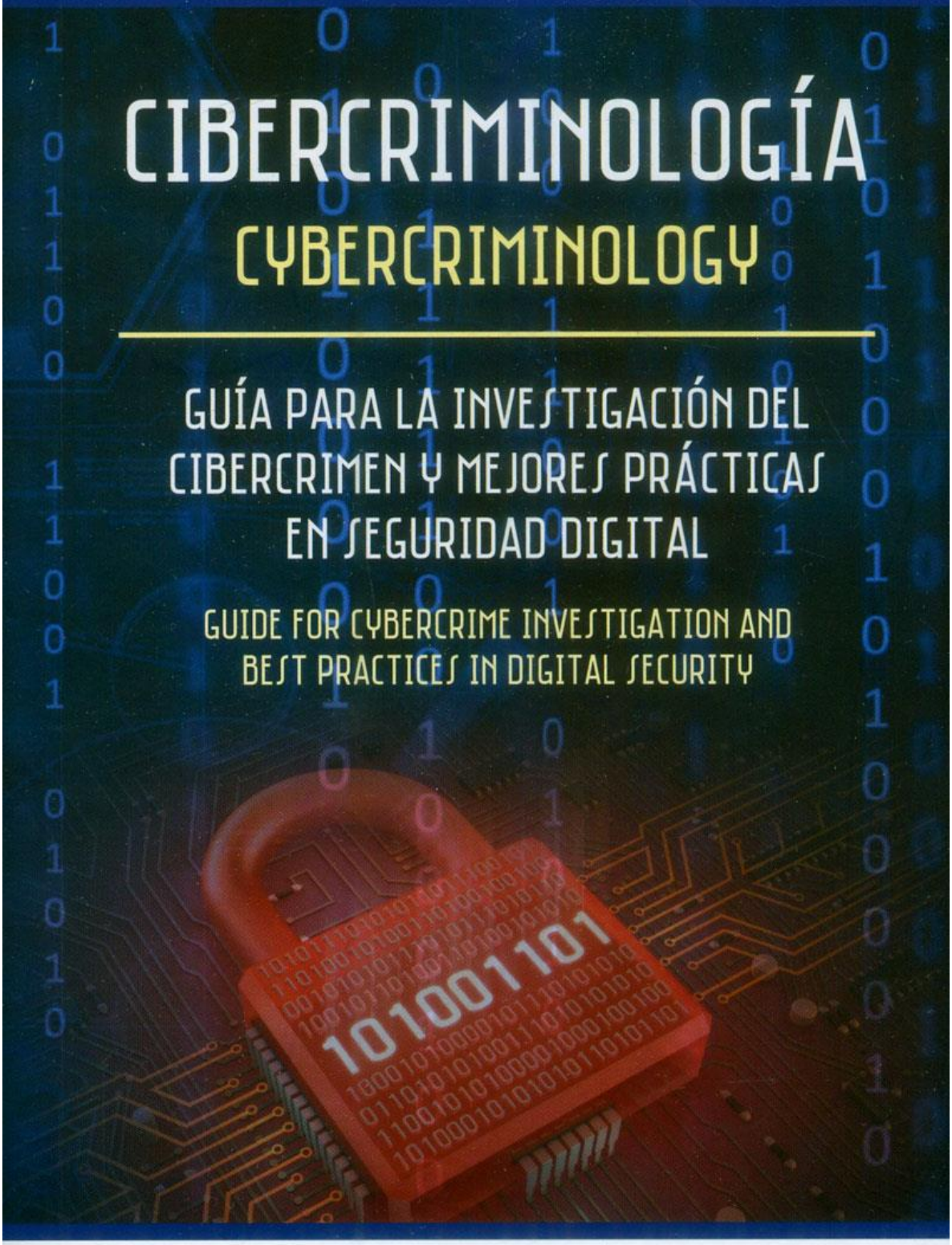
KYUNG-SHICK CHOI · MARLON MIKE TORO-ÁLVAREZ

CIBERCRIMINOLOGÍA
CYBERCRIMINOLOGY

GUÍA PARA LA INVESTIGACIÓN DEL CIBERCRIMEN Y MEJORES PRÁCTICAS EN SEGURIDAD DIGITAL

GUIDE FOR CYBERCRIME INVESTIGATION AND BEST PRACTICES IN DIGITAL SECURITY



UAN
UNIVERSIDAD
ANTONIO NARIÑO

BOSTON
UNIVERSITY

PARTE I. LA AMENAZA DEL CIBERCRIMEN YLOS DELITOS INFORMÁ TICOS

Capítulo l.
Definición del cibercrimen y los delitos informáticos
1.1. Definiciones de cibercrimen
1.2. El Convenio sobre ciberdelincuencia de Budapest
1.3. La jurisdicción en el ciberespacio
1.4. Pensamiento crítico de un experto en ciberseguridad y cibercriminología

