Symantec™
Security Response

The Elderwood Project

Gavin O'Gorman
Geoff McDonald

Contents

Overview

In 2009, Google was attacked by a group using the Hydraq (Aurora) Trojan horse. Symantec has monitored this group's activities for the last three years as they have consistently targeted a number of industries. Interesting highlights in their method of operations include: the use of seemingly an unlimited number of zero-day exploits, attacks on supply chain manufacturers who service the target organization, and a shift to "watering hole" attacks (compromising certain websites likely to be visited by the target organization). The targeted industry sectors include, but are not restricted to; defense, various defense supply chain manufacturers, human rights and non-governmental organizations (NGOs), and IT service providers.

These attackers are systematic and re-use components of an infrastructure we have termed the "Elderwood platform". The name "Elderwood" comes from a source code variable used by the attackers. This attack platform enables them to quickly deploy zero-day exploits. Attacks are deployed through spear phishing emails and also, increasingly, through Web injections in watering hole attacks.

Although there are other attackers utilizing zero-day exploits (for example, the Sykipot or Nitro, or even Stuxnet), we have seen no other group use so many. The number of zero-day exploits used indicates access to a high level of technical capability. Here are just some of the most recent exploits that they have used:

- Adobe Flash Player Object Type Confusion Remote Code Execution Vulnerability (CVE-2012-0779)
- Microsoft Internet Explorer Same ID Property Remote Code Execution Vulnerability (CVE-2012-1875)
- Microsoft XML Core Services Remote Code Execution Vulnerability (CVE-2012-1889)
- Adobe Flash Player Remote Code Execution Vulnerability (CVE-2012-1535)

It is likely the attackers have gained access to the source code for some widely used applications, or have thoroughly reverse-engineered the compiled applications in order to discover these vulnerabilities. The vulnerabilities are used as needed, often within close succession of each other if exposure of any of the vulnerabilities is imminent.

The scale of the attacks, in terms of the number of victims and the duration of the attacks, are another indication of the resources available to the attackers. Victims are attacked, not for petty crime or theft, but for the wholesale gathering of intelligence and intellectual property. The resources required to identify and acquire useful information—let alone analyze that information—could only be provided by a large criminal organization, attackers supported by a nation state, or a nation state itself.

Background

Serious zero-day vulnerabilities, which are exploited in the wild and affect a widely used piece of software, are relatively rare; there were approximately eight in 2011. The past few months however has seen four such zero-day vulnerabilities actively exploited in the wild. Two of the zero-day exploits were in Adobe Flash, the other two in Internet Explorer.

In April 2012, we identified seven different Trojans that were being used in conjunction with CVE-2012-0779. Within one month, two more zero-day exploits were identified in the wild. These were CVE-2012-1875 and CVE-2012-1889. The timing of the release of these three exploits was suspicious. As soon as one had been identified, the next became active. We investigated the three exploits and found connections between them all. In the past few weeks, yet another zero-day exploit was detected in the wild, CVE-2012-1535. We have tied this zero-day exploit back to all the others. They may only be the tip of the iceberg.

In early 2010, Google documented an attack against their infrastructure. They stated that they were attacked in December 2009 and that the attacks originated in China. The attackers utilized a Trojan called Hydraq, (also known as Aurora), which was delivered using an Internet Explorer zero-day exploit. We believe the Hydraq attack and the recent attacks that exploit the vulnerabilities outlined above are linked.

Figure 1

Timeline of zero-day exploits attributable to the one group

In March 2011, at least two Adobe Flash zero-day attacks were utilized in similar attacks against the same types of victims. In September 2011, yet another Adobe Flash zero-day exploit was used

to attack visitors to the Amnesty International Hong Kong site. The very same website was again compromised in the most recent set of attacks. Our analysis shows that a single group has been using these zero-day exploits, along with others over the past couple of years, in targeted attacks against individuals, companies, governments, and even entire sectors. A timeline for these various zero-day exploits is shown in Figure 1.

The attacks conducted by this group are carried out using several different techniques.

