Hackers, Haciendo la Diferencia

Carlos Perez, Research Lead

Quien Soy?

Hacker

67 languages

Article Talk | Read View source View history

From Wikipedia, the free encyclopedia

For other uses, see Hacker (disambiguation).

This article **possibly contains original research**. Please improve it by verifying the claims made and adding inline citations. Statements consisting only of original research should be removed. *(October 2020)* *(Learn how and when to remove this template message)*

A **hacker** is a person skilled in information technology who uses their technical knowledge to achieve a goal or overcome an obstacle, within a computerized system by non-standard means. Though the term *hacker* has become associated in popular culture with a *security hacker* – someone who utilizes their technical know-how of bugs or exploits to break into computer systems and access data which would otherwise be inaccessible to them – hacking can also be utilized by legitimate figures in legal situations. For example, law enforcement agencies sometimes use hacking techniques in order to collect evidence on criminals and other malicious actors. This could include using anonymity tools (such as a VPN, or the dark web) to mask their identities online, posing as criminals themselves.[1][2] Likewise, covert world agencies can employ hacking techniques in the legal conduct of their work. On the other hand, hacking and cyber-attacks are used extra- and illegally by law enforcement and security agencies (conducting warrantless activities), and employed by state actors as a weapon of both legal and illegal warfare.

People taking part in the Coding da Vinci hackathon on April 26 and 27, 2014, in Berlin

Que es ser un Hacker

- Hacker != Offensivo, ni Criminal
- Hacker != Infosec
- Hacker != Cyber
- Hacker == Pensar mas haya de la influencia
- Hacker == Conseguir una meta aun con retos grandes
- Hacker == Communidad
- Hackers == La busqueda de conocimiento


