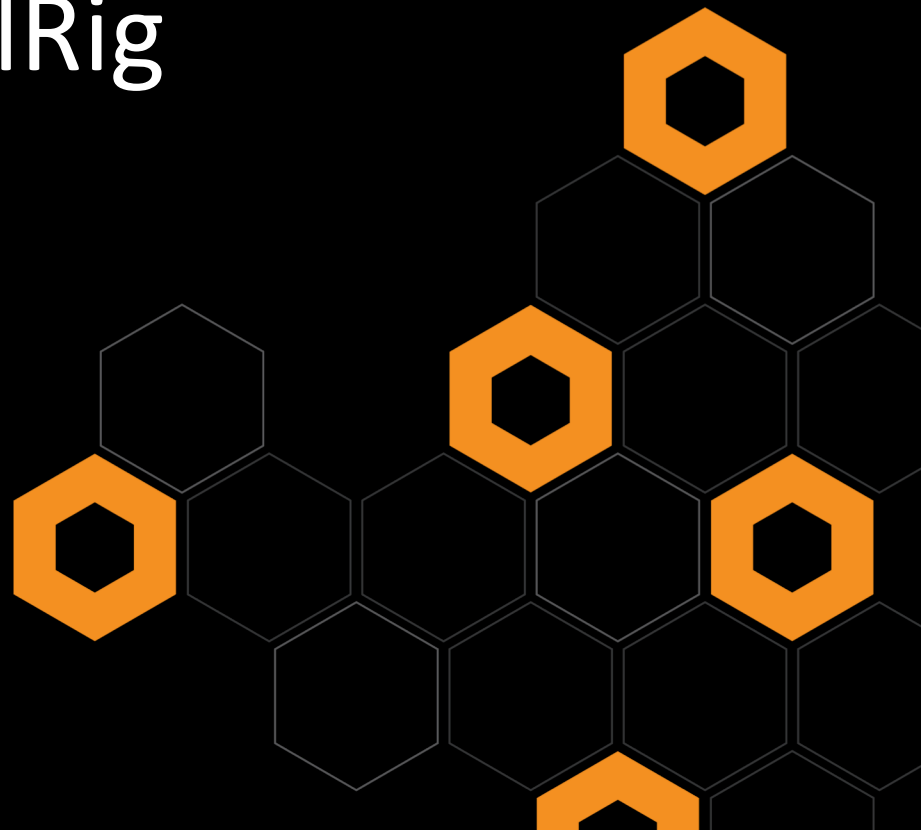


(Re)Building the OilRig Playbook

Mike Harbison, Threat Researcher
Palo Alto Networks



OARIG

ESPIONAGE ADVERSARY
BASED IN THE MIDDLE EAST



USES POPULAR
MULTISCANNERS FOR TESTING

LEVERAGES MALICIOUS
MACRO DOCUMENTS



EVIDENCE OF RELATIONSHIP TO
OTHER THREAT GROUPS

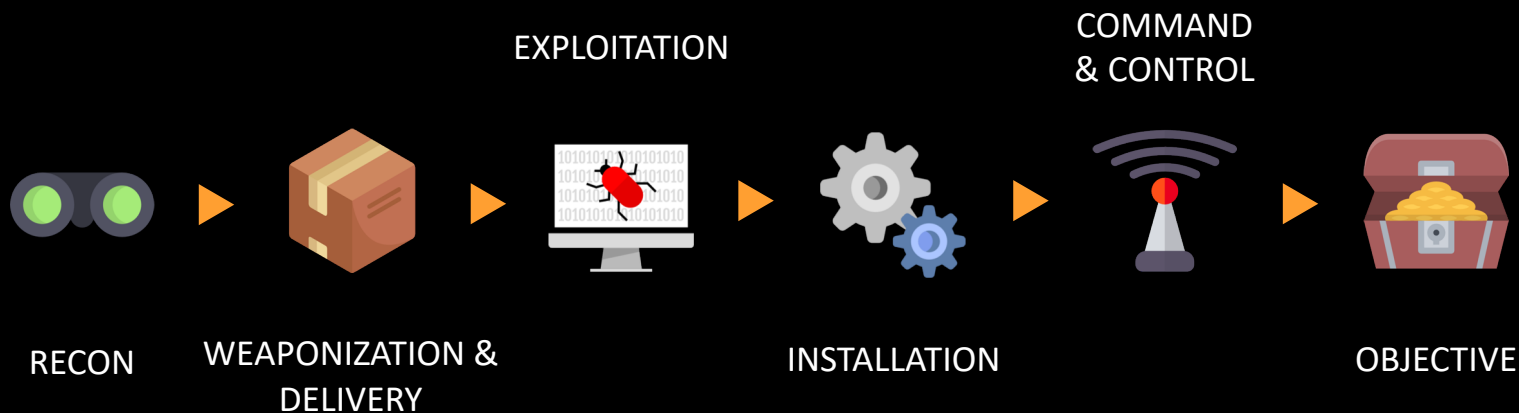
USES CUSTOM TOOLS



USES WEBSHELLS ON
COMPROMISED SERVERS



ATTACK LIFE CYCLE



ATT&CK™
Adversarial Tactics, Techniques
& Common Knowledge

STIX™

4 | © 2017, Palo Alto Networks. All Rights Reserved.

Deconstructing the Attack Life Cycle

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Command-Line Interface	Audio Capture	Automated Exfiltration	Commonly Used Port
AppCert DLLs	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Dynamic Data Exchange	Automated Collection	Data Compressed	Communication Through Removable Media
Applnit DLLs	AppCert DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Vulnerability	Execution through API	Browser Extensions	Data Encrypted	Connection Proxy
Application Shimming	Applnit DLLs	Code Signing	Credentials in Files	Network Service Scanning	Logon Scripts	Execution through Module Load	Clipboard Data	Data Transfer Size Limits	Custom Command and Control Protocol
Authentication Package	Application Shimming	Component Firmware	Exploitation of Vulnerability	Network Share Discovery	Pass the Hash	Graphical User Interface	Data Staged	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol

