



Universidad del  
**Rosario**

Escuela de Ingeniería,  
Ciencia y Tecnología



**MACC**  
Matemáticas Aplicadas y  
Ciencias de la Computación



**HINNT**  
Hub de INNOvación  
y Transferencia

# INFORMATICA FORENSE

**Daniel Díaz-López**

Líder de Ciberseguridad - MACC  
Profesor principal de carrera

[danielo.diaz@urosario.edu.co](mailto:danielo.diaz@urosario.edu.co)



@MACC\_URosario



@MACC.URosario



macc\_u  
r

# Agenda

- i. ¿Qué es Informática Forense?
- ii. ¿Qué es Análisis de Malware?
- iii. Repositorios de malware
- iv. Tipos de firmas
- v. Técnicas de análisis de malware
- vi. Tipos de malware
- vii. Caso de uso -> Análisis de un malware

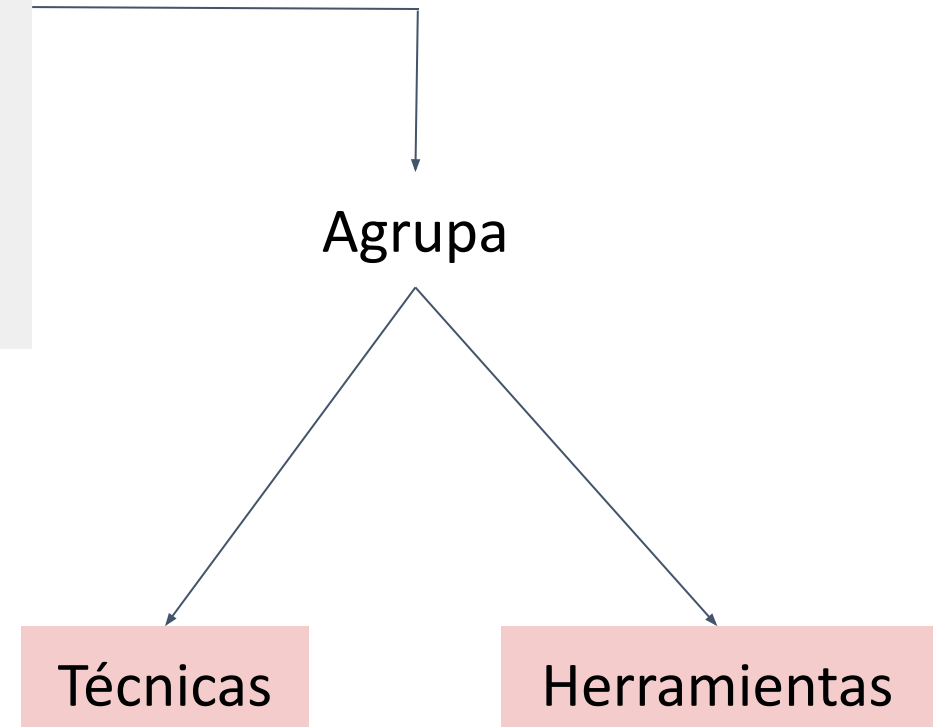
## ¿Qué es Informática Forense?

- Análisis de sistemas informáticos para encontrar evidencias que soporten una causa judicial, lo cual implica procesos de recopilación, análisis y presentación.
- Integra conceptos del derecho y de la informática con el propósito de que la evidencia sea admisible como prueba en un tribunal de justicia.
- Dentro de los posibles elementos de análisis en informática forense se encuentran: redes de comunicaciones cableadas e inalámbricas, dispositivos de almacenamiento, sistemas operativos, aplicativos, entre otros.

## ¿Qué es Análisis de Malware?

Es el arte de disecar malware para:

- Entender cómo funciona
- Entender cómo identificarlo
- Entender cómo defenderse
- Entender cómo eliminarlo



## Repositorios de malware

<https://github.com/ytisf/theZoo>

### 🔗 theZoo - A Live Malware Repository

contributions welcome hits 175687 Star 6.3k Made with Python



theZoo is a project created to make the possibility of malware analysis open and available to the public. Since we have found out that almost all versions of malware are very hard to come by in a way which will allow analysis, we have decided to gather all of them for you in an accessible and safe way. theZoo was born by Yuval tist Nativ and is now maintained by Shahak Shalev.

**theZoo is open and welcoming visitors!**

If you are about to interact with our community please make sure to read our `CODE-OF-CONDUCT.md` prior to doing so. If you plan to contribute, first - thank you. However, do make sure to follow the standards on `CONTRIBUTING.md`.

### Disclaimer

theZoo's purpose is to allow the study of malware and enable people who are interested in malware analysis (or maybe even as a part of their job) to have access to live malware, analyse the ways they operate, and maybe even enable advanced and savvy people to block specific malware within their own environment.

# Repositorios de malware

<https://bazaar.abuse.ch/browse/>

bazaar.abuse.ch/browse/ 🏠 ☆

**MALWARE** bazaar by ABUSE|™ 🔍 Browse 📁 Upload 🔗 API 📄 Export 📊 Statistics 📄 FAQ 🏠 About 👤 Login

## MalwareBazaar Database

You are browsing the malware sample database of MalwareBazaar. If you would like to contribute malware samples to the corpuse, you can do so through either using the [web upload](#) or the [API](#).

  
428  
Submissions (past 24 hours)

  
[ZLoader](#)  
Most seen malware family (past 24 hours)

  
247'661  
Malware samples in corpuse

Using the form below, you can search for malware samples by a hash (MD5, SHA256, SHA1), imphash, tlsh hash, ClamAV signature, tag or malware family.

## Browse Database

See search syntax see below, example: tag:TrickBot

Search

# Repositorios de malware

<https://vx-underground.org>

vx-underground.org/apts.html

```
u
88Nu. u. uL ..
'88888,o888c .@88b @88R
^8888 8888 'Y888k/"*P
8888 8888 Y888L
8888 8888 8888
8888 8888 `888N
.8888b.888P .u./"888&
^Y8888*" d888" Y888*"
`Y" ` "Y Y"
`Y" 'YP
"" 'Y"
`888*" "8888%
"" "YP'
.dwi `88E
4888~ J8%
^"===*"

archive | code | zines | papers | apt collection | samples | supporters | contact
```


▶ APT Papers

▼ APT samples

- ▶ APT1 | Comment Crew | [China's People's Liberation Army (PLA)]
- ▶ APT3 | Gothic Panda | [People's Republic of China]
- ▶ APT-C-23 | AridViper [Arab Republic of Egypt]
- ▶ APT28 | Fancy Bear | Sofacy Group | [Russian Federation]

# Repositorios de malware

<https://vx-underground.org/APTs/2010/2010.09.30%20-%20W32%20Stuxnet%20Dossier>



## W32.Stuxnet Dossier

Version 1.4 (February 2011)

