Activity

By GReAT on February 20, 2018. 2:00 pm

Sofacy, also known as APT28, Fancy Bear, and Tsar Team, is a highly active and prolific APT. From their high volume 0day deployment to their innovative and broad malware set, Sofacy is one of the top groups that we monitor, report, and protect against. 2017 was not any different in this regard. Our private reports subscription customers receive a steady stream of YARA, IOC, and reports on Sofacy, our most reported APT for the year.

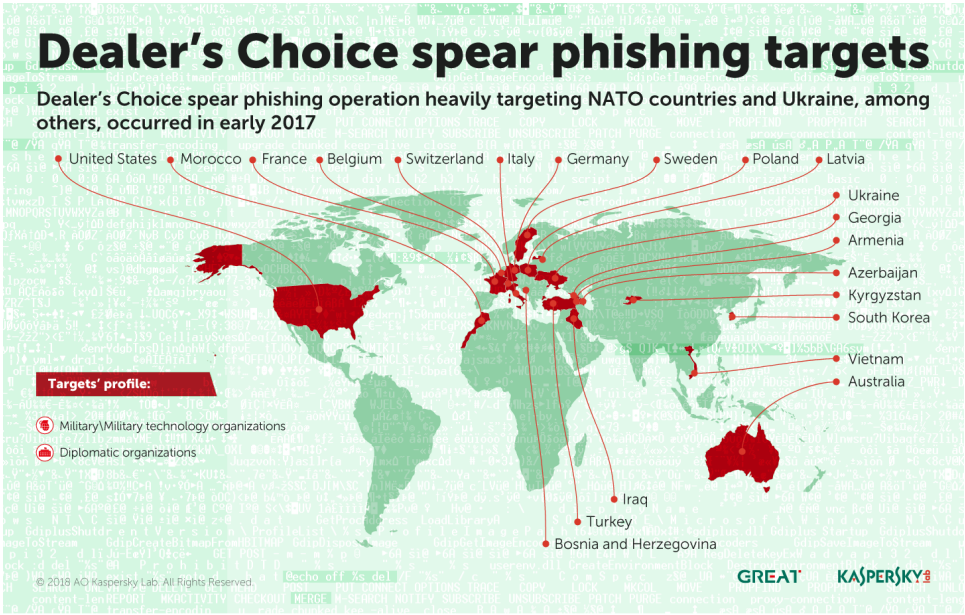
This high level of cyber-espionage activity goes back years. In 2011-2012, the group used a relatively tiny implant (known as "Sofacy" or SOURFACE) as their first stage malware, which at the time had similarities with the old Miniduke implants. This made us believe the two groups were connected, although it looks they split ways at a certain point, with the original Miniduke group switching to the CosmicDuke implant in 2014. The division in malware was consistent and definitive at that point.

In 2013, the Sofacy group expanded their arsenal and added more backdoors and tools, including CORESHELL, SPLM (aka Xagent, aka CHOPSTICK), JHUHUGIT (which is built with code from the Carberp sources), AZZY (aka ADVSTORESHELL, NETUI, EVILTOSS, and spans across 4-5 generations) and a few others. We've seen quite a few versions of these implants, which were relatively widespread at some point or still are. In 2015 we noticed another wave of attacks which took advantage of a new release of the AZZY implant, largely undetected by antivirus products. The new wave of attacks included a new generation of USB stealers deployed by Sofacy, with initial versions dating to February 2015. It appeared to be geared exclusively towards high profile targets.

Sofacy's reported presence in the DNC network alongside APT29 brought possibly the highest level of public attention to the group's activities in 2016, especially when data from the compromise was leaked and "weaponized". And later 2016, their focus turned towards the Olympics' and the World Anti-Doping Agency (WADA) and Court of Arbitration for Sports (CAS), when individuals and servers in these organizations were phished and compromised. In a similar vein with past CyberBerkut activity, attackers hid behind anonymous activist groups like "anonpoland", and data from victimized organizations were similarly leaked and "weaponized".

