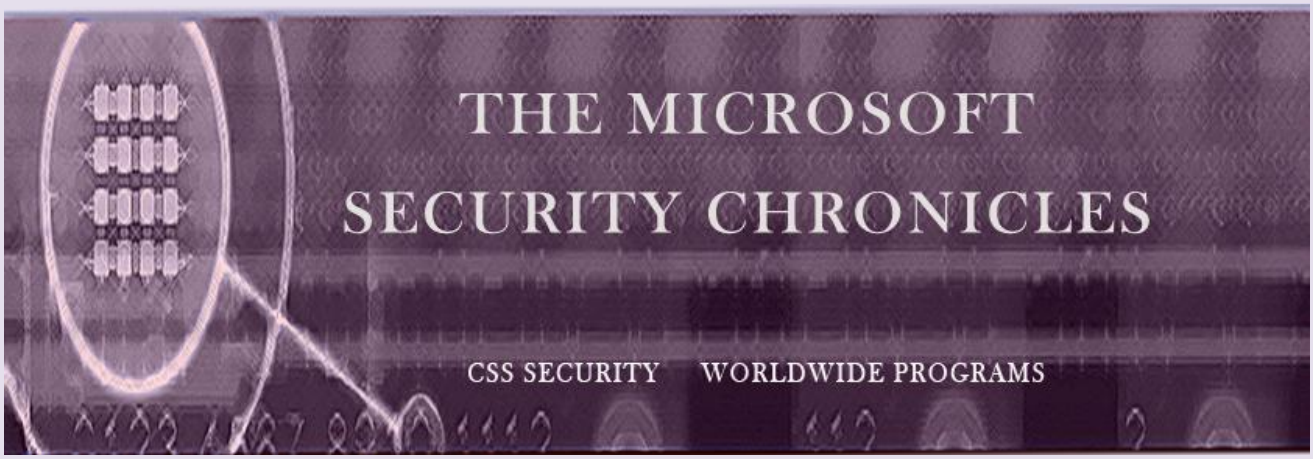

April 14, 2011

INSIDE THIS ISSUE

MICROSOFT RESOURCES

Microsoft Security Home

Microsoft Trustworthy Computing

Microsoft Security Sites Worldwide

FBI and DOJ Take on the Coreflood Botnet

Microsoft

Today [April 13, 2011], the FBI and U.S. Department of Justice announced a legal and technical operation to take down the Coreflood botnet, using a civil suit for a temporary restraining order against the operators of the botnet and criminal seizure warrants in order to disable the botnet's infrastructure.

Analysis:

In March 2011, Microsoft took legal action to take down the Rustock botnet and earlier, in February 2010, it had taken legal action to bring down the Waledac botnet. Symantec reported (PDF) that disrupting Rustock cut down global spam volumes by one-third. Microsoft recently provided an update on the initial revelations and results of the Rustock takedown, reporting that it was continuing the legal proceedings and working with its partners to keep the botnet down.

On April 13, 2011, the U.S. Department of Justice (DOJ) and the U.S. Federal Bureau of Investigation (FBI) announced that they had undertaken a legal and technical operation to take down the Coreflood botnet, using a civil suit for a temporary restraining order against the operators of the botnet and criminal seizure warrants in order to disable the botnet's infrastructure.

The FBI reported that investigation of Coreflood began in April 2009 when a Connecticut-based company realized that hundreds of computers on its networks had been infected.

The Coreflood botnet is a network of hundreds of thousands of computers infected with a malicious software program known as Coreflood, which installs

SECURITY CALENDAR

April 2011

16 Infiltrate 2011 - Miami

20 SOURCE Conference Boston 2011

22 Thotcon – Chicago

28 SyScan 2011 - Singapore

May 2011

05 Microsoft Bulletin Advance Notification

10 Microsoft Security Bulletin Release

15 AusCERT2011 – Australia

16 YStS – Brazil

24 HITB Amsterdam

itself by exploiting a vulnerability in computers running Windows operating systems.

A news story reported that rather than merely sending spam, Coreflood stole banking and other financial information from infected systems. This harvested information was then sent to the command-and-control servers, and according to court filings, allowed criminals to steal hundreds of thousands of dollars from victims. The Coreflood software has been around since 2003 and over the course of its life, infected more than two million machines.

Microsoft commended the FBI and DOJ for the action against Coreflood. In coordination with the FBI, the Microsoft Malware Protection Center has added Win32/Afcore (Coreflood) malware detection in its Malicious Software Removal Tool to help minimize the malware's future impact.

Microsoft has a dedicated website to provide free information and tools to help people get rid of botnet malware in order to regain control of their computers. Microsoft also provided an intelligence report on botnets in the latest edition of its Security Intelligence Report V9.

Expect Targeted Attacks After Massive Epsilon Email Breach, Say Experts

Computerworld

Security experts today [April 04, 2011] warned users to be on the watch for targeted email attacks after a breach at a major marketing firm that may have put millions of addresses in the hands of hackers and scammers.

Analysis:

Reports of enterprise data breach incidents continue to rise. On April 01, 2011, in a data breach considered to be the largest breach in U.S. history, email marketing company, Epsilon announced that an incident was detected where a subset of Epsilon clients' customer data was exposed by an unauthorized entry into Epsilon's email system.

It was reported that companies hire Epsilon to send out a total of more than 40 billion messages on their behalf each year. With millions of email addresses thought to have been stolen, the problem could be a serious one. Once scammers know their victims' names and email addresses, along with the companies that they do business with, they can craft very targeted spear

phishing email attacks that try to trick victims into revealing more sensitive information such as passwords or account numbers.