Nicolas Falliere, Liam O Murchu, and Eric Chien

*While the bulk of the analysis is complete, Stuxnet is an incredibly large and complex threat. The authors expect to make revisions to this document shortly after release as new information is uncovered or may be publicly disclosed. This paper is the work of numerous individuals on the Symantec Security Response team over the last three months well beyond the cited authors. Without their assistance, this paper would not be possible.*

### Contents

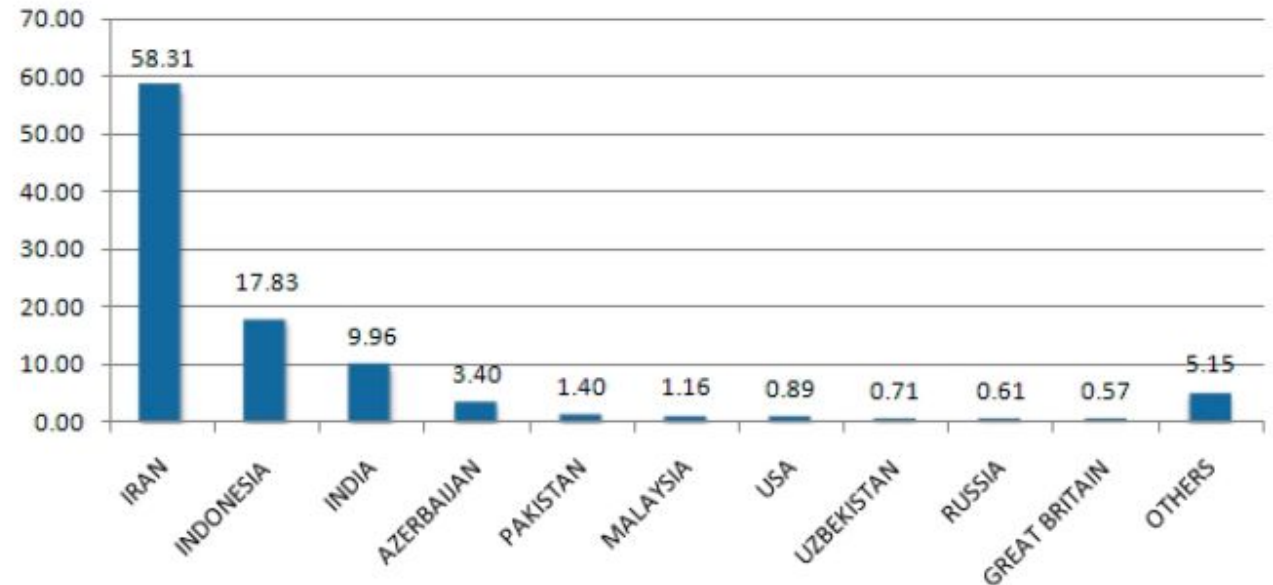
- Introduction ..... 1
- Executive Summary ..... 2
- Attack Scenario ..... 3
- Timeline ..... 4
- Infection Statistics ..... 5
- Stuxnet Architecture ..... 12
- Installation ..... 16
- Load Point ..... 20
- Command and Control ..... 21
- Windows Rootkit Functionality ..... 24
- Stuxnet Propagation Methods ..... 25
- Modifying PLCs ..... 36
- Payload Exports ..... 50
- Payload Resources ..... 51
- Variants ..... 53
- Summary ..... 55
- Appendix A ..... 56
- Appendix B ..... 58
- Appendix C ..... 59
- Revision History ..... 68

### Introduction

W32.Stuxnet has gained a lot of attention from researchers and media recently. There is good reason for this. Stuxnet is one of the most complex threats we have analyzed. In this paper we take a detailed look at Stuxnet and its various components and particularly focus on the final goal of Stuxnet, which is to reprogram industrial control systems. Stuxnet is a large, complex piece of malware with many different components and functionalities. We have already covered some of these components in our [blog series](#) on the topic. While some of the information from those blogs is included here, this paper is a more comprehensive and in-depth look at the threat.

Stuxnet is a threat that was primarily written to target an industrial control system or set of similar systems. Industrial control systems are used in gas pipelines and power plants. Its final goal is to reprogram

Figure 3  
Geographic Distribution of Infections



## Tipos de firmas

- **Antivirus signatures**
  - Identifican características propias del malware, no de la máquina víctima.
- **Host-based signatures**
  - Identifican elementos en el equipo víctima, por ejemplo: archivos creados, llaves de registro modificadas, etc.
- **Network Signatures**
  - Identifican aspectos relevantes en las comunicaciones provenientes o dirigidas hacia el equipo víctima.

## Técnicas de análisis de malware

| Técnica                    | Qué se inspecciona                                                                          | Producto obtenido                                                                                         | Herramientas utilizadas        |
|----------------------------|---------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|--------------------------------|
| Análisis estático básico   | Examina el archivo de manera superficial sin ejecutarlo.                                    | Identificación rápida de un archivo malicioso.<br>Información para producir firmas básicas.               | Hash calculator<br>Virus Total |
| Análisis dinámico básico   | Ejecuta el malware y observa su comportamiento básico.                                      | DLLs consumidas.<br>Librerías importadas y exportadas en tiempo de ejecución.<br>Nuevos archivos creados. | Sandbox (Cuckoo)               |
| Análisis estático avanzado | Realiza ingeniería inversa sobre el malware para analizar las instrucciones.                | Conocimiento de la funcionalidad y algoritmos de malware.                                                 | Disassembler (OllyDBG)         |
| Análisis dinámico avanzado | Ejecuta el malware con un <i>debugger</i> para analizar la rutina de ejecución paso a paso. | Conocimiento preciso del algoritmo del malware, revisando variables y comportamiento paso a paso.         | Debugger                       |

## Tipos de malware

- *Backdoor*: Puerta trasera, permite el acceso remoto a un sistema víctima con poca o ninguna autenticación.
- *Botnet*: Red de equipos bots controlados remotamente por un Servidor de Comando y Control.
- *Downloader*: Malware simple que permite descargar e instalar otros malwares.
- *Information-stealing malware*: Malware de espionaje.
- *Launcher*: Malware que ejecuta otro malware.