This write-up will survey notables in the past year of 2017 Sofacy activity, including their targeting, technology, and notes on their infrastructure. No one research group has 100% global visibility, and our collected data is

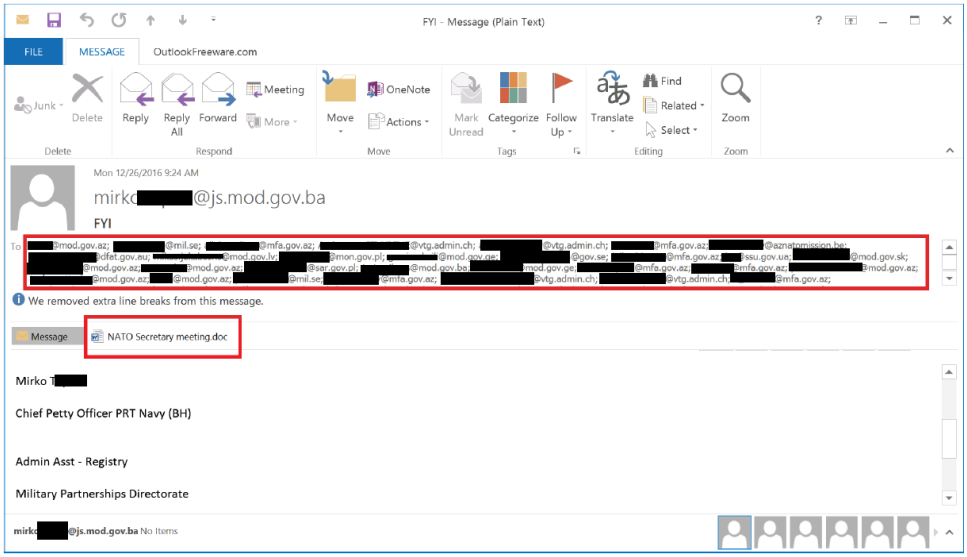
presented accordingly. Here, external APT28 reports on 2017 Darkhotel-style activity in Europe and Dealer's Choice spearphishing are of interest. From where we sit, 2017 Sofacy activity starts with a heavy focus on NATO and Ukrainian partners, coinciding with lighter interest in Central Asian targets, and finishing the second half of the year with a heavy focus on Central Asian targets and some shift further East.



Dealer's Choice

The beginning of 2017 began with a slow cleanup following the Dealer's Choice campaign, with technical characteristics documented by our colleagues at Palo Alto in several stages at the end of 2016. The group spearphished targets in several waves with Flash exploits leading to their carberp based JHUHUGIT downloaders and further stages of malware. It seems that many folks did not log in and pull down their emails until Jan 2017 to retrieve the Dealer's Choice spearphish. Throughout these waves, we observed that the targets provided connection, even tangential, to Ukraine and NATO military and diplomatic interests.

In multiple cases, Sofacy spoofs the identity of a target, and emails a spearphish to other targets of interest. Often these are military or military-technology and manufacturing related, and here, the DealersChoice spearphish is again NATO related:



The global reach that coincided with this focus on NATO and the Ukraine couldn't be overstated. Our KSN data showed spearphishing targets geolocated across the globe into 2017.
AM, AZ, FR, DE, IQ, IT, KG, MA, CH, UA, US, VN

DealersChoice emails, like the one above, that we were able to recover from third party sources provided additional targeting insight, and confirmed some of the targeting within our KSN data:
TR, PL, BA, AZ, KR, LV, GE, LV, AU, SE, BE

0day Deployment(s)