Capítulo 2.
De los cibercriminales, hackers y otros tipos de
l delincuentes
2.1. Doce perfiles criminales cibernéticos
2.2. Tipos de explotaciones cibernéticas criminales
2.2.1. Formas de código malicioso
•Virus
•Bombas de tiempo/bombas lógicas
•Caballo de Troya
• Malware
2.2.2. Ataques dirigidos
• Ataques de empleado

• Ataques de contraseña
• Sniffing
• Spoofing (cibersuplantación)
• Desfiguración de sitios web
• Suplantación de direcciones IP
• Redirección de dominio o hijacking
• Suplantación de protocolo ARP
• Ataques de hombre-en-el-medio
• Ataques de capa de aplicación
• Denegación de Servicio (DoS) y DDoS
• Ingeniería social
2·3. Estudio experimental: entrevistas y respuestas de hackers
2·3·1. Antecedentes de la investigación
2·3·2. Conclusiones basadas en la perspectiva teórica • Clasificación de los participantes

2·3·3· Revisando la teoría de las actividades cotidianas
2·3-4. Consideraciones metodológicas
•Enfoque cualitativo
•Selección de participantes

•Entrevista
2·3·5· Desafíos metodológicos
Ganar la confianza de los hackers
• Datos falsificados
• Factores de validez
• 2.3.6. Discusión y futuras investigaciones
2·3·7. Conclusiones
2-4. Pensamiento crítico de un experto en

ciberseguridad y cibercriminología
Capítulo 3.
Estafa en línea, robo de identidad y phishing
3·1. El impacto en cifras
3.1.1. Pérdida financiera mundial
3.1.2. Pérdida de tiempo y daño psicológico
3·2. Tendencias: principales clases de fraude en
Internet
3.2.1. Fraude contra el reloj (ransomware)
3.2.2. Robo de identidad
3.2.3. Phishing
•Métodos comunes
- Correo electrónico
- Mensajería instantánea (MI)
- Sitio web
•Tipos de ataques de phishing
- Los ataques del Hombre-en-el-medio Proxies transparentes Envenenamiento de caché de DNS Configuración de proxy del navegador
- Phishing basado en software malicioso
(malware)
Keyloggers y screenloggers
Secuestro de sesión (hijacking) Envenenamiento de archivos de host
- Ataques de phishing basados en DNS (pharming)
- Phishing del motor de búsqueda 3.2-4. La estafa nigeriana
3.2.5. Fraude de subasta en Internet
3·3· Pensamiento crítico de un experto en
ciberseguridad y cibercriminología
Capítulo 4.
Ransomware: hallazgos y recomendaciones
4.1. Fundamentación criminológica
4·2. Metodología y medición de variables
4.2.1. Fechas de los casos reportados
4.2.2. Estados víctimas
4.2·3· Tamaño del departamento de policía
4·2·4. Cantidad de rescate
• Rescate pagado por la policía y método de ataque de ransomware
4·3· Motivación criminal y estilo de vida online de
las víctimas
4·3.1. Delincuente motivado
4·3·2. Estilo de vida online
4·3·3· Custodia Digital Capaz (ciberseguridad)
4-4· Discusiones y conclusiones
4·5· Pensamiento crítico de un experto en
ciberseguridad y cibercriminología
Capítulo 5.
Crímenes interpersonales en el ciberespacio
5·1. Tráfico humano
5·2. Violencia sexual
5·3. Catfishing
5·4. Acoso cibernético (cyberstalking)
5-4.1. Tipos de cyberstalking
5-4.2. Análisis comportamental del ciberacoso
5·5· Acoso sexual cibernético