## Tipos de malware

- *Rootkit*: Malware que se oculta en archivos propios del sistema operativo
- *Scareware*: Malware que persuade a un usuario a comprar una supuesta solución de antivirus
- *Spam-sending malware*: Malware que envía mensajes de spam
- **Worm**: Malware que se auto propaga infectando otras máquinas
- **Virus**: Malware que requiere la actividad del usuario para propagarse

## Laboratorio: Caso de uso

1. Seleccionar un malware existente en uno de los repositorios existentes, por ejemplo <https://github.com/ytisf/theZoo/blob/master/malware/Binaries/Ransomware.WannaCry/Ransomware.WannaCry.zip>
1. En el caso de que sea un malware descargado de **theZoo**, realizar la descompresión del malware con el password: infected
2. Subir el malware a VirusTotal: <https://www.virustotal.com/gui/>
  - Seleccionar un malware que tenga un score de al menos 50/70, lo que indica que es un malware conocido y previamente analizado por VirusTotal
3. Identificar en el reporte de VirusTotal los siguientes elementos e identificar para cada uno si a partir del mismo puede extraerse una firma de tipo: *antivirus*, *host-based* o *network*:
  - Hashes
  - Strings
  - Secciones
  - URLs contactadas
  - Registry actions
  - Process and services actions
4. ¿Cuáles son las desventajas de un antivirus?
5. ¿Cuál cree que sería el reporte de VirusTotal si el malware subido fuera completamente nuevo?



Universidad del  
**Rosario**



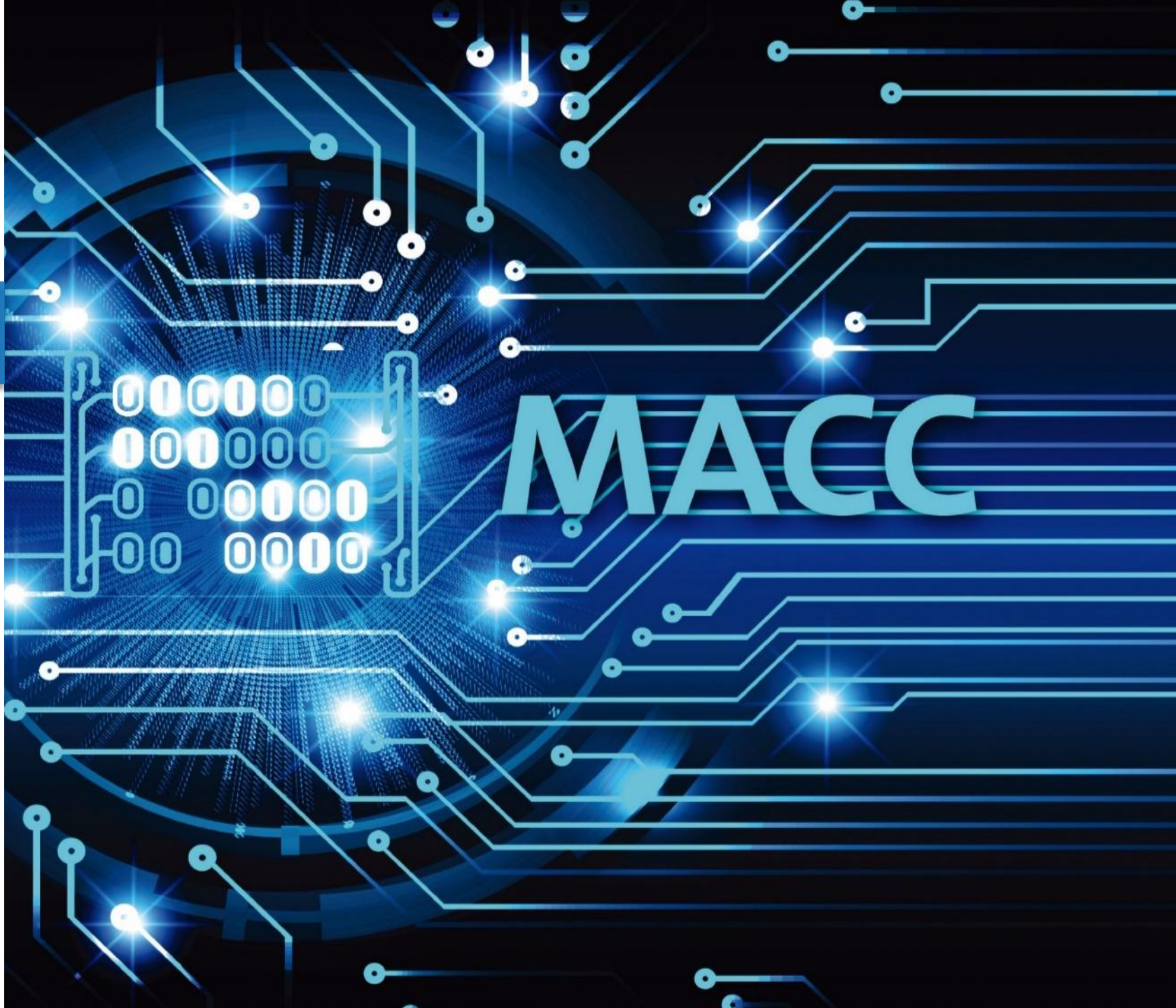
**MACC**  
Matemáticas Aplicadas y  
Ciencias de la Computación

## Malware Threats

### Hacking Ético

**Daniel Orlando Díaz López, PhD**

Profesor principal  
Departamento MACC  
Universidad del Rosario  
[danielo.diaz@urosario.edu.co](mailto:danielo.diaz@urosario.edu.co)

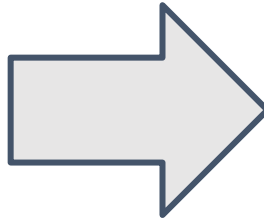


## ¿Que es el malware?

Software **malicioso** que daña sistemas de cómputo y otorga **control** (parcial o total) al creador del malware para propósitos de **robo o fraude**

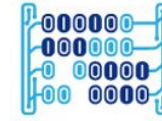
## ¿Cuales son los tipos de malware?

- Troyanos
- Virus
- Gusanos
- Rootkits
- Backdoors
- Botnets
- Ransomware
- Spyware
- Adware
- Scareware
- Crapware
- Crypters
- Keyloggers
- etc.



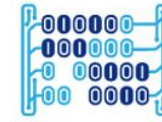
## ¿Que impactos tiene el malware?

- Robo de información personal
- Afectar el desempeño de un sistema
- Causar fallas en el hardware
- Borrar información valiosa
- Habilitar zombies para atacar a otros equipos
- Enviar mensajes de spam
- etc.



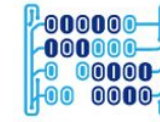
## ¿Cómo se distribuye el malware?