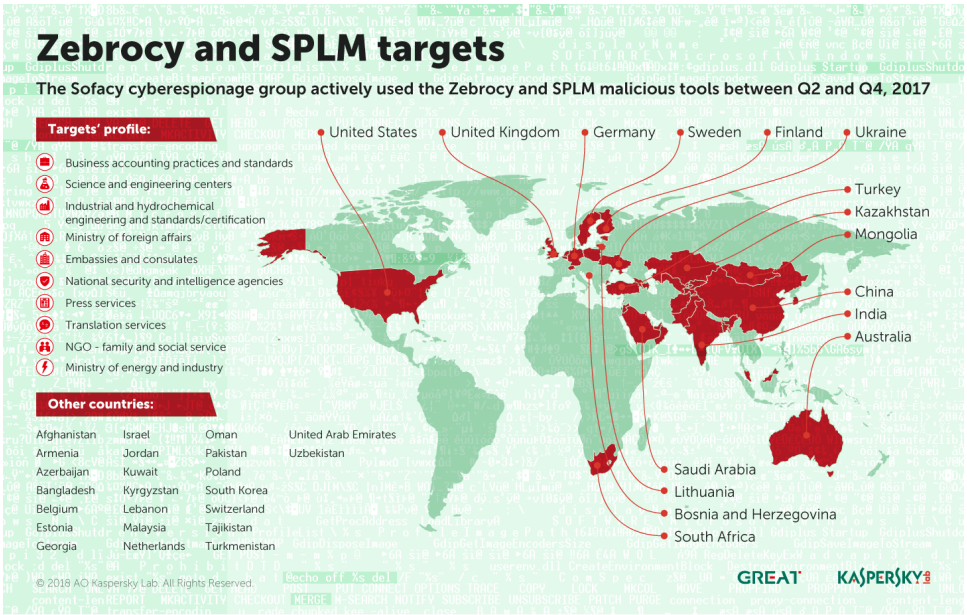
Sofacy kicked off the year deploying two 0day in a spearphish document, both a Microsoft Office encapsulated postscript type confusion exploit (abusing CVE-2017-0262) and an escalation of privilege use-after-free exploit (abusing CVE-2017-0263). The group attempted to deploy this spearphish attachment to push a small 30kb backdoor known as GAMEFISH to targets in Europe at the beginning of 2017. They took advantage of the Syrian military conflict for thematic content and file naming "Trump's_Attack_on_Syria_English.docx". Again, this deployment was likely a part of their focus on NATO targets.

Light SPLM deployment in Central Asia and Consistent Infrastructure

Meanwhile in early-to-mid 2017, SPLM/CHOPSTICK/XAgent detections in Central Asia provided a glimpse into ongoing focus on ex-Soviet republics in Central Asia. These particular detections are interesting because they indicate an attempted selective 2nd stage deployment of a backdoor maintaining filestealer, keylogger, and remoteshell functionality to a

system of interest. As the latest revision of the backdoor, portions of SPLM didn't match previous reports on SPLM/XAgent while other similarities were maintained. SPLM 64-bit modules already appeared to be at version 4 of the software by May of the year. Targeting profiles included defense related commercial and military organizations, and telecommunications.

Targeting included TR, KZ, AM, KG, JO, UK, UZ



Heavy Zebrocy deployments

Since mid-November 2015, the threat actor referred to as "Sofacy" or "APT28" has been utilizing a unique payload and delivery mechanism written in Delphi and AutoIT. We collectively refer to this package and related activity as "Zebrocy" and had written a few reports on its usage and development by June 2017 – Sofacy developers modified and redeployed incremented versions of the malware. The Zebrocy chain follows a pattern: spearphish attachment -> compiled Autoit script (downloader) -> Zebrocy payload. In some deployments, we observed Sofacy actively developing and deploying a new package to a much smaller, specific subset of targets within the broader set.

Targeting profiles, spearphish filenames, and lures carry thematic content related to visa applications and scanned images, border control administration, and various administrative notes. Targeting appears to be widely spread across the Middle East, Europe, and Asia:</p style="margin-bottom:0!important">

- Business accounting practices and standards
- Science and engineering centers
- Industrial and hydrochemical engineering and standards/certification
- Ministry of foreign affairs
- Embassies and consulates

- National security and intelligence agencies
- Press services
- Translation services
- NGO – family and social service
- Ministry of energy and industry

We identified new MSIL components deployed by Zebrocy. While recent Zebrocy versioning was 7.1, some of the related Zebrocy modules that drop file-stealing MSIL modules we call Covfacy were v7.0. The components were an unexpected inclusion in this particular toolset. For example, one sent out to a handful of countries identifies network drives when they are added to target systems, and then RC4-like-encrypts and writes certain file metadata and contents to a local path for later exfiltration. The stealer searches for files 60mb and less with these extensions:</p style="”margin-bottom:0!important”>

