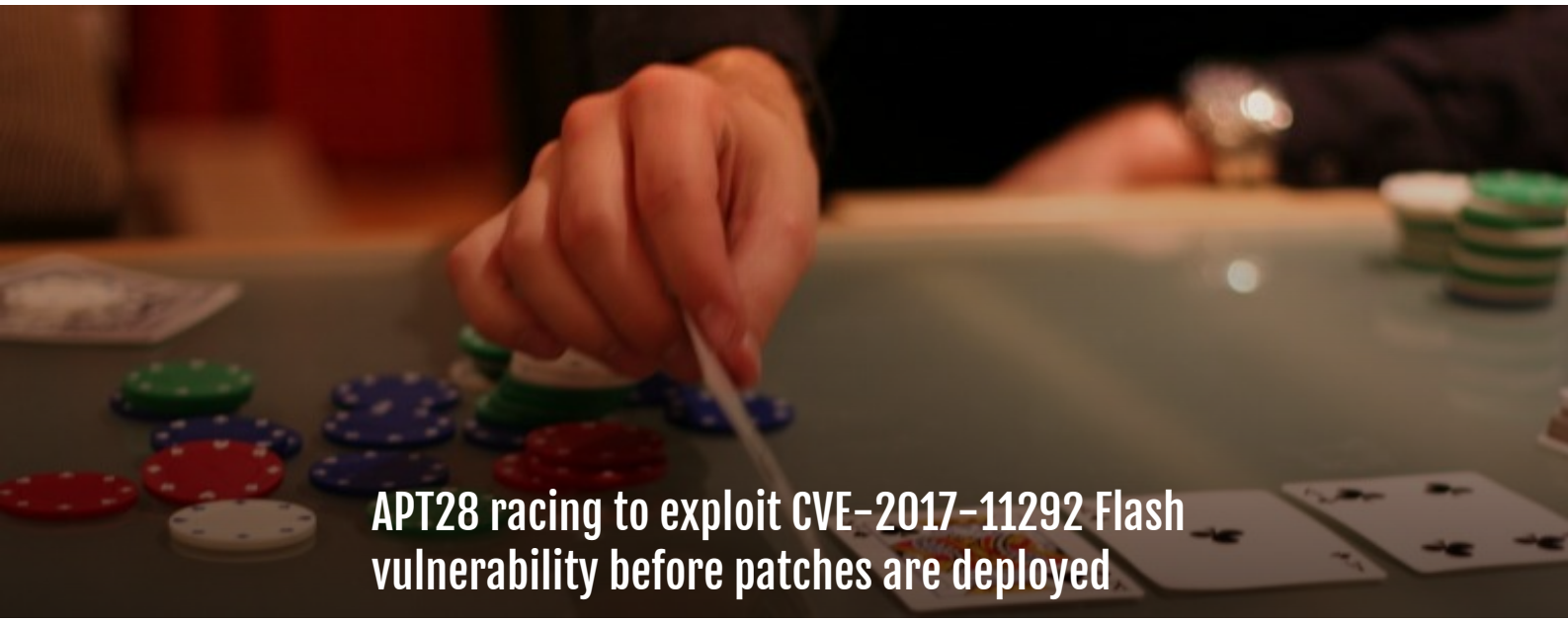

APT28 racing to exploit CVE-2017-11292 Flash vulnerability before patches are deployed

OCTOBER 19, 2017 | KAFEINE, PIERRE T

Editor's Note

This post will be updated as the threat is mitigated with additional C&C takedowns; for now we are only sharing basic information related to this campaign to avoid enabling actions by other threat actors. We have already included new IOCs following initial takedown operations and will continue to monitor and engage in mitigation efforts.

Overview

On Tuesday, October 18, Proofpoint researchers detected a malicious Microsoft Word attachment exploiting a recently patched Adobe Flash vulnerability, CVE-2017-11292. We attributed this attack to APT28 (also known as Sofacy), a Russian state-sponsored group. Targeting data for this campaign is limited but some emails were sent to foreign government entities equivalent to the State Department and private-sector businesses in the aerospace industry. The known geographical targeting appears broad, including Europe and the United States. The emails were sent from free email services.

As we examined the document exploitation chain, we found that DealersChoice.B [2], the attack framework that the document uses, is now also exploiting CVE-2017-11292, a Flash vulnerability that can lead to arbitrary code execution across Windows, Mac OS, Linux, and Chrome OS systems. The vulnerability was announced and patched on Monday, October 16 [1]. At that time Kaspersky attributed the exploit use to the BlackOasis APT group, which is distinct from APT28. We suspect that APT28, who also possess this exploit (whether purchased, discovered on their own, or reverse engineered from the BlackOasis attack), may now seek to benefit from it as quickly as possible before the patch is widely deployed.