Several companies warned customers that their names and email addresses had been breached by someone outside the company. Epsilon's parent company, Alliance Data Systems, confirmed that the company was working with authorities and external experts to investigate the breach. It said that it believed the greatest risk from this breach was the potential loss of clients.

A benchmark study of 51 U.S. companies by Ponemon Institute – U.S. Cost of a Data Breach – had found that data breaches in 2010 cost their companies an average of US$214 per compromised record.

One week after the Epsilon breach, the Better Business Bureau warned that it was seeing one of the first Epsilon data breach phishing scams. The emails were being sent from a fake 'Chase Bank,' one of the companies whose data was compromised. The email warns that 'your account' will be deactivated or deleted if you do not update your profile immediately. The email instructs consumers to update their account by clicking on the link provided.

Several U.S. senators and House representatives are demanding more details about the magnitude of Epsilon's data breach and how the email thefts are impacting consumers. They have also asked for specific details on the timeline of events as well as details as to what the firm has done since then to mitigate the effects of the breach and prevent future incidents.

The FBI provides information for consumers on how spear phishing works and recommendations to avoid becoming a spear phishing victim. Microsoft also provides guidance on how customers can recognize a phishing email message.

RSA Explains How it Was Hacked

All Things Digital

In the end, even computer security companies suffer from the kind of human failings that make securing computers such a challenge. That's at least one lesson to draw from the explanation from RSA, the company which makes the widely used security tokens like the ones in the picture [in article]. It disclosed last month that it had come under an "extremely sophisticated attack," and that some information concerning the tokens has been taken by unknown attackers.

Analysis:

The RSA suffered a sophisticated data breach in March 2011, resulting in information about RSA's SecurID authentication tokens used by millions of people, including government and bank employees, being stolen. The company's investigation led it to believe that the attack was in the category of Advanced Persistent Threat (APT) and that the stolen information could potentially be used to reduce the effectiveness of a customer's two-factor authentication implementation as part of a broader attack.

RSA recently provided a blog post explaining how the hacking attack had worked. It found that:

1. *The attacker sent two different phishing emails over a two-day period to two small groups of employees; you wouldn't consider these users particularly high profile or high value targets. The email subject line read "2011 Recruitment Plan." The email was crafted well enough to trick one of the employees to retrieve it from their Junk mail folder, and open the attached excel file. It was a spreadsheet titled "2011 Recruitment plan.xls." The spreadsheet contained a zero-day exploit that installs a backdoor through an Adobe Flash vulnerability.*

2. *The attacker then installed a remote administration tool that allowed the attacker to control the machine. It was a Poison Ivy variant set in a reverse-connect mode that makes it more difficult to detect, as the PC reaches out to the command and control rather than the other way around.*

3. *Having set remote access, the attacker started digital shoulder surfing to establish the employee's role and their level of access. In the RSA attack, the timeline was shorter than in other typical attacks, but still there was time for the attacker to identify and gain access to more strategic users.*

4. *The attacker then established access to staging servers at key aggregation points. Then they went into the servers of interest, removed data, and moved it to internal staging servers where the data was aggregated, compressed, and encrypted for extraction.*

5. *The attacker then used FTP to transfer many password protected files from the RSA file server to an outside staging server at an external,*

compromised machine at a hosting provider. The files were subsequently pulled by the attacker and removed from the external compromised host to remove any traces of the attack.

In another data breach incident, security firm Barracuda Networks became the latest victim of a SQL injection attack on its website on April 12, 2011, that compromised lead and partner contact information.

Barracuda Networks confirmed the attack and provided information on how the SQL injection attack on its website was executed. The company's investigation indicated that:

1. *The firewall in front of its website was unintentionally placed in passive monitoring mode and was offline through a maintenance window that started on the night of April 08, 2011, after close of business.*
2. *On Saturday night, an automated script began crawling their website in search of unvalidated parameters. After approximately two hours of nonstop attempts, the script discovered a SQL injection vulnerability in a simple PHP script that serves up customer reference case studies by vertical market. This customer case study database shared the SQL database used for marketing programs which contained names and email addresses of leads, channel partners, and some Barracuda Networks employees.*
3. *The attack utilized one IP address initially to do reconnaissance and was joined by another IP address about three hours later. The company has logs of all the attack activity, and believes it now fully understands the scope of the attack.*

Web Attacks Skyrocketed 93% in 2010

Information Week

The volume and sophistication of online attacks continues to increase. In fact, the daily volume of web-based attacks increased by 93 percent from 2009 to 2010, while attack toolkits grew to account for two-thirds of all web-based threats.

Analysis:

According to Symantec's Internet Security Threat Report, released on April 05, 2011, the year 2010 saw significant escalation in daily threat volume, sophistication, and cost of security breaches. Some of the key points in the report include:

1. *The volume of web-based attacks increased by 93 percent from 2009 to 2010 due to the growing proliferation of web attack toolkits and use of shortened URLs.*
2. *The average number of identities exposed in each of the data breaches caused by hacking in 2010 was 260,000.*
3. *In 2010, there was a 42 percent increase in the number of reported mobile operating system vulnerabilities, compared to 2009. Most malicious code for mobile devices consists of Trojans that pose as legitimate applications. These applications are uploaded to mobile app marketplaces in the hopes that users will download and install them.*
4. *The number of attacks propagating using executable files sharing increased by 74 percent from 2009 to 2010.*
5. *The 14 zero-day vulnerabilities in 2010 were found in applications such as Internet Explorer, Adobe Reader, and Adobe Flash Player. Industrial Control System software was also exploited.*

Microsoft recently published a Security Update Guide with in-depth information on protecting IT infrastructure while creating safer, more secure computing and Internet environment. The guide was developed to help IT professionals better understand and maximize Microsoft security update release information, processes, communications, and tools.