- .doc
- .docx
- .xls
- .xlsx
- .ppt
- .pptx
- .exe
- .zip
- .rar

At execution, it installs an application-defined Windows hook. The hook gets windows messages indicating when a network drive has been attached. Upon adding a network drive, the hook calls its “RecordToFile” file stealer method.

```
protected override void WndProc(ref Message message)
{
    base.WndProc(ref message);
    if (message.Msg != 537 || message.LParam == IntPtr.Zero)
    {
        return;
    }
    Form1.DEV_BROADCAST_VOLUME dEV_BROADCAST_VOLUME = (Form1.DEV_BROADCAST_VOLUME)
    Marshal.PtrToStructure(message.LParam, typeof(Form1.DEV_BROADCAST_VOLUME));
    if (dEV_BROADCAST_VOLUME.dbcv_devicetype == 2)
    {
        int num = message.WParam.ToInt32();
        if (num != 32768)
        {
            if (num != 32772)
            {
                return;
            }
        }
        else
        {
            this.Driver = this.ToDriveName(dEV_BROADCAST_VOLUME.dbcv_unitmask);
            this.RecordToFile();
        }
    }
}
```

Zebrocy spearphishing targets:
AF, AM, AU, AZ, BD, BE, CN, DE, ES, FI, GE, IL, IN, JO, KW, KG, KZ, LB, LT,

MN, MY, NL, OM, PK, PO, SA, ZA, SK, SE, CH, TJ, TM, TR, UA, UAE, UK, US, UZ

SPLM deployment in Central Asia

SPLM/CHOPSTICK components deployed throughout 2017 were native 64-bit modular C++ Windows COM backdoors supporting http over fully encrypted TLSv1 and TLSv1.2 communications, mostly deployed in the second half of 2017 by Sofacy. Earlier SPLM activity deployed 32-bit modules over unencrypted http (and sometimes smtp) sessions. In 2016 we saw fully functional, very large SPLM/X-Agent modules supporting OS X.

The executable module continues to be part of a framework supporting various internal and external components communicating over internal and external channels, maintaining slightly morphed encryption and functionality per deployment. Sofacy selectively used SPLM/CHOPSTICK modules as second stage implants to high interest targets for years now. In a change from previous compilations, the module was structured and used to inject remote shell, keylogger, and filesystem add-ons into processes running on victim systems and maintaining functionality that was originally present within the main module.

The newer SPLM modules are deployed mostly to Central Asian based targets that may have a tie to NATO in some form. These targets include foreign affairs government organizations both localized and abroad, and defense organizations' presence localized, located in Europe and also located in Afghanistan. One outlier SPLM target profile within our visibility includes an audit and consulting firm in Bosnia and Herzegovina.

Minor changes and updates to the code were released with these deployments, including a new mutex format and the exclusive use of encrypted HTTP communications over TLS. The compiled code itself already is altered per deployment in multiple subtle ways, in order to stymie identification and automated analysis and accommodate targeted environments. Strings (c2 domains and functionality, error messages, etc) are custom encrypted per deployment.

Targets: TR, KZ, BA, TM, AF, DE, LT, NL

SPLM/CHOPSTICK/XAgent Modularity and Infrastructure

This subset of SPLM/CHOPSTICK activity leads into several small surprises that take us into 2018, to be discussed in further detail at SAS 2018. The group demonstrates malleability and innovation in maintaining and producing familiar SPLM functionality, but the pragmatic and systematic approach towards producing undetected or difficult-to-detect malware continues. Changes in the second stage SPLM backdoor are refined, making the code reliably modular.

Infrastructure Notes

Sofacy set up and maintained multiple servers and c2 for varying durations, registering fairly recognizable domains with privacy services, registrars that accept bitcoin, fake phone numbers, phony individual names, and 1 to 1 email address to domain registration relationships. Some of this activity and patterns were publicly disclosed, so we expect to see more change in their process in 2018. Also, throughout the year and in previous years, researchers began to comment publicly on Sofacy's fairly consistent infrastructure setup.

