Lazarus campaigns and backdoors 2022-2023

Virus Bulletin 2023, London, UK

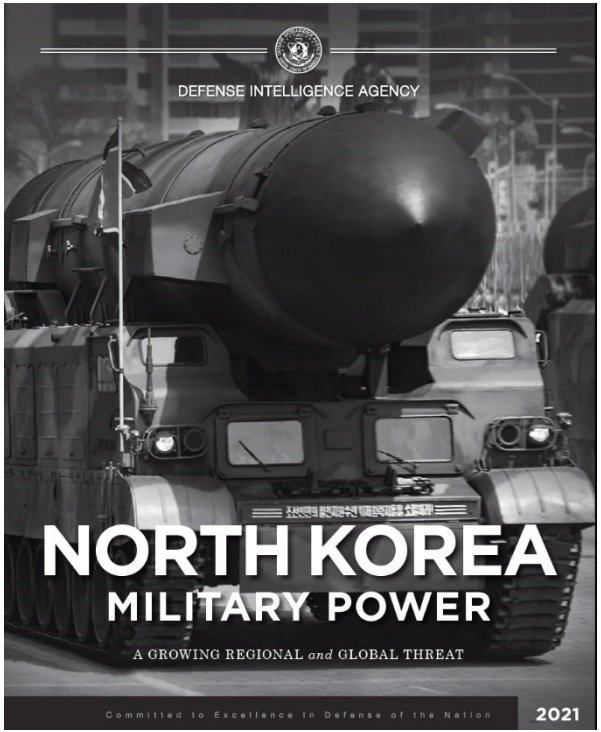
Peter Kálnai

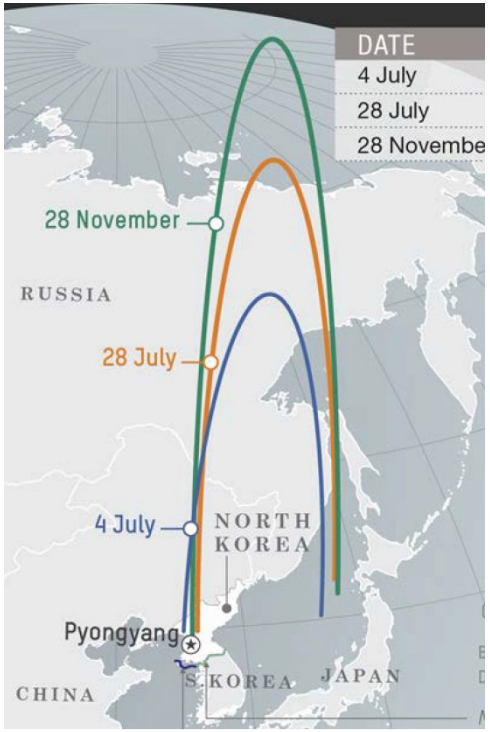
Senior Malware Researcher

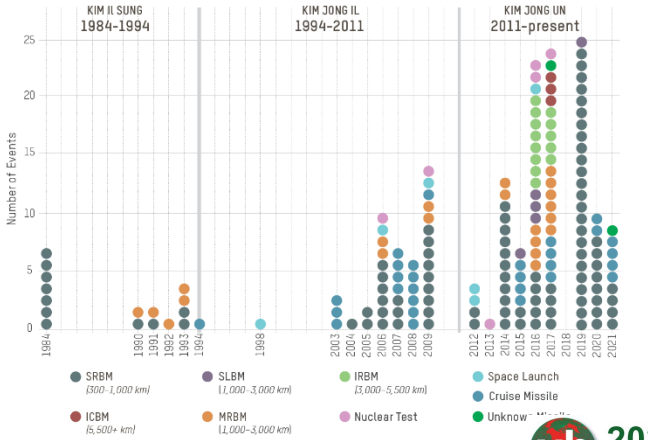
ESET Digital Security
Progress. Protected.