- Aplicaciones de mensajería
- Discos duros portables / USBs
- Vulnerabilidades en navegadores
- Servidores no parchados
- Software descargado de fuentes no fiables
- Descargas de internet no controladas
- Archivos adjuntos
- Redes físicas (ethernet) inseguras
- Servicios de compartición de archivos (Ftp, SMB)
- Instalación de malware por otro malware
- Redes inalámbricas inseguras



## ¿Cuales son las técnicas de distribución de malware?

- Blackhat Search Engine Optimization (SEO)
- Social engineered click jacking
- Phishing sites
- Malvertising
- Compromise legitimate websites
- Drive-by downloads
- Spam emails

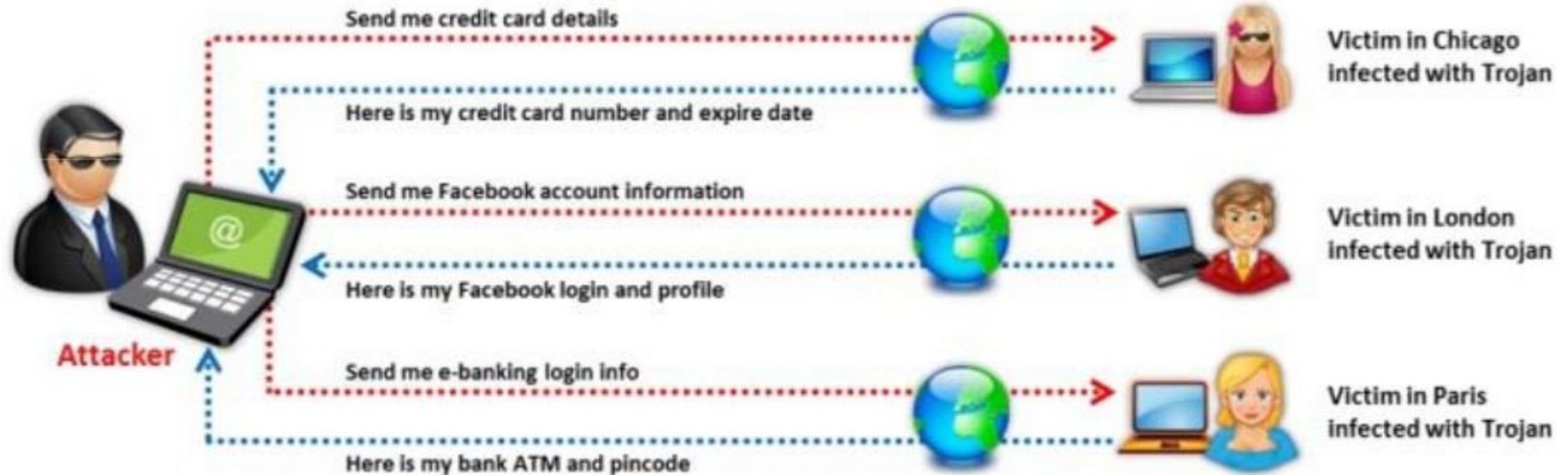


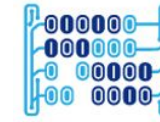
## Trojanos

- Software malicioso contenido **dentro de** un software aparentemente inofensivo
- El software malicioso puede servir para tomar control del equipo víctima o causar daño
- Síntomas de afectación de un troyano son:
  - Comportamiento anormal del sistema
  - Actividades de red inusuales, e.g. deshabilitación del antivirus, redirección a páginas desconocidas
  - Mas
  - Mas
  - Mas
- Los troyanos crean un canal de comunicación encubierto (***Covert channel***) entre el computador víctima y la máquina atacante
- El troyano recibe órdenes del computador atacante, al cual se le llama técnicamente: Servidor de Comando y Control (***CCC - Command Control Center***)



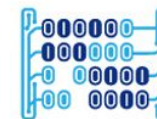
## Extracción de información de víctimas por medio de troyanos





## ¿Cómo se comunica un Troyano?

- Los troyanos utilizan un canal de comunicación encubierto (Covert channel), que es lo opuesto a un canal de comunicación abierto (Overt channel)
- La técnica utilizada para crear canales encubiertos es el **Tunneling**, que es la transmisión de un protocolo dentro de otro
- Los puertos de un computador tienen diferentes estados (*Open, Listen, Time\_wait, Established, etc.*) sin embargo los más sospechosos de estar asociados a un troyano son los puertos en estado **LISTEN** o **LISTENING**
- El estado LISTEN o LISTENING indica que el puerto está escuchando atento por alguna conexión entrante
- Algunos troyanos utilizan 2 puertos:
  - Uno para escuchar las órdenes del servidor de comando y control
  - Otro para las transferencias de datos



## Ejemplos de puertos usados por Troyanos

| Port    | Trojan                                                          | Port    | Trojan                   | Port         | Trojan                       | Port     | Trojan                    |
|---------|-----------------------------------------------------------------|---------|--------------------------|--------------|------------------------------|----------|---------------------------|
| 2       | Death                                                           | 1492    | FTP99CMP                 | 5569         | Robo-Hack                    | 21544    | GirlFriend 1.0, Beta-1.35 |
| 20      | Senna Spy                                                       | 1600    | Shivka-Burka             | 6670-71      | DeepThroat                   | 22222    | Prosiak                   |
| 21      | Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash | 1807    | SpySender                | 6969         | GateCrasher, Priority        | 23456    | Evil FTP, Ugly FTP        |
| 22      | Shaft                                                           | 1981    | Shockrave                | 7000         | Remote Grab                  | 26274    | Delta                     |
| 23      | Tiny Telnet Server                                              | 1999    | BackDoor 1.00-1.03       | 7300-08      | NetMonitor                   | 30100-02 | NetSphere 1.27a           |
| 25      | Antigen, Email Password Sender, Terminator, WinPC, WinSpy,      | 2001    | Trojan Cow               | 7789         | ICKiller                     | 31337-38 | Back Orifice, DeepBO      |
| 31      | Hackers Paradise                                                | 2023    | Ripper                   | 8787         | BackOfrice 2000              | 31339    | NetSpy DK                 |
| 80      | Executor                                                        | 2115    | Bugs                     | 9872-9875    | Portal of Doom               | 31666    | BOWhack                   |
| 421     | TCP Wrappers trojan                                             | 2140    | The Invasor              | 9989         | iNi-Killer                   | 33333    | Prosiak                   |
| 456     | Hackers Paradise                                                | 2155    | Illusion Mailer, Nirvana | 10607        | Coma 1.0.9                   | 34324    | BigGluck, TN              |
| 555     | Ini-Killer, Phase Zero, Stealth Spy                             | 3129    | Masters Paradise         | 11000        | Senna Spy                    | 40412    | The Spy                   |
| 666     | Satanz Backdoor                                                 | 3150    | The Invasor              | 11223        | Progenic trojan              | 40421-26 | Masters Paradise          |
| 1001    | Silencer, WebEx                                                 | 4092    | WinCrash                 |              |                              | 47262    | Delta                     |
| 1011    | Doly Trojan                                                     | 4567    | File Nail 1              | 12223        | Hack'99 KeyLogger            | 50505    | Sockets de Troie          |
| 1095-98 | RAT                                                             | 4590    | ICQTrojan                | 12345-46     | GabanBus, NetBus             | 50766    | Fore                      |
| 1170    | Psyber Stream Server, Voice                                     | 5000    | Bubbel                   | 12361, 12362 | Whack-a-mole                 | 53001    | Remote Windows Shutdown   |
| 1234    | Ultors Trojan                                                   | 5001    | Sockets de Troie         | 16969        | Priority                     | 54321    | SchoolBus .69-1.11        |
| 1243    | SubSeven 1.0 – 1.8                                              | 5321    | Firehotcker              | 20001        | Millennium                   | 61466    | Telecommando              |
| 1245    | VooDoo Doll                                                     | 5400-02 | Blade Runner             | 20034        | NetBus 2.0, Beta-NetBus 2.01 | 65000    | Devil                     |

[Commonly used ports - Enterprise - MITRE attack](#)

[Trojan Ports - Clearpath security](#)

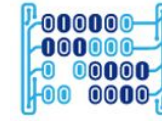
## ¿Como se hace la infección de un troyano?

