Operation CloudyOmega: Ichitaro zero-day and ongoing cyberespionage campaign targeting Japan

JustSystems has issued an update to its Ichitaro product line (Japanese office suite software), plugging a zero-day vulnerability. This vulnerability is being actively exploited in the wild to specifically target Japanese organizations.

The exploit is sent to the targeted organizations through emails with a malicious Ichitaro document file attached, which Symantec products detect as Bloodhound.Exploit.557. Payloads from the exploit may include Backdoor.Emdivi, Backdoor.Korplug, and Backdoor.ZXshell; however, all payloads aim to steal confidential information from the compromised computer.

The content of the emails vary depending on the business interest of the targeted recipient's organization; however, all are about recent political events associated with Japan. Opening the malicious attachment with Ichitaro will drop the payload and display the document. Often such exploitation attempts crash and then relaunch the document viewer to open a clean document in order to trick users into believing it is legitimate. In this particular attack, opening the document and dropping the payload are done without crashing Ichitaro and, as such, users have no visual indications as to what is really happening in the background.

CloudyOmega

As Security Response previously discussed, unpatched vulnerabilities being exploited is nothing new for Ichitaro. However, during our investigation of this Ichitaro zero-day attack, we discovered that the attack was in fact part of an ongoing cyberespionage campaign specifically targeting various Japanese organizations. Symantec has named this attack campaign CloudyOmega. In this campaign, variants of Backdoor.Emdivi are persistently used as a payload. All attacks arrive on the target computers as an attachment to email messages. Mostly the attachments are in a simple executable format with a fake icon. However, some of the files exploit software vulnerabilities, and the aforementioned vulnerability in Ichitaro software is only one of them. This group's primary goal is to steal confidential information from targeted organizations. This blog provides insights into the history of the attack campaign, infection methods, malware payload, and the group carrying out the attacks.

Timeline

The first attack of the campaign can be traced back to at least 2011. Figure 1 shows the targeted sectors and the number of attacks carried out each year. The perpetrators were very cautious launching attacks in the early years with attacks beginning in earnest in 2014. By far, the public sector in Japan is the most targeted sector hit by Operation CloudyOmega. This provides some clue as to who the attack group is.

