



Universidad del
Rosario



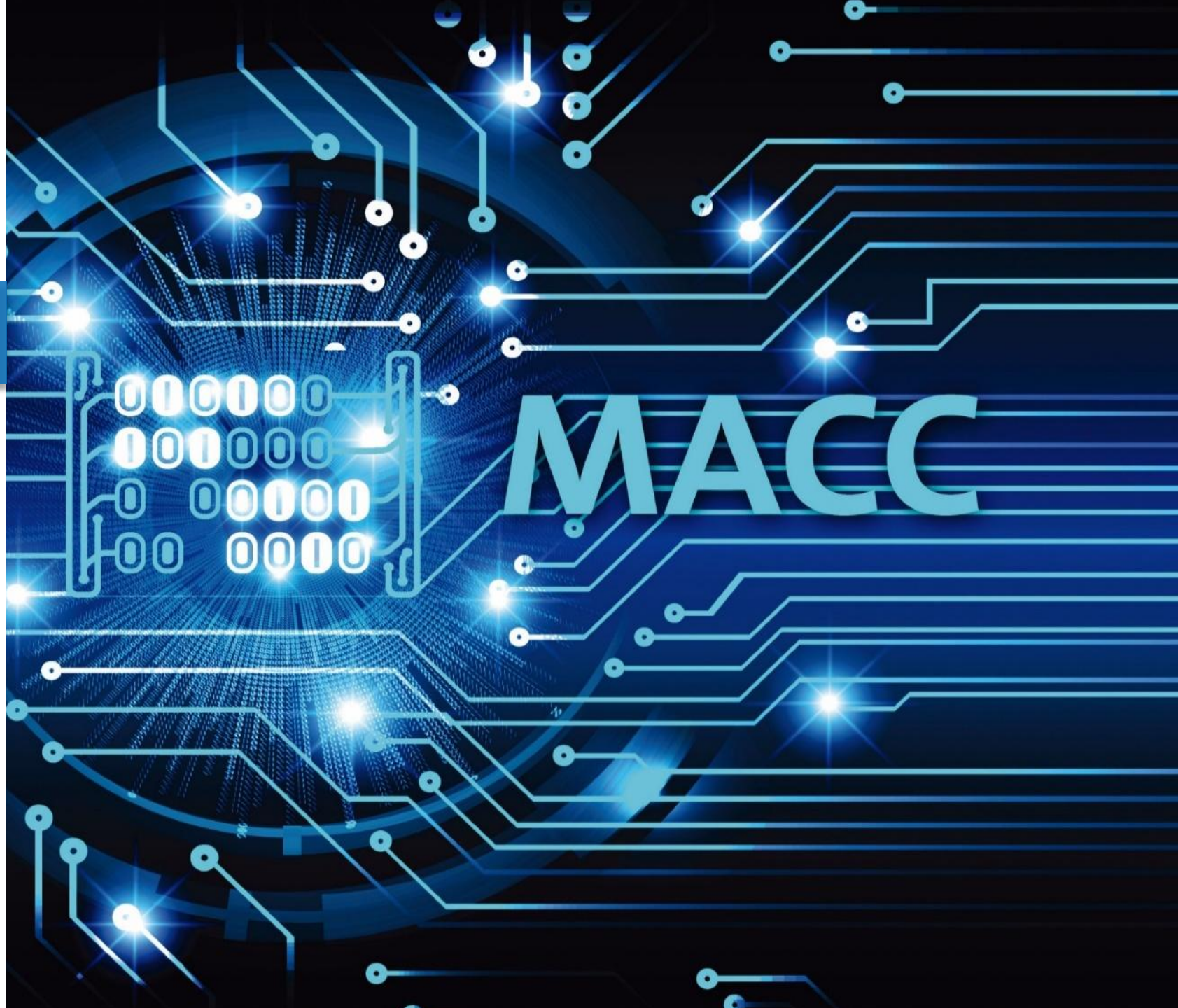
MACC
Matemáticas Aplicadas y
Ciencias de la Computación

Malware Threats

Hacking Ético

Daniel Orlando Díaz López, PhD

Profesor principal
Departamento MACC
Universidad del Rosario
danielo.diaz@urosario.edu.co

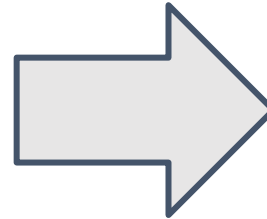


¿Que es el malware?

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

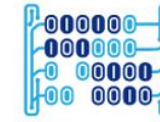
¿Cuales son los tipos de malware?

