



- » Home
- » In the News
- » Virus Report
- » Subscribe Now Online
- » Media Kit
- » Archives
- » Contacts
- » Calendar of Events
- » Articles
- » Article Submissions
- » Web Seminars
- » White Papers
- » Inside Current Issue

Inside Current Issue: Cover Story

Organized Cyber Criminals Use Botnets to Target Businesses By Brian Contos

Organized cyber criminals are only different from independent cyber criminals in that they have more resources in terms of number of people working on exploits and scams, money to spend, access to technology and some semblance of organizational leadership. The perpetrators of organized cybercrime can be loosely divided into two categories.

The first category consists of traditional crime organizations that have discovered there is value to be had by leveraging cybercrime. These groups operate like legitimate businesses in terms of offering goods, services and trade. However, their business is illegal and in terms of cybercrime they may be trafficking in corporate secrets, identity information, extortion, committing various frauds and scams, money laundering and distributing illegal materials. These groups can be global, highly structured, crime syndicates and drug cartels or some less ordered, less fantastic variant. They can be found virtually anywhere, but are commonly based in areas of political, economic or social transition where government communication is poor and laws are not enforced. Some examples of organized crime groups are the Italian Mafia, Russian Mafia, Colombian and Mexican Cartels, Asian Triads, and Nigerian Criminal Enterprises.

The second category consists of individuals that have banded together in an effort to reduce personal risk and increase revenue opportunities. As with any business, criminal or otherwise, organizing helps to nurture growth and push the risk verses reward pendulum closer to reward. These individuals tend to approach cybercrime from being technically sophisticated first and criminals second. By working collectively towards a common goal, usually money, they can be more efficient and effective.

Generally these groups are not terrorists or nation-state threats. While cyber terrorism is certainly a possibility, it is over sensationalized in the media. It simply doesn't have the prevalence of a basic criminal trying to make money. Terrorism typically has to do with force or violence against people or property in hopes of bringing about political, social, religious or ideological change. While a terrorist may feel that hacking a power grid, throwing financial networks into chaos or interrupting communication networks are an interesting target, it is far more likely for a criminal to simply steal your identity, credit card information or intellectual property. However, terrorist may find that cybercrime can be an additional revenue source, a supplement for other agendas, and can be used as an information gathering technique.

Nation-state threats such as intelligence agencies tend to have military-level funding and pose the most significant risk. They may have political motivations or they may be assisting in industrial espionage for businesses run by their countrymen. For example, North Korea's government-sponsored hackers attend a five-year college called the



June 2006 Issue

Automated Warfare Institute. South Korea's National Assembly Defense Committee reported that North Korea has trained an army of over 500 computer hackers, and produces an additional 100 annually. Many countries have similar cyber warfare organizations within their government, often much larger. However, as with terrorism, nation-state threats are less common threats for most organizations when compared to organized cybercrime for profit.

Botnets Explored

There are a number of crimes that can be perpetrated by organized cyber criminals. Perhaps one of the most prolific mechanism for committing these crimes is through botnets.

Botnets (also called bots, robots, zombies and botnet fleets) are malicious software programs that are loaded on a target system unbeknownst to the victim. There are hundreds of botnets and botnet variants. Once installed, these botnets can be controlled through a Trojan horse backdoor by whoever controls the botnet controller, which is like a central management system for the botnet fleet. With the controller, one or many systems can simultaneously act on command.

Common uses for botnets are to forward transmissions such as phishing scams and spam and to distribute more malicious software such as viruses and keyloggers. Another use is to have the botnets perpetrate distributed denial-of-service (DDoS) attacks rendering a target site sluggish or unavailable; bots will commonly have code designed to issue SYN-floods and UDP-floods. There are other attacks botnets can affect, but these are the primary issues as they relate to business. Because of their prevalence and capabilities, many security experts agree that botnets pose a bigger risk than even worms or viruses on the Internet.

The targets can be virtually any unprotected system, but they are usually unprotected home computers connected to the Internet with high-speed links. In some cases, the end goal is to use these victimized home computers to attack specific business targets. Some of these botnet fleets number in the hundreds of thousands which make them a formidable adversary for an organization and a lucrative revenue stream for a criminal that rents out the botnets as an hourly service to other criminals.

Impact of Botnets on Business

Since the organized cyber criminals that put these botnets in place can attack, relatively anonymously, from virtually anywhere, and move their base of operations around, they can be difficult to stop. Additionally, they have the resources to continue research into new methods of exploitation once the vulnerability they currently use to install the bot becomes broadly patched or the attack is otherwise protected against with safeguards like firewalls and malware detectors.