ESTAMOS EN EL
MISMO EQUIPO

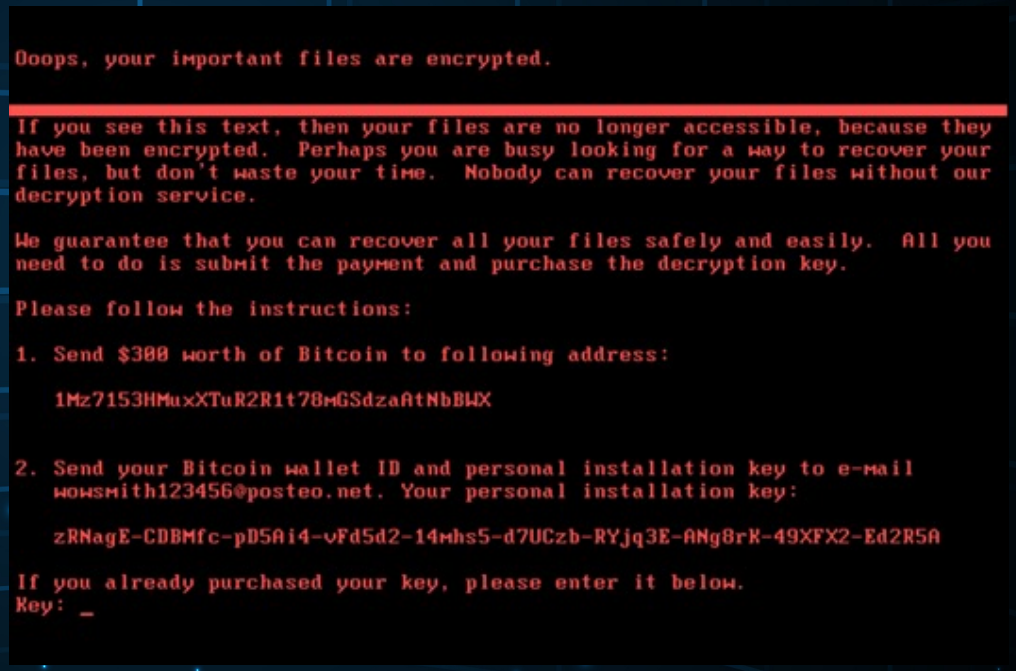
El Campo de Batalla esta Evolucionando

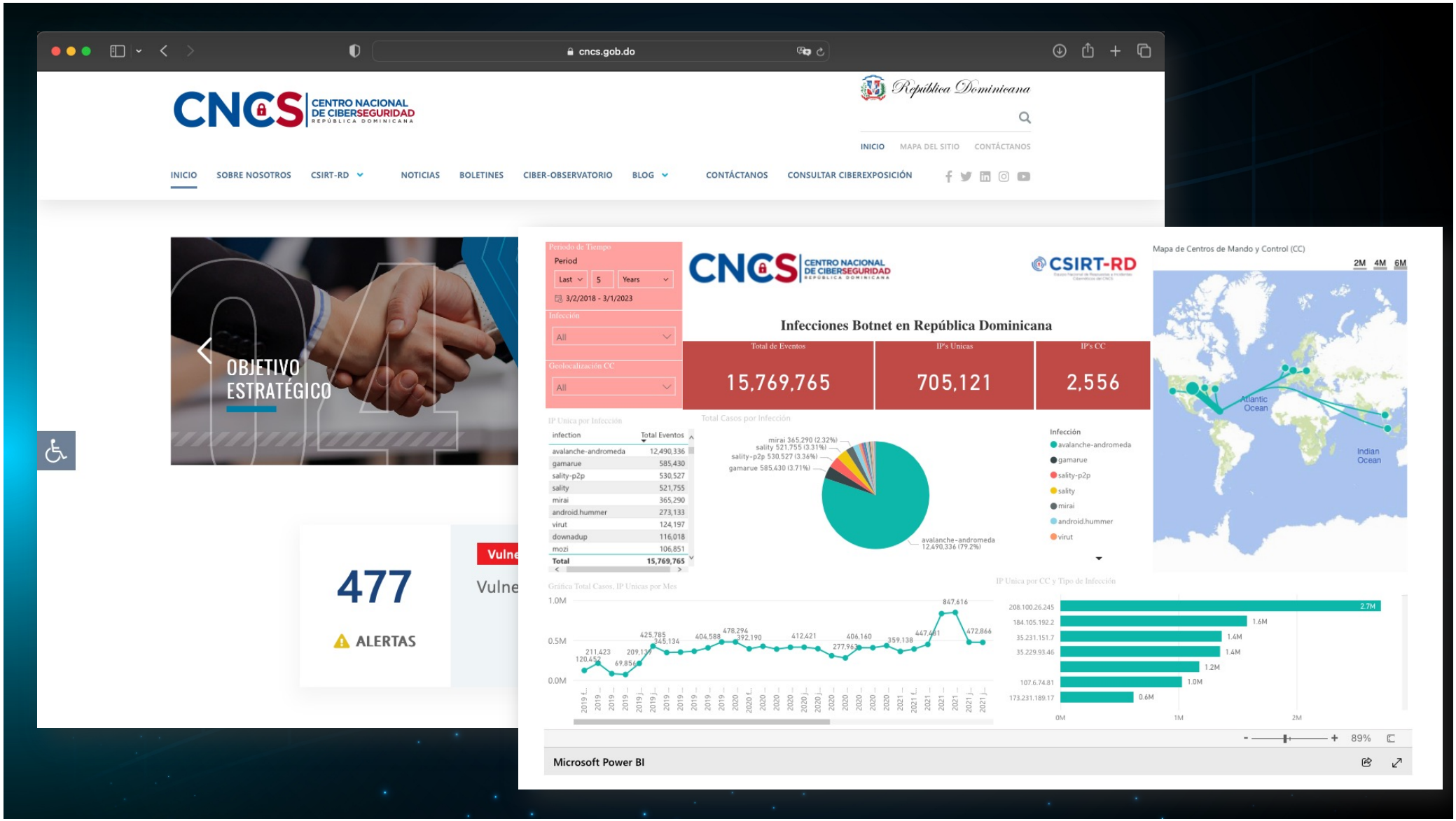
- Sistemas operativos ya incluyen AV y controles avanzados.
- Mejores productos de seguridad siguen llegando al mercado.
- El tiempo de vida útil de una herramienta ofensiva cada vez es mas corto cuando detectada.
- Hoy en día hay mas información y herramientas de bajo costo o de ningún costo que antes.

Mayor Complejidad en el Entorno

- Tenemos mas jugadores en el campo
  - Hacktivist
  - Criminales
  - Naciones
  - Compañias
- La oportunidad de estar en una red o sistema donde hay otro actor es mayor ahora que antes.
- El costo de entrada en terminos de conocimiento y herramientas es bien bajo.