Thus, while this exploit is no longer a zero-day, this is only the second known campaign utilizing it reported in public. APT28 burned their CVE-2017-0262 EPS 0-day in a similar fashion in April after Microsoft pushed an EPS exploit mitigation, which significantly reduced the impact of this exploit. [3]

Analysis

The document "World War 3.docx" contacts DealersChoice.B, APT28's attack framework that allows loading exploit code on-demand from a command and control (C&C) server. DealersChoice has previously been used to exploit a variety of Flash vulnerabilities, including CVE-2015-7645, CVE-2016-1019, CVE-2016-4117, and CVE-2016-7855 via embedded objects in crafted Microsoft Word documents.

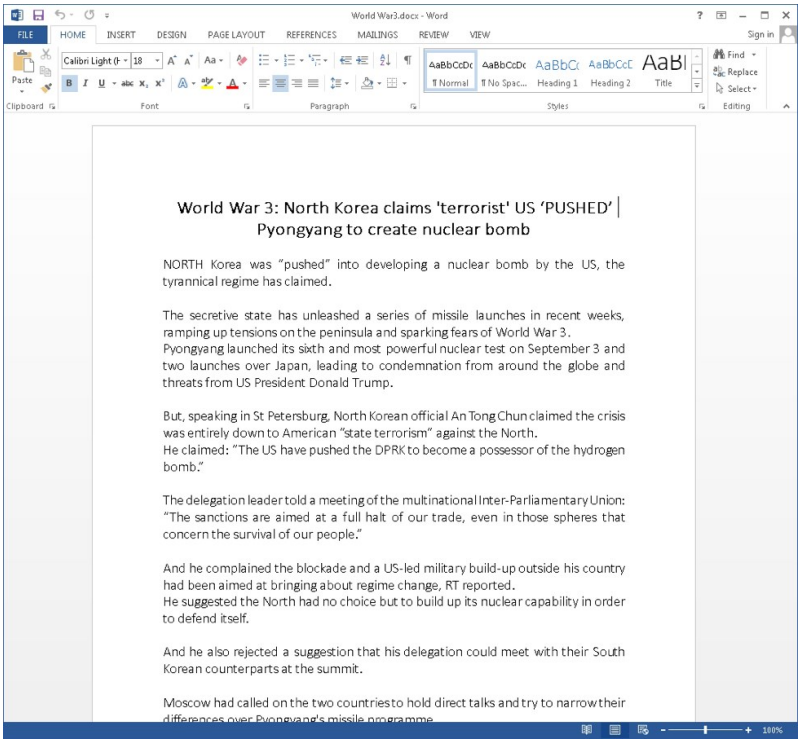

Figure 1: Decoy document used

This malicious document embeds the same Flash object twice in an ActiveX control for an unknown reason, although this is likely an

operational mistake. The Flash files work in the same manner as the last known attack using this tool: the embedded Flash decompresses a second Flash object that handles the communication with the exploit delivery server. The only difference is that this second Flash object is no longer stored encrypted. There are other signs that this campaign was devised hastily: for example, the actors did not change the decryption algorithm constants as they have in the past. These particular constants were already used in a late December 2016 campaign. Each document uses a different domain for victim exploitation, while the communication protocol with the server stayed the same as well.

December 2016

```
private function unpack(param1:ByteArray, param2:uint) : ByteArray
{
   param1.position = 0;
   var key:uint = param2;
   var i:uint = 0;
   while(i < param1.length)
   {
      key = key >> 1 ^ ((key & 64) >> 6 ^ (key & 32) >> 5 ^ (key & 2) >> 1 ^ (key & 8) >> 3) << 7;
      param1[i] = param1[i] ^ key;
      i++;
   }
   param1.position = 0;
   param1.uncompress();
   param1.position = 0;
   return param1;
}
```

October 2017

```
private function unpack(param1:ByteArray, param2:uint) : ByteArray
{
   param1.position = 0;
   var key:uint = param2;
   var i:uint = 0;
   while(i < param1.length)
   {
      key = key >> 1 ^ ((key & 64) >> 6 ^ (key & 32) >> 5 ^ (key & 2) >> 1 ^ (key & 8) >> 3) << 7;
      param1[i] = param1[i] ^ key;
      i++;
   }
   param1.position = 0;
   param1.uncompress();
   param1.position = 0;
   return param1;
}
```

Figure 2: Comparison of the decryption functions (lightly edited for readability) showing that the decryption algorithm constants were not changed

We performed testing and found exploitation to be successful on:

- Windows 7 with Flash 27.0.0.159 and Microsoft Office 2013
- Windows 10 build 1607 with Flash 27.0.0.130 and Microsoft Office 2013

At this point, despite the potential impact across operating systems of this particular Flash vulnerability, Mac OS does not appear to be targeted by this campaign. Users running 64-bit versions of Microsoft Office 2016 and Windows 10 RS3 should be protected against this exploit as well.

