The Spring Dragon APT

By Kurt Baumgartner

Published: 2015-06-17 · Archived: 2026-04-02 12:24:05 UTC

APT reports

APT reports

17 Jun 2015

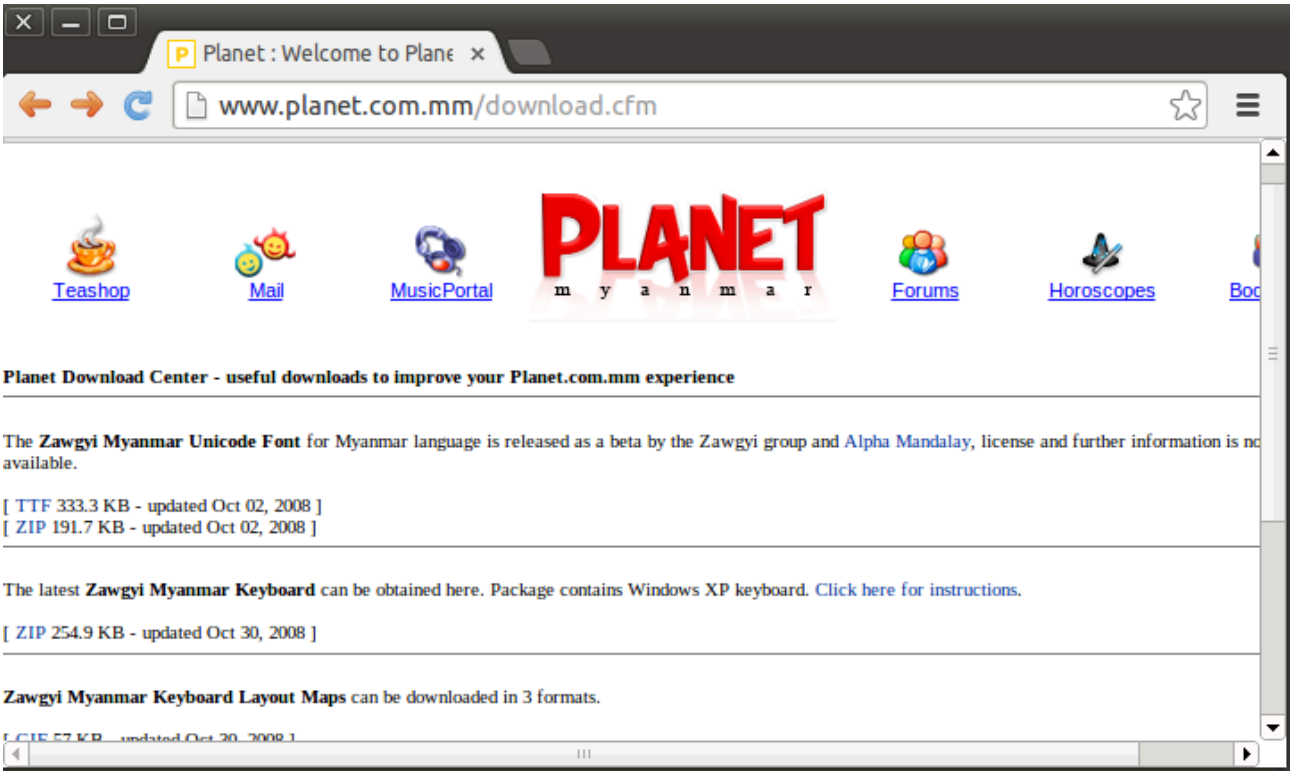
2 minute read

More Intrusion Techniques Rolled In

Let’s examine a couple of interesting delivery techniques from an APT active for the past several years, the Spring Dragon APT. A paper released today by our colleagues at Palo Alto Networks presented a portion of data on this crew under the label “the Lotus Blossom Operation“, likely named for the debug string present in much of the “Elise” codebase since at least 2012: “d:\lstudio\projects\lotus\…”.

```
)7B79: 00 00 00 00 A0 00 10 E0  8B 00 10 03 00 00 00 52        ►à‹ ►♥   R
)7B89: 53 44 53 0C F7 6A 51 58  52 69 4E 84 93 DC 9C 3F  SDS♀÷jQXRiN„“Üœ?
)7B99: F3 C4 52 02 00 00 00 64  3A 5C 4C 53 74 75 64 69  óÄR☻   d:\LStudi
)7BA9: 6F 5C 50 72 6F 6A 65 63  74 73 5C 4C 6F 74 75 73  o\Projects\Lotus
)7BB9: 5C 45 6C 69 73 65 5C 52  65 6C 65 61 73 65 5C 45  \Elise\Release\E
)7BC9: 6C 69 73 65 44 4C 4C 2E  70 64 62 00 00 00 00 00  liseDLL.pdb
)7BD9: 00 00 00 00 00 00 00 A4  52 00 00 6D 77 00 00 18        ¤R  mw  ↑
```