In the past, it was months between the discovery of a vulnerability and the creation of an exploit -- called the vulnerability threat window. This window has been shrinking from many months to weeks or days, partly because of organized crime. For example, the Witty worm and Zotob worm were examples of a one-day vulnerability threat window; it is believed Zotob was written expressly by an exploit writer under contract to build an attack that would lead to financial gain. As with many exploits today, they are designed to assist in acts such as fraud that will lead to revenue. It is also argued that Zotob was written by a lone 18-year-old without the resources and funding of an organized crime group.

The way that organized cyber criminals can attack businesses using botnets vary. An attack on a single target business can spread like a pandemic across an organization's global footprint. Because the attacks are targeted, they will spread more quickly and relentlessly than opportunistic attacks. Here are a few ways that organized cyber criminals can leverage botnet-based attacks.

Denial-of-Service Attacks

Online gambling organizations have been a popular target of attacks and exploitation. The business will be contacted with some form of extortion demanding money to prevent DoS attacks that will shut down their web sites. This typically comes directly before a major sporting event like the Super Bowl where an outage of just a couple hours could cost millions in lost revenue. Additionally, customer confidence diminishes, partner and investor relations may be strained, and the organization may lose existing and future customers over the incident. As a demonstration of power, the criminals may crash a couple servers to help create a compelling event. A fleet of botnets that is either owned or rented by the criminals provides most of what is needed for this type of attack to work.

Spam and Phishing

Botnets can be used by organized crime to target businesses with spam and phishing scams. Exploits of this nature can also lead to compliance-related fines and litigation costs. Just as individuals can be targeted to divulge sensitive information, or download malicious code, individuals within a specific business may be targeted. The organized criminals may not be looking for identity information and account numbers, but rather intellectual property such as new marketing strategies, customer contact lists, employee salaries, product development plans and so forth.

There are potentially competitive organizations that would pay for this valuable information and the fact that industrial espionage can be conducted with a simple e-mail makes for an inexpensive information extraction method. Also, since botnets can target virtually every person in the business; even if only 1 percent of the targets respond, it is still a success.

Malware

Botnets may deliver a spam message that tricks the victim into downloading malware. Also, the botnet itself can compromise a system if it is vulnerable and exposed. Once behind an organization's perimeter defenses, these types of attacks tend to spread quickly when the proper safeguards are not in place. Keystroke loggers and sniffers can capture information and forward it back to the criminal.

Many bots are enabled with filters defined by the criminal to capture specific information and report it back to the criminal. The bots may also use rootkit functionality to evade detection, and have automatic upgrade mechanisms to keep the bot up-to-date and safer from detection. Finally, since the botnet allows for the criminal to control the bot, they can control the target machine, or at least issue a predetermined set of commands to cause further chaos.

Business Considerations

Businesses have to consider cyber-crime when evaluating risk. This isn't the old risk model where concerns were around web defacements and viruses that were more of a nuisance than criminally motivated. While traditional attacks like these haven't gone away, the more critical threats are related to the exploitation of sensitive information, fraud and extortion. Botnets are one vehicle to commit these crimes quickly and on a large scale. Risk must be evaluated in these terms and security safeguards need to consider these threats.

[Five steps for businesses to protect themselves.](#)

1. **Participation in information sharing liaisons** with government agencies, law enforcement and organizations in similar vertical markets helps businesses understand threats more holistically across their industry.
2. **Employee background checks** with annual employee reviews and investigations into partners should be thorough. This will reduce exposure to criminal activity from inside and unwittingly getting into a partnership with an organization that is a front for organized crime.
3. **A combination of incident prevention, detection and management solutions need to be deployed organization-wide.** Technology needs to be considered as part of the equation, but should not be the only factor addressed. In security, it is about people, process and technology. Sensitive data should be secured with need-to-know access, separation of duties, strong authentication and other preventative measures. Monitoring technology should be deployed to overlap the prevention capabilities and fill in any gaps that prevention may leave.
4. **Employee awareness programs, policies, and procedures** need to be implemented, updated, and communicated. Education needs to be repeated at regular intervals to be effective.
5. **Defense-in-depth best practices** should be followed to ensure that the perimeter and the internal network are resilient to botnet attacks. This includes patching, malware detection, intrusion detection, access control, real-time event correlation and analysis, incident management procedures, network segmentation, automated remediation capabilities, etc.

The Internet is simply a new medium to commit old crimes, and botnets are a vehicle. An individual doesn't have to belong to an organized crime syndicate to create and use botnets. However, these organizations have the funds, technology and human resources to develop exploits faster than lone criminals do. In addition, they create their exploits not to be recognized by their peers as great hackers or out of general malice, but around deriving profits.

About the Author:

Brian Contos, CISSP, is the Chief Security Officer for ArcSight. He can be reached at bcontos@arcsight.com.

[Go Back](#)

© IMPIRE Communications, LLC All Rights Reserved.
Website designed & managed by [Oculus Networks](#)