

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.

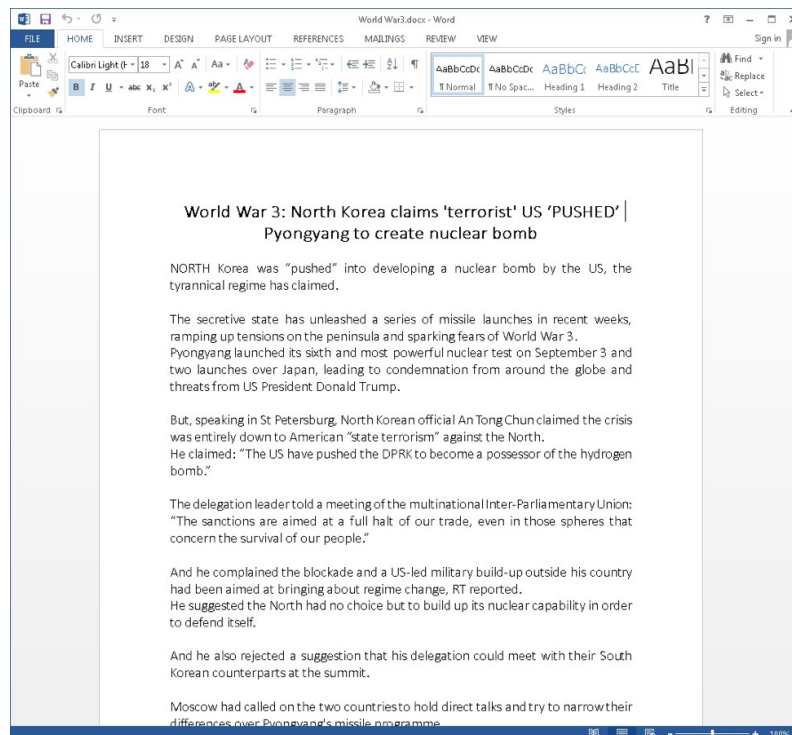


Figure 1: Decoy document used

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

```
private function unpack(param1:ByteArray, param2:uint) : ByteArray December 2016
{
    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;
}
```

```
private function unpack(param1:ByteArray, param2:uint) : ByteArray October 2017
{
    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;
}
```