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



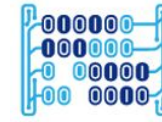
¿Que impactos tiene el malware?

- 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.



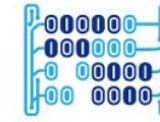
¿Cómo se distribuye el malware?

- 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



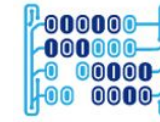
¿Cuales son las técnicas de distribución de malware?

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



Componentes de Malware

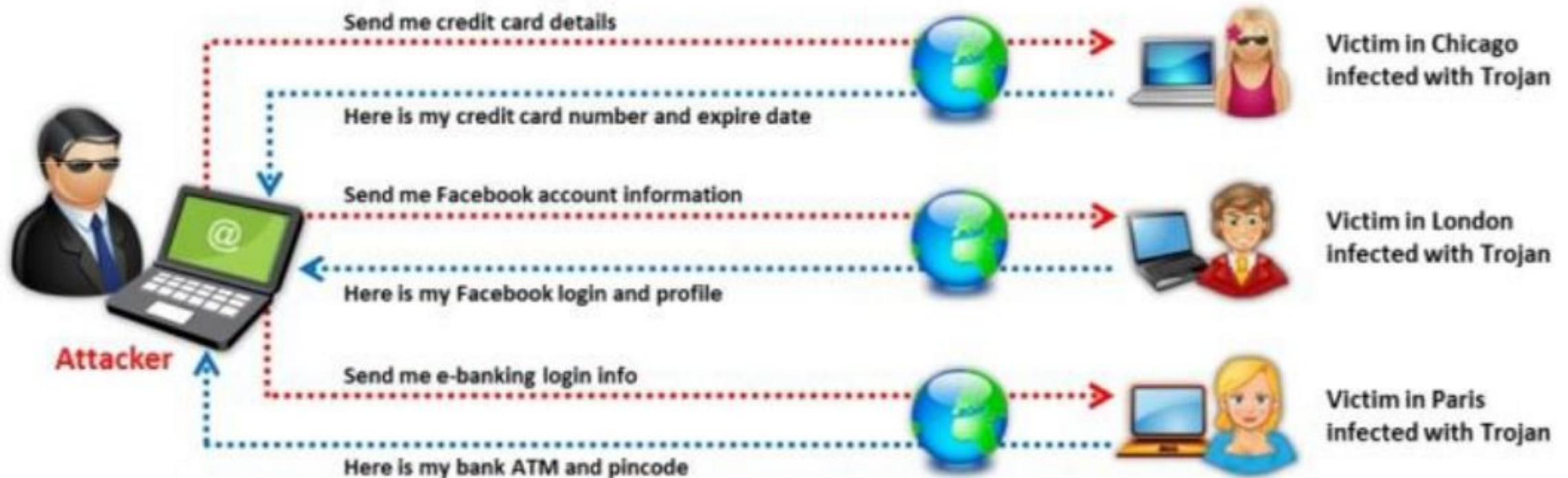
-



Trojanos

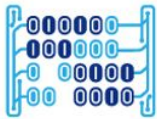
- Software malicioso contenido **dentro de** un software aparentemente inofensivo
- El software malicioso puede servir para tomar control del equipo víctima o causar daño
- Síntomas de afectación de un troyano son:
 - Comportamiento anormal del sistema
 - Actividades de red inusuales, e.g. deshabilitación 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	BackOrifice 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

¿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

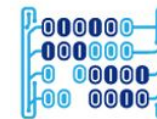
Mas información:

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

Despliegue de Quasar RAT



Universidad del
Rosario



MACC
Matemáticas Aplicadas y
Ciencias de la Computación

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	Nombre del equipo HE1001
Estado En ejecución	Sistema operativo Windows (Windows 10 Pro N)
Ubicación East US	Tamaño Estándar D2 (2 vcpu, 7 GiB de memoria)
Suscripción (cambiar) Azure para estudiantes	Disco de SO efímero N/D
Id. de suscripción dd5d31d9-0ebe-4b98-acd5-08373056d6da	Dirección IP pública 40.112.59.191
	Dirección IP privada 10.0.1.4
	Red virtual/subred HEvnet969/default
	Nombre DNS Configurar

