector, organization or individual. Typical examples of such attacks include:

- A hacker defacing US government websites for political reasons
- A company hiring hackers to steal information from rivals or perform distributed denial of service (DDoS) attacks to shut down their websites
- Malicious actors targeting specific individuals are targeted to steal money from them or gain elevated privileges on a network

By early summer 2005 Operation Horse Race (HotWorld Scandal) was announced, revealing one of the biggest industrial espionage and targeted attack incidents in the history of computing. Both NISCC and CERT organizations later warned of different targeted Trojan attacks in the summer of 2005, gaining widespread media attention. Targeted attacks have always been a focus of concern for many years. However, recent reports suggest that lower-level attackers are now attempting to target high level executives and persons of interest in targeted attacks. These attacks, contrary to many former targeted attacks, are less sophisticated and often rely upon social engineering for success.

More recent targeted attacks attempt to exploit much older vulnerabilities, likely patched by well defended networks. It is common for these vulnerabilities to be at least one to three years old when utilized in a targeted attack:

- Exploit-MhtRedir (MS04-013) Exploit
- VBS/Psyme (knowledgebase article 870669) Exploit
- Microsoft Word (MS03-050) Exploit
- Visual Basic (MS03-037) Exploit
- Exploit-ByteVerify (MS03-011) Exploit
- Index Server (MS01-033) Exploit

Sophisticated targeted attackers often profile a target and know many things about the victim before any attack is launched. This information is then used as leverage for an attack. The impact of an attack is directly related to what is compromised in the attack. Most targeted individuals are high-ranking leaders in their given organization, and are likely to have increased access rights compared to that of the average employee. This may provide attackers with greater access to sensitive company documents, trade secrets, formulas, employee data, banking information or other data of interest.

The most troubling trend with recent targeted attacks is not the sophistication but the lack of sophistication. It shows that many other hackers are now adopting such practices and will likely become more skilled and sophisticated in their targeted attacks over a period of time. This will greatly increase risk, over time, for any high profile executive, organization, or entity likely to be the focus of a targeted attack.

2 Select Examples & Reports of Targeted Attacks

2.1 NISCC Report on Targeted Trojan Attacks

In June 2005, the UK National Infrastructure Security Co-Ordination Centre (NISCC) released a report regarding targeted Trojan horse attacks (see ID# 414389, June 20, 2005). MessageLabs claims to have discovered the attack, and indicated that only 17 e-mail addresses were targeted.

The targets were reportedly high-ranking or well-known company employees of four targeted domains, which suggests a possible industrial espionage motive. The targeted attacks were reportedly designed to exploit a vulnerability in Microsoft Word (MS03-050) to silently execute arbitrary code on the targeted computer. At least two instances of targeted attacks against one company occurred over a one-month period. At least three instances of a Petite-packed Trojan horse were reportedly intercepted by MessageLabs in just a few days in early July 2005.

One of the Trojans used in the attack contains the URL http://longdiy.myrice.com and e-mail address of wfsh9411@yahoo.com.cn. The URL in this attack is related to a translation service that has not been updated for several years. It is likely that this is a victimized website abused in the attack.

The e-mail address belongs to Yaojie Zhang, of the Chinese Culture Research Institute, and has appeared multiple times on the Internet. It is possible his e-mail account was compromised for the attacks. It is also possible that this attack is politically motivated, with the Chinese government potentially considering Zhang a dangerous person for reporting society's gray side and prompting peoples' rights in China. In one online article, Zhang claims to have changed his e-mail address at least a dozen times since he believed his e-mail was being monitored by the Chinese government.

2.2 CERT Warns of Targeted Trojan Attacks

On July 8, 2005, CERT reported that various corporate websites were under targeted attacks from Trojan horse programs (http://www.us-cert.gov/cas/techalerts/TA05-189A.html). Although the advisory was extremely vague and short on details, it stated that the Trojans used in these attacks were sent to individual, targeted e-mail addresses; that they were specifically tailored to evade anti-virus protection; that they were designed to steal proprietary data (including usernames and passwords for e-mail accounts, critical system information and network drive enumeration); that they had the ability to attack other computers on the network to update code on the infected computer and upload stolen data to a remote computer.

