13/06/2023

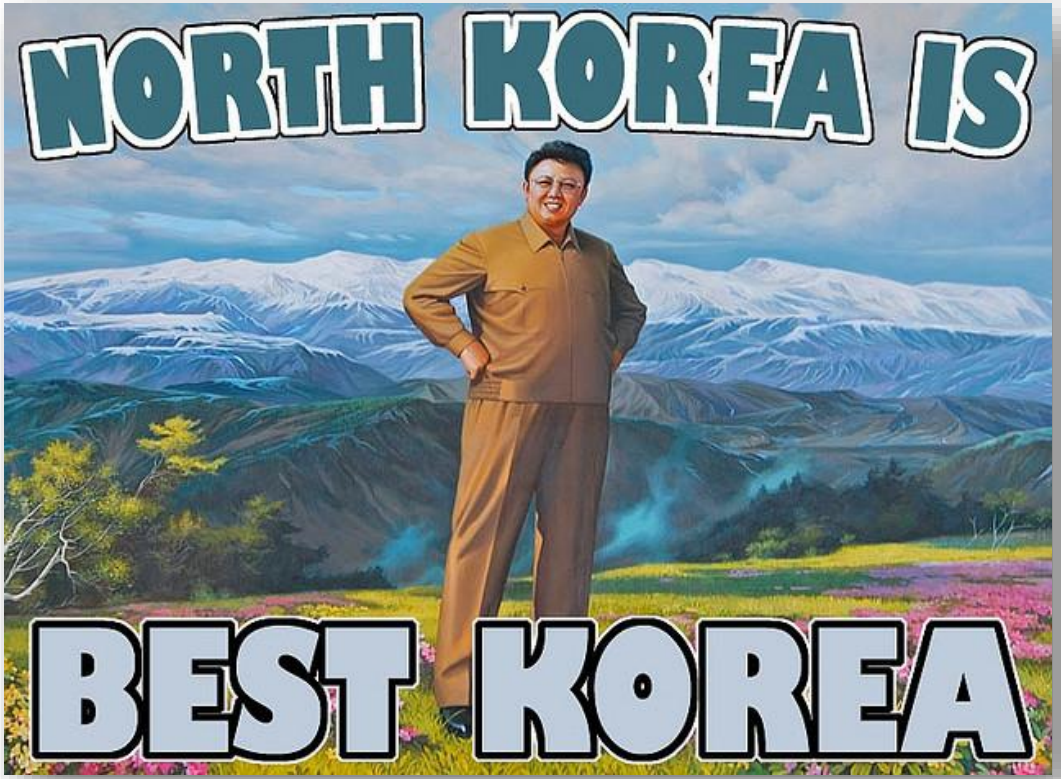
Siguiendo el rastro al Grupo APT Lazarus y sus actividades

Josep Albors

Responsible de investigación y concienciación

Digital Security
Progress. Protected.

Bienvenidos a Corea del Norte



Falta de comida y problemas de salud

BBC Sign in Home News Sport Reel Worklife

NEWS

Home | War in Ukraine | Coronation | Climate | Video | World | UK | Business | Tech | Science

North Korea food crisis looms behind displays of military prowess

22 February

The country is no stranger to chronic food shortages

North Korea tells officials that 350,000 people died of diseases this year

Many of the deaths are likely related to COVID-19, sowing doubt about officially reported figures.

By Chang Gyu Ahn and Jieun Kim for RFA Korean
2022.09.29

Army medics involved medicine distribution work amid the COVID-19 pandemic in Pyongyang, North Korea, May 22, 2022.

KCNA via Reuters

North Korea sees spike in tuberculosis cases

"North Korea still lacks sufficient facilities and technology to diagnose tuberculosis, as well as the proper drugs to treat it," an expert told Daily NK

By **Seulkee Jang** - 2024.02.05 10:30am

North Korean doctors in a photo published in the Rodong Shinmun on Nov. 30, 2021. (Rodong Shinmun - News 1)

Desarrollo aeroespacial

NK NEWS MAY 02, 2023

North Korea says it tested 'Hwasong-18' solid-fuel ICBM for first time

'Successful' test should cause enemies to 'suffer from fear and anxiety,' Kim Jong Un says

Colin Zwirko April 14, 2023

New Hwasong-18 ICBM reportedly being launched on April 13, 2023 | Image: Rodong Sinmun (April 14, 2023)

North Korea claims successful launch of spy satellite after prior failures

22 November 2023

North Korea missile tests

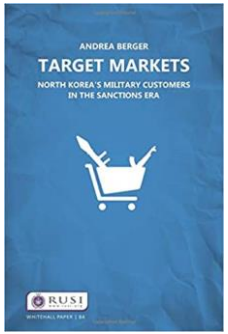
A spy satellite is a coveted prize for North Korean leader Kim Jong Un