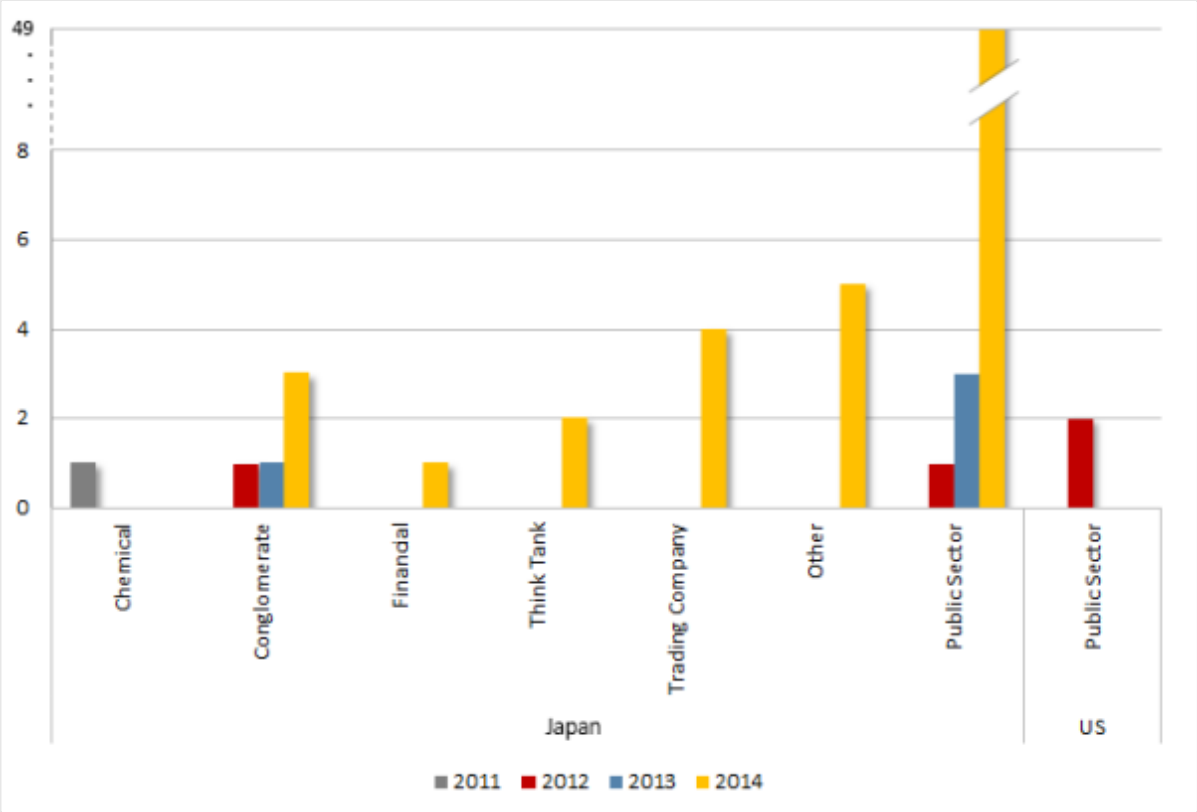

Figure 1. Targeted sectors and number of attacks

Attack vector

Email is the predominant infection vector used in this campaign.

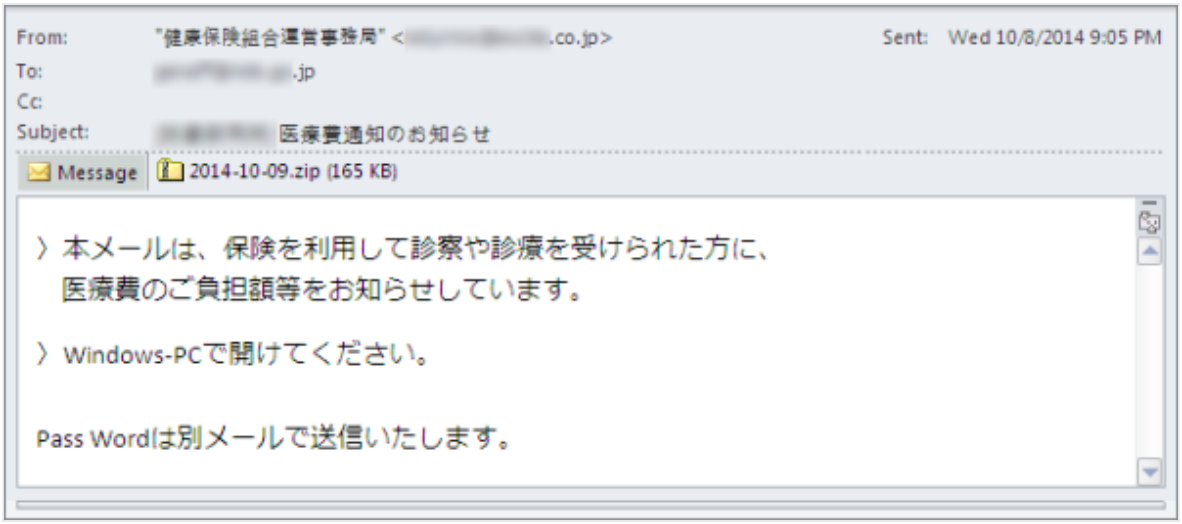

Figure 2. Sample email used in attack campaign

Figure 2 is an example of an email used in recent attacks prior to those exploiting the Ichitaro zero-day vulnerability. The emails include password-protected .zip files containing the malware. Ironically, the attackers follow security best practices by indicating in the first email that the password will be sent to the recipient in a separate email. This is merely to trick the recipient into believing the email is from a legitimate and trustworthy source. The body of the email is very short and claims the attachment includes

a medical receipt. The email also requests that the recipient open the attachment on a Windows computer. The file in the attachment has a Microsoft Word icon but, as indicated within Windows Explorer, it is an executable file.

