Cyber Espionage APT group using Hacking Team’s 0-day Exploit

By Deepen Desai

Published: 2015-08-14 · Archived: 2026-04-05 19:35:12 UTC

Introduction

As predicted following the leak of Hacking Team exploit codes covered here, the Zscaler security research team has recently started seeing a Chinese cyber espionage group weaponizing malware payloads using the 0-day exploits found in the leaked Hacking Team archives. As such, this new attack represents a dangerous new hybrid combining the work of a notorious cyber criminal gang with Chinese cyber espionage group to attack a financial services firm.

Zscaler's cloud sandboxes recently detected a Remote Access Trojan (RAT) being delivered by a well-known Chinese cyber espionage group using the Hacking Team’s 0-day exploits. This attack was specifically targeting a well-known financial services firm. The exploit files involved were identical to the Hacking Team's leaked exploit HTML, JavaScript, and ShockWave Flash 0-day files. The end payload that was installed is the HttpBrowser RAT, known to be used by the Chinese group in previous targeted attacks against governments.

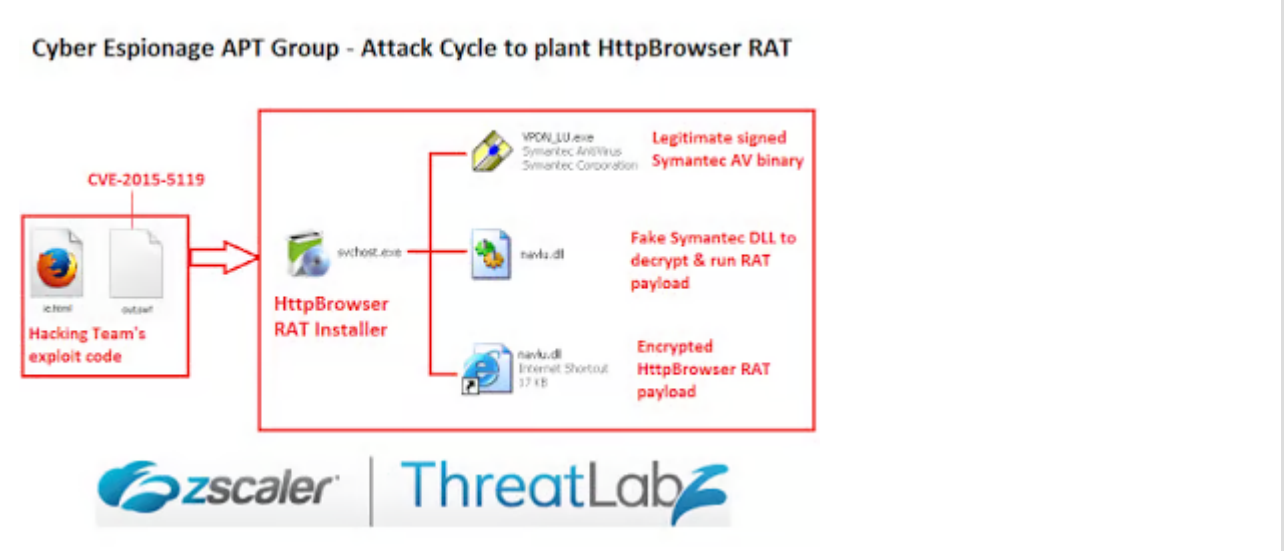

Figure 1: Chinese APT attack cycle to plant HttpBrowser RAT

Hacking Team Exploits

The attack involved targeted users visiting a malicious URL delivered via a spear phishing attack. The malicious URL points to a remote server located in Hong Kong (IP Address - 210.209.89.162) that downloads and executes a malicious ShockWave Flash payload through a specially crafted HTML & JavaScript. The exploit files involved are identical to the ones that we found during our analysis of the Hacking Team leaked code as seen below:

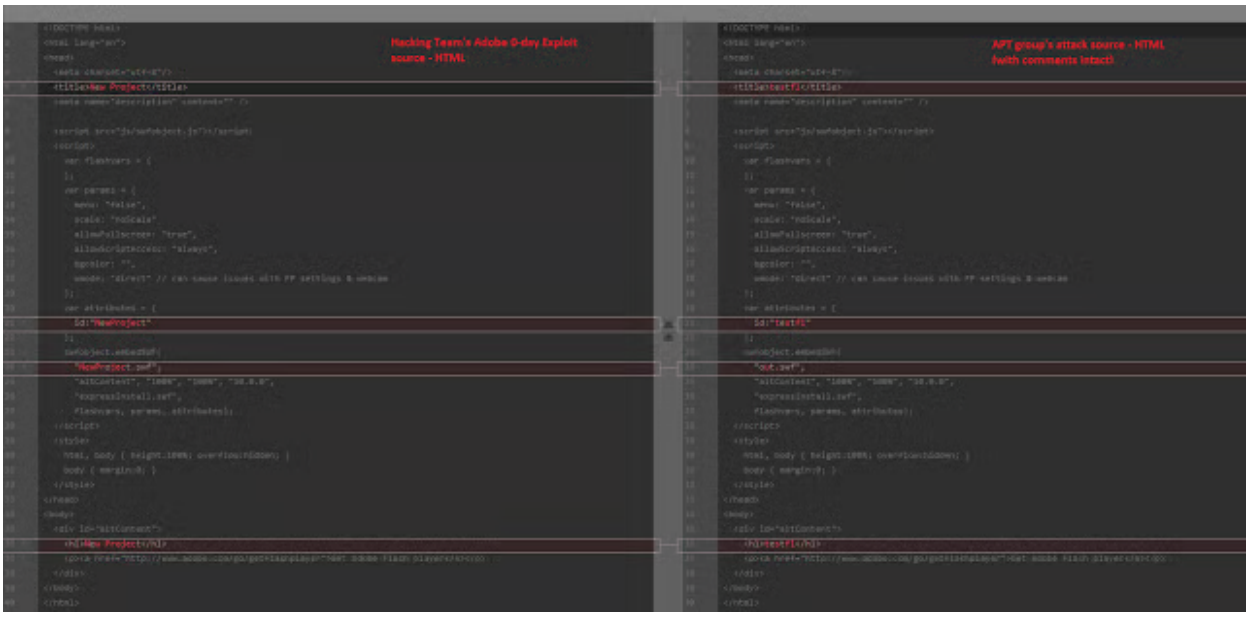

Figure 2: Resemblance with Hacking Team's exploit HTML

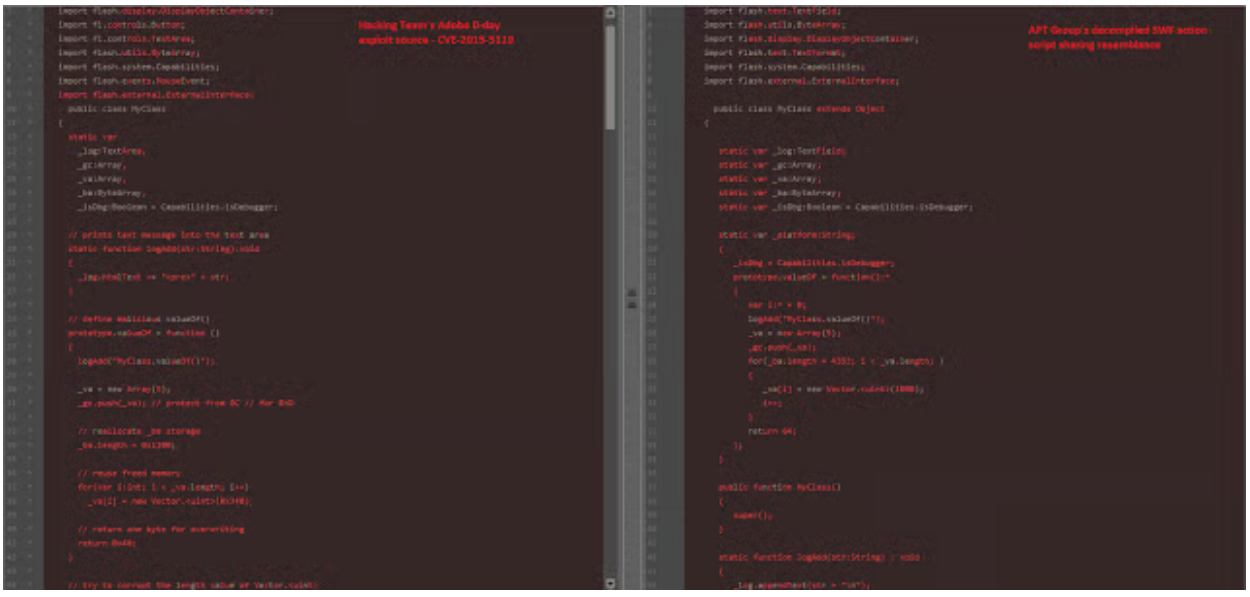

Figure 3: Resemblance with Hacking Team's SWF exploit

The Adobe ShockWave exploit (CVE-2015-5119) if successful will download and install a variant of the HttpBrowser RAT from the same Hong Kong based server which eventually also serves as the Command & Control (C&C) server.