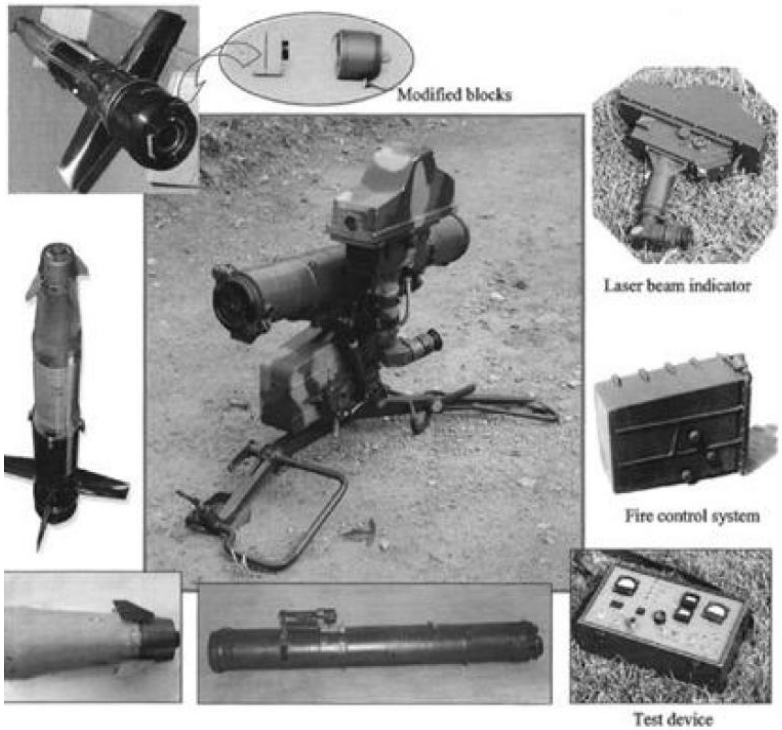
By Kathryn Armstrong & Kelly Ng

in London and Singapore

Industria militar

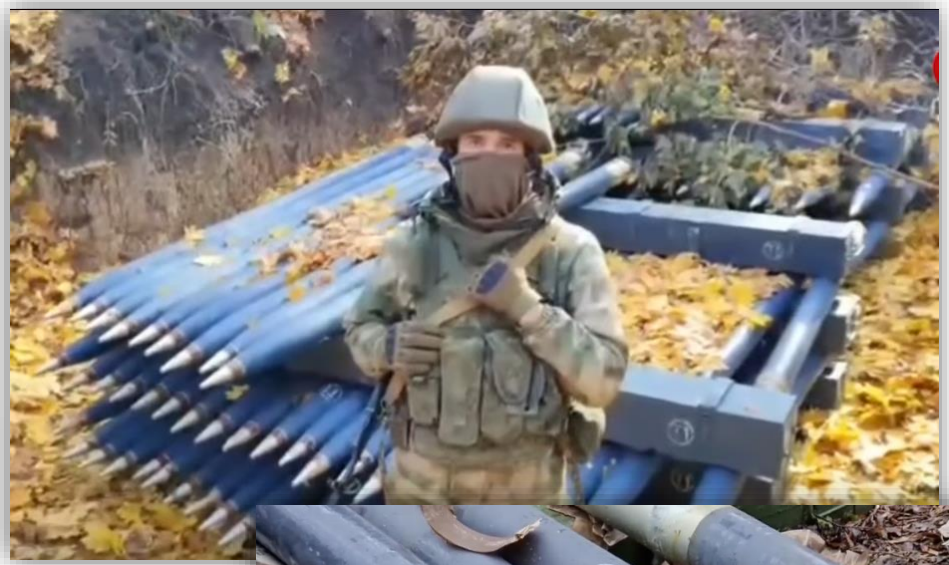
- Catálogo de exportaciones militares con productos y servicios diversos
  - Sistemas de armas convencionales
  - Piezas de repuesto
  - Munición
  - Servicios de reparación y mantenimiento
  - Diseño de armas y cadenas de producción





- Ganas de vender
- Compradores gubernamentales y privados con
- Interés en esquivar sanciones internacionales
- La calidad y la sofisticación de este material no son precisamente los más avanzados

Industria militar



Industria militar

Sanciones

CENTER FOR ARMS CONTROL AND NON-PROLIFERATION

North Korea Sanctions

Since North Korea carried out its first nuclear weapon test in 2003, it has been the target of multiple sanctions regimes in an attempt to discourage its nuclear development. The UN and the United States, as well as the European Union, Japan, South Korea, and Australia, have sanctioned North Korea over the past 16 years.

UN Sanctions

- Resolution 1718: Passed on October 14, 2006 after North Korea's first nuclear test. Imposed sanctions on heavy weaponry supplies, missile technology and material, and luxury goods.
- Resolution 1874: Passed on June 12, 2009 after North Korea's second nuclear test. Strengthened sanctions on North Korea.
- Resolution 2087: Passed on January 22, 2013 after North Korea's satellite launch. Condemned the launch and North Korea's nuclear program activities.
- Resolution 2094: Passed on March 7, 2013 after North Korea's third nuclear test. Imposed harsher sanctions, expanding the list of sanctioned industries and individuals.
- Resolution 2270: Passed on March 2, 2016 after North Korea's fourth nuclear test. Imposed broader sanctions, including the banning of states from supplying North Korea with aviation fuel.
- Resolution 2321: Passed on November 30, 2016 after North Korea's fifth nuclear test. Expanded sanctions, including a ban on mineral exports and the sale of helicopters.
- Resolution 2371: Passed on August 5, 2017 after North Korea's two ICBM tests. Expanded sanctions, including a ban on coal and iron exports.
- Resolution 2375: Passed on September 11, 2017 after North Korea's sixth nuclear test. Expanded sanctions, including a ban on natural gas imports and textile exports, and a limited ban on refined petroleum and crude oil imports and labor exports.
- Resolution 2397: Passed on December 22, 2017. Expanded sanctions, including restrictions on oil imports and metal, agricultural, and labor exports.