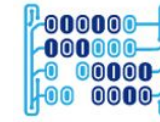
Máquina Víctima

Conectar Iniciar Reiniciar Detener Captura Eliminar Actualizar	
Grupo de recursos (cambiar) HE	Nombre del equipo victima1
Estado En ejecución	Sistema operativo Windows (Windows 10 Pro)
Ubicación East US	Tamaño B1s estándar (1 vcpu, 1 GiB de memoria)
Suscripción (cambiar) Azure para estudiantes	Disco de SO efímero N/D
Id. de suscripción dd5d31d9-0ebe-4b98-acd5-08373056d6da	Dirección IP pública 40.117.103.174
	Dirección IP privada 10.0.1.5
	Red virtual/subred HEvnet969/default
	Nombre DNS Configurar

Despliegue de Quasar RAT

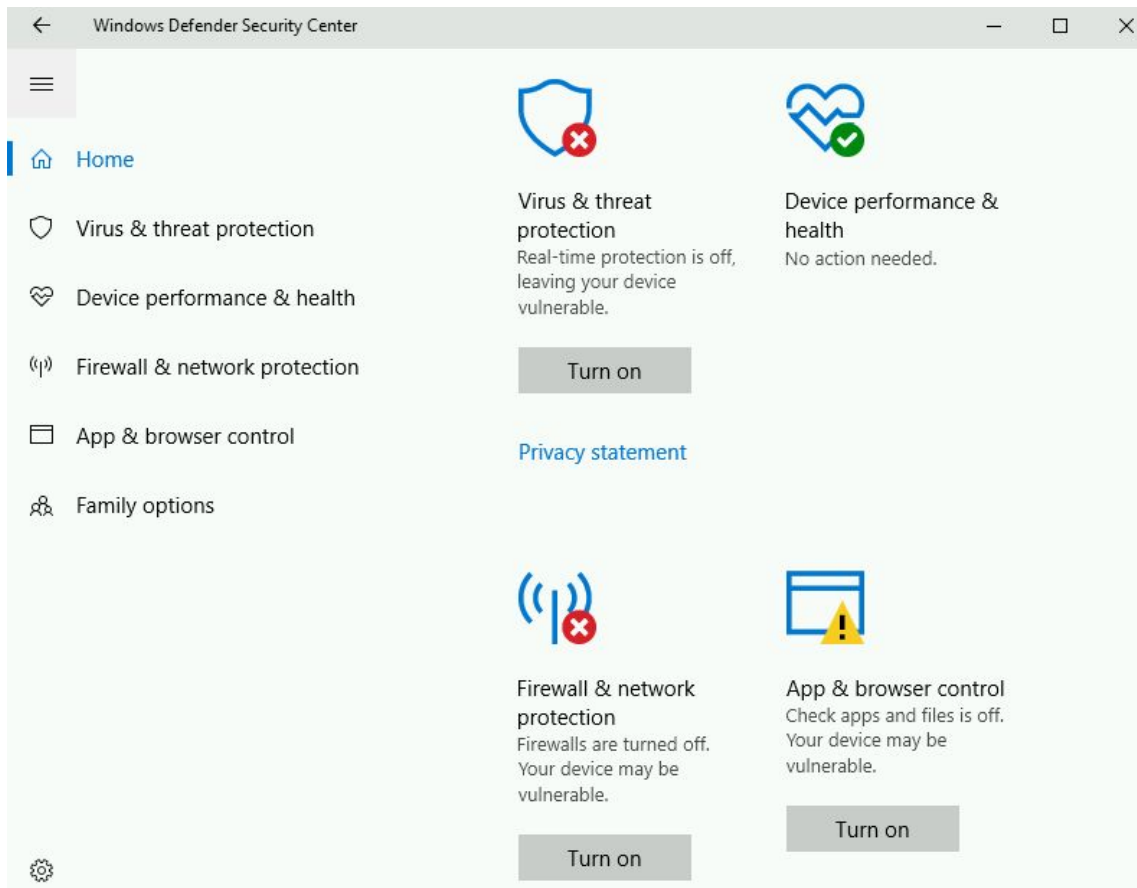


Universidad del
Rosario



MACC
Matemáticas Aplicadas y
Ciencias de la Computación

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
```

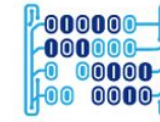
```
C:\Users\dodiazlopez>ping 10.0.1.4 -t

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

4. 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: 30a4ec904324aab10b9f771271