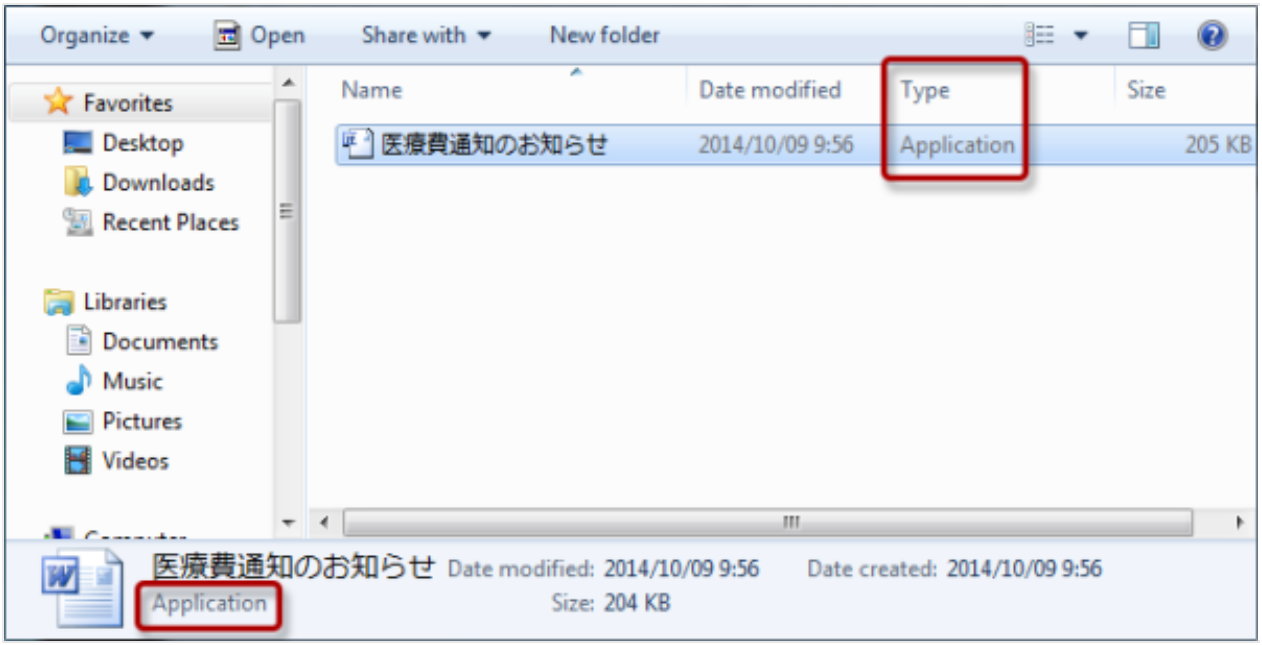

Figure 3. Attached "document" is actually a malicious executable file

Payload

The malicious payload is Backdoor.Emdivi, a threat that opens a back door on the compromised computer. The malware is exclusively used in the CloudyOmega attack campaign and first appeared in 2011 when it was used in an attack against a Japanese chemical company. Emdivi allows the remote attacker executing the commands to send the results back to the command-and-control (C&C) server through HTTP.

Each Emdivi variant has a unique version number and belongs to one of two types: Type S and Type T. The unique version number is not only a clear sign that Emdivi is systematically managed, but it also acts as an encryption key. The malware adds extra words to the version number and then, based on this, generates a hash, which it uses as an encryption key.

Both Emdivi Type S and Type T share the following functionality:

- Allow a remote attacker to execute code through HTTP
- Steal credentials stored by Internet Explorer

Type T is primarily used in Operation CloudyOmega, has been in constant development since the campaign was first launched in 2011, and is written in the C++ programing language. Type T employs techniques to protect itself from security vendors or network administrators. Important parts of Type T,

such as the C&C server address it contacts and its protection mechanisms, are encrypted. Type T also detects the presence of automatic analysis systems or debuggers, such as the following:

- VirtualMachine
- Debugger
- Sandbox

Type S, on the other hand, was used only twice in the attack campaign. Type S is a .NET application based on the same source code and shared C&C infrastructure as Type T. However, protection mechanisms and encryption, essential features for threat survival, are not present in Type S. One interesting trait of Type S is that it uses Japanese sentences that seem to be randomly taken from the internet to change the file hash. For instance, in the example shown in Figure 4, it uses a sentence talking about the special theory of relativity.

```
時空の性質としてローレンツ変換から導引き出している。屈折率を（ｎ）の水の媒質中の
光速度（Ｗ）は光速度を（ｃ）、水の速度を（ｖ）として、フィゾーの実験式は
```

Figure 4. Japanese text used by Emdivi Type S variant

Who is Emdivi talking to?