US, South Korea issue fresh North Korea sanctions on 'illicit' IT workforce

By Christopher Bing and Doina Chiacu

May 24, 2023 12:28 AM GMT+2 · Updated 13 days ago

U.S. and North Korean national flags are seen at the Capella Hotel on Sentosa island in Singapore June 12, 2018. REUTERS/Jonathan Ernst/File Photo

Estado mafioso

WIKIPEDIA
The Free Encyclopedia

Search Wikipedia

Illicit activities of North Korea

6 languages

Article Talk Read Edit View history Tools

From Wikipedia, the free encyclopedia

The alleged **illicit activities of the North Korean state** include manufacture and sale of illegal drugs, the manufacture and sale of counterfeit consumer goods, human trafficking, arms trafficking, wildlife trafficking, counterfeiting currency (especially the United States dollar and Chinese yuan), terrorism, and other areas.[1][2][3] It is alleged many of these activities are undertaken at the direction and under the control of the North Korean government and the ruling Workers' Party of Korea, with their proceeds going towards advancing the country's nuclear and conventional arms production, funding the lifestyles of the country's elite, and propping up the North Korean economy.[4]

Capacidades cyber

Criminales más buscados

WANTED BY THE FBI

JON CHANG H

Conspiracy to Commit Wire Fraud and Bank Fraud; Cons
Related Fraud (Computer Intrus

DESCRIPTION

Aliases: Quan Jiang, Alex Jiang	
Place of Birth: Democratic People's Republic of Korea (North Korea)	**Hair:** Black
Eyes: Brown	**Sex:** Male
Race: Asian	**Languages:** English

REMARKS

Jon is a North Korean citizen last known to be in North Korea. Jon has traveled to China in the

WANTED BY THE FBI

KIM IL

Conspiracy to Commit Wire Fraud and Bank Fraud; Consp
Related Fraud (Computer Intrusi

DESCRIPTION

Aliases: Julien Kim, Tony Walker	
Place of Birth: Democratic People's Republic of Korea (North Korea)	**Hair:** Black
Eyes: Brown	**Sex:** Male
Race: Asian	**Languages:** English,

REMARKS

Kim is a North Korean citizen last known to be in North Korea. Kim has traveled to Singapore and
birth in 1994.

WANTED BY THE FBI

PARK JIN HYOK

Conspiracy to Commit Wire Fraud and Bank Fraud; Conspiracy to Commit Computer-Related Fraud (Computer Intrusion)

DESCRIPTION

Aliases: Jin Hyok Park, Pak Jin Hek, Pak Kwang Jin	
Place of Birth: Democratic People's Republic of Korea (North Korea)	**Hair:** Black
Eyes: Brown	**Sex:** Male
Race: Asian	**Languages:** English, Korean, Mandarin Chinese

REMARKS

Park is a North Korean citizen last known to be in North Korea. Park has traveled to China in the past and has reported dates of birth in 1984 and 1981.

Campañas de Lazarus

SONY PICTURES

Capacidades cyber

Lazarus es un actor de amenazas vinculado a Corea del Norte que realiza ciberataques alineados con los objetivos del pais.

Campañas de Lazarus 2022-2023

Date	Theme	Country	Activity type	Industry
2022-01	**BAE Systems**	**Turkey**	**Operation In(ter)ception**	**Defense**
2022-01	Lockheed Martin	Italy	Operation In(ter)ception	
2022-02	JP Morgan Chase	Ukraine	DangerousPassword	
2022-03	**Programming challenges**	**Spain**	**Operation DreamJob**	**Aerospace**
2022-03	Northrop Grumman	Turkey	Operation In(ter)ception	Defense
2022-03	Airbus	South Africa	Operation DreamJob	
2022-04		Italy	DangerousPassword	Media
2022-04		Canada	DangerousPassword	Finance
2022-07	Coinbase	Argentina	Operation In(ter)ception	Trading
2022-07	New Salary Adjustments	Israel	DangerousPassword	Crypto
2022-09	**MUFG**	**Tanzania**	**DangerousPassword**	**Finance**
2022-11	Signature Bank JDs	Poland & USA	Operation In(ter)ception	Trading & Finance
2023-01	**Accenture**	**India**	**Operation DreamJob**	**Tech**
2023-02	Boeing	Poland	Operation DreamJob	Defense
2023-02		Netherlands	DangerousPassword	Trading/Crypto

Campañas de Lazarus

Vulnerabilidades

Campañas de Lazarus 2023

Lazarus hackers drop new RAT malware using 2-year-old Log4j bug

By Bill Toulas

December 11, 2023 04:25 PM 0

The notorious North Korean hacking group known as Lazarus co
44228, aka "Log4Shell," this time to deploy three previously unse
DLang.

SUPPLY CHAIN SECURITY

North Korean Hackers Exploiting Recent TeamCity Vulnerability

Multiple North Korean hacking groups have exploited a recent Tear
vulnerability and Microsoft warns of potential supply chain attacks

By Ionut Arghire
October 19, 2023

**Multiple North Korean threat actors have been observed exploiting a rec
vulnerability in JetBrains' TeamCity continuous integration and continuo
deployment (CI/CD) server, Microsoft warns.**

Tracked as CVE-2023-42793, the critical-severity flaw allows unauthentic
attackers to execute code remotely on vulnerable on-premises TeamCity ir
gain administrator-level permissions.

JetBrains released patches for the bug on September 21, with the first in-t
exploitation attempts reported only one week later.

Lazarus hackers target Windows IIS web servers for initial access

By Bill Toulas

May 29, 2023 09:00 AM 1

The notorious North Korean state-backed hackers, known as the Lazarus Group, are now targeting vulnerable Windows Internet Information Services (IIS) web servers to gain initial access to corporate networks.

Ataques de cadena de suministro

Campañas de Lazarus 2023

North Korean Cyberspies Target GitHub Developers

The North Korean APT is setting up legitimate accounts on GitHub and social media platforms to pose as developers or recruiters — ultimately to fool targets into loading npm repositories with malicious code.

Elizabeth Montalbano, Contributing Writer
July 24, 2023

4 Min Read

SOURCE: BEEVBRIGHT VIA SHUTTERSTOCK

The North Korean state-sponsored Lazarus adv
with yet another impersonation scam, this time
legitimate GitHub or social media accounts.