COM
& CC



2.0

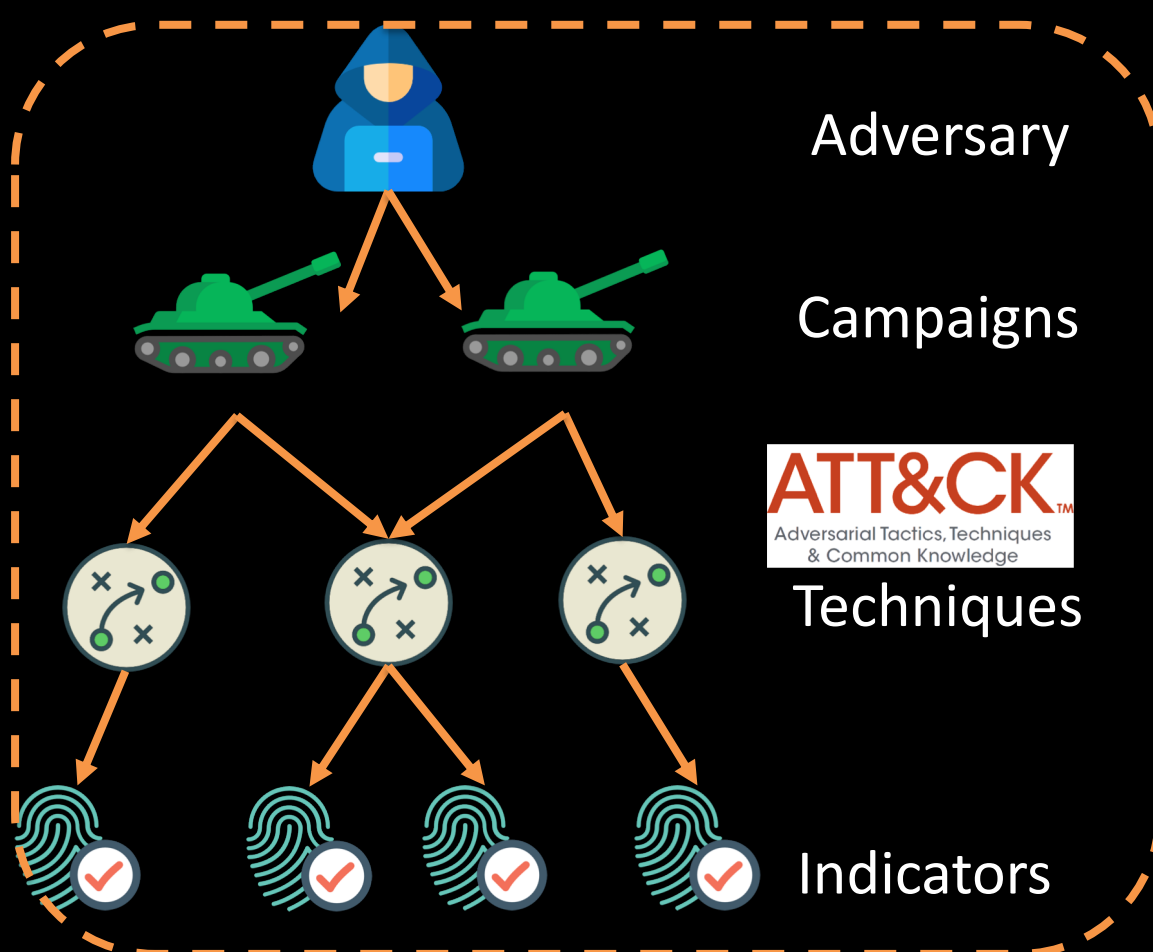


Indicates



Sighting-Of





ATT&CK[™]
 Adversarial Tactics, Techniques
 & Common Knowledge



UNIT 42 [0:38] 14-7 OILRIG

	FOSTER	JONES	FOSTER	HOPKIN
ZCP				
ASBP				

4 DOWN 2 [+20 +50 20] 2 QTR



OILRIG

'Nafti'

or

نفتی

Persian for
'petroleum' or 'oil'



Rob Falcone 🇺🇸 09:09

nice

نفتی (nafti)

thats translates to oil

boom

we could always use that in the campaign name



Bryan Lee 🇺🇸 09:12

OilRig is a cool name



Rob Falcone 🇺🇸 09:12

ooo

i kinda like that

OilRig Campaign



Bryan Lee 🇺🇸 09:12

yeah that's kinda fun

ATTACK TIMELINE



ASSOCIATED TOOLS

ENDPOINT



CLAYSLIDE



HELMINTH



ISMAGENT



ALMA Communicator

SERVER



TWOFACE



RGDOOR



CLAYSLIDE



XLS files containing
malicious macros
and decoy
documents



Delivered via spear
phishing



Uses filenames and
variables associated
with vendors

Scratch
Inbox - Outlook Data File - Outlook

FILE HOME SEND / RECEIVE FOLDER VIEW

Clean Up - Junk - Delete Reply Reply All Forward Meeting Move to: ? To Manager Team Email Done Reply & Delete Create New Move OneNote Unread/Read Categorize Follow Up Search People Address Book Filter Email

Search Current Mailbox (Ctrl-E) Current Mailbox

All Unread By Date Newest ↓

Older

Motty Thomas Important 6/18/2017
Hello dear colleague, please find the file attached, it's very

Reply Reply All Forward Sun 6/18/2017 4:42 AM

Motty Thomas <Motty.Thomas@emarattech.onmicrosoft.com>
Important

To Shahzad.Khurram

We removed extra line breaks from this message.

Message Important.xls (470 KB) how.png (18 KB) 2

Hello dear colleague, please find the file attached, it's very important. looking forward to your reply, thank you.

Note 1: Don't open in the browser, download the file and open in due to incompatibility of excel version, and if you see the incomparability message, please click on "Enable Content" as pictured, thank you.

See more about Motty Thomas.

