ciphertrust.com

June 2005

Zombies: The Digital Undead

Like the living dead, armies of "zombie" computers are disrupting corporate networks and sucking the life out of business-critical systems around the world. Zombies strike fear into the hearts of IT personnel responsible for maintenance of corporate networks, and particularly those charged with protecting and ensuring the availability of vital corporate e-mail systems.

A zombie is a computer that has been compromised by attackers, typically for the purpose of sending spam e-mail and viruses to literally millions of recipients. Zombies are created by the use of Trojans, malicious programs disguised as legitimate e-mail attachments or file downloads. Once installed on the victim's computer, the Trojan allows a remote hacker to take control of the machine and use it for any of a number of nefarious purposes. In fact, today's hackers (the "zombie masters") have become so sophisticated that they have begun creating coordinated networks of zombie computers that can launch a full-scale attack at a moment's notice. These attacks result in a wave of message traffic, usually directed at corporate systems. This traffic can include:

- Spam
- Phishing scams
- Viruses
- Distributed Denial of Service attacks
- Redirects to websites containing malicious code

Once zombie networks have been established, they are often auctioned or traded among underground networks of attackers. Thus, a single compromised system may be under the control of multiple criminals, each with a different purpose in mind.

Anatomy of a Zombie

Zombies can be created in several ways, including via peer-to-peer networks and maliciously encoded websites. However, the most popular method for distributing the Trojans that create zombies is via an e-mail attachment masquerading as an innocent file, such as a digital photo or contest entry form. When the user executes the attachment, the Trojan installs itself onto the user's machine. Once installed, the Trojan sends a notification to the network operator that the machine is now ready to be controlled remotely. There is typically no notification to the user that any of this has happened, so they are often completely unaware that their system has been compromised. In fact, many users voluntarily pass the Trojan on by forwarding the email to others.

The first generation of zombies was made up mostly of corporate-based machines such as Web, e-mail, or DNS servers. Because these machines were on high-speed networks, they provided an ideal platform from which damaging attacks could be launched. However, corporate systems have become increasingly secure and more tightly monitored, making them less attractive to hackers.

Now, the hackers have turned to the next set of victims, vulnerable home computer users. These computers are easy targets, as home users often lack the Internet savvy necessary to adequately protect their machines with firewalls and up-to-date anti-virus protection; many will also willingly open email attachments from unknown senders, enticed by the promise

Terms to Know:

Zombie *– A computer that has been compromised by attackers, typically for the purpose of sending spam e-mail and viruses as part of a network of similarly compromised machines*

Trojan *– A malicious program disguised as a legitimate file.. Once installed on the victim's computer, the Trojan allows a remote hacker to take control of the machine and use it for any of a number of nefarious purposes.*

DDoS *– Acronym for Distributed Denial of Service., a flood of traffic targeted at a specific network, eventually resulting in system overload and shutdown*

of easy money or cheap prescriptions. In addition, the widespread availability of always-on, high-speed home connections using cable and DSL has made the home user an obvious target for zombie masters. In fact, this alone is the single largest contributing factor to recent escalations in spam, phishing attacks and Distributed Denial of Service (DDoS) attacks.

How Zombies Attack

Zombie networks can be configured to attack enterprises in a number of ways. Among the most popular is to create a globally dispersed "spam cannon," sending massive volumes of unwanted email, including dangerous phishing scams that prey on unsuspecting end users. When the attacks involve distribution of viruses via spam techniques, the stakes are raised even higher.

The most damaging type of zombie attack, however, is the DDoS, which is a flood of traffic targeted at a specific network, eventually resulting in system overload and shutdown. These attacks have been known to continue for days on end, and enterprises that are not prepared for them can be brought to their knees, as loss of the email system can cause a major disruption in the flow of business activities. A service degradation attack is a similar type of attack, except that rather than sending huge amounts of traffic all at once, the zombies increase traffic to an email system gradually until the system is eventually overloaded and knocked offline.

The costs of a DDoS attack can be crippling to today's enterprise, resulting in lost sales during downtime and recovery, and more importantly, loss of trust from partners and customers should the attack become public information. Realizing the strength of the hand they hold, zombie masters have put a new twist on an old game, extorting money from corporations in exchange for assurance that the corporate networks will not be brought down by an attack. In addition, an evolving threat is the commissioning of attacks on rival companies. In one case, a business owner paid as little as $1000 to have DDoS attacks carried out on two competitors' websites in order to shut them down for hours at a time.

To understand just how large a zombie network can grow, consider this: a Norwegian telecommunications provider recently discovered and shut down a network consisting of over 10,000 zombie machines. Taking into consideration that each zombie involved in a recent DDoS attack launched 64 connection attempts per second against the targeted corporation, it's easy to see how even the most robust systems can wilt under the massive load inflicted upon them.