Once infected, Emdivi connects to hardcoded C&C servers using the HTTP protocol.

So far, a total of 50 unique domains have been identified from 58 Emdivi variants. Almost all websites used as C&C servers are compromised Japanese websites ranging from sites belonging to small businesses to personal blogs. We discovered that 40 out of the 50 compromised websites, spread across 13 IP addresses, are hosted on a single cloud-hosting service based in Japan.

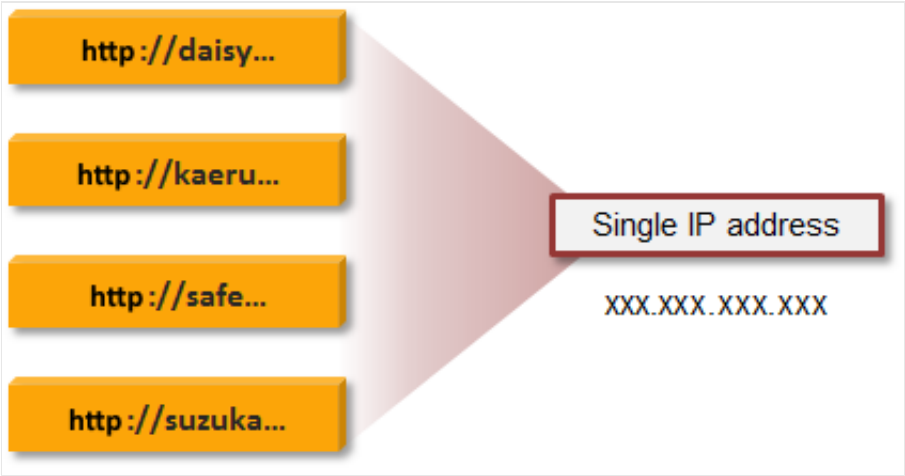

Figure 5. Single IP hosts multiple compromised websites

The compromised sites are hosted on various pieces of web server software, such as Apache and Microsoft Internet Information Services (IIS), and are on different website platforms. This indicates that the sites

were not compromised through a vulnerability in a single software product or website platform. Instead, the attacker somehow penetrated the cloud service itself and turned the websites into C&C servers for Backdoor.Emdivi.

The compromised cloud hosting company has been notified but, at the time of writing, has not replied.

Symantec offers two IPS signatures that detect and block network communication between infected computers and the Emdivi C&C server:

- System Infected: Backdoor.Emdivi Activity
- System Infected: Backdoor.Emdivi Activity 2

Zero-day and links to other cybercriminal groups

During our research, multiple samples related to this attack campaign were identified and allowed us to connect the dots, as it were, when it came to CloudyOmega's connections to other attack groups.

In August 2012, the CloudyOmega attackers exploited the zero-day Adobe Flash Player and AIR 'copyRawDataTo()' Integer Overflow Vulnerability (CVE-2012-5054) in an attack against a high-profile organization in Japan. The attackers sent a Microsoft Word file containing a maliciously crafted SWF file that exploited the vulnerability. Once successfully exploited, the file installed Backdoor.Emdivi. As CVE-2012-5054 was publicly disclosed in the same month, the attack utilized what was, at the time, a zero-day exploit.

Interestingly, the Flash file that was used in an Emdivi attack in 2012 and the one used in the LadyBoyle attack in 2013 look very similar.

Figure 6 shows the malformed SWF file executing LadyBoyle() code that attempts to exploit the Adobe Flash Player CVE-2013-0634 Remote Memory Corruption Vulnerability (CVE-2013-0634). The Flash file seems to have been created using the same framework used by the CloudyOmega group, but with a different exploit.