Lazarus hackers deploy fake VMware PyPI packages in VMConnect attacks

By **Bill Toulas**

August 31, 2023 02:47 PM 0

North Korean state-sponsored hackers have uploaded malicious packages to the PyPI (Python Package Index) repository, camouflaging one of them as a VMware vSphere connector module named vConnector.

Microsoft: Lazarus hacke
CyberLink in supply chai

By **Sergiu Gatlan**

November 22, 2023 01:06 PM 0

Microsoft says a North Korean hacking group has breached Taiwanese multimedia software company CyberLink and trojanized one of its installers to push malware in a supply chain attack targeting potential victims worldwide.

Lazarus Hackers Repeatedly Breach Developer to Deploy SIGNBT Malware

/ News / By protergomarketing

The Lazarus hacking group has persistently breached a software vendor despite patches and warnings from the developer. These repeated breaches suggest that the hackers were intent on stealing valuable source code or manipulating the software supply chain.

The breach was uncovered in July 2023, revealing that Lazarus employed a diverse infection chain and post-compromise toolset. This attack is part of a broader campaign where Lazarus targeted multiple software vendors from March to August 2023.

Ataques relacionados con criptomonedas

Campañas de Lazarus 2023

FBI: North Korean hackers stole $100 million in Harmony crypto hack

By Bill Toulas

January 24

The FBI has confirme
'Lazarus' and APT38
million worth of Ethe
2022

Lazarus hackers linked to $60 million

Blockchain analysts blame the North Korean La
group for a recent attack on payment processin
where the attackers stole almost $60 million in

3,000,000,000$

Estonian crypto-payments service provider CoinsPaid has announced that it experienced a cyber attack on July 22nd, 2023, that resulted in the theft of $37,200,000 worth of cryptocurrency.

North Korea's state hackers stole $3 billion in crypto since 2017

North Korean-backed state hackers have stolen an estimated $3 billion in a long string of hacks targeting the cryptocurrency industry over the last six years since January 2017.

Operaciones destacadas

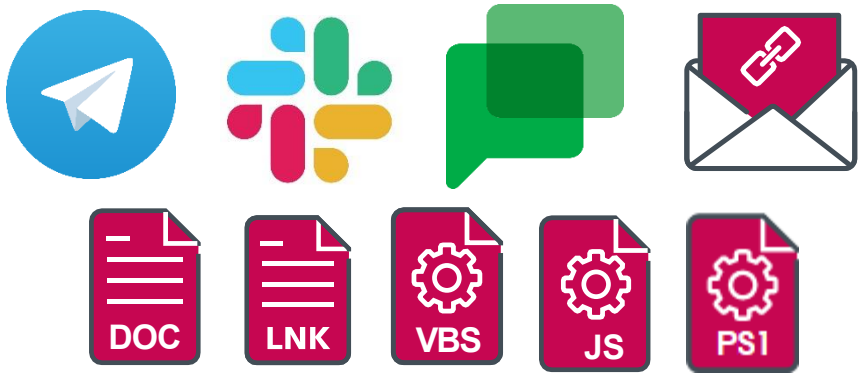
Lazarus: DangerousPassword

Descubrimiento

ThreatBook

Objetivos

Acceso inicial



Finalidad

Lazarus: Operation In(ter)ception

Descubrimiento

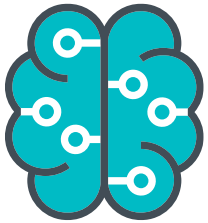
Digital Security
Progress. Protected.

Objetivos

Acceso inicial

LinkedIn

Finalidad



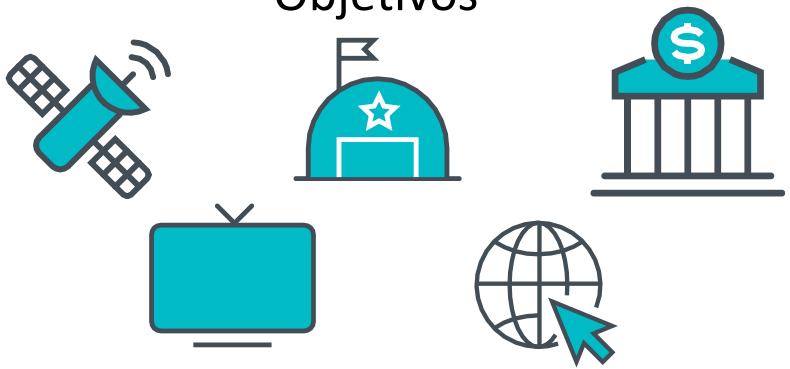
BEC

Lazarus: Operation DreamJob

Descubrimiento

ClearSky®

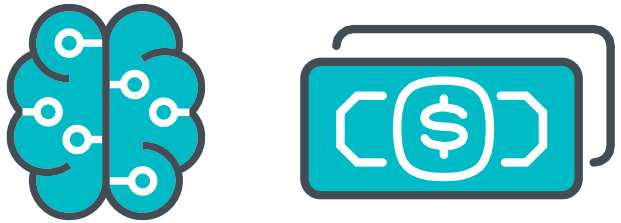
Objetivos



Acceso inicial

LinkedIn

Finalidad



?