One of the methods used, called a watering hole attack, shown in figure 2, is a clear shift in their method of operations. The concept of the attack is similar to a predator waiting at a watering hole in a desert. The predator knows that victims will eventually have to come to the watering hole, so rather than go hunting, he waits for his victims to come to him. Similarly, attackers find a Web site that caters to a particular audience in which the attackers are interested. For example, people who visit the Amnesty International Hong Kong website are most

Figure 2

Web injection process used in watering hole attacks

likely visiting because they are interested in human rights issues in Hong Kong. Having identified this website, the attackers hack into it using a variety of means. For example, the site may be vulnerable to a SQL injection, or perhaps the attackers compromise the machine of an individual with publishing rights to the website. The

attackers then inject an exploit onto public pages of the website that are hopefully visited by their ultimate target. Any visitor susceptible to the exploit is compromised and a back door Trojan is installed onto their computer. The attacker then has complete control over the victim's computer.

Three of the most recent zero-day exploits were used in watering hole attacks, an indication that this approach is gaining momentum.

The more traditional technique is to send a "spear-phishing" email, containing an attachment, to the target. That attachment is a document containing an exploit which, when opened, then drops a Trojan onto the target computer. This works if the exploit is embeddable in a document. If not, then an alternative approach is to host the exploit on a Web server and then email the target with a link to that Web server. The link used is quite unique, it is not hosted on a common Web site, so it will only be encountered by the chosen target. When the target clicks on the link, the exploit is triggered and a back door is installed.

The Elderwood gang has shown their resourcefulness over the past few years by leveraging a large number of zero-day vulnerabilities. The full list of vulnerabilities is shown below.

Table 1

Zero-day vulnerabilities associated with the Elderwood gang

CVE	BID	Description	Application
2012-0779	53395	Object Type Confusion Remote Code Execution Vulnerability	Adobe Flash Player
2012-1875	53847	Same ID Property Remote Code Execution Vulnerability	Microsoft Internet Explorer
2012-1889	53934	Remote Code Execution Vulnerability	Microsoft XML Core Services
2012-1535	55009	Remote Code Execution Vulnerability	Adobe Flash Player
2011-0609	46860	'SWF' File Remote Memory Corruption Vulnerability	Adobe Flash Player
2011-0611	47314	'SWF' File Remote Memory Corruption Vulnerability	Adobe Flash Player
2011-2110	48268	Adobe Flash Player Remote Memory Corruption Vulnerability	Adobe Flash Player
2010-0249	37815	'srcElement()' Remote Code Execution Vulnerability	Internet Explorer

We have analyzed four of the most recent exploits (CVE-2012-0779, CVE-2012-1875, CVE-2012-1889, and CVE-2012-1535) and their associated malicious documents, the Trojans, and the infrastructure utilized in the attacks. There are several common features used in the attacks. Some of these features hint at the potential infrastructure, or platform, developed to support these attacks. From this analysis we have identified an increase in watering hole attacks by this group and developed a theory describing the possible infrastructure the attackers are utilizing. We also describe the various targeted industry sectors and provide evidence that a single gang is most likely to be behind the attacks.

Targets

The targets of the four recent zero-day exploits were attacked through both email (CVE-2012-0779 and CVE-2012-1535) and Web vectors (CVE-2012-0779, CVE-2012-1875, and CVE-2012-1889). Identifying the target profile and related industry to which the target belongs is straight forward when email is used in an attack. Identifying the profile of the targets when the Web is used as the attack vector is difficult. For example, if an aeronautical website was compromised, the attackers may be trying to infect visitors from the Defense industry, the aeronautical company employees themselves, or perhaps visitors from others aeronautical companies. For our analysis, we have had to presume that the industry sector being targeted is the same as that of the watering hole website, understanding that in reality this may not always be the case.

The primary targets identified are defense, or more precisely manufacturers that are in the defense supply chain. These are companies who manufacture electronic or mechanical components which are then sold to top-tier defense companies. The attackers may use the manufacturers as a stepping stone to gain access to top-tier defense contractors, or obtain intellectual property used in the production of parts that make up larger products produced by a top-tier defense company.

Figure 3

Target sectors

The second most common target is the general area of human rights, or Non Governmental Organizations (NGOs). A number of websites generally relating to religion, Taiwan, Hong Kong and China were compromised for this purpose. The CVE-2012-1875 exploit is almost exclusively used in this target sector, with some crossover from the CVE-2012-1889 exploit.