ITEMS: 1 UNREAD: 1



HELMINTH



Dropped as both
script and PE
variants



Fully featured
backdoor allowing
for recon and
additional actions



Capable of using
DNS tunneling for C2

C:\USERS\PUBLIC\LIBRARIES\~WINDOWS\
C:\USERS\ADMINISTRATOR\APPDATA\ROAMING\MICROSOFT\INTERNET EXPLORER\USERS\
KRATOS
PLATO
JOHN-PC
ADMINISTRATOR
30
KERNEL.WS



ISMAGENT



Previously associated with the Greenbug group

DNS

Capable of using DNS tunneling for C2



Similarities with Helminth

```

Sub HideSheets()
  If ActiveWorkbook.Worksheets(1).Visible Then
    Dim WS_Count As Integer
    Dim i As Integer
    WS_Count = ActiveWorkbook.Worksheets.Count
    For i = 1 To WS_Count
      ActiveWorkbook.Worksheets(i).Visible = True
    Next i
    ActiveWorkbook.Worksheets(1).Visible = False
    ActiveWorkbook.Worksheets(2).Activate
  End If
End Sub

```

```

Sub InitEx()

```

```

Paltofp1 = "TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
Paltofp1 = Paltofp1 + "AAAAAAEAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1v"
Paltofp1 = Paltofp1 + "ZGUuDQ0KJAAAAAAAAAAAtSGbjaSkIsGkpCLBpKQiw3bX5sGUpCLDdtfuw5ykIsN21+rBwKQiw94nP"
Paltofp1 = Paltofp1 + "sGgpCLCMcAuxeikIsIxwDbFLKQiwjHAMSXgpCLBgUZuweCkIsGkpCbAHKQiw3ABsWgpCLCbCpew"
Paltofp1 = Paltofp1 + "aCkIsJtwCrFoKQiwUmljaGkpCLAAAAAAAAAFAFBFAABMAQUAEphZwQAAAAAAAAAAAA4AAcAQsBDgAA"
Paltofp1 = Paltofp1 + "pAEAAJ4AAAAAAAAACW0AAAAABAAAADAAQAAAEAAAABAAAAACAAAFAAEAAAAAAAAUAAQAAAAAAAAJACAAAE"
Paltofp1 = Paltofp1 + "AAAAAAAAAgBAGQAAEAAAQAAAAQAAAAQAAAAQAAAAQAAAAQAAAAQAAAAQAAAAQAAAAQAAAAQAAAAQAAAA"
Paltofp1 = Paltofp1 + "AAAAAAAAAAAAAAAAAAAAAAAAAAcAIA9BIAAJAcAgBwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
Paltofp1 = Paltofp1 + "AB0CAEAAAAAAAAAAAAAAAAAAAAAAQCMQAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
Paltofp1 = Paltofp1 + "owEAABAAAAcKAQAABAAAAAAAAAAAAAAAAAAAAAAATAAATAAATAAATAAATAAATAAATAAATAAATAAATAAATAAAT"
Paltofp1 = Paltofp1 + "AAAAAAAAAAAAAAAAEAAAEAuZGF0YQAAPLAAAAAAAAAAAAAAAAAAAAAAAgAAAAAAAAAAAAAAAAAAAAA"
Paltofp1 = Paltofp1 + "cmMAAADgAQAAAGACAAAPLAAAAAAAAAAAAAAAAAAAAAAQAAAAQC5yZWxvYwAA9BIAAAABwAgAAFAAA"
Paltofp1 = Paltofp1 + "ACYCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
Paltofp1 = Paltofp1 + "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
Paltofp1 = Paltofp1 + "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
Paltofp1 = Paltofp1 + "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
Paltofp1 = Paltofp1 + "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"