North Korea: facts

North Korea: Aerospace



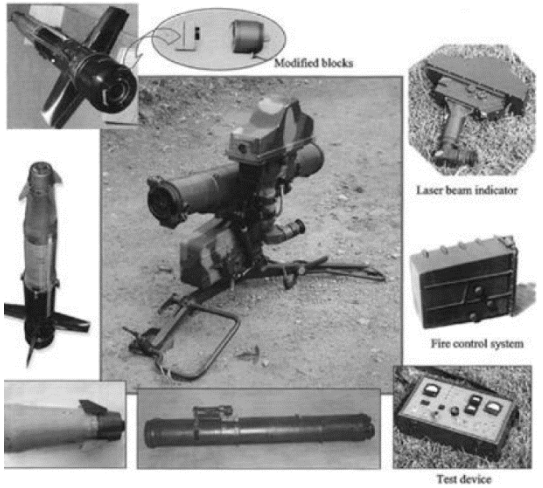




- Defense Intelligence Agency: “North Korea Military Power”, 2021

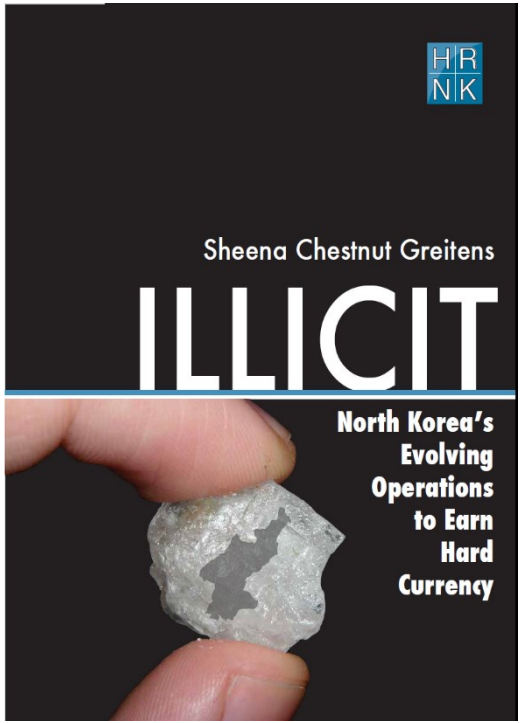
North Korea: Defense

- Defense-export catalogue of indigenous products and services:
  - Conventional weapon systems
  - Spare parts
  - Munition
  - Repair and maintenance services
  - Designs of arms and manufacturing lines
- Willingness to sell
- Business with state and non-state actors
- Quality & sophistication behind trends



- Andrea Berger: "Target Markets: North Korea's Military Customers in the Sanction Era", 2017

North Korea: Illicit activities



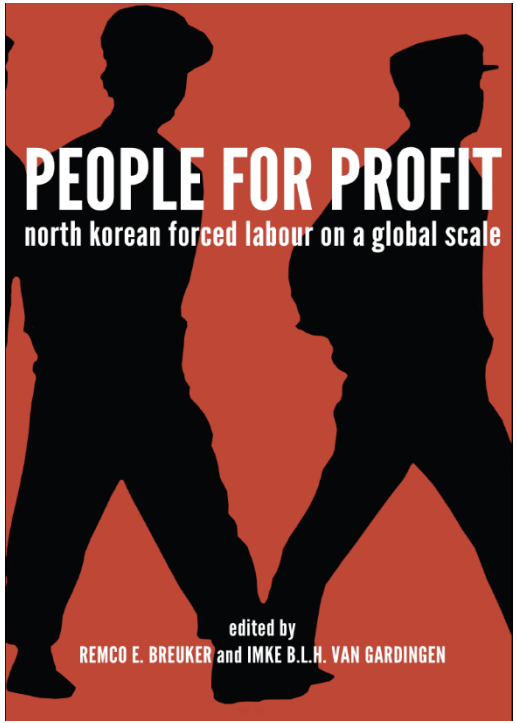
Licit earnings:

- Trade with China
- Tourism
- Remittances from abroad
- Cell phones (hardware, services)
- Kaesong Industrial Complex (defunct since 2016)

Illicit earnings:

- Manufacturing and sale of drugs
- Counterfeiting consumer goods
- Counterfeiting foreign currency
- Trafficking of wildlife
- Arms trafficking
- Export of labor, modern slavery

(Cybercrime 2014+)

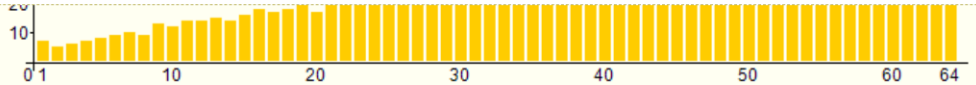


- Sheena Chestnut Greitens: "Illicit: North Korea's Evolving Operations to Earn Hard Currency", 2014
- Remco Breuker et al.: "People for Profit: North Korean Forced Labour on a Global Scale", 2017

