

Battling the botnets and the zombies

BrandProtect puts malware in its place

The proliferation of malware is a cause for increasing concern for businesses and consumers. While many instances of malware are little more than a nuisance for users, others can have a much more insidious impact on a company's online credibility. For one online consumer services site that had many thousands of visitors a day, a malware invasion known as Storm Worm turned thousands of personal computers into an army of zombies known as a botnet. With the help of BrandProtect, the perpetrators were traced, infected users identified and notified, and the botnet threat was mitigated.



The building of a botnet army

In the summer of 2007, the online consumer service organization received an ominous notice from a consumer. It appeared that the person had received an email from what they thought was the consumer service organization that contained a link to its site. The email was a fake designed to lure recipients to a location in order to trigger a malware download onto their PC. The intent of the malware – identified as the Storm Worm - was to turn the recipient's machine into a zombie or robot to serve a global botnet.

Botnets are used by perpetrators to conduct various malicious activities, such as launching denial of service attacks against specific organizations. It does this by using a global network of zombies to flood Internet connections with spam and ultimately prevent connectivity to legitimate sites. In this particular case, the downloaded malware caused infected PCs to send out spam emails containing the location of the malware download in order for it to propagate to even more unsuspecting users.

Upon making some initial inquiries, the company unearthed 10 emails that referenced their brand and included unique IP addresses that were distributing the malware. BrandProtect was then engaged to investigate the matter further. In doing so, they quickly found that they had uncovered the tip of a

huge iceberg. Within two hours, BrandProtect logged hundreds of similar types of emails from unique IP addresses of infected systems. These infected systems were acting as a download source for the Storm Worm – and it appeared that the infection was rapidly expanding to thousands of machines by the hour.

Drawing the bees to the honey

Catching malware perpetrators is a highly complex exercise that requires a vast network of connections and creative thinking. To put the scope of this job in perspective, this Storm Worm attack generated 20 times more instances than a largescale phishing attack at a financial institution. This meant the volume of malicious emails generated easily reached the hundreds of thousands within a matter of days.

To begin, BrandProtect used a “honeypot” strategy. This is a comprehensive trap that is used to detect attempts to spoof an organization's brand. In simple terms a honeypot is a mailbox that is made to appear to be part of a network, but is isolated and monitored. The mailbox collects spam messages, which are then parsed based on client keyword matches. The main purpose is to attract malicious or unauthorized activities and provide a means to trace the sources of attacks.

The BrandProtect Honeypot allowed the team to track the thousands of IP addresses hosting the malware in question.

BrandProtect then used the information to begin mitigation procedures. Once the infected addresses were identified, BrandProtect began contacting the ISPs worldwide who were responsible for the IP addresses. The ISPs in turn had to determine the specific machine that was using the address at the time, temporarily suspend the machine from the network, notify the individual, and request the owner clean the system.

This was no small task. Since there were hundreds of ISPs involved, BrandProtect mobilized their Incident Response Analysts and engaged the services of dedicated Internet Response Teams around the world, to help coordinate the mitigation efforts in their specific geographic regions.

At the same time BrandProtect applied reverse engineering procedures on the malware in a lab environment. This allowed the research team to identify the domains that were being used to coordinate the attack. A total of 13 different domains were identified – all of which were registered through a single registrar in Estonia, which was identified as having suspect motives.

Battling the botnets and the zombies

GLOSSARY

Malware, short for malicious software, is software designed to infiltrate a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

A zombie computer (often shortened as zombie) is a computer connected to the Internet that has been compromised by a hacker, a computer virus, or a trojan horse. Generally, a compromised machine is only one of many in a botnet, and will be used to perform malicious tasks of one sort or another under remote direction. Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies.

A Botnet is a collection of software agents, or robots, that run autonomously and automatically. but it can also refer to a network of computers using distributed computing software.

This made contacting the registrar a questionable option as they could potentially alert the perpetrators to BrandProtect's actions.

In addition to filing formal complaints with international regulatory authorities and international accreditation organizations, BrandProtect found the most expedient and effective action plan was working with ISPs to "black hole" the domains and make them inaccessible to users on their networks. By September, the domains were no longer accessible through any major ISP network in North America, thereby preventing infected systems from contacting their command center.

Deflecting the army

By blocking the offending domains, BrandProtect made it impossible for perpetrators to reach their victims. As soon as all aspects of the mitigation strategy had been implemented there was an immediate decline in numbers of active IP addresses and the perpetrators were no longer referencing the online consumer service organization in their spam messages. After approximately two months, BrandProtect saw all monitored IP addresses were no longer hosting the malware and no new active IPs have appeared since, which indicated that they had successfully channeled this attack away from the client. BrandProtect continues to perform monitoring services to ensure that there is no recurrence of a malware attack.

The Storm Worm is the most prevalent piece of malware and the biggest threat to Internet security today. The measures taken by BrandProtect to mitigate the Storm Worm, along with the recommendations to further secure their client's brand from falling victim to future targeted attacks, have enabled the consumer service organization to begin rebuilding the confidence of their customers while retaining a valuable revenue stream.

About the Storm Worm

With the Storm Worm, spam is sent out claiming to provide an item of interest to the recipient – be it a sports score tracker, an e-card, etc. When the user clicks on the link, they are sent to a compromised system - a zombie - that has already been infected. The Storm Worm Trojan covertly downloads onto the user's machine without the user's knowledge and their computer is then opened up for use by the perpetrators. The infected computer is now part of a botnet, which can be used to engage in any number of illegal activities, such as denial of service attacks.



About BrandProtect

As the leader in internet reputation management, BrandProtect empowers organizations to gain control over how they are represented online by uncovering and mitigating the issues that put their reputation at risk and erode customer trust. BrandProtect's Response Services help detect, uncover and mitigate brand and trademark infringement issues, phishing attacks, web traffic diversions, website integrity issues and defamatory discussions. BrandProtect was the first company of its kind to be offered full membership by the Forum for Incident Response and Security Teams (FIRST). It also has relationships with more than 4,000 Internet Service Providers globally, accounting for more than 90 percent of the traffic flowing across the internet.

For more information:
www.brandprotect.com
onlinesales@brandprotect.com
1.866.721.3725