```

ISMAgent



ALMA COMMUNICATOR



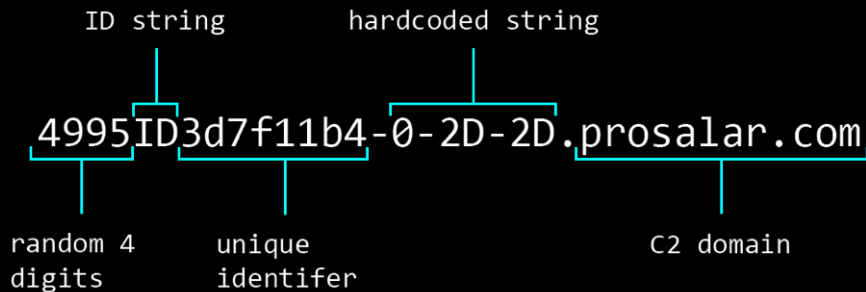
No internal
configuration

DNS

Limited DNS
tunneling for C2;
newer versions use
DNS and HTTP



Bundled with
Mimikatz tool

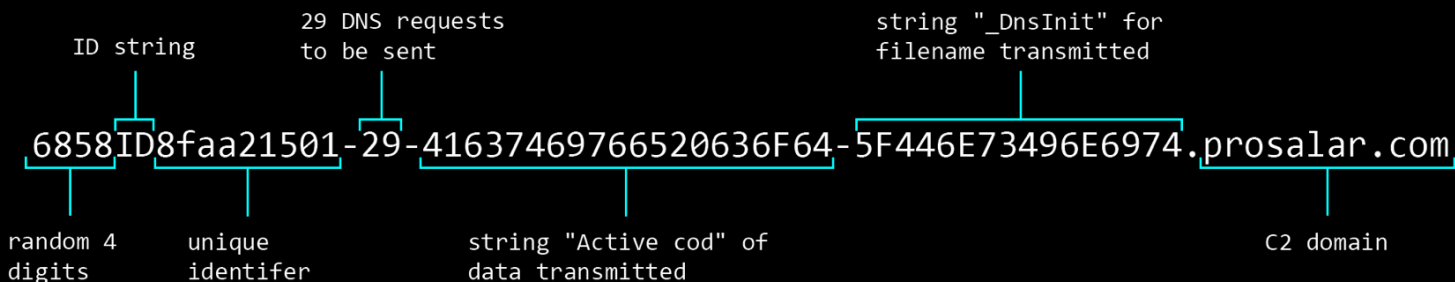


CHECK FOR COMMANDS

```
36.37.94.33 //START DATA
95.68.110.115 //_Dns
73.110.105.116 //Init
46.98.97.116 //.bat
...
```

4 BYTES RECEIVED
PER REQUEST

FILE CREATED AND
COMMANDS EXECUTED



10 BYTES SENT
PER REQUEST

MIMIKATZ TOOL (758,272 BYTES) TAKES 189,568 DNS REQUESTS TO DOWNLOAD



TWOFACE



Requires authentication to access additional features



Contains embedded secondary webshell



Discovered on multiple legitimate web servers



مجلس التعاون لدول الخليج العربية

الأمانة العامة - قواعد المعلومات البلدية

[خريطة الموقع | اتصل بنا | English](#)

- الرئيسية
- وزراء شؤون البلديات
- العمل البلدي
- المؤتمرات والاجتماعات
- الفرق واللجان
- المشاريع المتبعة

اجتماع اصحاب السمو والسعادة الوزراء المعنيين بشؤون البلديات



عقد أصحاب السمو والمعالى وزراء الشؤون البلدية بدول مجلس التعاون لدول الخليج العربية ظهر أمس اجتماعهم السادس عشر بفندق القورسيوزن بالرياض برئاسة صاحب السمو الملكي الأمير الدكتور منصور بن متعب بن عبدالعزيز وزير الشؤون البلدية والقروية الذي رحب في بداية الاجتماع بأصحاب السمو والمعالى مشيراً إلى أن هذا الاجتماع يأتي في إطار الأهداف التي قام عليها مجلس التعاون تحقيقاً للترباط والتكامل بين دول المجلس في ظل ما يسودها من علاقات أخوية وسمات مشتركة ووحدة في الهدف والحس المشترك، مستعرضاً ما يحتل به القطاع البلدي من دعم واهتمام من أصحاب الجلالة والسمو قادة دول المجلس إدراكاً منهم لأهمية هذا القطاع وأثره البالغ فيما تشهده دول المجلس من تطور ونماء ونهضة في شتى المجالات.