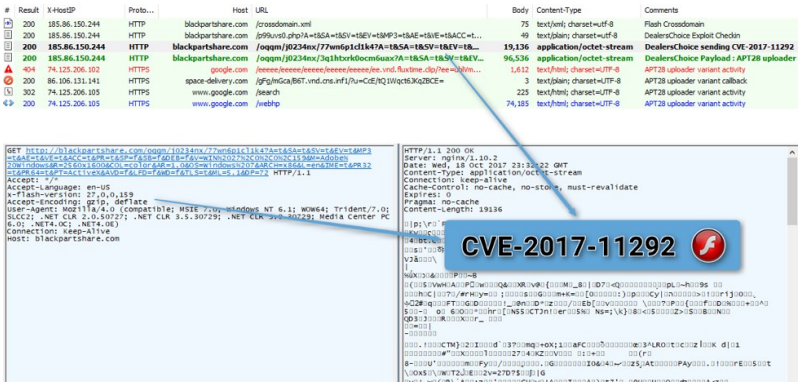

Figure 3: Flash 27.0.0.159 exploited by DealersChoice's CVE-2017-11292 on Windows 7 via Microsoft Office 2013

Figure 4: DealersChoice Flash checkin under Windows 10 build 1607, Microsoft Word 2013, and Flash 27.0.0.130

The CVE-2017-11292 exploit (Figure 5) delivered by the server is then decrypted and executed by the Flash object handling the communications. Upon successful execution, the payload is requested, decrypted, and executed on the target system.

```
1  package
2  {
3     import com.adobe.tvsdk.mediacore.BufferControlParameters;
4     public class P3 extends BufferControlParameters
5     {
6        public var addr:uint;
7        public var addrH:uint;
8        public var oAddr:uint;
9        public var oAddrH:uint;
10       public var o;
11       public function P3()
12       {
13          super(0,1);
14       }
15    }
16 }
```

Figure 5: Use of the vulnerable mediacore.BufferControlParameters class

After exploitation, DealersChoice typically delivers a stage 1 implant named Uploader [4]. In this case, it delivered only the Uploader payload component (build 0x2125181f) without the intermediate dropper. This malware has basic capabilities used for reconnaissance on the target systems. Uploader is also used to deploy further tools and implants on the system. It is worth noting that the timestamp (Wed Oct 18 01:54:28 2017 GMT) present in in the payload indicates a very short delay between the setup of this attack and its launch.

Conclusion

APT28 appears to be moving rapidly to exploit this newly documented vulnerability before the available patch is widely deployed. Because Flash is still present on a high percentage of systems and this vulnerability affects all major operating systems, it is critical that organizations and end users apply the Adobe patch immediately. APT28 is a sophisticated state-sponsored group that is using the vulnerability to attack potentially high-value targets but it is likely that other threat actors will follow suit and attempt to exploit this vulnerability more widely, whether in exploit kits or via other attack vectors.

References

[1] https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/

[2] https://researchcenter.paloaltonetworks.com/2016/12/unit42-let-ride-sofacy-groups-dealerschoice-attacks-continue/

[3] https://www.fireeye.com/blog/threat-research/2017/05/eps-processing-zero-days.html

[4] https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf

Indicators of Compromise (IOCs)

IOC	IOC Type	Description
25f983961eef6751e53a72c96d35448f8b413edf727501d0990f763b8c5e900b	sha256	Decoy/Exploit Document
416467f8975036bb06c2b5fca4daeb900ff5f25833d3cdb46958f0f0f26bec82	sha256	APT28 Uploader Variant
blackpartshare[.com|185.86.150.244	Domain|IP	DealersChoice C&C (now taken down)
mountainsgide[.com|185.86.150.244	Domain|IP	DealersChoice C&C (now taken down)
contentdeliverysrv[.net|142.91.104.106	Domain|IP	DealersChoice C&C (now taken down)
space-delivery[.com|86.106.131.141	Domain|IP	APT28 uploader C&C

ET and ETPRO Suricata/Snort Signatures

2014726 || ET POLICY Outdated Flash Version M1

2823078 || ETPRO TROJAN APT28 DealersChoice CnC Beacon M1

2823642 || ETPRO TROJAN APT28 DealersChoice CnC Beacon Response

2023916 || ET TROJAN APT28 Uploader Variant CnC Beacon

2828341 || ETPRO TROJAN APT28 DealersChoice DNS Lookup

2828342 || ETPRO TROJAN APT28 Uploader DNS Lookup