1. Crear el “Payload” del troyano utilizando un “Trojan Horse Construction Kit”
2. Crear un “Dropper” que implante el *payload* del punto anterior
3. Crear un “Wrapper” que instale el *Dropper*
4. Lograr que el *Wrapper* llegue a la víctima
5. Ejecutar el *Dropper*
6. Ejecutar el *Payload*

“DarkHorse Trojan Virus Maker”  
Senna Spy Trojan Generator  
Batch Trojan Generator  
Umbra Loader

*petite.exe*, *graffiti.exe*, IExpress  
Wizard, Elite Wrap

Aplicaciones de mensajería, discos duros portables / USBs, software descargado de fuentes no fiables, descargas de internet no controladas, archivos adjuntos, servicios de compartición de archivos (Ftp, SMB), etc.



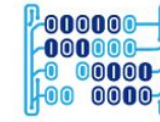
Quasar es un troyano para tomar control remoto de máquinas víctimas de sistema operativo Windows (Windows XP SP3, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2012, Windows 8/8.1, Windows 10), el cual cuenta con las siguientes funcionalidades:

- Compressed (QuickLZ) & Encrypted (TLS) communication
- No-Ip.com Support
- Visit Website (hidden & visible)
- Show Messagebox
- Task Manager
- File Manager
- Startup Manager
- Remote Desktop
- Remote Shell
- Download & Execute
- Upload & Execute
- System Information
- Computer Commands (Restart, Shutdown, Standby)
- Keylogger (Unicode Support)
- Reverse Proxy (SOCKS5)
- Password Recovery (Common Browsers and FTP Clients)
- Registry Editor

Mas información:

<https://github.com/quasar/QuasarRAT>

# Despliegue de Quasar RAT



1. Desplegar 2 máquinas virtuales Windows 10 en Microsoft Azure, ambas máquinas tienen que estar en la misma ubicación (e.g. East US), misma red virtual (e.g. HEvnet969) y estar en el mismo segmento de red (e.g. 10.0.1.0/24) y permitir el acceso por RDP remotamente:

## Máquina Atacante

Conectar ▶ Iniciar ▶ Reiniciar ■ Detener 📷 Captura 🗑️ Eliminar ↻ Actualizar

Grupo de recursos [\(cambiar\)](#)  
HE

Estado  
En ejecución

Ubicación  
East US

Suscripción [\(cambiar\)](#)  
Azure para estudiantes

Id. de suscripción  
dd5d31d9-0ebe-4b98-acd5-08373056d6da

Nombre del equipo  
HE1001

Sistema operativo  
Windows (Windows 10 Pro N)

Tamaño  
Estándar D2 (2 vcpu, 7 GiB de memoria)

Disco de SO efímero  
N/D

Dirección IP pública  
40.112.59.191

Dirección IP privada  
10.0.1.4

Red virtual/subred  
HEvnet969/default

Nombre DNS  
[Configurar](#)

## Máquina Víctima

Conectar ▶ Iniciar ▶ Reiniciar ■ Detener 📷 Captura 🗑️ Eliminar ↻ Actualizar

Grupo de recursos [\(cambiar\)](#)  
HE

Estado  
En ejecución

Ubicación  
East US

Suscripción [\(cambiar\)](#)  
Azure para estudiantes

Id. de suscripción  
dd5d31d9-0ebe-4b98-acd5-08373056d6da

Nombre del equipo  
victima1

Sistema operativo  
Windows (Windows 10 Pro)

Tamaño  
B1s estándar (1 vcpu, 1 GiB de memoria)

