Yet Another Zero-Day: Japan Hit with Ichitaro Vulnerability

Created: 14 Nov 2013 14:03:17 GMT • Updated: 23 Jan 2014 18:03:07 GMT • Translations available: 日本語

Symantec Security Response SYMANTEC EMPLOYEE

+2 2 Votes

Symantec. Official Blog

Share Tweet submit

The security industry, as well as IT administrators across the globe, has been busy recently dealing with multiple zero-day vulnerabilities emerging in quick succession. Before anyone has time to draw a breath after the barrage, yet another zero-day has appeared, ready to cause people problems. Well, for people in Japan at least, since the vulnerability is in the Japanese word-processing software Ichitaro.

Ichitaro developer JustSystems recently announced that the Multiple Ichitaro Products Unspecified Remote Code Execution Vulnerability (CVE-2013-5990), allowing the execution of arbitrary code, exists in Ichitaro products. In September 2013, Symantec discovered attacks in the wild attempting to exploit this vulnerability; however, the exploits did not properly work to compromise the system in our testing environment. As always, we exercised the responsible vulnerability disclosure process following this discovery.

Our analysis revealed that the samples, detected as Trojan.Mdropper, for these attacks all contained the same back door Trojan, which Symantec detected as Backdoor.Vidgrab. If the exploit is successful, in theory the shell code would be executed to drop and launch the simplified Chinese version of notepad.exe while compromising the system, with the back door connecting to a remote site. Coincidently, the identical Backdoor.Vidgrab variant was used as a payload for a watering hole attack exploiting the Microsoft Internet Explorer Memory Corruption Vulnerability (CVE-2013-3893), which was patched in October 2013. It is reasonable to assume that the same malware group, or another group with close connections, is behind the attacks that utilized the Internet Explorer and Ichitaro vulnerabilities. Backdoor.Vidgrab is known to be used to target the Asia-Pacific region with government sectors being the primary targets according to TrendMicro. Symantec telemetries do not dispute this claim.

Although Trojan.Mdropper is sent to targets as email attachments with the Ichitaro file extension .jtd, the files are actually .rtf or rich text format files. The files cannot be opened using Microsoft Word as they are designed to work only with Ichitaro. An interesting point of this attack campaign is that the malware group used unusual subject lines and email content that are not commonly used in targeted attacks. One of the emails used in this targeted attack campaign can be seen in the following figure.

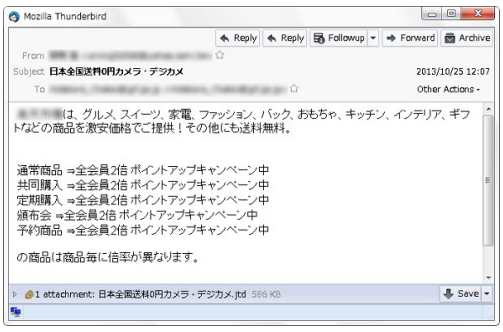

Figure. *Email used in targeted attack*

The email solicits a recipient to buy various goods from a popular Japanese online shopping site. The email also states that all members will earn double the usual points for their purchases and will also receive free shipping. The email attachment is a flyer containing the Ichitaro exploit.

In June 2013, Symantec came across a similar Trojan.Mdropper variant with the .jtd file extension, sent to an organization that received the malware mentioned above. The main difference is the file format. While rich text format was used in the recent attacks, a Microsoft Word document file with an embedded Microsoft graph chart was used for the previous attack campaign. The specially-crafted Word document was created with Microsoft Office in the Simplified Chinese language. According to our research, this exploit code also failed to successfully exploit a vulnerability. If successful, the shellcode would have downloaded malware from the following URL :

http://googles.al[REMOVED]my.com/index.html

The server hosting this domain has been associated with the group referred to as APT 12 by Mandiant. The malware itself is detected as Trojan.Krast.

The attackers, possibly belonging to the APT12 group who may have also developed BackdoorVidgrab, are persistently targeting similar, if not the identical, targets by attempting to exploit Ichitaro. The attackers may also be using the targets as guinea pigs to test if the exploit code works properly. The attack may also be a precursor, the attackers could have run the tests in order to find effective email contents and subject lines, for example, that are enticing enough lure targets into opening the malicious attachment.

The .jtd files described in this blog are detected as Trojan.Mdropper. Also Symantec's .Cloud products effectively block emails with the malicious Ichitaro attachment.

To prevent a possible compromise, Ichitaro users are advised to download and apply the latest patch from JustSystems.

Blog Entry Filed Under:
Security, Security Response, Endpoint Protection (AntiVirus), Backdoor.Vidgrab, Ichitaro, Japan, Trojan.Krast, Trojan.Mdropper, zero-day

Links

- Technical Support
- Symantec Training
- Symantec.com
- Purchase Endpoint Protection Small Business Edition
- Purchase SSL Certificates

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

- Snapchat Fruit Spam Delivered by Real, Compromised Accounts • Satnam Narang • 12 Feb 2014 18:59:14 GMT
- Microsoft Patch Tuesday – February 2014 • Dinesh Theerthagiri • 11 Feb 2014 19:49:38 GMT
- My (Failed) Visits to Spammers' Offices • Eric Park • 11 Feb 2014 17:55:34 GMT
- The Mask • Stephen Doherty • 12 Feb 2014 01:22:41 GMT
- Tiylon: A Modern Bank Robber • Christian Trippuli • 07 Feb 2014 13:13:29 GMT

Filter by:

Author

English

Recently on Twitter

- NIST releases guide to bolster US critical infrastructure cybersecurity http://t.co/scITz5CNaE #CyberSecurity #CriticalInfrastructure
  13 Feb 2014
- 4 out of 5 IT professionals pressured to roll out IT projects despite security worries http://t.co/5dAh3WCuLI #InfoSec #Security
  13 Feb 2014
- #Snapchat Fruit #Spam Delivered by Real, Compromised Accounts http://t.co/NN2z7fuQHt http://t.co/cTDwuLt0JO
  12 Feb 2014
- Bitcoin exchanges suffer denial of service attacks http://t.co/kZKNLfebKN #DenialOfService #Bitcoin
  12 Feb 2014
- You can find Symantec's blog post on MSFT's February #PatchTuesday updates here: http://t.co/dXQhcqXzlw
  11 Feb 2014

Blog Tags

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

Security Response Blog Archive

- February 2014 (12)
- 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 (19)
- October 2012 (14)
- 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 (29)
- 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 (42)
- October 2007 (45)
- September 2007 (31)
- August 2007 (41)
- July 2007 (35)
- June 2007 (34)
- May 2007 (38)
- April 2007 (41)
- March 2007 (55)
- February 2007 (45)
- January 2007 (43)
- December 2006 (43)
- November 2006 (40)
- October 2006 (30)
- September 2006 (26)
- August 2006 (31)
- July 2006 (33)
- June 2006 (14)
- May 2006 (19)
- April 2006 (1)