DeepSight™ INTELLIGENCE

SOFACY/SEDNIT/APT28 GROUP IDENTIFIED IN ACTIVE CYBER ESPIONAGE AGAINST EUROPEAN GOVERNMENT ENTITIES

MANAGED ADVERSARY AND THREAT INTELLIGENCE

DEEPSIGHT™ INTELLIGENCE | INTELLIGENCE REPORT | SYMC - 300212 | V.1
23 JUN 2015 GMT

LEGAL NOTICE

SYMANTEC PROPRIETARY & CONFIDENTIAL - PERMITTED USE ONLY

Symantec assigns a high, medium, or low degree of confidence to assessments within its DeepSight™ Intelligence Portal Managed Adversary and Threat Intelligence (MATI) products. Confidence levels are determined against a three-point spectrum of source validity: variety and non-conflictive disparity of original sources, quality of source reporting, and reliability of source reporting. Confidence levels may be increased based on independent corroboration of information. High confidence generally suggests a solid judgment can be made, though such a judgment carries the risk of being wrong. Low confidence generally suggests tenuous inferences can be made, though information used to do so may have been questionable, fragmented, or singular.

Information Cut-Off Date: 21 Jun 2015 GMT

Sofacy/Sednit/APT28 Group Identified in Active Cyber Espionage against European Government Entities

DeepSight™ Intelligence | Intelligence Report | SYMC - 300212 | V.1 | 23 Jun 2015 GMT

KEY FINDINGS

A newly discovered cyber espionage campaign targeting multiple European government entities is ongoing as of the writing of this report.

The campaign has links to the network infrastructure used in prior Russia-based Sofacy/Sednit/APT28 group operations including the use of common domain names, name servers, and registrant information.

EXECUTIVE SUMMARY

In early June 2015, DeepSight Intelligence learned of a cyber espionage operation targeting multiple Europe-based government organizations. This operation used network infrastructure linked to prior activity by the Russia-based cyber espionage group known as Sofacy, Sednit, or APT28. DeepSight Intelligence believes the recent activity is a continuation of the group's late 2014 campaign focused on collecting intelligence from Europe-based government organizations.

DETAILS

A cyber espionage campaign was discovered in June 2015 targeting European government organizations. DeepSight Intelligence identified multiple connections between network infrastructure used in this operation and that used in prior Sofacy/Sednit/APT28 group cyber espionage operations. This current operation is most likely a continuation of the group's prior campaign against European government and diplomatic organizations.

Sofacy/Sednit/APT28 Connections

Two samples observed as part of the June 2015 operation create a mutex that was also created by a sample that communicates with at least two domains associated with previously reported Sofacy/Sednit/APT28 group activity. One of the group's domains shares a registrant email address with one of the domains previously identified with the group, further substantiating the association of this activity to the Sofacy/Sednit/APT28 group.

Two samples observed in the operation (MD5s: 09a0d08aae85a5e111a293a31dcb4b3c and 44fade31201739bb6caf71f63a727638) create the mutex, AZZYMutex. This mutex was also created by a previously observed sample (MD5: 260fe728ae06298c2c8ffda762262136) that connects to the three domains testservice24[.]net, updatepc[.]org, and updatesoftware24[.]com. These three domains have been linked to Sofacy/Sednit/APT28 group operations either directly through previous PricewaterhouseCooper reporting or through other characteristics. Figure 1 shows the relationship between the samples and the basis for associating these domains to the Sofacy/Sednit/APT28 group.