Keep Zombies at Bay

Some basic tenets of security should be followed at all times, whether you want to protect your enterprise network from spam, viruses and DDoS attacks spewed forth by zombie networks, or protect your home computer from joining the ranks of the undead.

Enterprise Protection

The single most effective way to ensure that zombies don't find their way into your corporate networks is to trust your e-mail security to a hardened gateway appliance. The best-of-breed appliances available offer both inbound and outbound protection via an

objective, dynamic reputation system, connection management technology and robust anti-virus capabilities.

Sender Reputation *– A measure of the historical quality of messages sent by a particular entity. Today's most effective reputation systems are able to assign reputation "scores" to individual IP addresses, ensuring that senders who attempt to disguise their identity are flagged and their messages subsequently blocked.*

Connection Management *– The process of combining sender reputation scoring with traffic shaping technology to limit the ability of unwanted senders to connect to the target mail server.*

Reputation Systems

The purpose of a reputation system is to determine who the "good" senders are. These can be defined simply as those who have historically sent legitimate mail on a regular basis. By evaluating senders based on their past behavior, a more accurate picture of their intentions and legitimacy can be discerned. Has the sender engaged in spamming, virus distribution or phishing attacks? If they have, an effective reputation system knows and flags the message. Has the sender ever been seen before? If not, a reputation system should pay close attention to ensure that the sender is not a zombie machine.

Click here to learn how CipherTrust's TrustedSource reputation system defines sender reputation for every IP address around the world, giving organizations an accurate view of who is sending them mail and how likely that mail is to b e spam sent by zombie networks.

Connection Management

Connection management technology works by combining an objective reputation system with traffic shaping technology. If the reputation system determines that the sender is unwelcome, an effective technique for encouraging them to focus their efforts elsewhere is to reject connections from their IP address altogether for pre-defined intervals. And since having to scan fewer messages reduces throughput needs, robust connection management technology provides a significant boost to your return on investment.

Outbound Anti-Virus Protection

Should a situation arise in which a workstation on your corporate network is infected by a Trojan, outbound anti-virus scanning will ensure that it is unable to spread outside the network via e-mail. You don't need to be told about the disastrous consequences of spreading viruses to partners and customers, and keeping your email server from becoming a "spam cannon" is of paramount importance to protecting your company's reputation as a responsible sender.

IronMail Connection Control is the first offering to combine traffic shaping and reputation services to dramatically increase your organization's message handling capability and reduce your spam-fighting costs. Click here to learn more.

Home Protection

The best way to ensure that a personal computer is not taken over by a zombie-inducing Trojan is to protect it. To that end, some basic security steps should be followed at all times:

Get Vaccinated

Be sure to keep the anti-virus software on your computer up-to-date. Many anti-virus programs offer automatic updating to keep up with the ever-changing virus landscape. Take advantage of this feature if it's available from your anti-virus software. If it's not, find a solution that offers it. Anti-virus protection without automated updating is obsolete before it's ever installed.

Firewall Your System

A firewall is designed to stop unwanted traffic flowing into our out of a system, and "hide" your computer from would-be snoops. The Microsoft Windows XP operating system has built-in firewall functionality, and many free personal firewall programs are available for private use.

Don't Talk to Strangers

Never open unanticipated file attachments, especially when they come from unknown sources. If you're not sure about an attachment, save it to your hard drive first and scan it with anti-virus software to check for dangerous files.

Slaying the Zombies

All jokes about shotguns and baseball bats aside, fighting zombies is not easy work. Zombies exist in huge numbers and are designed to be disposable so that if some are "killed," or taken offline, the zombie master hardly notices. The lifespan of a zombie is short, and most are useful for only a few days or weeks before they are repaired or otherwise compromised. To combat their short life expectancy, zombies are self-propagating, constantly infecting new computers. As of June 2005, CipherTrust identified an average of over 172,000 new zombie machines each day.

At CipherTrust, we've long been the leading provider of solutions to companies looking to protect their enterprise email gateways from spam, viruses, phishing attacks, or other malicious behavior. Now, we've zeroed in on zombies, and our customers are reaping the benefits. IronMail, the e-mail security appliance that protects over 1500 corporate networks and nearly 10 million enterprise end users, employs a variety of techniques to identify and respond to zombie networks, not the least of which is CipherTrust's proprietary TrustedSource reputation system, which tracks email sending behavior to stop attacks before they ever reach your mail server. To learn more about IronMail and how it protects enterprises of all sizes from zombie attacks, visit CipherTrust online at www.ciphertrust.com or call 1-877-448-8625.