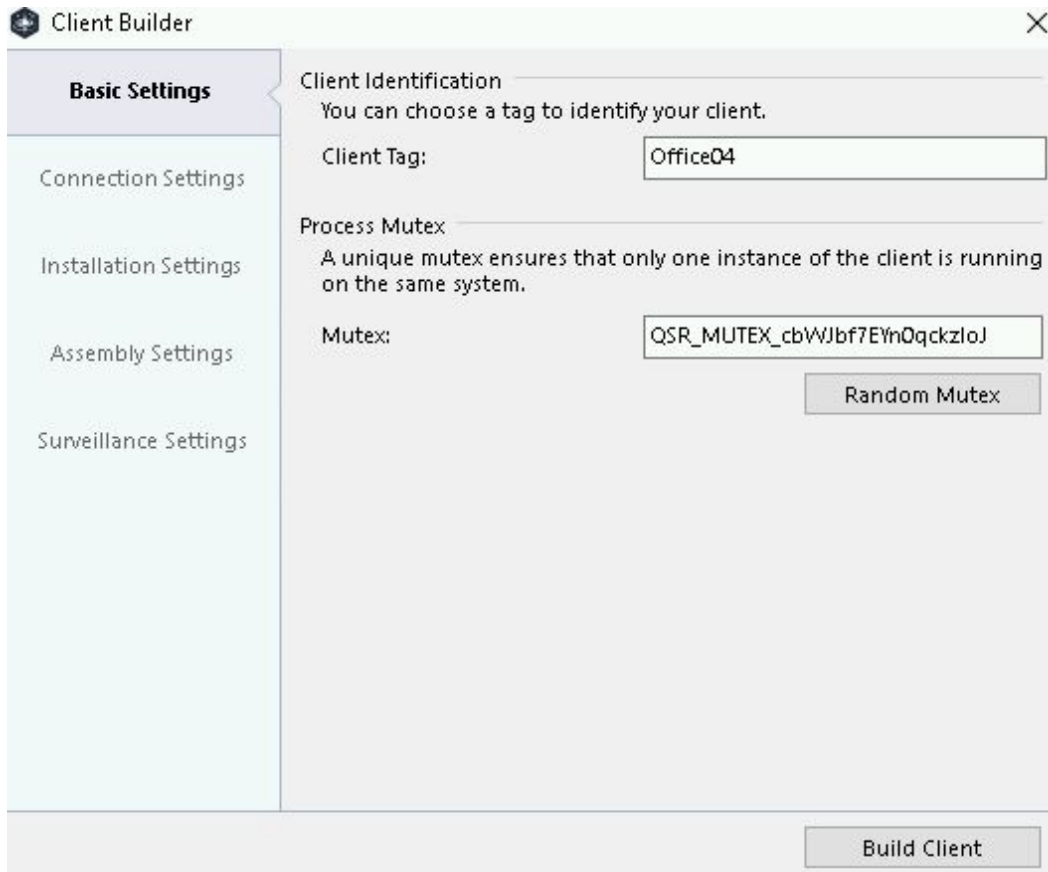
▼ **Assets** 3

Quasar.v1.3.0.0.zip

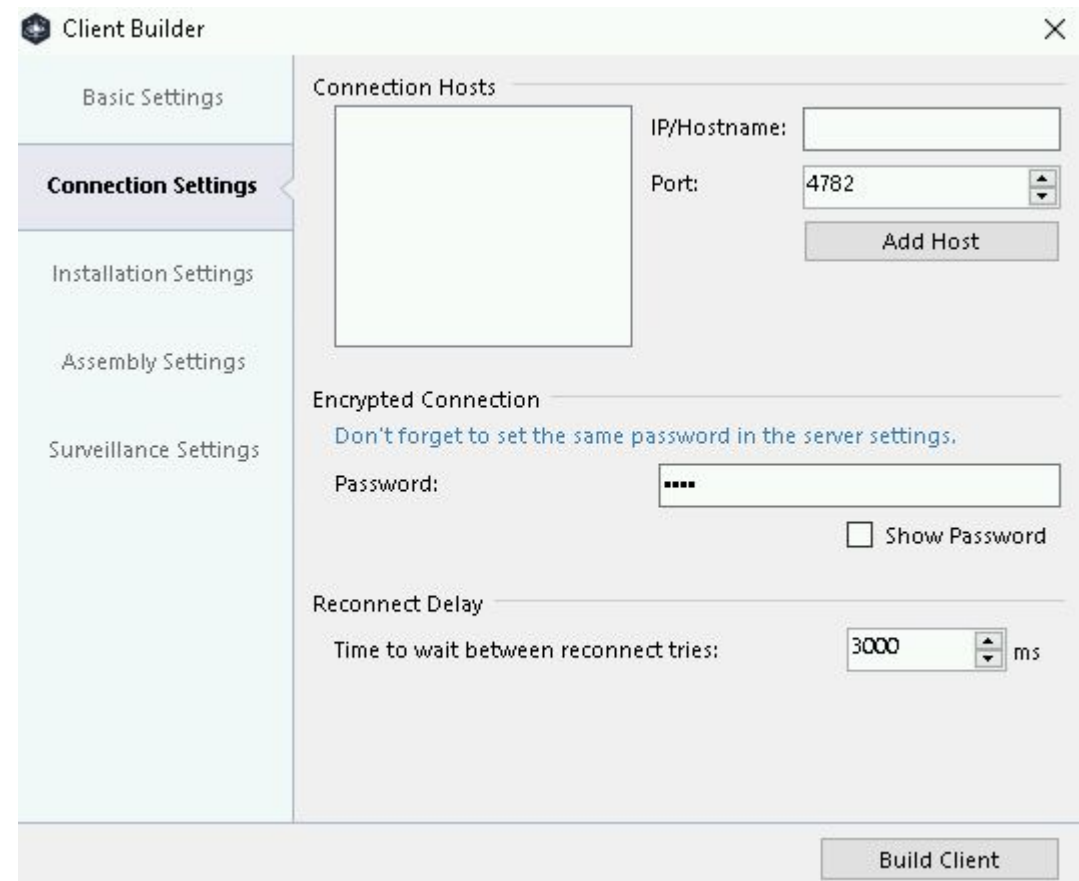
Source code (zip)