كما اتخذ الوزراء عدداً من القرارات والتوصيات ومنها:

- إقرار الإنظار العام للدليل الاسترشادي لإدارة النفايات البلدية الصلبة في دول المجلس
- إقرار الدليل الاسترشادي لمعايير تطوير المرافق الخدمية على الطرق السريعة

POST /NEWSPAGES/NEWS1.ASPX

Address: Current : C:\inetpub\wwwroot\shell\ Use Reset Form

Login: Do it : Do it

Command: Process : cmd.exe
Command : whoami Execute

Upload: File name : Browse...
Save as : Is virtual path
New File name : Upload

Download: File name : Download

Upload Base64: Base64 File :
File Path and Name : Is virtual path
Upload

Sql Server: Standard Connection Sample Trusted Connectin Sample
Connection String :
Query : Run

Change Creation Time: File name : Get
From This File : Set
New Time : Set

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
c:\windows\system32\inetrv>whoami
iis apppool\defaultappool

Location: C:\inetpub\wwwroot\2222.aspx

1	<input type="text" value="DarkShe11PasswordSet"/>
2	<input type="text" value="c:\windows\system32\cmd.exe"/> <input type="text" value="echo 'This is a command I ran!!'"/> <input type="button" value="Run"/>
3	<input type="text"/> <input type="button" value="Browse..."/> <input type="text"/> <input type="button" value="Upload"/>

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
c:\windows\system32\inetsrv>echo 'This is a command I ran!!'
'This is a command I ran!!'
c:\windows\system32\inetsrv>exit
```



RGDOOR



Fully functional IIS
module backdoor



Stealthier and
harder to detect
than webshell



Discovered on
multiple legitimate
web servers

Internet Information Services (IIS) Manager

WIN-NULVN97QTV7

File View Help

Connections

- Start Page
- WIN-NULVN97QTV7 (WIN-NULVN97QTV7)
- Application Pools
- Sites
 - Default Web Site

Modules

Use this feature to configure the native and managed code modules that process requests made to the Web server.

Group by: No Grouping

Name	Code	Module Type	Entry Type
FailedRequestsTraci...	%windir%\System32\inetsrv\iisfrec.dll	Native	Local
FileAuthorization	System.Web.Security.FileAuthorizationModule	Managed	Local
FormsAuthentication	System.Web.Security.FormsAuthenticationMo...	Managed	Local
HttpCacheModule	%windir%\System32\inetsrv\cachhttp.dll	Native	Local
HttpLoggingModule	%windir%\System32\inetsrv\loghttp.dll	Native	Local
HTTPParser	c:\windows\system32\inetsrv\HTTPParser.dll	Native	Local
IsapiFilterModule	%windir%\System32\inetsrv\filter.dll	Native	Local

Actions

- Add Managed Module...
- Configure Native Modules...
- Edit...
- Lock
- Remove
- View Ordered List...
- Help
- Online Help

```
POST / HTTP/1.1
Host: 192.168.45.5
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.13.0
Cookie: RGSESSIONID=54NzkwcCM80zU5PQ==
Content-Length: 0
```

```
HTTP/1.1 200 OK
Content-Type: text/plain
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Tue, 03 Oct 2017 19:14:26 GMT
Content-Length: 40
```