Disco de SO efímero  
N/D

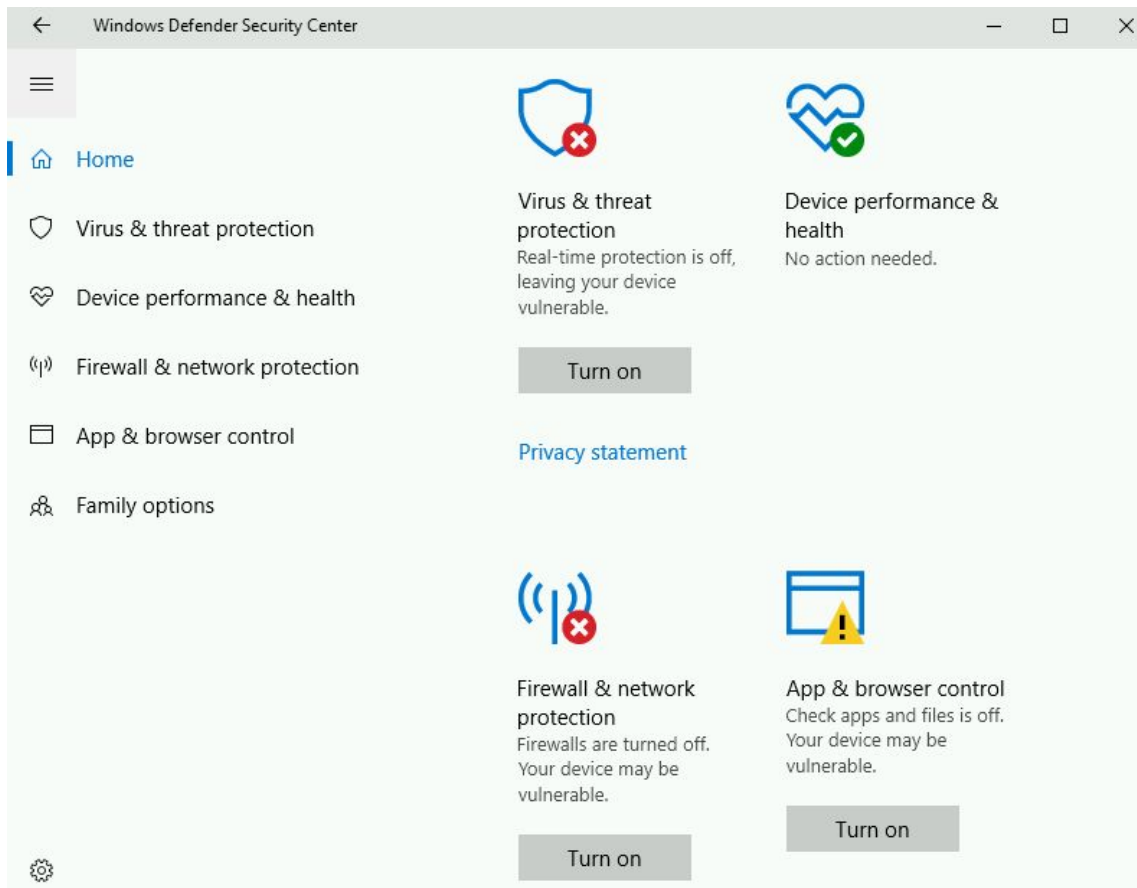
Dirección IP pública  
40.117.103.174

Dirección IP privada  
10.0.1.5

Red virtual/subred  
HEvnet969/default

Nombre DNS  
[Configurar](#)

2. Deshabilitar las funciones de seguridad de ambas máquinas virtuales.
  - a. En Windows Defender Security Center: Apagar todas las características de “Virus & Threat protection”, “Firewall & network protection” y “App & Browser control”
  - b. En Windows Defender Firewall: Apagar “Private networks” y “Guest or Public Networks”



3. Validar conectividad entre ambas máquinas virtuales con un ping sostenido (argumento -t) entre ambas máquinas:

```
C:\Users\dodiazlopez>ping 10.0.1.5 -t

Pinging 10.0.1.5 with 32 bytes of data:
Reply from 10.0.1.5: bytes=32 time=2ms TTL=128
Reply from 10.0.1.5: bytes=32 time=2ms TTL=128
Reply from 10.0.1.5: bytes=32 time=2ms TTL=128
Reply from 10.0.1.5: bytes=32 time=1ms TTL=128
Reply from 10.0.1.5: bytes=32 time=1ms TTL=128
Reply from 10.0.1.5: bytes=32 time=2ms TTL=128
Reply from 10.0.1.5: bytes=32 time=1ms TTL=128
Reply from 10.0.1.5: bytes=32 time=1ms TTL=128
```

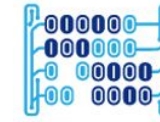
```
C:\Users\dodiazlopez>ping 10.0.1.4 -t

Pinging 10.0.1.4 with 32 bytes of data:
Reply from 10.0.1.4: bytes=32 time=2ms TTL=128
Reply from 10.0.1.4: bytes=32 time=2ms TTL=128
Reply from 10.0.1.4: bytes=32 time=2ms TTL=128
Reply from 10.0.1.4: bytes=32 time=1ms TTL=128
Reply from 10.0.1.4: bytes=32 time=2ms TTL=128
Reply from 10.0.1.4: bytes=32 time=2ms TTL=128
Reply from 10.0.1.4: bytes=32 time=2ms TTL=128
Reply from 10.0.1.4: bytes=32 time=2ms TTL=128
```

# Despliegue de Quasar RAT



Universidad del  
**Rosario**



**MACC**  
Matemáticas Aplicadas y  
Ciencias de la Computación

- Desde la máquina atacante descargar la versión compilada (v1.3.0.0) de Quasar del link:  
<https://github.com/quasar/QuasarRAT/releases>

**Dangerous** | github.com/quasar/QuasarRAT/releases

quasar / **QuasarRAT** Watch 324 Star 2,620

[Code](#) [Issues 116](#) [Pull requests 11](#) [Wiki](#) [Security](#) [Insights](#)

**Releases** [Tags](#)

**Latest release**

v1.3.0.0  
2564b2f

## Quasar v1.3.0.0

MaxXor released this on Sep 28, 2016 · 71 commits to master since this release

### Changelog

- Added Registry Editor
- Added Remote Webcam
- Added Windows DPI scaling support
- Added IPv6 support
- Added ability to elevate Client
- Added full Unicode support
- Added Remote TCP Connections Viewer
- Added option to hide sub directory of installation path
- Improved cryptography

### Quasar.v1.3.0.0.zip

SHA-256 checksum: 30a4ec904324aab10b9f771279

### Assets 3

[Quasar.v1.3.0.0.zip](#)

[Source code \(zip\)](#)

[Source code \(tar.gz\)](#)

5. Configurar Quasar para crear un RAT con el nombre de una aplicación de usuario con la cual usted considere podría engañar a un usuario. Configure las siguientes secciones: Basic, Connection, Installation, Assembly y Surveillance.

The screenshot shows the 'Client Builder' application window with the 'Basic Settings' tab selected. The left sidebar contains a list of settings categories: Basic Settings, Connection Settings, Installation Settings, Assembly Settings, and Surveillance Settings. The main content area is titled 'Client Identification' and includes the following fields and options:

- Client Tag:** A text input field containing 'Office04'.
- Process Mutex:** A section with the text 'A unique mutex ensures that only one instance of the client is running on the same system.' Below it is a text input field containing 'QSR\_MUTEX\_cbWJbf7EYnOqckzloJ' and a 'Random Mutex' button.

