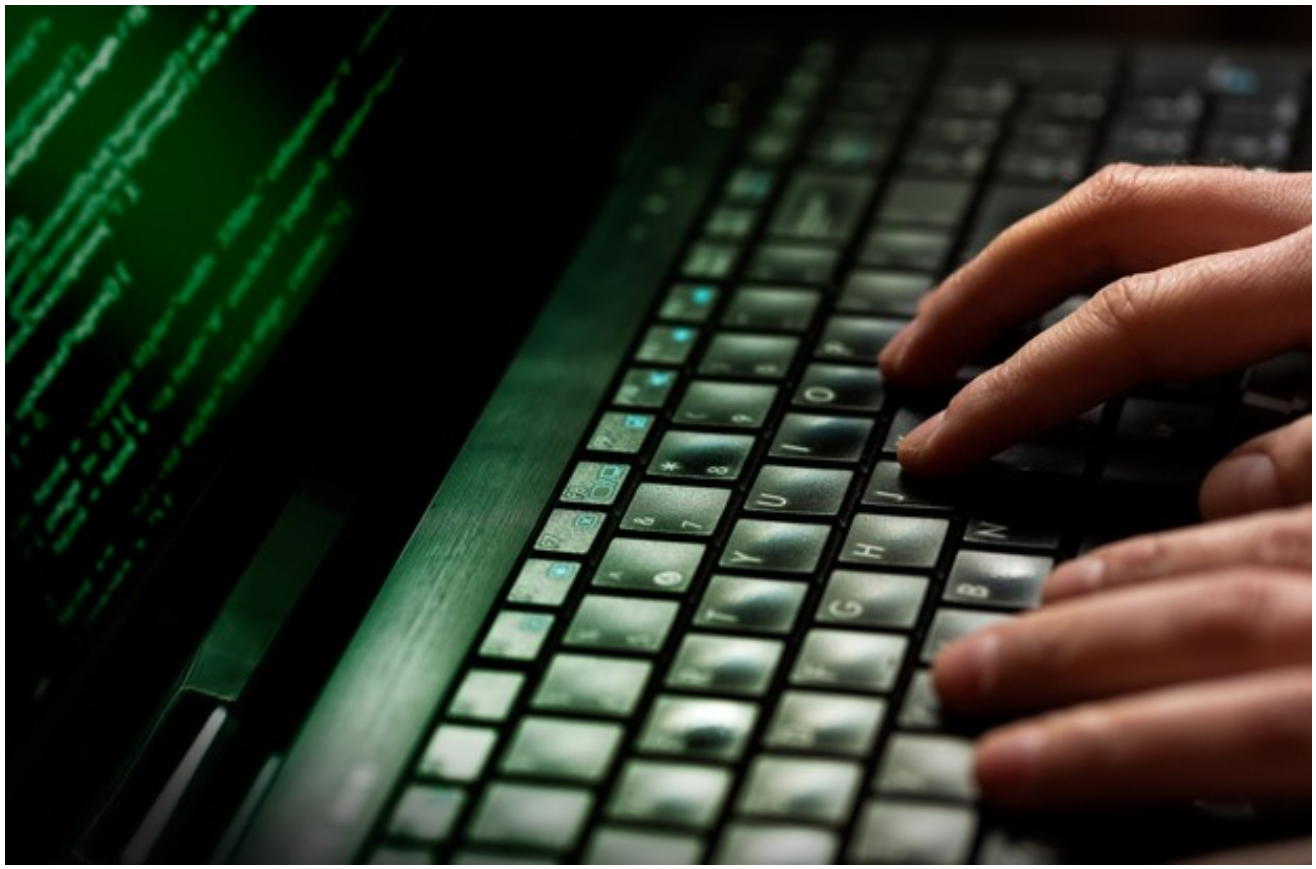
welivesecurity
News, views, and insight from the ESET security community

Sednit APT Group Meets Hacking Team

BY ESET RESEARCH POSTED 10 JUL 2015 - 01:52PM



The infamous Sednit espionage group is currently using the Hacking Team exploits disclosed **earlier this week** to target eastern European institutions.

More than 400GB of internal data from the company Hacking Team were released on the Internet last weekend. According to its website, Hacking Team develops and sells *"easy-to-use offensive technology to the worldwide law enforcement and intelligence communities*". The leaked data contain a variety of information, from business proposals to the source code of the software sold by the company.