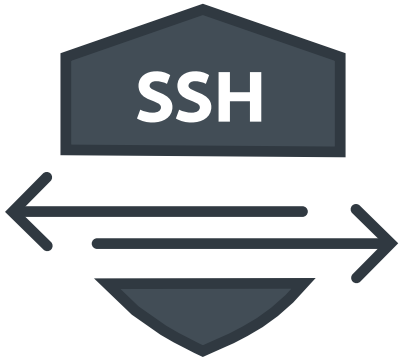
Temática: Areoespacial/Militar

Temática: Financias/Cryptomonedas

Temática: Medios/Tecnología

Diferentes escenarios

Lectores PDF troyanizados



Herramientas de red troyanizadas

Retos de programación troyanizados

Escenario I: lectores PDF

SumatraPDF
(Krzysztof Kowalczyk)

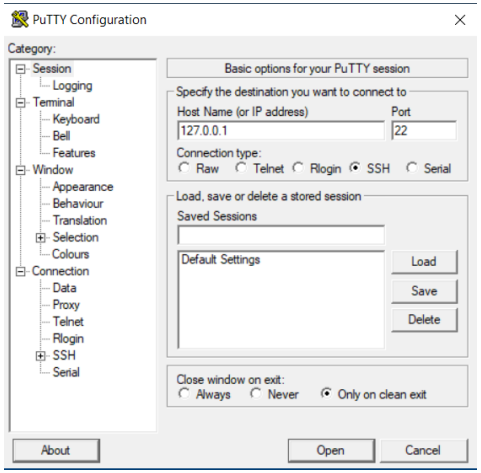
MµPDF
(Artifex)

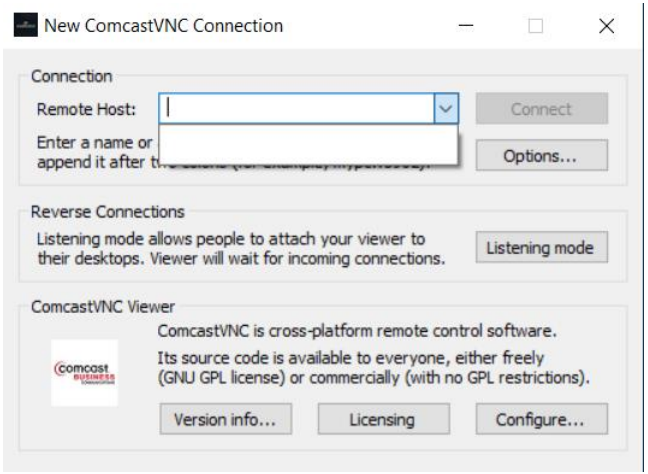
PDF Viewer
WinForms
(DevExpress)

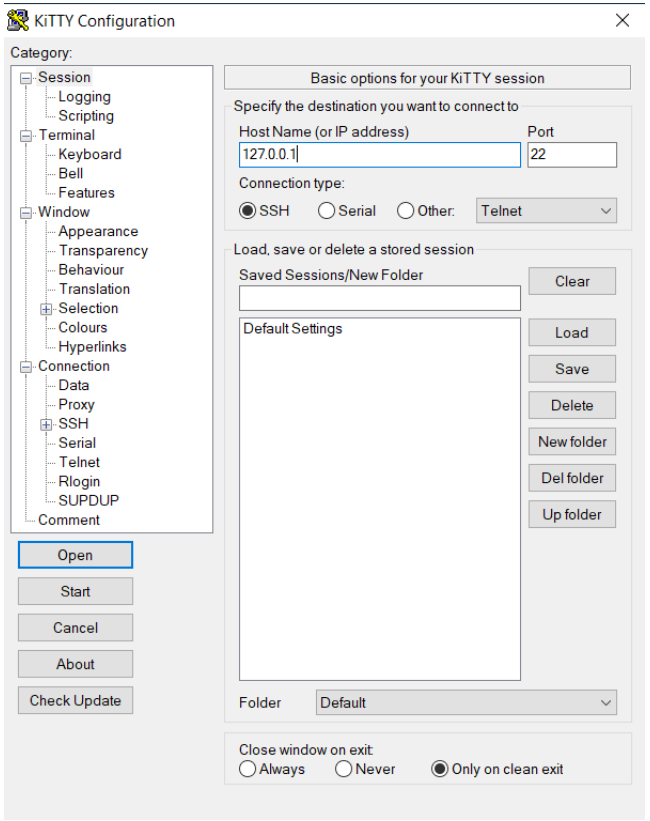
Tinker (Julius
Oklamcak)

- Visores de PDF funcionales troyanizados
- Acción maliciosa activada por un document PDF específico
- Se fuerza a la víctima a que utilice el software proporcionado
- Se descarga un fichero PDF, se muestra su contenido y se inicia la acción maliciosa

Escenario II: herramientas de red







- Clientes SSH troyanizados y herramientas de control remote
- Acción maliciosa activada por una conexión específica proporcionada por los atacantes
- Se obliga a la víctima a utilizar el software troyanizado

Scenario III: desafíos de programación

C:\tools\Quiz1.exe

```
Hello_World!
10
0 1 2 3 4 5 6 7 8 9
The End!
```

- Empaquetados en imágenes ISO con ficheros adicionales
- Aplicaciones de consola básicas
- Ambos ejemplos ejecutan la misma cadena de eventos maliciosos

C:\tools\Quiz2.exe

```
Start program
Input : 3537
1 2 3 5 8 13 21 34 55 89 144 233 377 610 987 1597 2584
Finished!
```

Lazarus: Payloads

- **NickelLoader**
- (mini-)BlindingCan
- LightlessCan
- ImprudentCook
- **ScoringMathTea**
- WebbyTea
- PostNapTea
- BackbitingTea
- SecondhandTea
- …

- **Inicial**: Droppers, loaders, downloaders simples
  - Fuerte cifrado, la clave se pasa como argumento usando la linea de comandos.
- **Posterior**: Downloaders complejos y RATs con muchas capacidades
  - Difíciles de adquirir
    - ➢ No están presentes en el sistema de ficheros en un formato sin ofuscar
    - ➢ Configuración de binarios
  - Múltiples servidores C&C

La sa
es en

Sector objetivo: empresa aeroespacial española

Steve Dawson (He/Him)
Recruiter at Meta

18 MAR

Attacker

Steve Dawson (He/Him) • 8:56

Hello [redacted] thank you for adding me to your network.
Hope you are doing well and safe.
How are you doing?