Figure 4: Hong Kong based server used in the attack [credit: domaintools.com]

Malware Payload - HttpBrowser RAT

HttpBrowser is a RAT that has become extremely popular in past two years among the APT adversaries, leveraged in various targeted attacks. The RAT has been leveraged as the primary payload by the APT group that is also known to install the nasty Backdoor PlugX RAT during lateral movement in the victim environment after compromise.

The HttpBrowser payload used for the attack was compiled just few days before the attack as seen below:

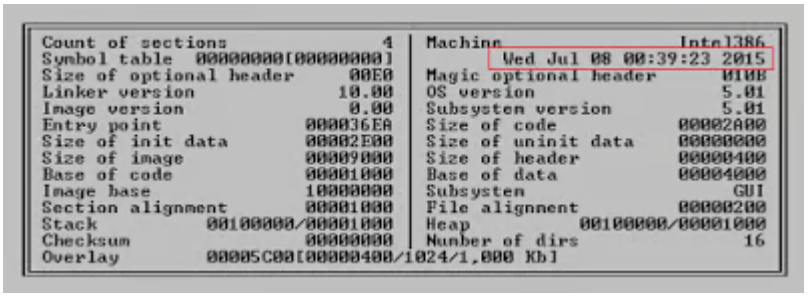

Figure 5: HttpBrowser payload compilation time

The HttpBrowser installer archive structure is very similar to that observed in previous PlugX attacks. The installer archive in our case was svchost.exe (saved as xox.exe) that consisted of the following three files:

- VPDN_LU.exe - A legitimate digitally signed Symantec Antivirus executable to evade detection

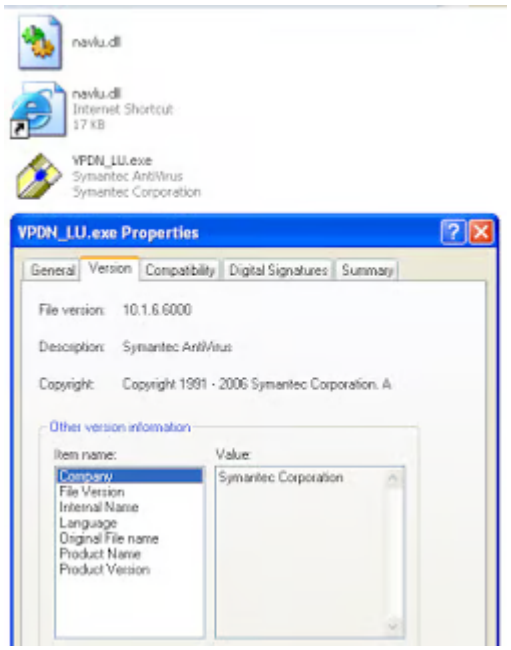

Figure 6: Legitimate Symantec Antivirus executable used in the attack

- navlu.dll - A fake Symantec DLL to decrypt and run the HttpBrowser RAT
- navlu.dll.url - Encrypted HttpBrowser RAT payload

The HttpBrowser RAT installer is responsible for dropping the above three files and running the legitimate Symantec Antivirus binary VPDN_LU.exe. The legitimate binary contains the navlu.dll in the import table ensuring that the DLL will be loaded before it runs. The navlu.dll that gets loaded in this case will be the fake Symantec DLL file present in the same directory and it will patch the entry point of the main executable file with a jump instruction to run the DLL's code instead.