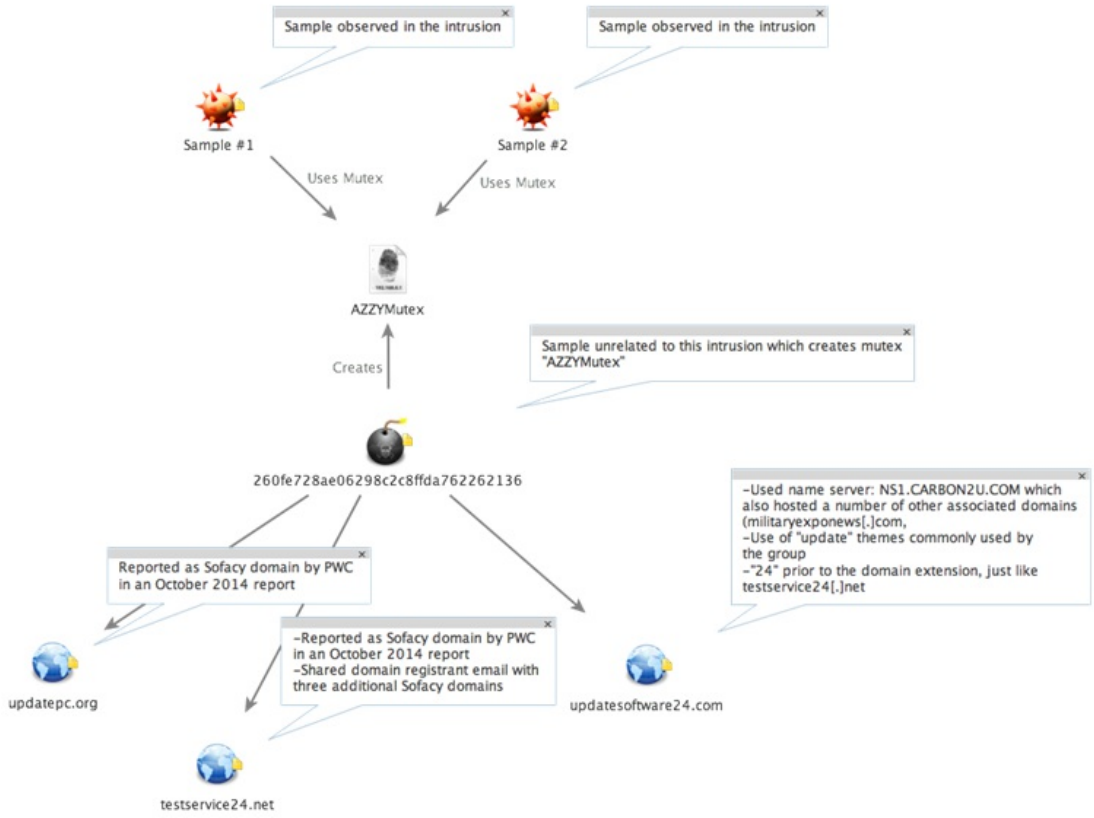

Figure 1: Relationship of two observed samples from European government operation and a sample that communicates with likely Sofacy/Sednit/APT28 group domains, Figure created by Symantec using Maltego®

The domain testservice24[.]net (see Figure 1) was established using the registrant email address lucas.ellery@yahoo[.]com. This email address was also used to register at least three other domains associated with Sofacy/Sednit/APT28 group activities in previous public reports. The three domains are counterterorexpo[.]com, baltichost[.]org, and yahoo-monitor[.]com.

Analysis of the domains associated with this activity revealed the same name server (NS) was also used by previously identified domains associated with the Sofacy/Sednit/APT28 group. While these name servers do not appear to be exclusively used for domains associated with this group's activity, the number of domains associated with the group hosted on the name server suggests that it is most likely used as part of the supporting infrastructure of Sofacy/Sednit/APT28 operations. Details of some of these relationships are detailed in Figure 2 below.

Name Server	Domains Observed	Previous Sofacy/Sednit/APT28 Group Domains
NS NS1.CARBON2U.COM	• driversupdate.info • microsofthelpcenter.infoupdatesoftware24.com	• militaryexponews.com • mfadaily.com • evrosatory.com • standartnevvs.com • sofexjordanx.com
admi180192.mercury.orderbox-dns.com	• updatepc.org	• google-settings.com • asisonlline.org
NS1.SERVICEPANTHER.COM	• testservice24.net • updatesoftware24.com • driversupdate.info	• scaninfo.info • checkmalware.org • baltichost.org

Figure 2: Domains observed in this operation that are linked to previous Sofacy/Sednit/APT28 by name server

Domains used by the malware as part of this operation also demonstrated prominent use of information technology (IT) themes including the names of known IT products and companies, such as Microsoft or Yahoo, or the use of the terms such as update, driver, helpcenter, or login.[1] This tactic has been noted in a body of public reporting on Sofacy/Sednit/APT28 operations but is not unique to the group. Domains associated with this activity with IT-related themes include microsofthelpcenter[.]info, updatepc[.]org, updatesoftware24[.]com, and driversupdate[.]info.