Victim • 12:25

Hi, I'm fine.

Thank you for your friend request!

LUNES

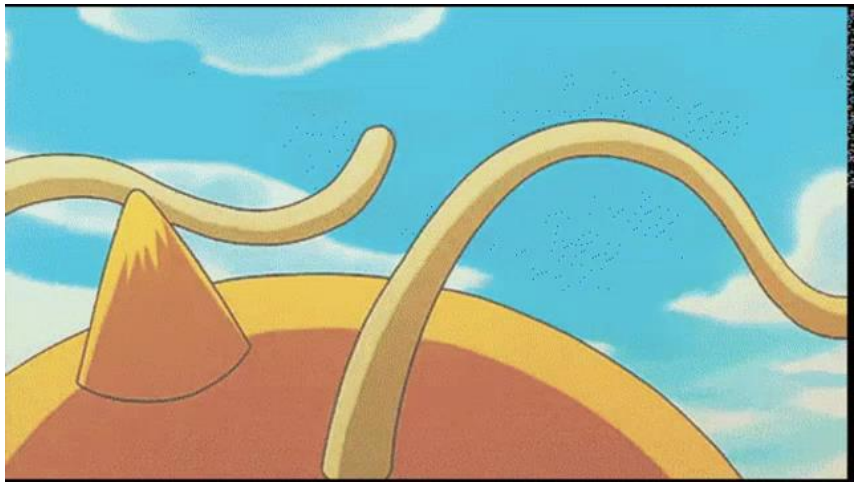
Attacker

Steve Dawson (He/Him) • 8:32

You're welcome.
Did you have a good weekend?

