WORMS

The New Weapons of Mass Destruction

By John Bumgarner

The Wriggling Threat

Worms and other malicious code have affected us all over the years. During the last two years alone, an explosion of worms attacking computers throughout the corporate world resulted in billions of dollars in lost productivity. Many of these worms caused massive shutdowns and gave black eyes to corporate reputations. The most popular worms were Slammer and Blaster.

In January 2003, the Slammer worm slithered across the world, disrupting the communication infrastructures of several countries and causing 13,000 ATM systems from one of the largest United States banks to fail. The worm even forced a 911 dispatch center in the state of Washington to use manual methods to track emergency calls.

The Slammer worm has been dubbed the fastest-spreading worm in history. That's because it used a method not normally used to propagate the connectionless protocol called User Datagram Protocol (UDP).

The Blaster worm exploded into the news in August 2003, sending businesses scrambling to patch systems and restrict network traffic to slow its movements. This worm had the potential to use the same UDP protocol, but its author instead used the Transmission Control Protocol (TCP), which is the de facto standard to propagate a worm.

Both worms had the potential to inflict widespread damage, but neither was designed for that sinister purpose. The majority of all malicious code is released into the entire Internet with no direct target, such as yourcompany.com.

Recently some virus writers are adding targeting capabilities to their code, but the viruses are still propagated across the global digital network as a whole and not targeted. Even with this lack of targeting, many corporations quickly discovered that their heavy investments in anti-virus applications did little to suppress these worms.

The vulnerabilities that these worms penetrated had been previously identified by vendors, who had published countermeasures months prior. None of these past threats can be classified as the *Holy Grail* that virus writers would like to achieve, which is the "zero-day" exploit. This type of exploit takes advantage of vulnerability on the same day that it becomes generally known to the public. The threat posed by these zero-day exploits can be extremely difficult to defend against.

The possibility of a zero-day computerized threat being released is probable in the coming years. It is feasible for someone to write and publish such an exploit, but the planning and development of such a threat is limited to a small sub-set of our global population. The two most likely scenarios for a zero-day exploit being released are either for financial and or political gains.

Targeted Attack Scenarios

The financial scenario would potentially be accomplished by professional criminals who have moved from traditional financial crimes to using the Internet to conduct their crimes. An example of this type of crime could be the development of malicious code targeted at a public accounting firm that maintains its customer books in applications such as Peachtree or QuickBooks. The malicious code could target employee Social Security numbers and banking information, which could later be used for more traditional crimes such as identify theft.

The political scenario could be accomplished by either a political activist organization or a hostile group with a political agenda. The attack could commence with a traditional Distributed Denial of Service (DDoS) aimed at targeted servers. The next phase could be aimed at individual campaign or party headquarters' computer systems. This phase could be accomplished by inserting malicious code into the computer systems that would execute on a pre-established schedule.

The third phase of this kind of attack could be a disinformation campaign suggesting that e-voting machines had been compromised in various states. If this disinformation were broadcast through media outlets such as CNN, the impact on any election could be severe. It could take days for election officials, information security personnel and the courts to sort things out.

Future Scenarios

There is also potential for a worm to be used offensively in a cyber war. It has been purported in the open-source media that countries such as China have developed offensive capabilities to wage cyber-warfare using viruses as a strategic weapon. It is more likely that this capability is being used to collect covert intelligence from computer systems within the United States. It is also likely that the United States intelligence community, especially the National Security Agency (NSA), has developed the same capabilities.

Beyond the zero-day exploits, it is possible today to develop a worm or other piece of malicious code that can be directed at a single target. A targeted attack has the potential to do great harm, especially with proper planning and testing in a lab environment. The psychological impact of such a threat on the intended target recipients is extremely high.

How would a targeted attack work? Imagine a piece of malicious code directed only at *yourcompany.com* and a single user ID. Using common system commands, the virus can determine if the pre-defined targeting information matches. If the information does not match, the virus can be programmed to check again at regular intervals. Once the information matches, the virus would run its pre-designed tasks.

The tasks could be something as simple as looking at all the open Microsoft Word documents for key words and if there is a match, executing a specific function such as sending the document to an offshore account via various methods. Those methods can include but not be limited to e-mail, file transfer protocol (FTP) or trivial file transfer protocol (TFTP).