As always, attackers make mistakes and give away hints about what providers and registrars they prefer. It's interesting to note that this version of SPLM implements communications that are fully encrypted over HTTPS. As an example, we might see extraneous data in their SSL/TLS certificates that give away information about their provider or resources. Leading up to summer 2017, infrastructure mostly was created with PDR and Internet Domain Service BS Corp, and their resellers. Hosting mostly was provided at Fast Serv Inc and resellers, in all likelihood related to bitcoin payment processing.

Accordingly, the server side certificates appear to be generated locally on VPS hosts that exclusively are paid for at providers with bitcoin merchant processing. One certificate was generated locally on what appeared to be a HP-UX box, and another was generated on "8569985.securefastserver[.]com" with an email address "root@8569985.securefastserver[.]com", as seen here for their nethostnet[.]com domain. This certificate configuration is ignored by the malware.

```
Certificate chain
 0 s:/C=--
/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/CN=8569985.secu
refastserver.com/emailAddress=root@8569985.securefastserver.com
   i:/C=--
/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/CN=8569985.secu
refastserver.com/emailAddress=root@8569985.securefastserver.com
-----BEGIN CERTIFICATE-----
MIIEKjCCAxKgAwIBAgICAcQwDQYJKoZIhvcNAQELBQAwgckxCzAJBgNVBAYTAi0t
MRIwEAYDVQQIDAlTb21lU3RhdGUxETAPBgNVBAcMCFNvbWVDaXR5MRkwFwYDVQQK
```

In addition to other ip data, this data point suggested that Qhoster at https://www.qhoster[.]com was a VPS hosting reseller of choice at the time. It should be noted that the reseller accepted Alfa Click, PayPal, Payza, Neteller, Skrill, WebMoney, Perfect Money, Bitcoin, Litecoin, SolidTrust Pay, CashU, Ukash, OKPAY, EgoPay, paysafecard, Alipay, MG, Western Union, SOFORT Banking, QIWI, Bank transfer for payment.

Conclusion

Sofacy, one of the most active APT we monitor, continues to spearphish their way into targets, reportedly widely phishes for credentials, and infrequently participates in server side activity (including host compromise with BeEF deployment, for example). KSN visibility and detections suggests a shift from their early 2017 high volume NATO spearphish targeting towards the middle east and Central Asia, and finally moving their focus further east into late 2017. Their operational security is good. Their campaigns appear to have broken out into subsets of activity and malware involving GAMEFISH, Zebrocy, and SPLM, to name a few. Their evolving and modified SPLM/CHOPSTICK/XAgent code is a long-standing part of Sofacy activity, however much of it is changing. We'll cover more recent 2018 change in their targeting and the malware itself at SAS 2018.

With a group like Sofacy, once their attention is detected on a network, it is important to review logins and unusual administrator access on systems, thoroughly scan and sandbox incoming attachments, and maintain two factor authentication for services like email and vpn access. In order to identify their presence, not only can you gain valuable insight into their targeting from intelligence reports and gain powerful means of detections with hunting tools like YARA, but out-of-band processing with a solution like KATA is important.

Technical Appendix

Related md5

8f9f697aa6697acee70336f66f295837
1a4b9a6b321da199aa6d10180e889313
842454b48f5f800029946b1555fba7fc
d4a5d44184333442f5015699c2b8af28
1421419d1be31f1f9ea60e8ed87277db
b1d1a2c64474d2f6e7a5db71ccbafa31
953c7321c4959655fdd53302550ce02d
57601d717fcf358220340675f8d63c8a
02b79c468c38c4312429a499fa4f6c81
85cd38f9e2c9397a18013a8921841a04