C:\tools\Quiz1.exe

```
Hello_World!
10
0 1 2 3 4 5 6 7 8 9
The End!
```



Tres hombres con un propósito

Peter Kálnai

Investigador Senior de Malware

ESET HQ

Josep Albors

Responsible de investigación y concienciación

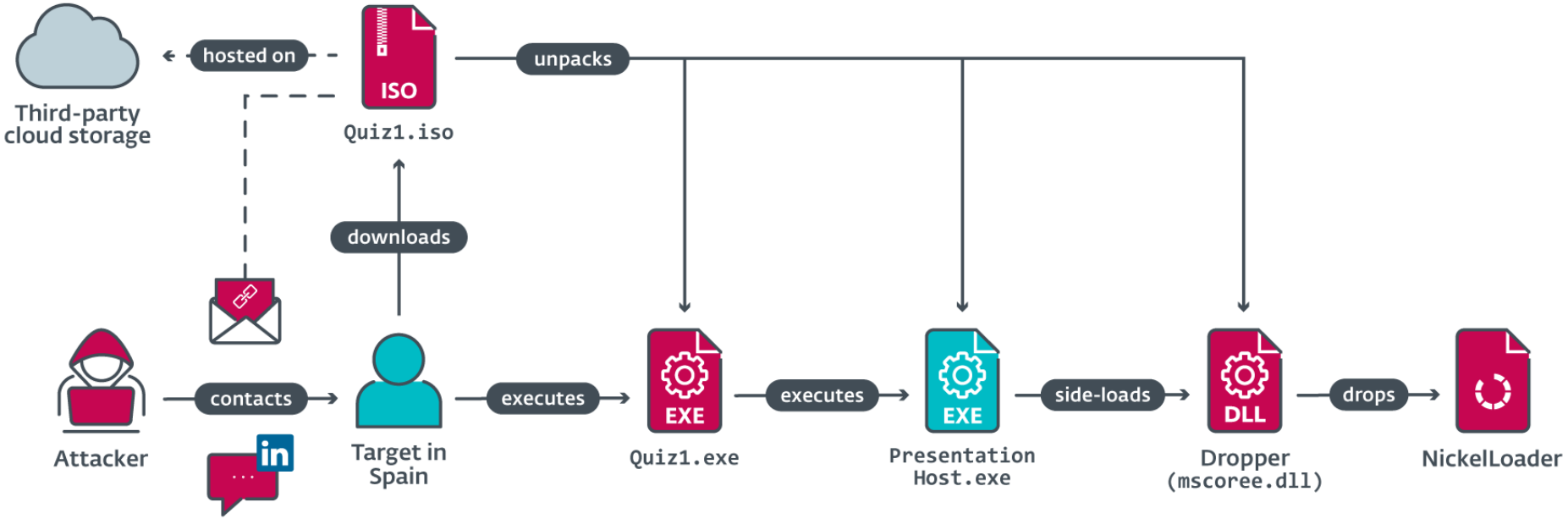
ESET España

Antonio Sanz

Responsable de DFIR and maestro de la palanqueta

S2 Grupo

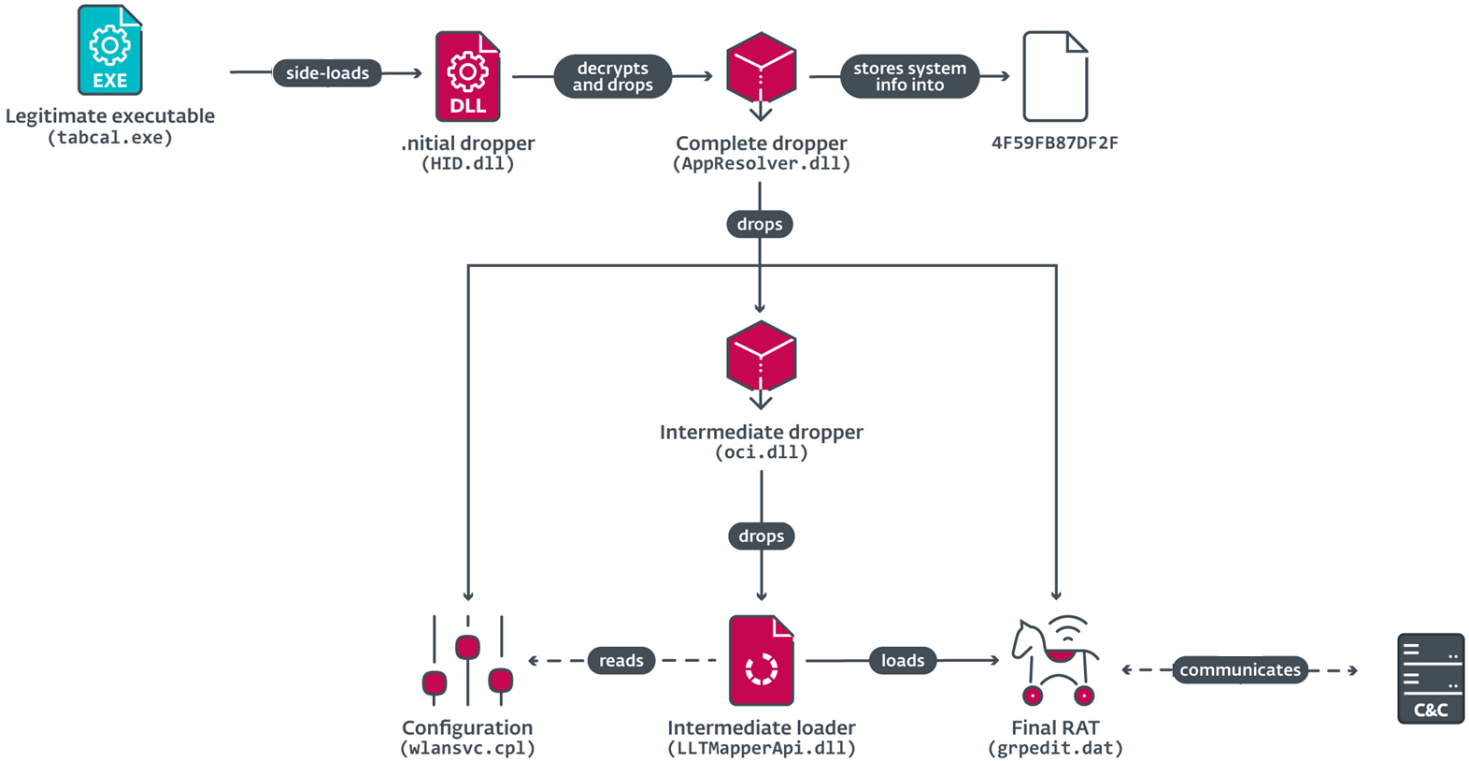
Sector objetivo: empresa aeroespacial española



Sector objetivo: empresa aeroespacial española

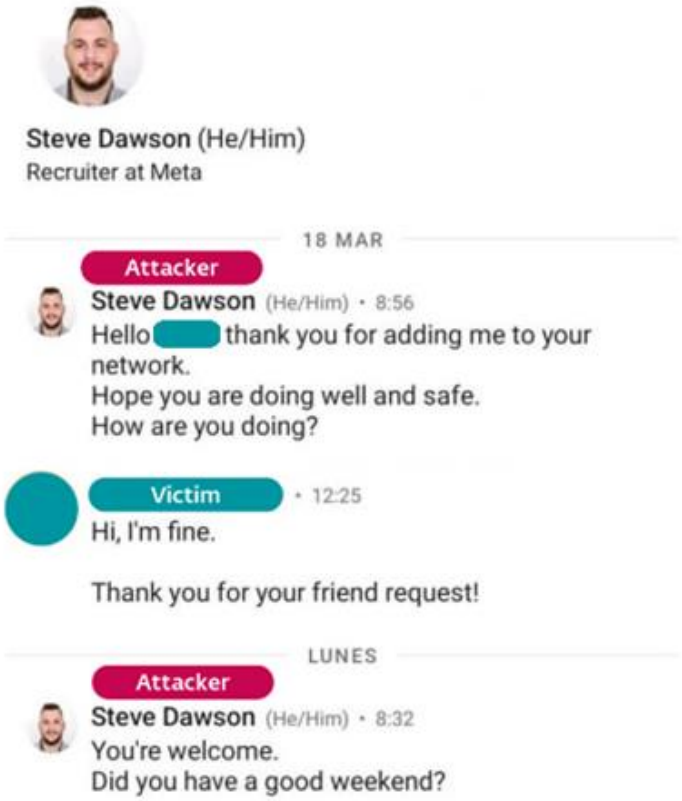
Location folder	Legitimate parent process	Malicious side-loaded DLL	Trojanized project	Final payload
C:\ProgramShared\	Presentation Host.exe	mscoree.dll	NppyPluginDll	NickelLoader
C:\ProgramData\Adobe\	colorcpl.exe	colorui.dll	LibreSSL 2.6.5	mini-BlindingCan
C:\ProgramData\Oracle\Java\	fixmapi.exe	mapistub.dll	Lua plugin for Notepad++ 1.4.0.0	LightlessCan
C:\ProgramData\Adobe\ARM\	tabcal.exe	HID.dll	MZC8051 for Notepad++ 3.2	LightlessCan

Sector objetivo: empresa aeroespacial española



“Casi siempre hay binarios o pistas en el sistema atacado que no son posibles de ver usando únicamente la telemetría del producto”.

Pistas encontradas: conversación de LinkedIn



- No es posible de adquirir usando únicamente la solución de seguridad.
- Muestra de mejor manera las características del ataque, sus TTPs y otras pistas (conversación original, suplantación de identidad, etc.)