2.3 Example of a Targeted Attack: HotWorld Industrial Espionage

In late May 2005 information was leaked to the press concerning the largest industrial-espionage incident in Israeli history, involving private-investigation firms using Trojan horse programs to steal proprietary data (see ID# 413474, June 16, 2005; ID# 405023, Dec. 14, 2004). More than 20 people allegedly involved in the incident were arrested in Israel and the United Kingdom. Authorities reportedly believe that as many as 80 companies were involved in the incident, which appears to have been underway for 18 months. Following the media release, anti-virus professionals obtained code for multiple variants of the previously unknown Trojan used in the attack (known as HotWorld). The programs are touted by some of the accused as completely legal applications.

Authorities were tipped off when an Israeli mystery writer found some of his research for a new novel on

the Internet months before it was shared with anyone else or published. This led authorities to a six-month investigation culminating in the arrest of Michael Haephrati and others in late May 2005. Haephrati, a 41-year-old programmer and Israeli citizen living in Germany and England with no former police record, was reportedly paid about 16,000 Shekels (about $3,600 USD) for each customized Trojan he authored. There are at least 15 known variants to date. The software was allegedly sold to three private-investigation agencies: Modi'in Ezrahi, Zvika Krochmal and Pilosof-Balali. According to Chief Inspector Nir Nativ, authorities believe that the program was customized for each victim that the private investigation agencies wanted to attack.

Haephrati reportedly performed installations of the customized software against targets via two methods. One was to send it to a victim via e-mail. The new code bypassed scanners, having no previously detected anti-virus signature; therefore, it was considered more trusted and was more likely to be installed by various users. The other method was to send a disk to the targeted company, claiming that the software was a business proposal from a well-known company. Once a computer was infected, the attacker gained full control over that computer and the entire network.

The investigation has reportedly implicated a car importer, two cellular phone providers (Pelephone and Cellcom) and Israel's primary satellite television company. Again, industrial espionage appears to be the primary motive for this attack. For example, the satellite company "Yes" reportedly spied on its rival, the cable television company "HOT." Malicious code was also reportedly found on computers of major companies such as Strauss-Elite, Shekem Electric and the business daily, *Globes*. Police were able to access several FTP servers in Israel and the US, each containing tens of thousands of documents belonging to major Israeli companies. Many of the files are reportedly labeled "internal" and "secret."

At least five executives from the implicated organizations have been arrested in Israel and the UK as part of a major international investigation dubbed "Operation Horse Race:" Uzi Mor, CEO of Mayer; Yoram Cohen, CEO of Hamafil; Moriah Katriel, Financial Vice President of Yes; Shai Raz, Director of Pelephone's security department; and Ofer Reichman, Director of Cellcom's security department. Police also arrested the 17-year-old son of one suspect, who allegedly attempted to erase information from his father's computer. All of those arrested reportedly claimed that contracts with private-investigation agencies explicitly prohibit any violation of the law, and that they were unaware that documents obtained through the companies were illegal.

3 Exploits and Codes Used in Targeted Attacks

Most targeted attacks to date use older codes and exploits. They are not very sophisticated — nor do they need to be to successfully infect the targeted computers or networks. Some, such as the Indian RAW operations, are more sophisticated and involve the use of newly authored code and various active hackers. Newer exploits that are easy to obtain and deploy will likely be adopted as targeted attacks continue. The following notable exploits and codes are related to incidents noted in this report.

Notable Exploits

- Exploit-MhtRedir (MS04-013) Exploit
- VBS/Psyme (knowledgebase article 870669) Exploit
- Microsoft Word (MS03-050) Exploit
- Visual Basic (MS03-037) Exploit
- Exploit-ByteVerify (MS03-011) Exploit
- Index Server (MS01-033) Exploit

Notable Codes

- Backdoor.Win32.Agent.bx
- Backdoor.Win32.Agent.hj
- Backdoor.Win32.Lecna.c
- Backdoor.Win32.Nethief
- Backdoor.Win32.Nethief.g
- Backdoor.Win32.Nethief.k
- DLoader.MM
- Downloader.Win32.Agent.kz
- HotWorld Trojans
- MSeal.A
- TK Worms
- Troj/Agent-BX
- Troj/Agent-T
- Troj/DDrop-A
- Troj/Dloader-KF
- Troj/Dloader-KZ
- Troj/Lecna-C
- Troj/Nethief-M
- Troj/Nethief-N
- Troj/Nethief-O
- Troj/Netter-A
- Troj/Riler-E
- Troj/Riler-F
- Troj/Riler-J
- Troj/RPE-A
- Troj/Sharp-F
- Troj/VBDrop-A
- Trojan.Win32.Agent.cu
- Trojan.Win32.Pusno.a
- Trojan.Win32.Riler.f
- Trojan.Win32.Riler.j
- Trojan.Win32.Zapchast
- Trojan/Exploit.MS03-37.Office.A
- Trojan-Download.Win32.Agent
- Trojan-Dropper.MSWord.1Table.a
- Trojan-Dropper.MSWord.1Table.b
- Trojan-Dropper.MSWord.Lafool.d
- Trojan-Dropper.Win32.MultiJoiner.13.b
- Trojan-Dropper.Win32.VB.gc
- Trojan-PSW.Win32.Lmir.aae
- W32/Sysgam.B
- WM97/Loof-D