f8e92d8b5488ea76c40601c8f1a08790
66b4fb539806ce27be184b6735584339
e8e1fcf757fe06be13bead43eaa1338c
953c7321c4959655fdd53302550ce02d
aa2aac4606405d61c7e53140d35d7671
85cd38f9e2c9397a18013a8921841a04
57601d717fcf358220340675f8d63c8a
16e1ca26bc66e30bfa52f8a08846613d
f8e92d8b5488ea76c40601c8f1a08790
b137c809e3bf11f2f5d867a6f4215f95
237e6dcbc6af50ef5f5211818522c463
88009adca35560810ec220544e4fb6aa
2163a33330ae5786d3e984db09b2d9d2
02b79c468c38c4312429a499fa4f6c81
842454b48f5f800029946b1555fba7fc
d4a5d44184333442f5015699c2b8af28
b88633376fbb144971dcb503f72fd192
8f9f697aa6697acee70336f66f295837
b6f77273cbde76896a36e32b0c0540e1
1a4b9a6b321da199aa6d10180e889313
1421419d1be31f1f9ea60e8ed87277db
1a4b9a6b321da199aa6d10180e889313
9b10685b774a783eabfecdb6119a8aa3
aa34fb2e5849bff4144a1c98a8158970
aced5525ba0d4f44ffd01c4db2730a34
b1d1a2c64474d2f6e7a5db71ccbafa31
b924ff83d9120d934bb49a7a2e3c4292
cdb58c2999eeda58a9d0c70f910d1195
d4a5d44184333442f5015699c2b8af28
d6f2bf2066e053e58fe8bcd39cb2e9ad
34dc9a69f33ba93e631cd5048d9f2624
1c6f8eba504f2f429abf362626545c79
139c9ac0776804714ebe8b8d35a04641
e228cd74103dc069663bb87d4f22d7d5
bed5bc0a8aae2662ea5d2484f80c1760
8c3f5f1fff999bc783062dd50357be79
5882a8dd4446abd137c05d2451b85fea
296c956fe429cedd1b64b78e66797122
82f06d7157dd28a75f1fbb47728aea25
9a975e0ddd32c0deef1318c485358b20
529424eae07677834a770aaa431e6c54
4cafde8fa7d9e67194d4edd4f2adb92b
f6b2ef4daf1b78802548d3e6d4de7ba7
ede5d82bb6775a9b1659dccb699fadcb
116d2fc1665ce7524826a624be0ded1c
20ff290b8393f006eaf4358f09f13e99
4b02dfdfd44df3c88b0ca8c2327843a4

c789ec7537e300411d523aef74407a5e
0b32e65caf653d77cab2a866ee2d9dbc
27faa10d1bec1a25f66e88645c695016
647edddf61954822ddb7ab3341f9a6c5
2f04b8eb993ca4a3d98607824a10acfb
9fe3a0fb3304d749aeed2c3e2e5787eb
62deab0e5d61d6bf9e0ba83d9e1d7e2b
86b607fe63c76b3d808f84969cb1a781
f62182cf0ab94b3c97b0261547dfc6cf
504182aaa5575bb38bf584839beb6d51
d79a21970cad03e22440ea66bd85931f

Related domains

nethostnet[.]com
hostsvcnet[.]com
etcrem[.]net
movieultimate[.]com
newfilmts[.]com
fastdataexchange[.]org
liveweatherview[.]com
analyticsbar[.]org
analyticstest[.]net
lifeofmentalservice[.]com
meteost[.]com
righttopregnantpower[.]com
kiteim[.]org
adobe-flash-updates[.]org
generalsecurityscan[.]com
globalresearching[.]org
lvueton[.]com
audiwheel[.]com
online-reggi[.]com
fsportal[.]net
netcorpscanprotect[.]com
mvband[.]net
mvtband[.]net
viters[.]org
treepastwillingmoment[.]com
sendmevideo[.]org
satellitedeluxpanorama[.]com
ppcodecs[.]com
encoder-info[.]tk
wmdmediacodecs[.]com
postlkwarn[.]com
shcserv[.]com
versiontask[.]com

webcdelivery[.]com
miropc[.]org
securityprotectingcorp[.]com
uniquecorpind[.]com
appexsrv[.]net
adobeupgradeflash[.]com

APT BACKDOOR CAMPAIGNS CYBER ESPIONAGE NATION STATE SPONSORED ESPIONAGE SOFACY TARGETED ATTACKS VULNERABILITIES AND EXPLOITS ZERO-DAY VULNERABILITIES

Related Posts

Zero-day vulnerability in Telegram

Gas is too expensive? Let's make it cheap!

Denis and Co.