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' window with the 'Basic Settings' tab selected. The left sidebar lists the following sections: Basic Settings, Connection Settings, Installation Settings, Assembly Settings, and Surveillance Settings. The main content area is divided into two sections: 'Client Identification' and 'Process Mutex'. Under 'Client Identification', there is a text box for 'Client Tag' containing 'Office04'. Under 'Process Mutex', there is a text box for 'Mutex' containing 'QSR_Mutex_cbWJbf7EYnQqckzloJ' and a 'Random Mutex' button. At the bottom right, there is a 'Build Client' button.

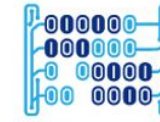


The screenshot shows the 'Client Builder' window with the 'Connection Settings' tab selected. The left sidebar lists the following sections: Basic Settings, Connection Settings, Installation Settings, Assembly Settings, and Surveillance Settings. The main content area is divided into two sections: 'Connection Hosts' and 'Encrypted Connection'. Under 'Connection Hosts', there is a large empty text box, a 'Port' dropdown menu set to '4782', and an 'Add Host' button. Under 'Encrypted Connection', there is a text box for 'Password' containing four dots, a 'Show Password' checkbox, and a 'Reconnect Delay' section with a text box for 'Time to wait between reconnect tries' set to '3000' ms. At the bottom right, there is a 'Build Client' button.

Despliegue de Quasar RAT



Universidad del
Rosario



MACC
Matemáticas Aplicadas y
Ciencias de la Computación

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.

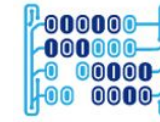
The screenshot shows the 'Client Builder' window with the 'Installation Settings' tab selected. The left sidebar contains links for Basic Settings, Connection Settings, Installation Settings (active), Assembly Settings, and Surveillance Settings. The main area is divided into sections: 'Installation Location' with a checked 'Install Client' checkbox and three radio buttons for 'Install Directory' (selected: 'User Application Data', others: 'Program Files', 'System'); 'Install Subdirectory' with a text box containing 'SubDir'; 'Install Name' with a text box containing 'Client.exe'; checkboxes for 'Set file attributes to hidden' and 'Set subdir attributes to hidden'; 'Installation Location Preview' showing the path 'C:\Users\dodiazlopez\AppData\Roaming\SubDir\Client.exe'; and 'Autostart' with a checkbox for 'Run Client when the computer starts' and a 'Startup Name' text box containing 'Quasar Client Startup'. A 'Build Client' button is at the bottom right.

The screenshot shows the 'Client Builder' window with the 'Assembly Settings' tab selected. The left sidebar is the same as the previous image. The main area is divided into 'Assembly Information' and 'Assembly Icon' sections. 'Assembly Information' includes a checked 'Change Assembly Information' checkbox and seven text boxes for: 'Product Name', 'Description', 'Company Name', 'Copyright', 'Trademarks', 'Original Filename', 'Product Version', and 'File Version'. 'Assembly Icon' includes a checkbox for 'Change Assembly Icon' and a 'Browse...' button. A 'Build Client' button is at the bottom right.