These codes are often minor variants of older, known malicious code families. Most of the exploits they employ are several years old, indicating that this vector has not matured well for most targeted attacks to date. As such attacks become increasingly organized and sophisticated, more advanced and newer exploits, such as the recent JView exploit, will likely be utilized in targeted attacks (ID# 414992, June 30, 2005).

3.1 Case Study: Brazilian Businesses

In August 2005 targeted attacks were performed against specific Brazilian business in an attempt to steal bank account information. This targeted attack is likely related to the onslaught of Banker, aka Bancos, Trojans launched by Brazilian attackers over the past twelve months in particular. E-mails sent in the targeted attack had the following content:

> E-mail Body: *Claims to contain a Symantec security update.*
> E-mail Attachment: 20050725-022-i32.zip

The ZIP file contains an executable that is 372,224 bytes in size. When the executable is run an error message is displayed with the title "Erro" and content "O Aplicativo executou uma opera o ilegal e ser fechado." Meanwhile it attempts to download a Banker/Bancos Trojan horse from a remote website. It is highly likely that the remote website used in this attack, as seen with dozens of similar Banker/Bancos attacks to date, is a victimized computer being used as a remote file server by the attackers.

The downloader event results in an executable being silently installed into the Windows System directory as 20050726-007-i32-1.exe. The Windows registry key is then updated in the HKLM/Run key to then execute the backdoor Trojan horse upon Windows startup. At the time of the attack detection of the backdoor Trojan horse was very low. It was only detected initially as Downloader-ADW [McAfee] and Trojan-Downloader.Win32.Dadobra.fn [F-Secure].

3.2 Case Study: Targeted Military Targets

Targeted attacks continue to be seeded in low levels against executives and others in the late summer and fall of 2005. In this case study example 13 interceptions were made of a hostile Microsoft Word document containing an exploit. Some of the data in this report was obtained from data managed by MessageLabs Corp. The first interception of this Trojan was on Sept. 1, 2005. Targets of the attack were strategic military personnel. The e-mails sent to the targets are related to their job, socially engineered for success.

> **Subject:** US MAY LOST THE WAR IN IRAN
> **Body Text:**
> <<NAME OF ORGANIZATION OMMITTED>>
>
> US MAY LOST THE WAR IN IRAN
> A war in Iran, a war in whole Islamic world
>
> by <<FIRST LAST OMMITTED>>
>
>))) full text attached(((
>
> **********
> Welcome to the <<NAME OF ORGANIZATION OMMITTED>>!
> Our mission is to <<SNIPPED>>.
> **********
>
> Copyright © 2003
> <<NAME OF ORGANIZATION OMMITTED>>

The hostile Microsoft Word document is likely to be highly trusted by recipients of the targeted attack. The message content is short, conversational, and appears to be from a trusted colleague. The content is related to the work performed by the targets. Upon the targeted victim opening the hostile DOC file an embedded MS03-050 exploit is attempted. If executed on a vulnerable computer, a backdoor Trojan horse is silently installed on the targeted computer. Meanwhile, the victim sees a Microsoft Word document that has garbled text:

••••••••••••••
▪ 告?▪ 胧3?腑zj•X墐荥 ▪ ▪ 壒叁 ▪ ▪ 墐玄 ▪ ▪ 峒玄 ▪ ▪ P峒叁 ▪ ▪ P峒荥 ▪ ▪ Ph餮 •h殆 •h•
▪ ▪ •? •咿t(咎@ •V▪ •(•h•• •h碄 •V救B •V柝?▪ V??▪ 僵?j•X?斧• •?卸M鬱? _^[擅?鎏 •
t•3烂?鎏 •• 钁?▪ j•X脙|$••u

The Trojan horse used in this attack is now known as Trojan-Dropper.MSWord.Lafool.f [KAV]. At the time of the attack detection of the backdoor Trojan horse was very low with only one leading anti-virus product detecting the code as Exploit-1Table [McAfee]. Lafool.F provides the attacker with complete control over the victimized computer. As a result, additional network resources may be compromised, passwords and other data stored or entered on the victimized computer may be stolen, and more. This type of attack provides the attacker with everything they need to fully attack the target and/or targeted network.