Figure 4

Number of targeted companies (Email) and compromised websites (Web) per exploit

The remaining target sectors include Finance, Energy (Oil/Gas), Education, and Government. There are a number of outlier victims, such as a hotel jobs site, which may have simply been targeted in error and are collateral damage. The vast majority of detections are in the United States. Figure 5 shows those detections.

Figure 5

Global detections of files used in the past year by the Elderwood gang

Escalation of watering hole attacks

As we have noted earlier, the number of watering hole attacks have been on the increase. The attacks begin with an attacker locating a vulnerability on a chosen website. This vulnerability allows the attacker to insert some JavaScript, or HTML, into the website. That piece of code contains a link, or iFrame, which points to another Web page that actually hosts exploit code for the chosen vulnerability. When a user connects to the hacked website, they are automatically referred to the malicious Web page which exploits a vulnerability allowing the attacker to install malware onto the victim's computer. Once the iFrame and malicious code are in place on the server, the attacker does not need to do anything but simply wait for victims to browse to the website, or visit the watering hole, and become infected.

Web injection attacks are not new and are commonly used in cybercrime. The difference between their use in cybercrime and in watering hole attacks is down to the choice of websites to compromise and use in the attacks. In a mass injection attack, criminals will indiscriminately compromise any website they can, but in watering hole attacks, the attackers are focused. They choose websites within a particular sector so as to infect persons of interest who likely work in that same sector and are likely to therefore visit related websites. Targeting a specific website is much more difficult than merely locating websites that contain a vulnerability. The attacker has to research and probe for a weakness on the chosen website.

Indeed, in watering hole attacks, the attackers may compromise a website months before they actually use it in an attack. Once compromised, the attackers periodically connect to the website to ensure that they still have access. This way, the attackers can infect a number of websites in one stroke, thus preserving the value of their zero-day exploit. They are even in a position to inspect the website logs to identify any potential victims of interest. This technique ensures that they obtain the maximum return for their valuable zero-day exploit.

Although watering hole attacks have been known about since approximately March of 2011, the activity outlined in this report marks a substantial increase. Three zero-day exploits, CVE-2012-0779, CVE-2012-1875, and CVE-2012-1889 have all been used within a 30-day period to serve up back door Trojans from compromised websites.

Figure 6

Elderwood platform

The increase in the use of this attack technique requires the attackers to sift through a much greater amount of stolen information than a targeted attack relying on email, as the number of victims compromised by a Web injection attack will be much greater. Although multiple emails are often sent to numerous victims, the scale of such attacks is much smaller than the number of victims infected by visiting one of a number of compromised websites. We believe, to solve this problem, the attackers have built a system that allows them to execute new campaigns by simply dropping in a new exploit and various other components, such as Trojans and hacked servers.

Attack platform

The attackers have leaked snippets of information that hint at the type of infrastructure that is likely to be used to implement these attacks. Figure 6 is a diagram of the various processes and steps that that the Elderwood attackers must go through to conduct their attacks.

All attacks require a Trojan to infect the target computer. This Trojan is packaged with a packer and also the address of the command-and-control (C&C) server. The next step is to deliver that packaged Trojan to the target. Delivery is either though an email or a Web based vector. We have identified two distinct elements in the delivery vector that demonstrate the potential attack infrastructure.

Document creation kit

The attackers often delivered their malicious code via documents attached to email. Based on our analysis, we believe the attackers have built a tool that easily allows them to automatically construct documents containing different payloads. The tool is able to take an arbitrary clean document file, specific exploit code, and a Trojan, and bundle them together to create a malicious document ready to be used in the next attack. This tool is one component of the Elderwood platform. The use of such a tool can be readily seen in samples that exploit the CVE-2012-0779 vulnerability where multiple document files were encoded in the same manner, but the Trojan payload differed.