Analysis of an additional sample used in the operation revealed that it is crafted to connect to the domain apec.dnsfreestore[.]com. While this domain has not been explicitly linked to the Sofacy/Sednit/APT28 group, previous reporting has noted that this group has previously used Asia-Pacific Economic Cooperation (APEC)-themed Microsoft Excel lure documents.

[1] This tactic is generally used to convince the victim that they are communicating with or using a legitimate service.

OUTLOOK

European government targets will almost certainly continue to remain high-priority targets that fulfill the intelligence requirements of the Sofacy/Sednit/APT28 group. The group's targeting priorities have historically been aligned with nation state interests. DeepSight Intelligence believes with high probability that the group has the resources to establish the infrastructure and develop tools that will enable them to have continued success against these organizations.

TECHNICAL DETAILS

See the ***Metadata*** tab for additional technical details related to this report.

METADATA

CAMPAIGNS

Name	ID	Status
Sednit/Sofacy Espionage Targeting	CE.0015	Active

EXTRACTED INDICATORS

Indicator	Indicator Related CVE	Indicator Type
566ab945f61be016bfd9e83cc1b64f783b9b8deb891e6d504d3442bc8281b092		file_sha256
d38afc228e513439244fbf96997ff3b6		file_md5
7ea1f240bf75b19fbb03b5fa7edb69f9282651d8cf8278800b68d0657b5315d6		file_sha256
55da85d5e2520f0739f6f077dea6d0c8ad5804419df65d5c06dc638b0a36bb35		file_sha256
svehost.dll		file_name
800af1c9d341b846a856a1e686be6a3e		file_md5
566ab945f61be016bfd9e83cc1b64f783b9b8deb891e6d504d3442bc8281b092		file_sha256
7ea1f240bf75b19fbb03b5fa7edb69f9282651d8cf8278800b68d0657b5315d6		file_sha256
260fe728ae06298c2c8ffda762262136		file_md5
55da85d5e2520f0739f6f077dea6d0c8ad5804419df65d5c06dc638b0a36bb35		file_sha256
testservice24.net		domain
updatepc.org		domain
updatesoftware24.com		domain
http://testservice24.net/update/		url
http://updatepc.org/update/		url
http://updatesoftware24.com/update/		url
microsofthelpcenter.info		domain
driversupdate.info		domain
militaryexponews.com		domain
mfadaily.com		domain
evrosatory.com		domain
standartnevvs.com		domain
sofexjordanx.com		domain
google-settings.com		domain
asisonlline.org		domain
scaninfo.info		domain
checkmalware.org		domain

Indicator	Indicator Related CVE	Indicator Type
baltichost.org		domain

FILES

Detection Name	Name	MD5	SHA 256	Malicious
Trojan Horse	/users/emgent/desktop/sednit cyber espionage ru/sample/svehost.dll,svehost.dll	800af1c9d341b846a856a1e686be6a3e	566ab945f61be016bfd9e83cc1b64f783b9b8deb891e6d504d3442bc8281b092	y
Trojan.Sofacy		d38afc228e513439244fbf96997ff3b6	7ea1f240bf75b19fbb03b5fa7edb69f9282651d8cf8278800b68d0657b5315d6	y
Trojan.Gen		260fe728ae06298c2c8ffda762262136	55da85d5e2520f0739f6f077dea6d0c8ad5804419df65d5c06dc638b0a36bb35	y
Trojan Horse,Undetermined	/users/emgent/desktop/sednit cyber espionage ru/sample/svehost.dll,svehost.dll	800af1c9d341b846a856a1e686be6a3e	566ab945f61be016bfd9e83cc1b64f783b9b8deb891e6d504d3442bc8281b092	y
WS.Reputation.1,Trojan.Sofacy		d38afc228e513439244fbf96997ff3b6	7ea1f240bf75b19fbb03b5fa7edb69f9282651d8cf8278800b68d0657b5315d6	y
WS.Reputation.1,Trojan.Gen		260fe728ae06298c2c8ffda762262136	55da85d5e2520f0739f6f077dea6d0c8ad5804419df65d5c06dc638b0a36bb35	y

TARGET INDUSTRIES

NAICS Code	Name
92	Public Administration

SOURCE REGIONS

Region	Europe
Subregion	Eastern Europe
Countries	Russia

TARGET REGIONS

Region	Europe
Subregion	
Countries	

THREAT DOMAINS

Cyber Espionage