4 Likelihood and Impact of Targeted Attacks

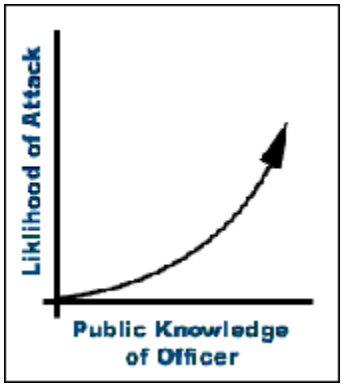
Attackers often profile the target and know many things about the victim before any attack is launched. This information is then used as leverage for an attack. For example, an attacker may use social engineering techniques in an e-mail to the target that is directly related to a project that the target is working on. This increases the chances of success that a hostile attachment is executed by the target. Additionally, much information is likely available on any given individual, including name, address, phone, e-mail and other contact information that may prove useful to an attacker seeking to compromise a specific target.

The impact of an attack is directly related to what is compromised in the attack. Most targeted individuals are high-ranking leaders in their given organization, and are likely to have increased access rights compared to that of the average employee. This may provide attackers with greater access to sensitive company documents, trade secrets, formulas, employee data, banking information or other data of interest. For example, Qaz was used to infect the Microsoft network in the summer of 2001. Media reports have speculated that many network resources were likely compromised during the multi-month infection, possibly including sensitive blueprints and other data for primary software packages developed by the company.

Security breaches have become increasingly damaging for companies in the past few years. New disclosure laws and leaks have led to significant drops in the stock price of publicly traded companies, such as CISCO in 2004, when a purported source code theft occurred. Espionage has now become big business in Israel, as can be seen in Operation Horse Race, through private investigator firms. Assets are becoming increasingly difficult to properly secure in a highly networked world complicated by outsourcing, disgruntled employee insider threats and porous perimeters.

The likelihood of an attack is influenced by how well known a particular company or individual may be to an attacker. In some cases hackers opportunistically identify a compromised network of interest, such as

a .mil domain, and work to rapidly exploit it. Other attacks target high-ranking company officials in a local or regional corporation of interest. For individual likelihood, the more well-known an individual is in the public, the more likely they are to become targeted by an attacker.



5 Mitigating Targeted Attacks

In general terms, older exploits and minor variants of older malicious code families are most commonly utilized in targeted attacks. Maintaining an aggressive patching and auditing policy, is the first logical step in the mitigation of these threats. Patching against vulnerabilities known to be regularly exploited (especially for targeted attacks), such as the MS-ITS URL-Handler exploit, is especially critical. The use of enterprise level encryption and certificate or token based authentication for e-mail also greatly reduces the ability of an attacker to spoof a sender's identity; this can drastically reduce the chances of an unsuspecting user being fooled into opening an attachment from an un-trusted source. Reducing the number of types of attachments allowed on e-mail systems, especially those which can contain executable files will also go a long way in reducing the number of ways in which an attacker can target a potential victim. The subsequent scanning of those attachments which are allowed to enter the enterprise, especially if multiple AV engines can be used in the process will also ensure that at least know malicious code threats can be blocked before they reach the end user.

For other types of attack involving social engineering, security awareness training and ongoing due-diligence training is required to help minimize the risk. Ultimately, the risk of a targeted attack can never be completely removed — but it can be dramatically lowered.

6 Concluding Comments

Targeted attacks are known to be the most difficult type of attack to defend against. Historically, targeted attacks have largely been restricted to more sophisticated attackers, limited in number. Today the landscape of attackers has dramatically changed with the onslaught of online fraud and crimeware exploitation. The targeted attackers of today are less sophisticated, preying upon social engineering, older exploits, and new malicious codes to attack targets of choice. This is a troublesome trend since it undoubtedly results in many high level executives and targeted individuals and organizations coming under attack in one form or fashion. Today the less sophisticated targeted attacks can be easily mitigated with safe computing practices. Tomorrow the knowledge base of this growing hacker population is likely to grow along with their ability to perform more sophisticated attacks.