Shared SWF file

Another component used in the attacks is a Shockwave Flash (SWF) file. Often, to ensure reliable execution of exploit code, code must be placed in the right areas of computer memory. In addition, exploit code often performs the same task of downloading a Trojan from a remote website for execution. Instead of developing code to perform these tasks for each different exploit, the attackers have developed a common SWF file that is used solely to create the correct conditions in memory and accepts a parameter specifying where to download the Trojan. In some attacks, the parameter name was “Elderwood.” The same SWF file was seen used when exploiting 3 different vulnerabilities (CVE-2012-0779, CVE-2012-1875, CVE-2012-1889).

By using a common SWF file, the attackers can simply deploy a new trigger, that is, a zero-day exploit, and the SWF handles the rest of the work, retrieving and decoding the back door Trojan.

These various re-usable components collectively make up the Elderwood attack platform, as shown in figure 6. There is no doubt that there are several other components that the attackers use in their various processes as well. Other possible components of the attack platform may include:

- A tool for the automated creation of accounts on Web-based email services
- Automated registration of domain names
- Information gathering on targets – searching for, and consolidating data on, a victim to identify potential website targets and relevant topics for email content
- An analysis platform for stolen information

The reuse of the identified components gives clues as to how the attackers may divide the labor amongst themselves. Technically skilled hackers (researchers) create exploits, document creation kits, re-usable trigger code (the SWF files), and compromise websites, and these are then made available to less technical attackers. These attackers (attack operators) are likely responsible for identifying targets and delivering the attack payload using the tools and infrastructure provided to them.

Once a target has been compromised, the less skilled attack operators can then proceed to move through the compromised network, identifying data of interest. The level of technical skill required to move through a compromised network is much lower than that required to establish the initial penetration.

Connecting the dots

The investigation into the various exploits began with a deep analysis of CVE-2012-0779. From this analysis, we identified several Trojans which were dropped from documents utilizing the exploit. These Trojans helped us begin the process of establishing links between the various zero-day exploits.

The code in one of those Trojans was obfuscated in a certain way. This same obfuscation was used on a Trojan dropped by CVE-2012-1875, establishing a link between the use of these two exploits. Going back in time, the Hydraq Trojan also displayed this obfuscation.

Additional links joining the various exploits together included a shared command-and-control infrastructure. Trojans dropped by different exploits were connecting to the same servers to retrieve commands from the attackers. Some compromised websites used in the watering hole attacks had two different exploits injected into them one after the other. Yet another connection is the use of similar encryption in documents and malicious executables. A technique used to pass data to a SWF file was re-used in multiple attacks. Finally, the same family of Trojan was dropped from multiple different exploits.

Figure 7 illustrates the connections between the various exploits.

Figure 7

Links between different exploits

Conclusion

Simple targeted attacks are quite common. Most (the Taidoor attackers for example) reuse exploits and are relatively simple to block, if one ensures that one's network and software is regularly patched. Somewhat more sophisticated attackers use zero-day exploits. The Elderwood hackers use multiple zero-day exploits, multiple Trojans, and multiple delivery vectors. They are responsible for compromising numerous websites, corporations, and individuals over the past three years. This group is focused on wholesale theft of intellectual property and clearly has the resources, in terms of manpower, funding, and technical skills, required to implement this task.

Although we have not conclusively established a connection between the most recent exploits and those used in attacks in 2011, there are similarities. Apart from the technical features in common, as mentioned previously (URL encoding), there is a noticeable similarity in the timing of the attacks and the types of vulnerabilities used between the 2012 and 2011 attacks. Both sets of attacks used multiple zero-day exploits one after the other, sometime around April to August, and both sets of attacks exploit Adobe Flash and Internet Explorer.

It may be the case that these initial "penetration" attacks are launched over a fixed period of time (several months from approximately April to August). After this initial compromise, the attackers consolidate their beachhead and begin to analyze the stolen information, spreading through networks and maintaining access as needed. By analyzing the information gathered, the attackers can identify yet more targets of interest. They may also eventually be detected and evicted from a compromised network. In later attacks, newly identified targets can be attacked and old victims can be targeted again. If this is the case, then companies and individuals need to be on their guard.

Any manufacturers who are in the defense supply chain need to be wary of attacks emanating from subsidiaries, business partners, and associated companies. It is possible that those trusted companies were compromised by the attackers who are then using them as a stepping-stone to the true intended target. Companies and individuals should prepare themselves for a new round of attacks in 2013 utilizing both Adobe Flash and Internet Explorer zero-day exploits. This is particularly the case for companies who have been compromised in the past and managed to evict the attackers. The knowledge that the attackers gained in their previous compromise will assist them in any future attacks.