Pistas encontradas: pequeño fichero de datos

Una clave de 16 bytes para descifrar un cifrado AES-128

- **yCD91qo0Lm7mQKGu**
- **LocalServiceNetw**
- **Tabcal.exe\x00\x00\x00\x00\x00\x00**

```
C:\ProgramData\Adobe\ARM\thumbs.db                              ↓FRO
00000000:  4C 6F 63 61-6C 53 65 72-76 69 63 65-4E 65 74 77  LocalServiceNetw
00000010:  6F 72 6B 52-65 73 74 72-69 63 74 65-64           orkRestricted
```

A	B	G
2021-02-22 07:49:02	2022-03-25 08:26:29	\ProgramData\Adobe\ARM
2021-11-30 08:14:46	2022-03-25 08:26:29	\ProgramData\Adobe\ARM\{291AA914-A987-4CE9-BD63-0C0A92D435E5}
2021-02-22 08:00:54	2022-03-25 08:26:29	\ProgramData\Adobe\ARM\{291AA914-A987-4CE9-BD63-AC0A92D435E5}
2021-11-30 08:53:53	2022-03-25 08:26:29	\ProgramData\Adobe\ARM\Acrobat_21.007.20099
2022-01-17 08:00:08	2022-03-25 08:26:29	\ProgramData\Adobe\ARM\Acrobat_21.011.20039
2022-03-23 10:22:45	2022-03-24 15:57:48	\ProgramData\Adobe\ARM\HID.dll
2021-11-29 17:47:54	2022-03-25 08:26:29	\ProgramData\Adobe\ARM\OnDemand
2021-10-18 07:32:06	2022-03-25 08:26:29	\ProgramData\Adobe\ARM\Reader_21.007.20099
2022-03-23 10:38:01	2022-03-23 10:38:35	\ProgramData\Adobe\ARM\tabcal.exe
2022-03-23 10:38:14	2022-03-24 15:57:48	\ProgramData\Adobe\ARM\thumbs.db
2022-03-22 09:00:03	2022-03-22 09:00:03	\ProgramData\Adobe\colorcpl.exe
2021-02-19 13:55:35	2022-03-25 08:26:29	\ProgramData\Adobe\Temp
		\ProgramData\Adobe\colorui.dll (path donde debería de estar, eliminada por

Comunicación con un usuario

- Posibles vías de contacto
  - Directo: Detalles de contacto ya existentes pero sin confinaza establecida
  - Distribuidor: Confianza ya establecida
  - Fuerzas y cuerpos de Seguridad / CERT Local

- Mayor interés de la víctima para cooperar
  - Bloqueo del ataque en curso

- Reacciones
  - Aspecto psicológico: miedo y ansiedad por parte del usuario
  - Borrado de pruebas. Ausente por vacaciones

- Recompensa
  - Informe detallado para la empresa (IoCs, análisis técnico)

Pistas encontradas: script PHP en el lado del servidor

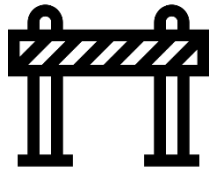
```php
<?php define('gCoECdYYhMhQqxSDArSF', 'pAJ9dk4OVq85jxKWoNfw1AG2C');
define('mOfktpaktoBEBvdPXDPQw', 'tSxEo8U5e7thdchbPv9fAydHV');
define('fVhHJGszdhxsOxxwjsV', 5);
define('QUtyJctfjrIBxywIfQnSewc', 4);
define('NypLPtjZddKRdPQgkuZaFQ', 7);
define('GtvETMvGLzAXPlVNmEsLvDA', 4);
define('ExaPshyXAuiaLUcIzAckZS', 5);
define('DuACgPSmTMKjjeAIfymsC', 6);
define('ASpjuHzSXbssqkfOPKNc', 7);
define('tBRXTDPqDiOsQBRchyegWM', 8);
define('paAqMwGORBwtwJdAxrdETk', '<!DOCTYPE html>');
define('jTEOYkiigWhxTenpJzhCo', ' ');
define('LiEGctFjANxwEQVIoAYvts', 'B8ew5jc:fGUX3AtOb9sm1TFhNP4-nYQRp
define('nENZpoYPChFMVkBoUxfzzU', '2019.gif');
define('zWzOyYXnpufsfhbtlRkI', '2020.gif');
define('yJkffOBvQNRmnAlTSCrbiVP', 170 * 1000);
define('focRURgUKhwEVkxiPqrxE', 'logo/');
$WORKS_DIR = '';
$PARAM_FIRST = '';
$PARAM_SECOND = '';
$lvFNJDnPoMbqIiqYgFpk = '';
ob_start();
```

- Facilita el análisis de las cominicaciones cliente-servidor
  - Autenticación en varios pasos
- Loggeo de session en PHP
  - Ofuscado, ~400 lineas
- Logs:

  Todos los objetivos y víctimas (incluidos aquellos fuera del alcance de la telemetría)
- Herramientas en el lado del servidor tan abuntantes como en el lado del cliente
  - Visibilidad limitada

Comunicacón con administrador web

- Dificultades para contactar
  - No es usuario de ESET



- Interés limitado en la cooperación
  - No ha sido afectado directamente por el ataque

- Reacción:
  - Ignorancia, silencio

- Posibles recompensas:
  - Arreglar las vulnerabilidades de su servidor
  - Licencias gratuitas de ESET

Objetivos

Campañas periódicas

- DangerousPassword
- Operation In(ter)ception
- Operation DreamJob

Conclusión

Herramientas troyanizadas

Empresa afectada

“Todos los delincuentes son muy atrevidos hasta que escuchan el sonido metálico de una palanqueta acercarse a sus espaldas…”

¿Preguntas?

In memoriam

@ngelucho

Digital Security
Progress. Protected.

Gracias