Cada vez el Impacto es Mayor




cncs.gob.do
CNCS
CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA
República Dominicana
INICIO
MAPA DEL SITIO
CONTÁCTANOS
INICIO
SOBRE NOSOTROS
CSIRT-RD
NOTICIAS
BOLETINES
CIBER-OBSERVATORIO
BLOG
CONTÁCTANOS
CONSULTAR CIBEREXPOSICIÓN
OBJETIVO ESTRATÉGICO
477
ALERTAS
Vulne
Vulne
Periodo de Tiempo
Period
Last
5
Years
3/2/2018 - 3/1/2023
Infección
All
Geolocalización CC
All
CNCS
CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA
CSIRT-RD
Infecciones Botnet en República Dominicana
Total de Eventos
15,769,765
IP's Unicas
705,121
IP's CC
2,556
IP Unica por Infección
infection
Total Eventos
avalanche-andromeda 12,490,336
gamarue 585,430
sality-p2p 530,527
sality 521,755
mirai 365,290
android.hummer 273,133
virut 124,197
downadup 116,018
mozi 106,851
Total 15,769,765
Total Casos por Infección
mirai 365,290 (2.32%)
sality 521,755 (3.31%)
sality-p2p 530,527 (3.36%)
gamarue 585,430 (3.71%)
avalanche-andromeda 12,490,336 (79.2%)
Infección
avalanche-andromeda
gamarue
sality-p2p
sality
mirai
android.hummer
virut
Mapa de Centros de Mando y Control (CC)
2M
4M
6M
Atlantic Ocean
Indian Ocean
Gráfica Total Casos, IP Unicas por Mes
1.0M
0.5M
0.0M
120,452
211,423
69,856
209,179
425,785
345,134
404,588
478,294
392,190
412,421
277,963
406,160
359,138
447,661
847,616
472,866
IP Unica por CC y Tipo de Infección
208.100.26.245
184.105.192.2
35.231.151.7
35.229.93.46
107.6.74.81
173.231.189.17
2.7M
1.6M
1.4M
1.4M
1.2M
1.0M
0.6M
0M
1M
2M
89%
Microsoft Power BI

Factor Humano CVSS 10

- El uso de CTI y de mejores practicas ya establecidas sigue siendo bajo.
- Aun cuando la comunidad ha logrado grandes avanzes en herramientas e information muchas organizaciones siguen atascadas en metodos antiguos.
- El costo de desarrollar personal, adquirrir herramientas y dedicar tiempo a establecer processos sigue siendo parte de la ecuacion pero no el mayor.

First Mover Advantage

- La industria se esta avanzando, y tu?
  - Cloud es ahora central para autenticacion y servicios.
  - SAML remplaza a Kerberos and NTLM.
  - Tokens y cookies remplazan hashes y password.
  - MFA es mas comun.
  - Artefactos moviles y IOT dominan.
- Nuevos lenguages de programacion como Rust, Go, Nim ..etc
  - Desarrollo de nuevas herramientas.
  - Modificacion y adatacion de herramientas existentes.

Como Ganamos?

- Ser más agiles
  - After Action, vemos que funciono, que no, documentamos y creamos un plan de acción
  - La información que obtenemos sea de IR o de una emulación se guarda y se utiliza.
- Minimizamos islas de conocimiento
  - Tenemos que desarrollar un plan de entrenamiento.
  - Tenemos que rotar funciones para que se gane xontexto.
- Ser flexible, programar ya no es “seria bueno pero no necesario”

Cobalt strike
MANUALS_V2
Active Directory

I Tier . Increasing privileges and collecting information

1 . Initial exploration

1.1 . Search for company income

Finding the company's website
On Google : SITE + revenue (mycorporation.com + revenue) ("mycorporation.com" "revenue")
check more than 1 site, if possible
(owler, manta, zoominfo, dnb, rocketrich)

1.2 . Defined by AB

1.3 . **shell whoami** < ===== who am I

1.4 . **shell whoami / groups** -> my rights on the bot (if the bot came with a blue monik)

1.5 . 1 . **shell nltest / dclist:** <===== domain controllers

net dclist < ===== domain controllers

1.5 . 2 . **net domain_ controllers** < ===== this command will show the ip addresses of domain controllers

1.6 . **shell net localgroup administrators** <===== local administrators

1.7 . **shell net group / domain "Domain Admins"** <===== domain administrators

1.8 . **shell net group "Enterprise Admins" / domain** <===== enterprise administrators