```
PT0ndDUkJCQ70zgIMDEyNSE4IDUKJCQ70zheVA==
```

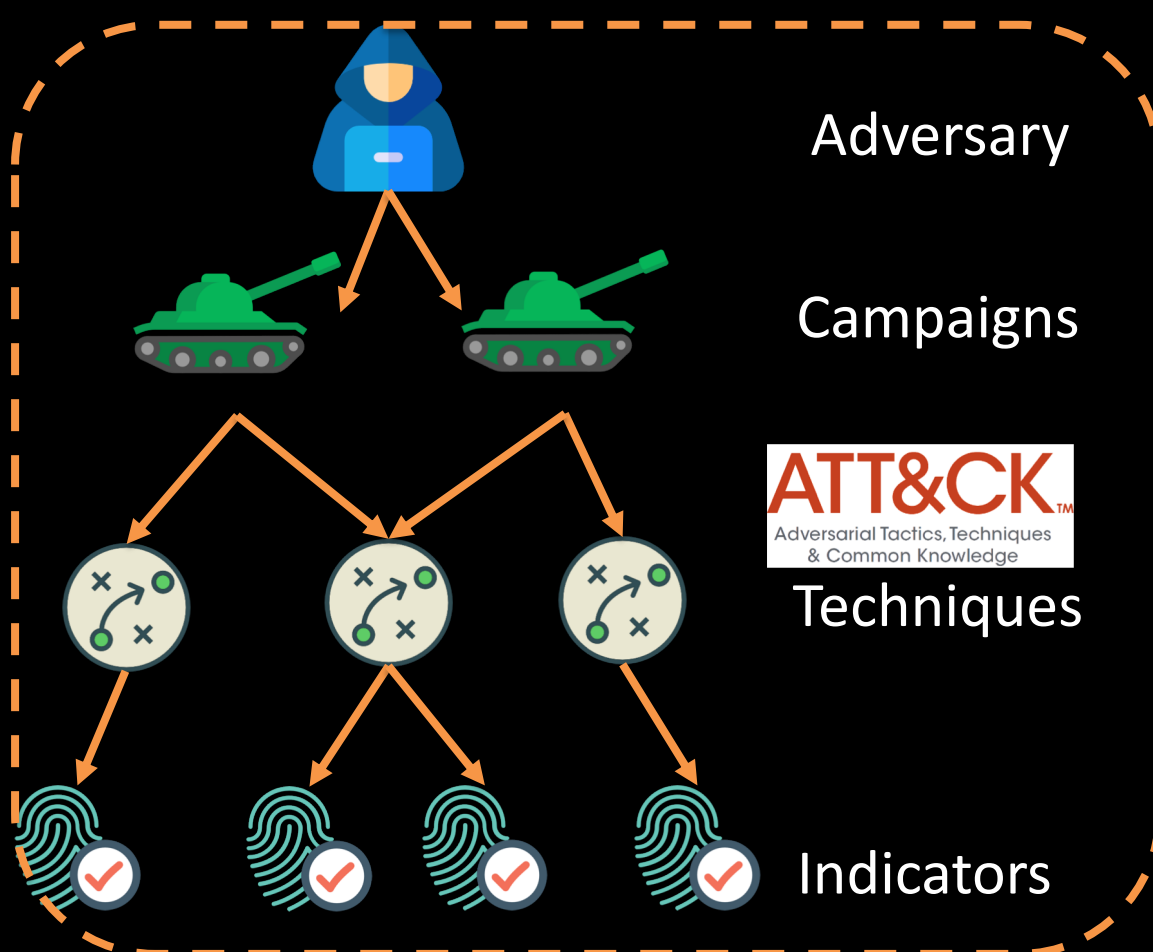
CMD\$WHOAMI

IIS APPPOOL\
DEFAULTAPPPOOL
\N\X00

32,195,532

ARCO end user systems





ATT&CK™
 Adversarial Tactics, Techniques
 & Common Knowledge



UNIT 42 [0:38] 14-7 OILRIG

	FOSTER	JONES	FOSTER	HOPKIN
ZCP				
ASBP				

4 DOWN 2 [+20] [+50] [20] 2 QTR

