



UNIVERSITY OF
CALGARY

A tutorial report for SENG 609.22

Agent Based Software Engineering

Course Instructor: Dr. Behrouz H. Far

Tutorial – Virus (Malicious Agents)

Written by: Kevin Tsui

Submitted on: October 22, 2001

1. Introduction

In the past, computer virus is known to destroy and manipulate personal computer's files and costing individual's inconvenient and some limited corporate loss. However, after the boom of the Internet, computer viruses, like the I-Love-You worm, are responsible for billions of dollars of damage to corporations and government agencies. Today's computer viruses are particularly aimed at shutting down services in our connected world and spying on corporations, as information is invaluable in today's business.

These intelligence computer viruses are known to be malicious agents, which is a piece of software that can carry out orders from the intruder. In this tutorial, we will discuss different types and behaviors of these agents. We will also present some advanced different infection strategies that these malicious agents use to attack a system or network. These strategies included different scanning methods and what agents can do to bypass corporation's firewalls.

In addition to infection strategies, some of the potential targets that these agents are aiming at will also be discussed. We will also discuss an example of an advance malicious agent (virus), by combining all the different strategies and properties. At the end, we will look at some potential defenses we can use to protect ourselves.

2. Types Of Malicious Agents

Generally, malicious agents are classified as four types: Rapidly Spreading, Spying, Remotely Controlled and Coordinated Attack agents.

Rapidly Spreading Agents are the malicious agents that tried to "spread" themselves (the virus program itself) to different hosts (computers) by modifying the host or its environment. This type of agents normally makes use of emails to bypass corporation's firewall and once it propagate from one machine to another by user executing it as the e-mail's attachment. Other propagation methods are guessing user's password on the network, or exploiting trusted features of the operating system, such as rexec and rsh. Example: The Morris worm and the Melissa worm.

Spying Agents are the malicious agents that aimed at transmitting sensitive information about the organizations outward. Normally, these agents use the built-in FTP function to send victim's information outward without the users or the administrator knowing it. Example: The Caligula virus and the Marker virus.

Remotely Controlled Agents are the more dangerous and also more difficult to be written. This is because this type of agents not only have to infest into a system, it will also need to contact the virus's author and authorize an external access to the system. Normally, these agents allow the intruder to perform keystroke logging, file share management, port redirection, cached password retrieval, process control ... etc. This basically allows the intruder to do whatever they wanted. Example: Back Orifice and NetBus.

Coordinated Attack Agents are probably the best-known virus by the public recently, because they aimed at disrupting normal system operations by overwhelming the network with a huge amount of traffics. They are the one that is responsible for shutting Yahoo!, eBay ... etc. large online services last year and earlier this year. These agents make use of UDP flood, Smurf-style attacks, emails ... etc. to overflow the predicted load of the victims. Example: Trinoo.

3. Advance Infection Strategies

The most commonly recognized virus by the public are mail worms, which they infest their victims through emails. However, active worms are much more dangerous and also received lower publicity. Active worms are malicious agents that can replicate themselves and potentially attack any connected servers, without any human interactions. It starts at one particular host and scans for other vulnerable host. In today's world, this will be the entire Internet. When the scan finds a potential host, it will send out a probe to infect the target. Once the probe has successfully established itself in the new host, the original worm will send a copy of itself to the probe, which will begin as another active worm.

The speed of infection is mainly limited by how fast the worm can find a new potential host and how fast the probe can infest it. This means that the rate of scan in the network is the key to its speed of infection. By making the worm multithreaded, the scanning rate can easily achieve 100 scans per second. In addition, the worm itself is relatively small in size (~100k), the probe will be even smaller (~5k), and this makes the connection bandwidth relatively small.

The most commonly used and easiest scanning method is random scan, which will randomly scan an IP address, check its vulnerability and attempt to infect the target. This scanning method results scatter the worm very quickly and the scans seems to come from everywhere. However, the spreading rate could substantially reduce after a while, because of fewer probe will discover new targets.