A plausible use for a targeted worm could be to gather intelligence from computer systems that process sensitive but unclassified information that could be combined with additional information to gain a better understanding of an issue. This method of targeting would be perfect for a foreign intelligence service seeking sensitive material, particularly on science and technology-related issues. These foreign intelligence officers can program their viruses to look at keywords, such as "unclassified," "official use only," "confidential information" or "proprietary information," to name but a few.

Worms can also be engineered with the intelligence to seek out the intended hosts to infect. This is similar to bio-weapons that target and weaken the human immune systems. Such specially designed worms can quickly overwhelm the digital immune system of a company before it has time to react to the spreading infection. These types of worms are sometimes referred to as "super worms" (aka Warhol worms, flash worms, pulse worms).

These super worms can be developed with multiples capabilities, which means they could learn what the host is doing to counter the infection and modify themselves to bypass countermeasures.

Such super worms can become a national security issue if they are targeted at critical infrastructure components such as public healthcare systems. Imagine a worm that targets the drug database in a hospital pharmacy and modifies the index. This could affect patient safety, especially if the wrong pharmaceuticals are mixed and administrated.

Another type of worm that could inflict widespread damage is the "sleeper worm," which is a worm designed to await remote commands or awaken on a preset event. The sleeper worm is a threat to security, especially if it has been designed to hide its presence from security scans.

One means of avoiding detection is a technique called polymorphism through which a worm changes its signature each time it executes. This capability is useful for evading signature intrusion detection systems and anti-virus applications. Another method is "metamorphism." Worms using this technique could dynamically alter their attack behavior by obscuring embedded capabilities using various encryption methods.

Another type of worm that we have not seen in the wild is a "self-aware worm." A worm of this type has the capability of understanding its own processes and to discern and interpret the processes of similar worms. Worms with this level of artificial intelligence could actively change their attack processes by sharing information. Such information could be used to modify attack payloads and/or modify communication channels between a worm's counterparts using processes similar to a "frequency hopping radio" while protecting the channel with military-grade encryption.

Another capability, which is plausible with this type of worm and others, is self-destruction after mission accomplishment. In this scenario, a worm could decrypt a self-destruction module and segment that portion into a separate program, which deletes the main worm using advance overwrite techniques that reduce forensic recovery.

The more technology-dependent a nation becomes, the more likely a targeted attack will be successful. The United States is one nation that is extremely dependent on technology, which means a well-planned attack has the potential to cause widespread disruption of network-enabled services. Such an attack also has the potential to affect commerce and even the psyche of the general population.

As *Sun Tzu* suggested in his teaching, "it is possible to destroy an enemy without fighting." Malicious code writers are fastly approaching that capability. Organizations will have a difficult time protecting themselves when that day is achieved.

Mitigation Techniques

Proactive security measures listed below are the most effective methods to counter targeted attacks that utilize malicious code as the attack vehicle.

1. **Create a "human firewall" within your network.** This concept is not new but still has not been fully embraced within the industry. Building a human firewall involves training people in basic information security techniques, such as not opening e-mail attachments or installing software on company computers without prior authorization. These simple security methods can help reduce the possibility of a targeted attack initiated through human interaction.
2. **Create an accreditation program within your organization that meets a minimum set of security standards before they are connected to the network.** Accreditation programs can help reduce common system misconfiguration that could be exploited by malicious code.
3. **Implement network-based and host-based countermeasures to protect systems that house critical business information.** The step uses Intrusion Detection Systems (IDS) to monitor the network for known threat signatures and network anomalies. Intrusion Protection Systems (IPS) are also used to automatically respond to events that violate network security policies. Host-based IDS and firewalls can also be used to identify and potentially mitigate malicious threats.
4. **Establish a sound patch management program.** Both the Slammer and Blaster worms could have been mitigated by installing the patches released by Microsoft before the worms struck. Most organizations like to test vendor patches prior to installing, but this technique, though important, may increase the organization's risk of exposure.
5. **Develop a well-prepared incident-handling program.** Creating such a program is critical to the recovery of systems compromised by targeted attacks. A key component to any incident-handling program is evaluation drills, which are used to test the effectiveness of the program's techniques and procedures.

The purpose of these mitigation techniques is not to make your organization bulletproof, but to make it bullet-resistant to common attacks. A sophisticated targeted worm attack may still be able to counter your defensives, but the majority of attacks will be repelled.

John Bumgarner is a Senior Security Consultant at Lucent Technologies.

At *The ISSA Journal*, we deliver!
Each month, we bring you the information you need to get your job done. From spam fighting techniques to security policy enforcement, *The ISSA Journal* addresses it all.
www.issa.org