Despliegue de Quasar RAT




Universidad del
Rosario



MACC
Matemáticas Aplicadas y
Ciencias de la Computación

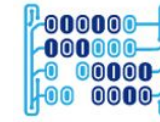
6. Redacte un email engañoso y adjunte el RAT (archivo .exe) que acaba de crear. Si el servicio de correo no le permite adjuntar el archivo, debe comprimirlo antes de adjuntarlo
7. Posteriormente abra el correo en la máquina víctima y descomprima y ejecute el archivo RAT
8. En este punto verá que la 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

Despliegue de Quasar RAT

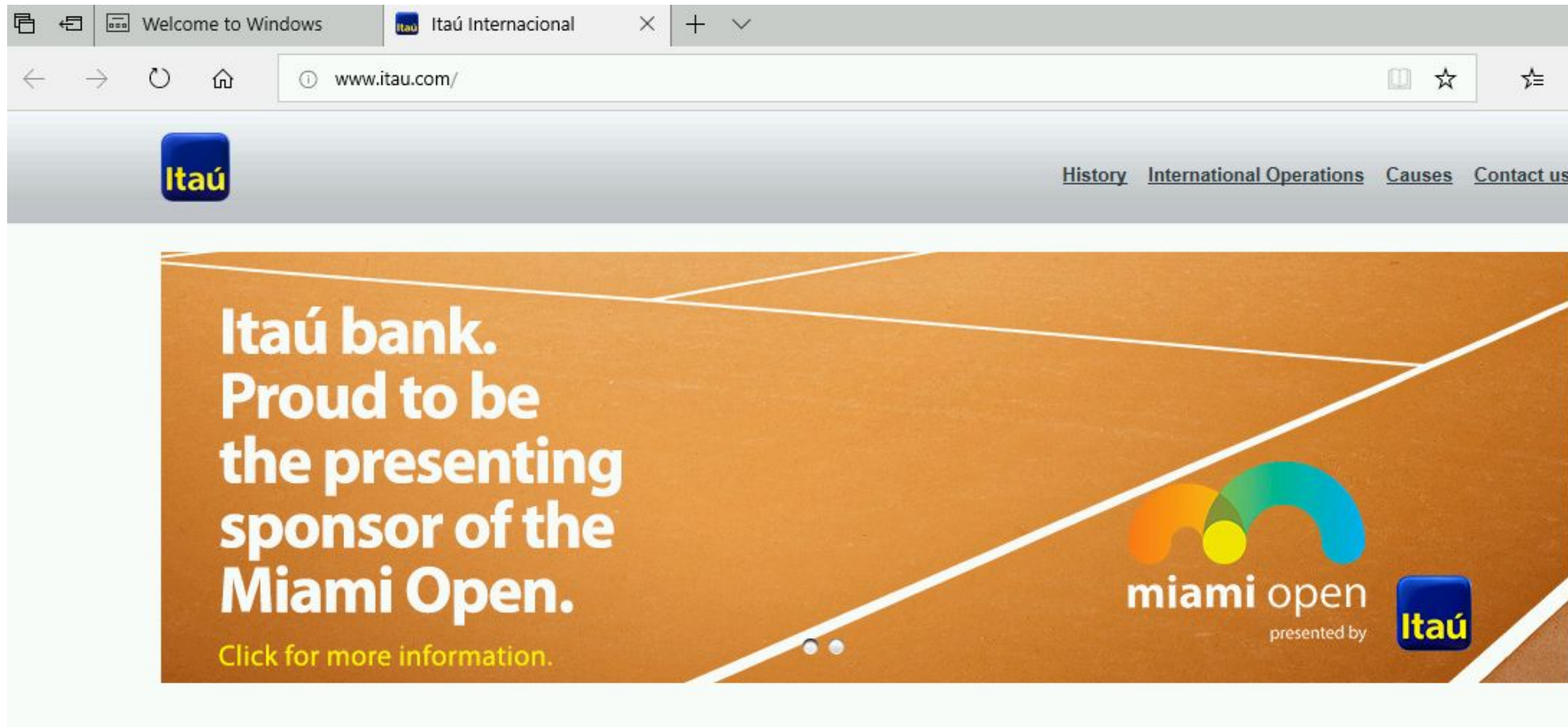


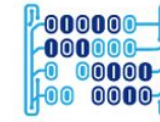
Universidad del
Rosario



MACC
Matemáticas Aplicadas y
Ciencias de la Computación

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