- 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

#	Result	IPVerID	Proto...	Host	URL	Body	Content-Type	Comments
200	200	185.86.150.244	HTTP	blackparchare.com	/crossdomain.xml	75	text/xml; charset=utf-8	Find Crossdomain
200	200	185.86.150.244	HTTP	blackparchare.com	/api/mgmt.php?A=1&B=1&CV=1&MP=1&ME=1&I=1&CC=1	75	application; charset=utf-8	Dealer's Config Endpoint
200	200	185.86.150.244	HTTP	blackparchare.com	/api/mgmt/0224m/77m6j01k1847A-185A-185V-185L-185C-185D-185E-185F-185G-185H-185I-185J-185K-185L-185M-185N-185O-185P-185Q-185R-185S-185T-185U-185V-185W-185X-185Y-185Z-185AA-185AB-185AC-185AD-185AE-185AF-185AG-185AH-185AI-185AJ-185AK-185AL-185AM-185AN-185AO-185AP-185AQ-185AR-185AS-185AT-185AU-185AV-185AW-185AX-185AY-185AZ-185BA-185BB-185BC-185BD-185BE-185BF-185BG-185BH-185BI-185BJ-185BK-185BL-185BM-185BN-185BO-185BP-185BQ-185BR-185BS-185BT-185BU-185BV-185BW-185BX-185BY-185BZ-185CA-185CB-185CC-185CD-185CE-185CF-185CG-185CH-185CI-185CJ-185CK-185CL-185CM-185CN-185CO-185CP-185CQ-185CR-185CS-185CT-185CU-185CV-185CW-185CX-185CY-185CZ-185DA-185DB-185DC-185DD-185DE-185DF-185DG-185DH-185DI-185DJ-185DK-185DL-185DM-185DN-185DO-185DP-185DQ-185DR-185DS-185DT-185DU-185DV-185DW-185DX-185DY-185DZ-185EA-185EB-185EC-185ED-185EE-185EF-185EG-185EH-185EI-185EJ-185EK-185EL-185EM-185EN-185EO-185EP-185EQ-185ER-185ES-185ET-185EU-185EV-185EW-185EX-185EY-185EZ-185FA-185FB-185FC-185FD-185FE-185FF-185FG-185FH-185FI-185FJ-185FK-185FL-185FM-185FN-185FO-185FP-185FQ-185FR-185FS-185FT-185FU-185FV-185FW-185FX-185FY-185FZ-185GA-185GB-185GC-185GD-185GE-185GF-185GG-185GH-185GI-185GJ-185GK-185GL-185GM-185GN-185GO-185GP-185GQ-185GR-185GS-185GT-185GU-185GV-185GW-185GX-185GY-185GZ-185HA-185HB-185HC-185HD-185HE-185HF-185HG-185HH-185HI-185HJ-185HK-185HL-185HM-185HN-185HO-185HP-185HQ-185HR-185HS-185HT-185HU-185HV-185HW-185HX-185HY-185HZ-185IA-185IB-185IC-185ID-185IE-185IF-185IG-185IH-185II-185IJ-185IK-185IL-185IM-185IN-185IO-185IP-185IQ-185IR-185IS-185IT-185IU-185IV-185IW-185IX-185IY-185IZ-185JA-185JB-185JC-185JD-185JE-185JF-185JG-185JH-185JI-185JJ-185JK-185JL-185JM-185JN-185JO-185JP-185JQ-185JR-185JS-185JT-185JU-185JV-185JW-185JX-185JY-185JZ-185KA-185KB-185KC-185KD-185KE-185KF-185KG-185KH-185KI-185KJ-185KK-185KL-185KM-185KN-185KO-185KP-185KQ-185KR-185KS-185KT-185KU-185KV-185KW-185KX-185KY-185KZ-185LA-185LB-185LC-185LD-185LE-185LF-185LG-185LH-185LI-185LJ-185LK-185LL-185LM-185LN-185LO-185LP-185LQ-185LR-185LS-185LT-185LU-185LV-185LW-185LX-185LY-185LZ-185MA-185MB-185MC-185MD-185ME-185MF-185MG-185MH-185MI-185MJ-185MK-185ML-185MM-185MN-185MO-185MP-185MQ-185MR-185MS-185MT-185MU-185MV-185MW-185MX-185MY-185MZ-185NA-185NB-185NC-185ND-185NE-185NF-185NG-185NH-185NI-185NJ-185NK-185NL-185NM-185NN-185NO-185NP-185NQ-185NR-185NS-185NT-185NU-185NV-185NW-185NX-185NY-185NZ-185OA-185OB-185OC-185OD-185OE-185OF-185OG-185OH-185OI-185OJ-185OK-185OL-185OM-185ON-185OO-185OP-185OQ-185OR-185OS-185OT-185OU-185OV-185OW-185OX-185OY-185OZ-185PA-185PB-185PC-185PD-185PE-185PF-185PG-185PH-185PI-185PJ-185PK-185PL-185PM-185PN-185PO-185PP-185PQ-185PR-185PS-185PT-185PU-185PV-185PW-185PX-185PY-185PZ-185QA-185QB-185QC-185QD-185QE-185QF-185QG-185QH-185QI-185QJ-185QK-185QL-185QM-185QN-185QO-185QP-185QQ-185QR-185QS-185QT-185QU-185QV-185QW-185QX-185QY-185QZ-185RA-185RB-185RC-185RD-185RE-185RF-185RG-185RH-185RI-185RJ-185RK-185RL-185RM-185RN-185RO-185RP-185RQ-185RR-185RS-185RT-185RU-185RV-185RW-185RX-185RY-185RZ-185SA-185SB-185SC-185SD-185SE-185SF-185SG-185SH-185SI-185SJ-185SK-185SL-185SM-185SN-185SO-185SP-185SQ-185SR-185SS-185ST-185SU-185SV-185SW-185SX-185SY-185SZ-185TA-185TB-185TC-185TD-185TE-185TF-185TG-185TH-185TI-185TJ-185TK-185TL-185TM-185TN-185TO-185TP-185TQ-185TR-185TS-185TT-185TU-185TV-185TW-185TX-185TY-185TZ-185UA-185UB-185UC-185UD-185UE-185UF-185UG-185UH-185UI-185UJ-185UK-185UL-185UM-185UN-185UO-185UP-185UQ-185UR-185US-185UT-185UU-185UV-185UW-185UX-185UY-185UZ-185VA-185VB-185VC-185VD-185VE-185VF-185VG-185VH-185VI-185VJ-185VK-185VL-185VM-185VN-185VO-185VP-185VQ-185VR-185VS-185VT-185VU-185VV-185VW-185VX-185VY-185VZ-185WA-185WB-185WC-185WD-185WE-185WF-185WG-185WH-185WI-185WJ-185WK-185WL-185WM-185WN-185WO-185WP-185WQ-185WR-185WS-185WT-185WU-185WV-185WW-185WX-185WY-185WZ-185XA-185XB-185XC-185XD-185XE-185XF-185XG-185XH-185XI-185XJ-185XK-185XL-185XM-185XN-185XO-185XP-185XQ-185XR-185XS-185XT-185XU-185XV-185XW-185XX-185XY-185XZ-185YA-185YB-185YC-185YD-185YE-185YF-185YG-185YH-185YI-185YJ-185YK-185YL-185YM-185YN-185YO-185YP-185YQ-185YR-185YS-185YT-185YU-185YV-185YW-185YX-185YY-185YZ-185ZA-185ZB-185ZC-185ZD-185ZE-185ZF-185ZG-185ZH-185ZI-185ZJ-185ZK-185ZL-185ZM-185ZN-185ZO-185ZP-185ZQ-185ZR-185ZS-185ZT-185ZU-185ZV-185ZW-185ZX-185ZY-185ZZ	19,136	application/octet-stream	Dealer'sChoice Endpoint CVE-2017-1129: 19,136

[illegible]

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.tv.sdk.media.core.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 }
```

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 the in the payload indicates a very short delay between the setup of this attack and its launch.

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.

[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

About

Overview
Why Proofpoint
Careers
Leadership Team
News Center
Investors Center

Threat Center

Latest Threat Report
Human Factor Report
Threat Glossary
Threat Blog
Daily Ruleset

Products

Email Protection
Advanced Threat Protection
Security Awareness Training
Cloud App Security
Archive & Compliance
Information Protection
Digital Risk Protection
Product Bundles
Nexus Platform

Resources

Whitepapers
Webinars
Datasheets
Events
Customer Stories
Blog
Free Trial

Connect

+1-408-517-4710
Contact Us
Office Locations
Request a Demo

Support

Support Login
Support Services
IP Address Blocked?

proofpoint.



© 2020. All rights reserved.

[Terms and conditions](#)

[Privacy Policy](#)

[Sitemap](#)