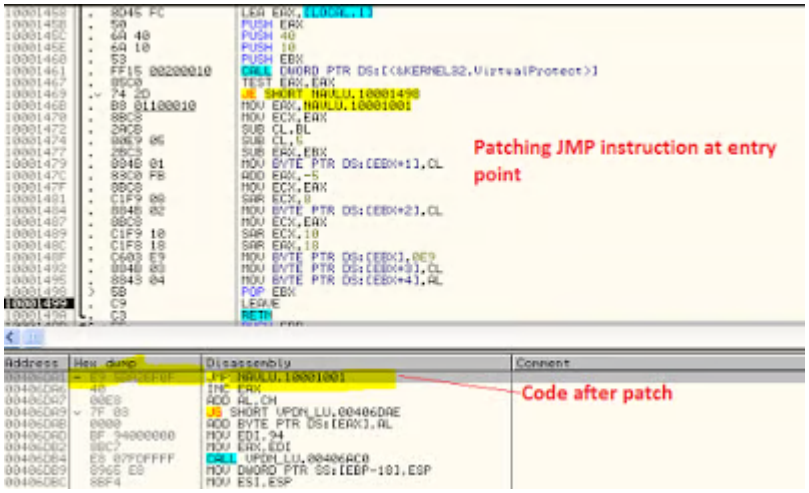

Figure 7: Legitimate executable entry point patched

This technique is also known as DLL Hijacking which ensures that the fake Symantec DLL gets loaded by abusing the Windows DLL load order. The DLL's code is responsible for decrypting and running the HttpBrowser

RAT payload from the navlu.dll.url file in the same memory space of the benign executable. The decryption routine consist of an incremental XOR as seen below:

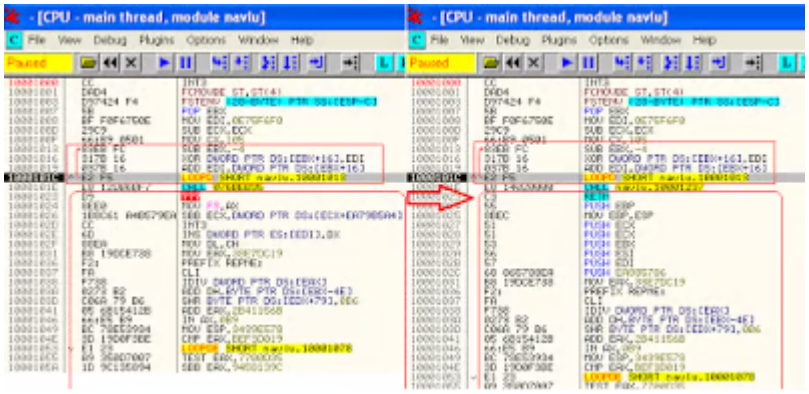

Figure 8: Incremental XOR routine to decrypt RAT payload

The HttpBrowser installer structure ensures that the malware evades detection by running in the context of the legitimate signed binary. This also ensures that the malicious DLL will not run by itself in automated analysis environments.

The malware then deletes the original installer file and moves the dropped files to the following location:

- %ALLUSERPROFILE%\%APPDATA%\vpdn\VPDN_LU.exe
- %ALLUSERPROFILE%\%APPDATA%\vpdn\navlu.dll
- %ALLUSERPROFILE%\%APPDATA%\vpdn\navlu.dll.dll

The malware also creates the following registry entry to ensure persistence:

- HKEY_USERS\Software\Microsoft\Windows\CurrentVersion\Run vpdn “%ALLUSERPROFILE%\%APPDATA%\vpdn\VPDN_LU.exe”

Command & Control communication

The HttpBrowser RAT variant was configured to connect to the following Command & Control server upon successful infection:

- update.hancominc[.]com:8080

It relays the following information of the victim machine in an encrypted format over SSL:

> */loop?c=&l=&o=&u=&r=&t=*

The commands supported by this RAT variant are:

Command	**Description**

init	start reverse shell and send list of drives on infected system.
setcmd	change the default (cmd.exe) shell
settime	Set sleep time
uninstall	uninstall itself
write	write command to shell
list	Send list of files and folders to C&C
upload	Download file from C&C
down	Upload file to C&C

Here are some sample decrypted C&C transactions from the HttpBrowser RAT:

Figure 9: List of drives sent as part of the init command

Figure 10: List of files sent as part of the list command

Conclusion

HttpBrowser RAT, due to the range of features including SSL based C&C channel, anti-detection & anti-analysis techniques, remains the popular malware of choice for APT attacks. There have been multiple instances where this RAT co-existed with PlugX RAT on the compromised network indicating an APT adversary group with a set attack tool arsenal. The network infrastructure leveraged in this attack against the financial services firm shows involvement of a previously known Cyber espionage APT group of Chinese origin. The main motive of this group is to monitor and exfiltrate intellectual property data from the target organization.

Zscaler's ThreatLabZ has confirmed coverage for these exploits and for the HttpBrowser variant, ensuring protection for organizations using Zscaler's Internet security platform.

Research by: Abhay Yadav, Avinash Kumar, Nirmal Singh, Deepen Desai

Explore more Zscaler blogs