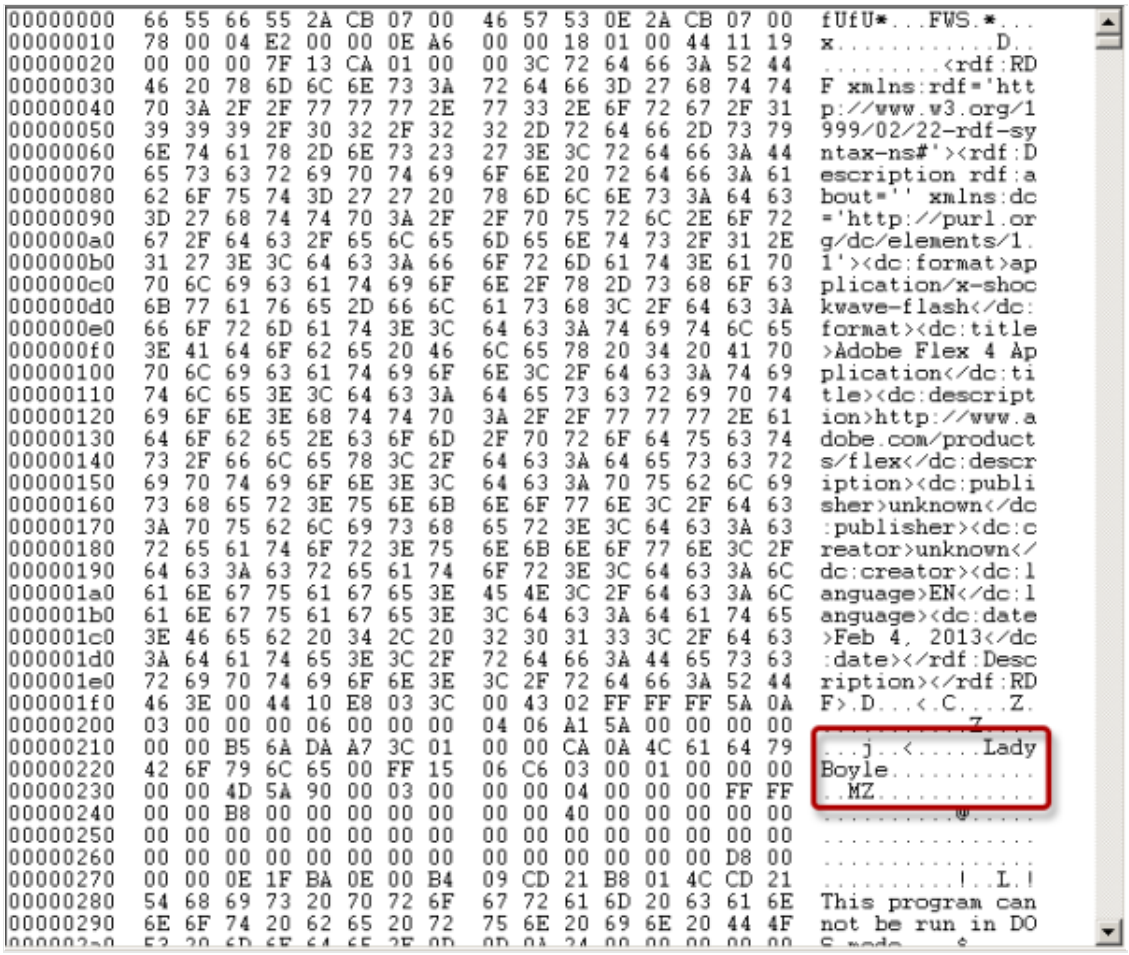

Figure 6. Malformed SWF file used in the LadyBoyle campaign in February 2013

Both attacks use a .doc file containing an Adobe Flash zero-day exploit that is used to install a back door. No other evidence connects these two different campaigns; however, as described previously in Symantec Security Response's Elderwood blog, it is strongly believed that a single parent organization has broken into a number of subgroups that each target a particular industry.