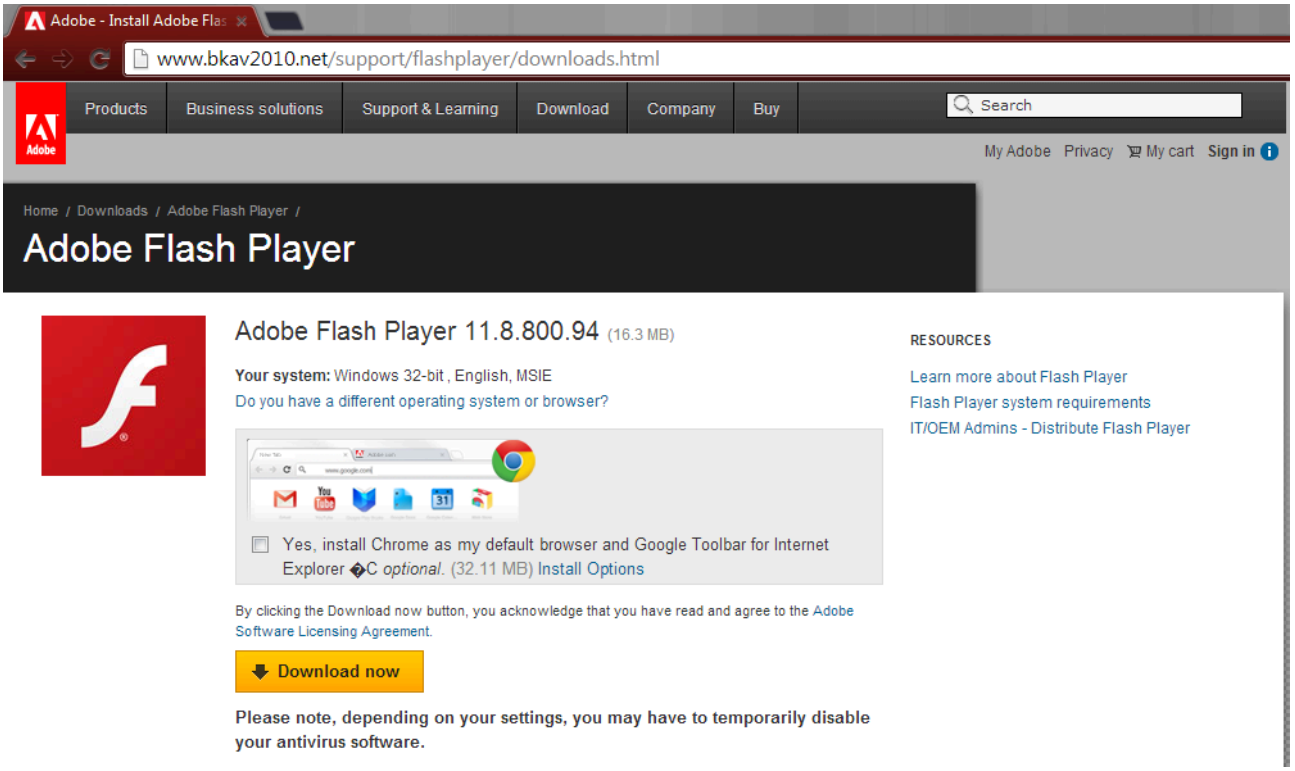
The group’s capabilities are more than the much discussed CVE-2012-0158 exploits over the past few years. Instead, the group is known to have employed half day spearphish exploits, strategic web compromises, and watering holes employing fake Flash player update re-directions. The group’s spearphish toolset includes PDF exploits, Adobe Flash Player exploits, and the common CVE-2012-0158 Word exploits including those generated from the infamous “Tran Duy Linh” kit. While ongoing attacks by the Spring Dragon APT take us back to a focus on Vietnam, they appear to have rolled out a steady mix of exploits against defense subcontractors around the world and government related organizations in VN, TW, PH, and other locations over the past few years. Let’s take a quick look at a couple more examples of their intrusion capabilities that haven’t been mentioned elsewhere.



Organizations located in Myanmar and targeted by Spring Dragon have gone unmentioned. But Spring Dragon's infiltration techniques there were not simply 0158 spearphish, they also compromised sites. In one case, they replaced specialized font installers needed to render Myanma font. You can see an image here of the "Planet Myanmar" website in late 2012 distributing such a package. All of the zip links were redirected to a poisoned installer zip file. The download name was "Zawgyi_Keyboard_L.zip", and it dropped a "setup.exe" that contained several backdoor components, including an Elise "wincex.dll" (a42c966e26f3577534d03248551232f3, detected as Backdoor.Win32.Agent.delp). It beacons out with the typical Elise GET request "GET /%x/page_%02d%02d%02d%02d.html", as documented in the Lotus Blossom paper.

Another APT later abused this exact site to deliver malicious VBS (CVE-2014-6332) exploits in November of 2014 with a Lurid variant payload. And that same group also served a malicious PDF exploit (CVE-2010-2883) from this site in June 2012 as "Zawgyi Unicode Keyboard.pdf". Even earlier than that, they spearphished with that same PDF exploit object later hosted on the website under different file names. In November 2011, they used filenames appropriate for their spearphishing targets with this exploit like "台灣安保協會「亞太區域安全與台海和平」國際研討會邀 請 函_20110907.pdf" ("Taiwan Security Association International Seminar Invitation – the Asia-Pacific regional security and peace in the Taiwan Strait"), "china-central_asia.pdf", "hydroelectric sector.pdf", and various governmental related proposals. In this case, there was unexpected overlap from two APT.

Another interesting technique that we observed in use against government targets was a campaign that lured recipients to a site redirecting users to a spoofed Flash installer site.



This site in turn redirected users to a Flash installer bundled with the common Elise backdoor, eventually communicating with 210.175.53.24 and its usual “GET /14111121/page_321111234.html HTTP/1.0”.

hxxp://www.bkav2010.net/support/flashplayer/downloads.html → redirected to hxxp://96.47.234.246/support/flashplayer/install_flashplayer.exe (Trojan-Dropper.Win32.Agent.ilbq)

While this particular actor effectively used their almost worn out CVE-2012-0158 exploits in the past, Spring Dragon employs more involved and creative intrusive activity as well.

Latest Posts

Latest Webinars

Reports

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT's infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.