In particular, there are two particularly interesting development projects in the leaked data:

1. A Flash exploit targeting the vulnerability labeled **CVE-2015-5119**. This vulnerability was patched on Wednesday the 8th of July in Adobe security bulletin **APSB15-16**, and the exploit was therefore a zero-day up till then. It allows an attacker to execute arbitrary code remotely, if the attacker can convince the potential victim to open a specially crafted Flash file. Strikingly, the exploit works against all major browsers and can also be deployed easily in Microsoft Office documents (Word, Excel, PowerPoint).Hacking Team's leaked data contain various tools for easy manipulation of the Flash exploit, and therefore it does not come as a surprise that various exploit kits integrated it very rapidly, as reported by the security researcher **Kafeine**. A Metasploit module is also now **available**.

2. A Windows local privilege escalation exploit, which is still unpatched and to which no CVE number has yet been allocated. This exploit allows an attacker to execute a program with maximum privileges.

Hence, the Hacking Team leak provides a complete exploitation chain, starting from a Flash exploit for the compromise, to a Windows escalation privilege exploit allowing the payload execution with elevated privileges.

This week ESET spotted a malicious team that rushed to integrate Hacking Team exploits into its arsenal: the Sednit group. This group, also known as APT28 or Fancy Bear, has been targeting various institutions since 2006 for espionage purposes. To do so, they develop their own software, including such tools as **specialized spying software** and **exploit kits**.

On Wednesday the 8th of July 2015 the Sednit group started to use the Hacking Team Flash exploit in their exploit kit. Targets were then exposed to the following exploitation chain (see our **blog post** for more details on the exploit kit):

1. The target receives a spear-phishing email containing an URL pointing to a domain name mimicking a legitimate domain name. In this particular case, we observed the domain “osce-press.org” being used, which mimics “osce.org/press”.

2. If the target opens the URL, the browser hits a landing page with JavaScript code, which collects detailed information on the computer.

3. If the computer matches certain criteria set by the Sednit operators (language, timezone…), the server then serves an exploit to the target. Since Wednesday, a Flash exploit is delivered under the name “flash_video_x86.swf”. The decompiled code of the exploit is almost the same as the Hacking Team exploit – more precisely, the version dubbed “scratch_ie_ff_bytearray” in the leaked data.The only difference between the two exploits appears to be that the Sednit version receives the shellcode to execute in an input parameter in a manner similar to Metasploit exploits, whereas in the Hacking Team version the shellcode is hardcoded in the Flash file. The following Figures show the Main function in the two cases.

```
public function Main():void
{
    if (stage) init();
    else addEventListener(Event.ADDED_TO_STAGE, init);

}
```

Figure 1 – Hacking Team Flash exploit main function

```
public var shellcode:Array;

public function Main()
{

 this.shellcode = this.root.loaderInfo.parameters.sh.split(",");

 if (stage) init();
          else addEventListener(Event.ADDED_TO_STAGE, init);
}
```

Figure 2 – Sednit Flash exploit main function

4. If the Flash exploitation works, the victim receives a first-stage backdoor – malware whose purpose is to make sure the victim is the intended target. This malware contains Hacking Team’s Windows escalation privilege exploit. Given the presence of syntactic differences, it appears the Sednit group recompiled the source code of the exploit, but without modifying its logic.

If the privilege escalation exploit works, the malware then sets its persistence on the machine through a scheduled task running with the highest privileges.

This story shows that advanced groups of attackers also employ opportunistic strategies. It took only a few days for the Sednit group to re-use the Hacking Team exploitation chain for their own purpose. The Webky group – another APT team – was also reported to have done the same **this week**. We strongly encourage users to upgrade their Flash software.

Indicators of Compromise

Indicator	Value
Exploit kit domain name	osce-press.org

Sednit Flash exploit SHA1	D43FD6579AB8B9C40524CC8E4B7BD05BE6674F6C
Sednit first-stage backdoor SHA1	51B0E3CD6360D50424BF776B3CD673DD45FD0F97
Payload persistence script name	fvecer.bat
Payload file name	api-ms-win-downlevel-profile-l1-1-0.dll
Payload SHA1	B8B3F53CA2CD64BD101CB59C6553F6289A72D9BB