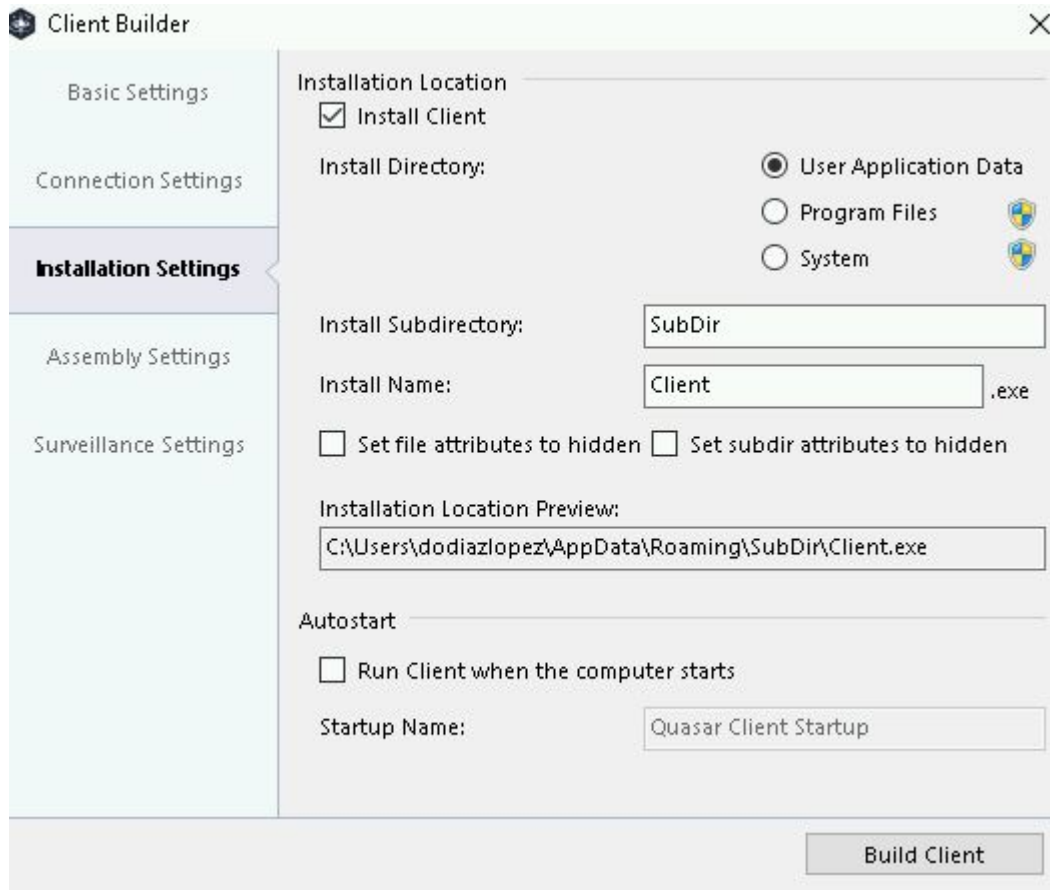
A 'Build Client' button is located at the bottom right of the window.

The screenshot shows the 'Client Builder' application window with the 'Connection Settings' tab selected. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Connection Hosts' and includes the following fields and options:

- IP/Hostname:** A text input field.
- Port:** A spinner control set to '4782'.
- Add Host:** A button to add a new connection host.
- Encrypted Connection:** A section with the text 'Don't forget to set the same password in the server settings.' Below it is a password input field with masked characters '....' and a 'Show Password' checkbox.
- Reconnect Delay:** A section with the text 'Time to wait between reconnect tries:' and a spinner control set to '3000' ms.

A 'Build Client' button is located at the bottom right of the window.

5. Configurar Quasar para crear un RAT con el nombre de una aplicación de usuario con la cual usted considere podría engañar a un usuario. Configure las siguientes secciones: Basic, Connection, Installation, Assembly y Surveillance.



Client Builder

Basic Settings

Connection Settings

**Installation Settings**

Assembly Settings

Surveillance Settings

Installation Location

Install Client

Install Directory:  User Application Data  Program Files  System

Install Subdirectory:

Install Name:  .exe

Set file attributes to hidden  Set subdir attributes to hidden

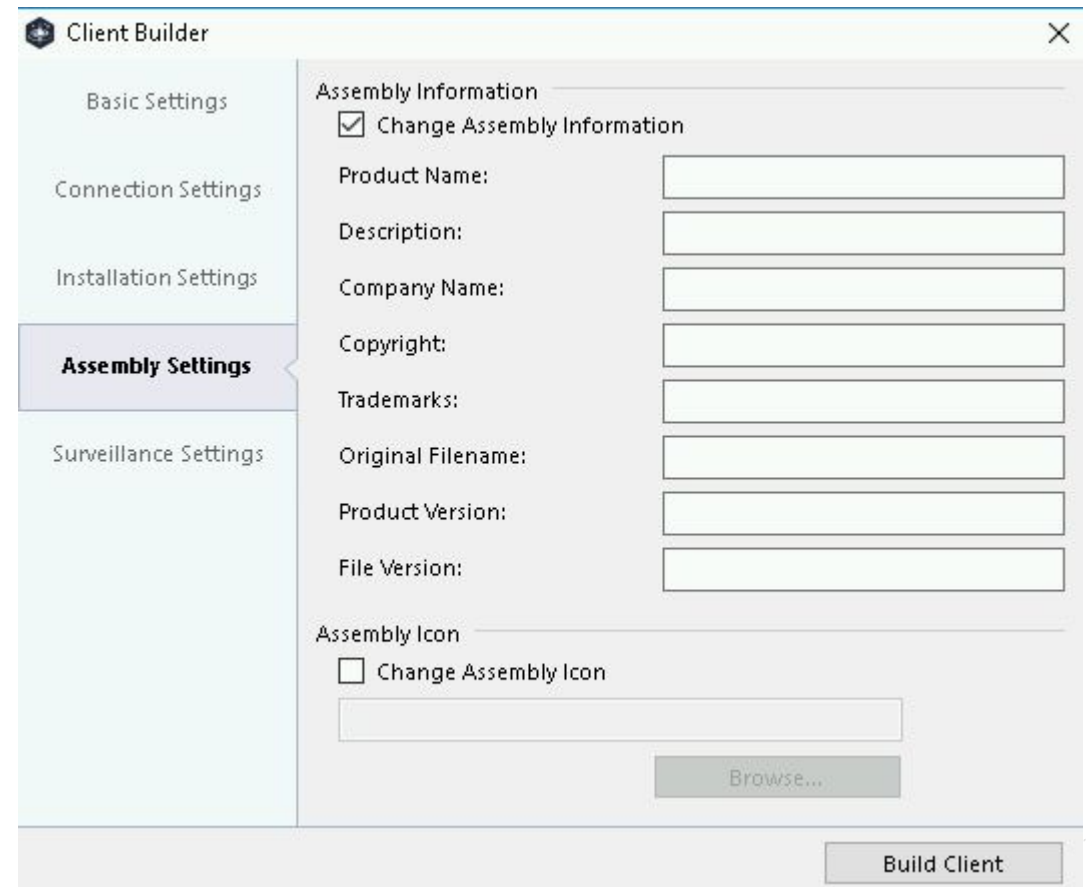
Installation Location Preview:

Autostart

Run Client when the computer starts

Startup Name:

Build Client



Client Builder

Basic Settings

Connection Settings

Installation Settings

**Assembly Settings**

Surveillance Settings

Assembly Information

Change Assembly Information

Product Name:

Description:

Company Name:

Copyright:

Trademarks:

Original Filename:

Product Version:

File Version:

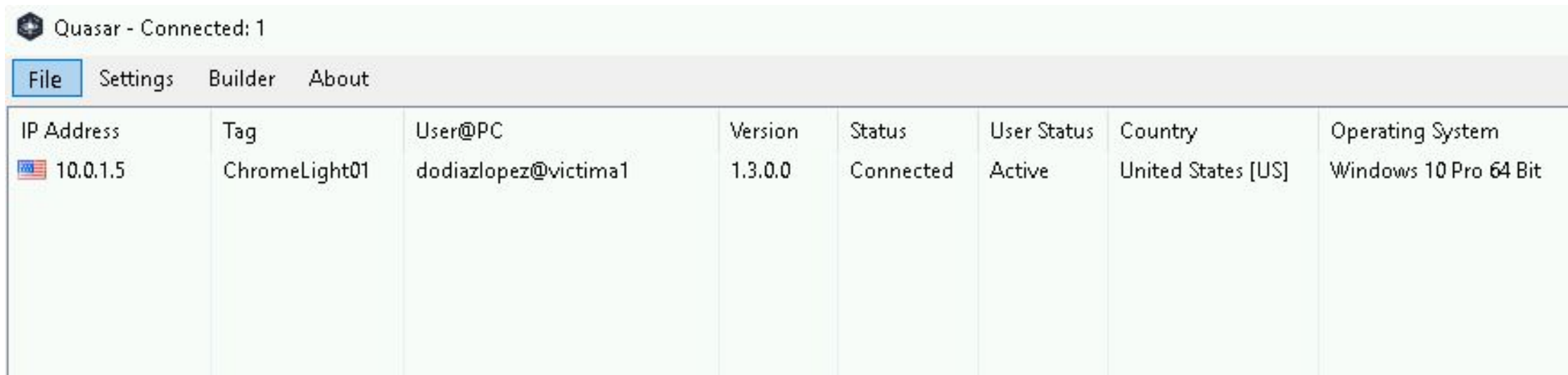
Assembly Icon

Change Assembly Icon

Browse...


Build Client

6. Redacte un email engañoso y adjunte el RAT (archivo .exe) que acaba de crear. Si el servicio de correo no le permite adjuntar el archivo, debe comprimirlo antes de adjuntarlo
7. Posteriormente abra el correo en la máquina víctima y descomprima y ejecute el archivo RAT
8. En este punto verá que la máquina víctima se incorpora a la lista de equipos que permiten ser controlados por la máquina atacante
9. Explore y documente las funcionalidades de Quasar RAT

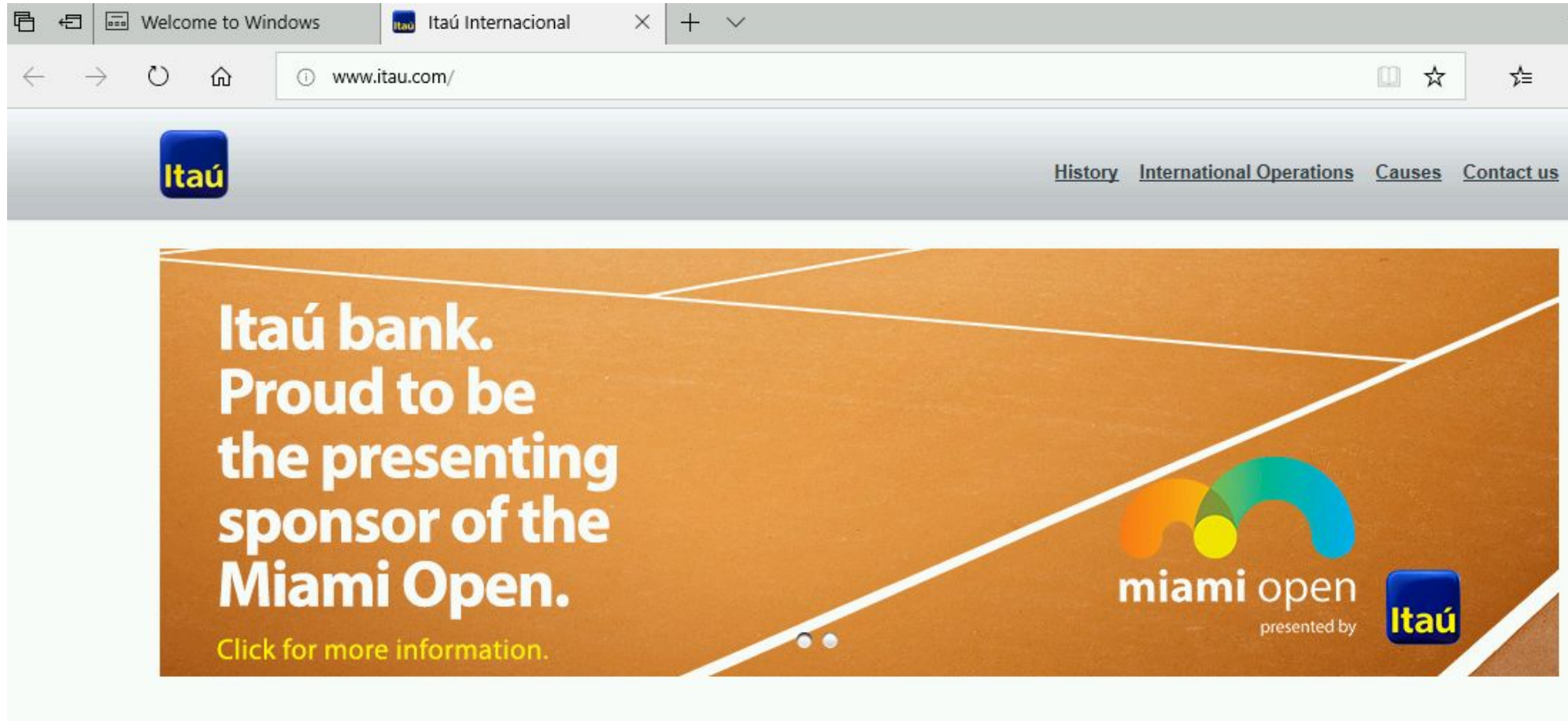


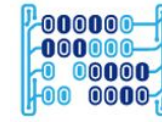
Quasar - Connected: 1

File Settings Builder About

| IP Address                                                                                 | Tag           | User@PC              | Version | Status    | User Status | Country            | Operating System      |
|--------------------------------------------------------------------------------------------|---------------|----------------------|---------|-----------|-------------|--------------------|-----------------------|
|  10.0.1.5 | Chromelight01 | dodiazlopez@victima1 | 1.3.0.0 | Connected | Active      | United States [US] | Windows 10 Pro 64 Bit |

## 6. Apertura de websites en la máquina víctima





## Laboratorio

1. Despliegue un troyano en una máquina víctima y tome control de ella.
  - a. Documentación de referencia: <https://www.youtube.com/watch?v=9Ws76thoFLc>
2. Revise los puertos de la máquina víctima y verifique si hay algún puerto sospechoso
  - a. Documentación de referencia:  
<https://www.e2enetworks.com/help/port-status-check/>
3. Explique cuáles serían las contramedidas que usted propondría para **prevenir** el ataque del punto 2
4. Explique qué pasos usted haría para **detectar** el ataque del punto 2



Universidad del  
**Rosario**



**MACC**



**HINNT**

Gracias