A more advance scanning method is Hitlist scanning. Before the deployment of the worm, the author will collect a list of potentially vulnerable hosts (generally a list of 10,000 to 50,000 is sufficient). At the release of the worm, it will first go through all the targets listed. Once a new machine is infected, it will split up the list in half, the original

worm will keep one half, the new worm will receive the other half for scanning. This quick division makes the infection extremely fast initially, and even a hitlist with a size of 200k can be reduced quickly. After this initial Hitlist scan, a worm can switch to random scan after for other possible hosts.

Although random scan and Hitlist scan works very well initially, the two scan methods start to die out after the hitlist is ran out or the number of uninfected hosts are reduced. Another scanning method known as permutation scanning can be used after the initial stage. Basically, permutation scanning means that all the infected machines will behavior differently than a potential target. If a worm finds one of these machines, it knows that it is an infected machine and it can move on to the next random machine. This can provide a semi-coordinated scan while maintaining the advantages of random scanning.

4. Potential Targets

There are three very popular targets for worms to exploit: Microsoft IIS (Internet Information Services), Microsoft Exchange, and various P2P/messenger programs. Microsoft IIS is one of the most vulnerable targets that a worm can attack. Not only newly holes are found continuously, Microsoft IIS is the installed by default with Windows 2000 server and this provides a highly homogeneous target for worms to exploit.

Microsoft Exchange could be the second target for worms. Since emails are needed to get into different networks, it provides an excellent way for worms to use this channel to bypass most of the firewalls and attack the internal networks, which generally are insecure.

In addition to Microsoft IIS and Exchange, active worms can also exploit holes in various peer-to-peer messaging applications (MSN messenger, AOL Instant messenger ... etc.). Although the connection of these targets may have poor connections, but every of these machines have information about other machines that are running the same applications. Windows XP will make this problem worse, simply because it included MSN messenger by default for every machine.

5. Potential Defenses

In order to defense the highly advanced virus mentioned above, most of the corporations and homes use Anti-virus program fight against these intrusion. Anti-virus program is effective only to those virus that infect their host by user interactions, such as email

attachments, file exchange ... etc. However, they provide no protection from the active worms, which require no human interactions.

The defense against these highly intelligence malicious agents required lot more efforts than installing a new anti-virus program. First, we have to start with software developers, network services have to be written in a more type-safe, bound-safe language and manner, to avoid buffer overflow attacks. Second, corporations should apply the “That which is not explicitly allowed is forbidden” policy. Context sensitive firewalls are installed externally, as well as internal to the network. Regular network examinations and backups are essential to prevent potential attack and to reduce losses if security has failed.

Based on a new research by Sandia National Laboratories, an agent is being trained to fight against these intelligence malicious agents.

“In March, 2000, Parks (the leader of Sandia’s government and corporate computer defence testing group) and his Red Team (government paid hackers) attacked a five computer network at Sandia protected by recently developed security bots known as cyberagents. The attack failed. The cyberagents, without outside assistance, held off four, experienced, human hackers for 16 hours.”

(Source from http://www.beyond2000.com/news/Jun_00/story_652.html)

This Cyberagent runs on every computer on the network and they protect the network in a cooperative manner. The agents will regularly exchange information about the network traffic and compare results to recognize odd attacks. They will automatically open ports, turn off services, tighten security, ... etc. to fight against intruders. In addition, the agents will replace old agents by fresh agents regularly to ensure the agent itself is not infested. Unfortunately, Cyberagent is not available to corporations and home users for a few years.

6. References

The Evolution of Malicious Agents By Lenny Zeltser
<http://www.zeltser.com/agents/agents.html>

I am Legion
http://www.beyond2000.com/news/Jun_00/story_652.html

New Anti-Virus Agent From Sandia National Labs Shows Promise
<http://www.botspot.com/news/00621Sandia.htm>

Warhol Worms: The Potential for Very Fast Internet Plagues
<http://www.cs.berkeley.edu/~nweaver/warhol.html>