5.6. Ciberintimidación, "mato neo digital" o cyberbullying
5.6.1. Características del cyberbullying
• Impacto
• Víctimas y perpetradores
• Ubicación
• Anonimato
• Motivación de la intimidación
• Evidencia
5.6.2. Medios de intimidación cibernética
Teléfono móvil
• Correo electrónico
• Mensajería instantánea (1M)
• Salas de chat y tableros de mensajes
• Redes sociales
• Juegos en la web
5.6.3. Tipos de cyberbullying
• Acecho o acoso
• Amenazas e intimidación
• Vilipendio o difamación
• Rechazo o exclusión de pares
• Publicación o envío de información o imágenes
personales o privadas
5.7. Pensamiento crítico de un experto en
ciberseguridad y cibercriminología
Capítulo 6.
Narcotráfico online: desde las calles al Internet
6.1. La Ruta de la Seda: la evolución del tráfico de
estupefacientes .
6.1.1. Ventas
6.2. Análisis criminológico del "más grande mercado
de drogas online"
6.3. El mercado negro en Internet y la tendencia
juvenil a adquirir drogas online
6.3.1. Metodología
6.3.2. Uso de las sales de baño en el área de Tayside en Escocia
6.3.3. Los resultados del estudio
6-4. Revelando la financiación del narcotráfico en la
red oscura (darknet)
6.5. Implicaciones de política para el control del
narcotráfico en línea
6.6. Pensamiento crítico de un experto en
ciberseguridad y cibercriminología

PARTE 11. VICTIMOLOGÍA y VICTIMIZACIÓN EN EL CIBERESPACIO: EL IMPACTO DE LOS DELITOS
INFORMÁTICOS

Capítulo 7.
Victimización causada por el cibercrimen
7.1. La oportunidad para el cibercriminal y el impacto del daño causado
7.2. Aspectos de la victimización online
7.2.1. Nivel primario o directo
7.2.2. Nivel indirecto o secundario

~

• Espacio slack
• Espacio libre
15·2. Información y equipos como evidencia en una
investigación
15.2.1. Contrabando o frutos del crimen 15.2.2. Instrumentos
15.2.3. Evidencia
15·3· Entendiendo una investigación criminal con informática forense

15.3.1. Personal forense
• Investigadores forenses
• Profesionales de TI
• Manejadores de incidentes
• 15.3.2. Principios y requisitos operativos para la investigación forense
15.4. Búsqueda legal de la evidencia digital
15.4.1. El requisito de la orden de registro
15.4.2. Doctrinas de búsqueda de evidencia tecnológica
sin orden judicial
15.5. Incautar evidencia digital
15.5.1. Etapa 1. Recopilar datos preliminares en el sitio
15.5.2. Etapa 2. Determinar el entorno para la investigación
15.5.3. Etapa 3. Asegurar y transportar evidencia
Documentar
Etiquetar
• Embalaje
• Transporte
15.5.4. Tratamiento del sospechoso
15.5.5. Reglas con dispositivos móviles (teléfonos y tabletas)
15.6. Pensamiento crítico de un experto en ciberseguridad y cibercriminología
Capítulo 16.
Informática forense e investigación aplicada al
sector público y privado
16.1. Las seis preguntas básicas
16.2. El proceso de la informática forense (REAR)
16.2.1. Recolectar
Imágenes forenses
- Archivo de imagen de flujo de bits (Bit Stream)

- Clon de unidad de flujo de bits (clon de unidad de disco directa)
• Hash/verificación
16.2.2. Examinar
•Localización de los archivos
•Extracción de los datos
16.2.3. Analizar
16.2-4. Reportar
16.3. Usar programas forenses
16.3.1. Visualizadores de archivos
16.3.2. Descomprimir archivos
16.3.3. Visualización gráfica de estructuras de directorios
16.3-4. Identificar archivos conocidos
16.3.5. Búsquedas de cadenas y coincidencias de patrones
16.3.6. Acceso a metadatos de archivos

16-4. Informática forense aplicada
16.4.1. Investigando el phishing
• Información del registrante del dominio
• Método de pago del dominio
• Dirección IP del dominio de phishing
• 16-4.2. Reconstruir un ataque por virus
• Revisión del código
• Registro e incautación
• Reconstruir la intrusión
• Visitar al sospechoso
1•Guías y protocolos
16-4.3. Rastreando ciberacosadores
• Cómo mejorar el nivel de cooperación de las
~timH
Medios a rastrear
Medidas de respuesta al acoso cibernético
16-4-4. Conteniendo el cyberbullying

• Desde el lado de las víctimas
• Dispositivos móviles
• Correos electrónicos
• Mensajería instantánea
• Salas de chat
• Redes sociales
• Identificando al intimidador (o bully)
16.5. Pensamiento crítico de un experto en ciberseguridad y cibercriminología
REFERENCIAS
Apéndice A. Análisis cualitativo del ciberofensor
motivado y el objetivo adecuado: desafíos metodológicos
en el estudio del hacker
Apéndice B. Listado de tablas
Apéndice C. Listado de figuras
CIBERGLOSARIO