```
{-
type
id: '
spec
obje
{-
type
id: '
crea
modi
name
desc
vari
appe
thei
orga
engi
vuln
lack
test
exfi
late
acco
netw
comp
orga
publ
obje
"rep
"rep
"rep
"int
], -
labe
"int
]-
}, -
{-
type
id: '
create
```



t are in a
well. It also
ons to attack
of specific
social
tched
y suggest a
zed evasion
data
ials for
entials to
ems on the
to access the
s at targeted

PLAYBOOKS

OILRIG

OilRig is a threat group operating primarily in the Middle East by targeting organizations in this region that are in a variety of different industries; however, this group has occasionally targeted organizations outside of the Middle East as well. It also appears OilRig carries out supply chain attacks, where the threat group leverages the trust relationship between organizations to attack their primary targets.

OilRig is an active and organized threat group, which is evident based on their systematic targeting of specific organizations that appear to be carefully chosen for strategic purposes. Attacks attributed to this group primarily rely on social engineering to exploit the human rather than software vulnerabilities; however, on occasion this group has used recently patched vulnerabilities in the delivery phase of their attacks. The lack of software vulnerability exploitation does not necessarily suggest a lack of sophistication, as OilRig has shown maturity in other aspects of their operations. Such maturities involve:

-Organized evasion testing used during development of their tools.
 -Use of custom DNS Tunneling protocols for command and control (C2) and data exfiltration.

- July 2017 to August 2017
- May 2016 to August 2017
- May 2016 to September 2017
- January 2018 to January 2018

Published Playbooks

Intrusion Set: OilRig Campaigns: 4 Indicators: 134 Attack Patterns: 23

RECON	DELIVERY	EXPLOIT	INSTALL	COMMAND	OBJECTIVE
	Spear phishing messages with malicious attachments	Authorized user performs requested cyber action	Process Hollowing	Custom Command and Control Protocol	Permission Groups Discovery
			Scheduled Task	Standard Application Layer Protocol	Process Discovery
				Fallback Channels	

Techniques Used

PLAYBOOKS

OILRIG

OilRig is a threat group operating primarily in the Middle East by targeting organizations in this region that are in a variety of different industries; however, this group has occasionally targeted organizations outside of the Middle East as well. It also appears OilRig carries out supply chain attacks, where the threat group leverages the trust relationship between organizations to attack their primary targets.

OilRig is an active and organized threat group, which is evident based on their systematic targeting of specific organizations that appear to be carefully chosen for strategic purposes. Attacks attributed to this group primarily rely on social engineering to exploit the human rather than software vulnerabilities; however, on occasion this group has used recently patched vulnerabilities in the delivery phase of their attacks. The lack of software vulnerability exploitation does not necessarily suggest a lack of sophistication, as OilRig has shown maturity in other aspects of their operations. Such maturities involve:

- Organized evasion testing used during development of their tools.
- Use of custom DNS Tunneling protocols for command and control (C2) and data exfiltration.

- July 2017 to August 2017
- May 2016 to August 2017
- May 2016 to September 2017
- January 2018 to January 2018

View Multiple Campaigns

Intrusion Set: OilRig Campaigns: 4 Indicators: 134 Attack Patterns: 23

RECON	DELIVERY	EXPLOIT	INSTALL	COMMAND	OBJECTIVE
	Spear phishing messages with malicious attachments	Authorized user performs requested cyber action	Scheduled Task	Custom Command and Control Protocol	Permission Groups Discovery
				Standard Application Layer Protocol	Process Discovery
				Fallback Channels	Automated Collection

View Specific Indicators for Technique

PLAYBOOKS

OILRIG

OilRig is a threat group operating primarily in the Middle East by targeting organizations in this region that are in a variety of different industries; however, this group has occasionally targeted organizations outside of the Middle East as well. It also appears OilRig carries out supply chain attacks, where the threat group leverages the trust relationship between

July 2017 to August 2017

May 2016 to August 2017

Technique: Standard Application Layer Protocol REFERENCE ✕

Description	Indicator Pattern
Standard Application Layer Protocol	<code>["http-request-ext:request_method = 'get' AND http-request-ext:request_value LIKE '/sysupdate.aspx?req=' AND http-request-ext:request_value LIKE '%5Cbat&m=d'"]</code>

Intrusion Set: OilRig

Campaigns: 4

Indicators: 134

Attack Patterns: 23

RECON

DELIVERY

EXPLOIT

INSTALL

COMMAND

OBJECTIVE

Spear phishing messages with malicious

Authorized user performs requested cyber action

Scheduled Task

Custom Command and Control Protocol

Permission Groups Discovery

https://pan-unit42.github.io/playbook_viewer/



How should
people use
this?



Simulations/R
anges



Defense
Evaluations



Application
Framework