Resources

Symantec Security Response Blog
http://www.symantec.com/connect/symantec-blogs/sr

Follow Symantec Security Response on Twitter
http://twitter.com/threatintel

Appendix

Malware detection names

The Elderwood gang uses multiple different Trojans. The ones identified to date are detected using the detection names in table 2.

Table 2
Trojans associated with Elderwood gang

Associated Trojans
Backdoor.Briba
Trojan.Hydraq
Trojan.Naid
Backdoor.Wiarp
Backdoor.Vasport
Trojan.Pasam
Backdoor.Darkmoon
Packed.Generic.379
Packed.Generic.374
Backdoor.Ritsol
Backdoor.Nerex
Backdoor.Linfo

Command-and-control servers

Table 3 shows the command and control servers.

Table 3
Command and control servers

C&C domains
qwby.gownsman.com
wwwcnas.org
gate-usa.com
3dvideo.ru
wt.ikwb.com
svr01.passport.serveuser.com
zfcay1751.chinaw3.com
web.cyut.edu.tw
srv001.proxydns.com
help.2012hi.hk
0207.gm.jetos.com
71.6.217.131
javaupdate.freeddns.com
yours.microtrendsoft.com
cpu.edu.tw
glogin.ddns.us
download.msdnblog.com
dd.pst.qpoe.com

Symantec protection

Many different Symantec protection technologies play a role in defending against this threat, including:

File-based protection (Traditional antivirus)

Traditional antivirus protection is designed to detect and block malicious files and is effective against files associated with this attack.

- Bloodhound.Exploit.469
- Bloodhound.Exploit.465
- Bloodhound.Exploit.466
- Bloodhound.Olexe.2
- Bloodhound.Flash.15
- Packed.Generic.379
- Packed.Generic.374
- Backdoor.Briba
- Trojan.Hydraq
- Trojan.Naid
- Backdoor.Wiarp
- Backdoor.Vasport
- Trojan.Pasam
- Backdoor.Darkmoon
- Backdoor.Ritsol
- Backdoor.Nerex
- Backdoor.Linfo
- Trojan.MDropper

Network-based protection (IPS)

Network-based protection in Symantec Endpoint Protection can help protect against unauthorized network activities conducted by malware threats or intrusion attempts.

- Adobe Flash Type Confusion CVE-2012-0779 (25718)
- RTMP Type Confusion CVE-2012-0779 2 (25721)
- MSIE MSXML CVE-2012-1889 3 (25783)
- MSIE MSXML CVE-2012-1889 2 (50331)
- MSIE MSXML CVE-2012-1889 (25786)
- Malicious SWF Download CVE-2012-1535 2 (25878)
- Malicious SWF Download 4 (25789)
- MSIE Same ID Property CVE-2012-1875 (25787)
- MSIE CVE-2010-0249 (23823)
- Malformed XLS SWF Remote Code Execution CVE-2011-0609 (24136)
- Flash Player CVE-2011-2110 (24336)
- Adobe Embedded SWF CVE-2011-0611 (24212)

Behavior-based protection

Behavior-based detection blocks suspicious processes using the Bloodhound.SONAR series of detections

Reputation-based protection (Insight)

- Norton Safeweb blocks users from visiting infected websites.
- Insight detects and warns against suspicious files as WS.Reputation.1

Email-based protection

Symantec MessageLabs Email Security.cloud can block emails associated with these attacks

Other protection

• **Application and Device Control (SEP) prevents malicious document files from dropping the backdoor Trojan**Symantec Critical System Protection can also prevent unauthorized applications from running.

• Browser Protection can protect against web based attacks which use exploits

• Symantec Critical System Protection can help to lock down system and prevent intrusions

• Data Loss Prevention (DLP) can prevent confidential data from being accessed or exfiltrated by the attacker

Symantec
Security Response

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Mountain View, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

About the authors

Geoff McDonald - Threat Analysis Engineer
Gavin O'Gorman - Sr Threat Intelligence Analyst

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527-8000
www.symantec.com