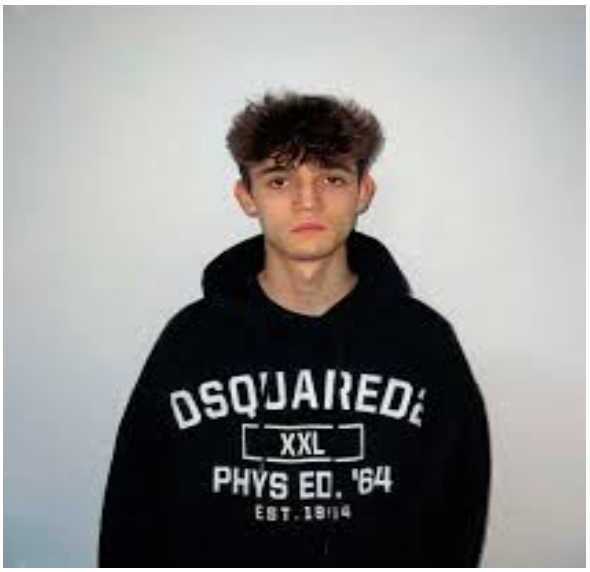
CICLOFORMATIVODEGRADOSUPERIOR-
TÉCNICOEN ADMINISTRACIÓN DE SISTEMAS
INFORMÁTICOS EN REDES

SEGURIDAD Y ALTA DISPONIBILIDAD

Wuke Zhang y Alvaro Gines

SOFTWAREANTIMALWARE



Tarea Software Antimalware_Wuke_Zhang_Alvaro_Gines

Índice

Enunciado

1. Realiza un trabajo de estudio de caso sobre un ejemplo actual (últimos6 meses) de ataques con códigos maliciosos o malware: ***(8.- ptos)***

- *El trabajo debe incluir:*
  - *Definición del malware (**TIPOLOGIA**) (1,5pts).*
  - *Analizar su método de infección o propagación (**TRANSMISIÓN**)(1,5pts).*
  - *Mecanismo de reparación (**RESPUESTA**)(1pts).*
  - *Analiza los ataques y medios de infección que han sucedido, así como las soluciones empleadas (**ANÁLISIS DE CASO**) (3pts).*
- *Debe incluir portada, índice, **conclusiones** y bibliografía (0,5pts)*
- *Entre3 y 5páginas. (No se cuenta portada ni índice)(0,20pts).*
- *Añadir en la portada el autor y título descriptivo del caso (0,05pts).*
- *Formato: Fuente Arial/Times New Roman 12 e interlineado sencillo (0,25 pts).*
- *Se entregará a través de la plataforma Moodle de ICSE(en formato .pdf)*

2. Realiza una presentación sobre el trabajo realizado***(2.-ptos)***

- *Realizar la presentación en PowerPoint, Google Slides o similar(1pts).*
- *Tiempo máximo de exposición 8 minutos.*
- *Evitar grandes cantidades de texto en las presentaciones.*
- *Debe incluir los apartados de Tipología, Transmisión, Respuesta y Análisisde Caso.*

Introducción

En este estudio de caso, analizaremos los ataques con malware realizados por el hacker español José Luis Huertas, conocido como Alcasec. Este joven hacker ha sido responsable de varios ataques cibernéticos de alto perfil en los últimos meses, afectando tanto a instituciones públicas como privadas en España. Su plataforma "Udyat" comprometió datos sensibles y fue utilizada para monetizar información ilícita, convirtiéndose en una amenaza grave para la Seguridad Nacional.

Tipología del Malware

El malware utilizado por Alcasec incluye varios tipos, entre ellos:

- ***Troyanos de acceso remoto (RAT):*** *Para infiltrarse y controlar sistemas de forma remota.*
- ***Infostealers:*** *Diseñados para robar información sensible como credenciales.*
- ***Ransomware:*** *Para cifrar datos y exigir un rescate.*
- ***Plataforma ilícita de datos:*** *Desarrollo de "Udyat" como un servicio de consulta y venta de datos personales.*

Método de Infección o Propagación

Alcasec ha utilizado diversas técnicas para infectar sistemas, incluyendo:

- ***Explotación de vulnerabilidades:*** *Uso del Punto Neutro Judicial para acceder a múltiples instituciones públicas.*
- ***Phishing:*** *Correos electrónicos diseñados para engañar a los usuarios y obtener sus credenciales.*
- ***Monetización y ocultación:*** *Uso de mixers de criptomonedas para evadir rastreos financieros.*

Respuesta y Mecanismo de Reparación

La respuesta al ciberataque incluyó:

1. ***Investigación exhaustiva:*** *Coordinación entre la Comisaría General de Información, Fiscalía de la Audiencia Nacional y el Centro Criptológico Nacional.*
2. ***Identificación del atacante:*** *Especialistas en ciberseguridad rastrearon las actividades de "Alcasec" hasta identificarlo.*
3. ***Operativo de detención:*** *Registro de domicilios y locales, incautación de dinero, documentación y dispositivos.*
4. ***Revisión de sistemas:*** *Implementación de medidas de seguridad en las instituciones afectadas para prevenir futuros ataques.*

Análisis del Caso

Detalles del Ciberataque

- ***Instituciones afectadas:*** *Consejo General del Poder Judicial, Agencia Tributaria y otras instituciones públicas.*
- ***Datos comprometidos:*** *Datos personales, números de cuenta y saldos bancarios.*
- ***Plataforma "Udyat":*** *Diseñada para ofrecer acceso a datos sensibles de la mayoría de los ciudadanos españoles.*

Perfil del Atacante

- ***Alias:*** *Alcasec.*
- ***Edad:*** *19 años.*
- ***Estilo de vida:*** *Vida de lujos financiada mediante actividades ilícitas.*
- ***Técnicas de evasión:*** *Uso de mixers de criptomonedas para ocultar el origen de los fondos.*

Intervenciones Realizadas

- ***Incautaciones:*** *Documentación, soportes informáticos, dinero en efectivo, vehículos de alta gama.*
- ***Resultado Legal:*** *Detención e ingreso en prisión del responsable.*

Conclusiones

El caso de "Alcasec" demuestra la importancia de:

1. *Fortalecer las infraestructuras críticas de las instituciones públicas.*
2. *Incrementar la cooperación entre entidades nacionales e internacionales para mitigar ciberamenazas.*
3. *Adoptar medidas preventivas y sistemas de monitorización para evitar la explotación de vulnerabilidades.*
4. *Mejor tenerle como aliado en vez de enemigo.*

Bibliografía

1. *Policía Nacional. (2023). Nota de prensa: "La Policía Nacional detiene a un peligroso delincuente informático...".*
2. *Centro Criptológico Nacional. (2023). Informes sobre ciberseguridad en infraestructuras públicas.*
3. *Noticias especializadas en ciberseguridad. (2023). "Alcasec y el impacto de Udyat en la Seguridad Nacional".*
4. *https://www.genbeta.com/tag/alcasec*
5. *https://www.elindependiente.com/espana/2023/07/02/historia-del-hacker-que-amenazo-al-estado-alcasec-el-nino-prodigio-que-vive-en-la-red/*