In terms of the latest attack on Ichitaro, we collected a dozen samples of JTD files, all of which are exactly the same except for their payload. The parent organization, it would seem, supplied the zero-day exploit to the different subgroups as part of an attack toolkit and each group launched a separate attack using their chosen malware. This is why three different payloads (Backdoor.Emdivi, Backdoor.Korplug, and Backdoor.ZXshell) were observed in the latest zero-day attack.

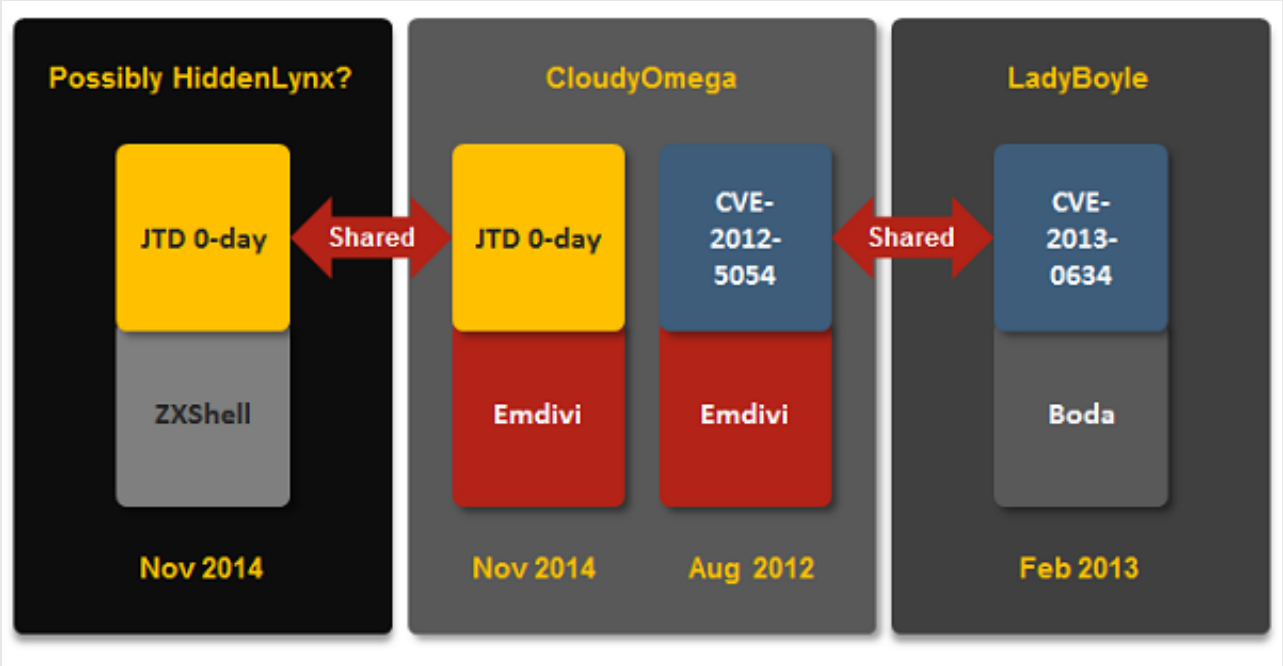

Figure 7. Parent group sharing zero-day exploit

Conclusion

Operation CloudyOmega was launched by an attack group that has communication channels with other notorious attack groups including Hidden Lynx and the group responsible for LadyBoyle. CloudyOmega has been in operation since 2011 and is persistent in targeting Japanese organizations. With the latest attack employing a zero-day vulnerability, there is no indication that the group will stop their activities anytime soon. Symantec Security Response will be keeping a close eye on the CloudyOmega group.

Protection summary

It is highly recommended that customers using Ichitaro products apply any patches as soon as possible.

Symantec offers the following protection against attacks associated with Operation CloudyOmega:

AV

- Backdoor.Emdivi
- Backdoor.Emdivi!gen1
- Backdoor.Emdivi!gen2
- Bloodhound.Exploit.557
- Trojan.Mdropper

IPS

- System Infected: Backdoor.Emdivi Activity
- System Infected: Backdoor.Emdivi Activity 2