1.9 . **the shell net group "the Domain Computers has" / domain** <===== total number - in the PC in the domain

Nuestro Reto

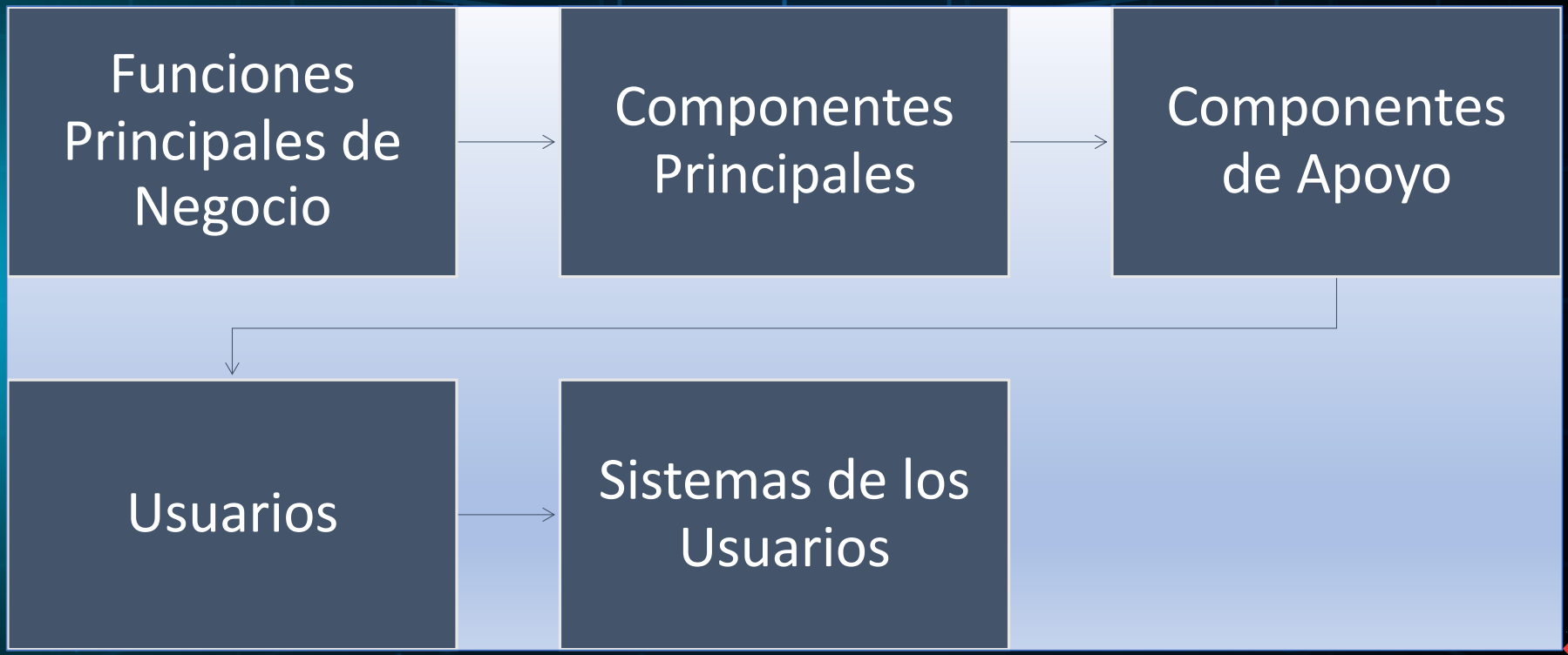
- Promedio de applicaccion de parchos de seguridad criticos, es 3 meses.
- 10 de cada 12 clientes no tienen configurado parametros de auditar eventos.
- Encontramos alertas en las applicaciones de seguridad que nadie miro.
- Todos los ataques trabajados tenian componentes de herramientas y/o tecnicas ya conocidas.

Estratégico, no tan Táctico

- Donde comienzo? Que aseguro?

Si conoces a los demás y te conoces
a ti mismo, ni en cien batallas
correrás peligro;
si no conoces a los demás, pero te
conoces a ti mismo, perderás una
batalla y ganarás otra;
si no conoces a los demás ni te
conoces a ti mismo, correrás peligro
en cada batalla.
Sun Tzu

Estratégico, no tan Táctico



Estratégico, no tan Táctico

Gracias