North Korea: Technical talent

International Mathematical Olympiad

IMO 2023 IMO 2024



Year	Team size			P1	P2	P3	P4	P5	P6	Total	Rank		Awards				Leader	Deputy leader	Data qu		
	All	M	F								Abs.	Rel.	G	S	B	HM			S	N	M
2019	6	6		41	41	17	42	42	4	187	4	97.30%	3	3	0	0	Jin Hyok Kim	Jong Min Ri	•	•	•
2016	6	6		41	30	2	42	31	22	168	6	95.37%	2	4	0	0	Yong Chol Ham	Kwang Nam O	•	•	•
2015	6	6		42	25	17	42	22	8	156	4	97.09%	3	3	0	0	Yong Chol Ham	Ryong Gol Yom	•	•	•
2014	6	6		42	30	7	42	28	5	154	14	87.00%	1	4	0	1	Yong Chol Ham	Ryong Gol Yom	•	•	•
2013	6	6		42	27	21	42	41	11	184	5	95.83%	2	4	0	0	Yong Chol Ham	Kwang Il Ri	•	•	•
2012	6	6		42	30	0	30	22	4	128	12	88.89%	2	1	3	0	Yong Chol Ham	Kwang Il Ri	•	•	•
2011	6	6		39	3	36	28	42	9	157	7	94.00%	3	3	0	0		Ryong Gol Yom	•	•	•
2010	6										Disqualified								•	•	•
2009	6	6		42	35	24	39	36	7	183	5	96.12%	3	2	1	0	Yong Chol Ham	Yong Ho Kim	•	•	•
2008	6	6		40	41	29	37	24	2	173	7	93.75%	2	4	0	0	Yong Chol Ham	Yong Ho Kim	•	•	•
2007	6	6		37	35	1	40	37	1	151	8	92.39%	1	4	0	1	Ham Yong Chol	Sin Se Hung	•	•	•
1992	6			34	27	15	32	0	18	126	16	72.73%	0	3	2	0			•	•	•
1991	6										Disqualified						Jang Nam Su	Kim Song Hak	•	•	•
1990	6			29	27	9	11	24	9	109	19	66.04%	0	1	3	0			•	•	•

icpc

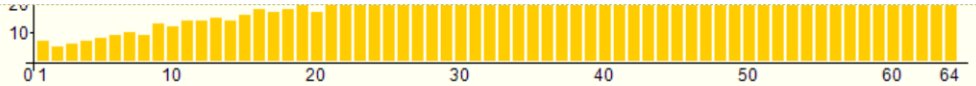
Results 2019

Place	Name	Solved
1	Moscow State University	10
2	Massachusetts Institute of Technology	9
3	The University of Tokyo	9
4	University of Warsaw	8
5	National Taiwan University	8
6	University of Wroclaw	8
7	Seoul National University	7
8	KimChaek University of Technology	7
9	Sharif University of Technology	7
10	Moscow Institute of Physics & Technology	7
11	National Research University Higher School of Economics	7
12	The Chinese University of Hong Kong	7

North Korea: Technical talent

International Mathematical Olympiad

IMO 2023 IMO 2024



Year	Team size			P1	P2	P3	P4	P5	P6	Total	Rank		Awards				Leader	Deputy leader	Data qu		
	All	M	F								Abs.	Rel.	G	S	B	HM			S	N	M
2019	6	6		41	41	17	42	42	4	187	4	97.30%	3	3	0	0	Jin Hyok Kim	Jong Min Ri	•	•	•
2016	6	6		41	30	2	42	31	22	168	6	95.37%	2	4	0	0	Yong Chol Ham	Kwang Nam O	•	•	•
2015	6	6		42	25	17	42	22	8	156	4	97.09%	3	3	0	0	Yong Chol Ham	Ryong Gol Yom	•	•	•
2014	6	6		42	30	7	42	28	5	154	14	87.00%	1	4	0	1	Yong Chol Ham	Ryong Gol Yom	•	•	•
2013	6	6		42	27	21	42	41	11	184	5	95.83%	2	4	0	0	Yong Chol Ham	Kwang Il Ri	•	•	•
2012	6	6		42	30	0	30	22	4	128	12	88.89%	2	1	3	0	Yong Chol Ham	Kwang Il Ri	•	•	•
2011	6	6		39	3	36	28	42	9	157	7	94.00%	3	3	0	0		Ryong Gol Yom	•	•	•
2010	6										Disqualified								•	•	•
2009	6	6		42	35	24	39	36	7	183	5	96.12%	3	2	1	0	Yong Chol Ham	Yong Ho Kim	•	•	•
2008	6	6		40	41	29	37	24	2	173	7	93.75%	2	4	0	0	Yong Chol Ham	Yong Ho Kim	•	•	•
2007	6	6		37	35	1	40	37	1	151	8	92.39%	1	4	0	1	Ham Yong Chol	Sin Se Hung	•	•	•
1992	6			34	27	15	32	0	18	126	16	72.73%	0	3	2	0			•	•	•
1991	6										Disqualified						Jang Nam Su	Kim Song Hak	•	•	•
1990	6			29	27	9	11	24	9	109	19	66.04%	0	1	3	0			•	•	•

icpc

Results 2019

WANTED BY THE FBI

PARK JIN HYOK

8	KimChaek University of Technology	7
9	Sharif University of Technology	7
10	Moscow Institute of Physics & Technology	7
11	National Research University Higher School of Economics	7
12	The Chinese University of Hong Kong	7

“Lazarus is a North Korean threat actor.”

FBI, US

“Lazarus is a North Korea-aligned threat actor…

ESET

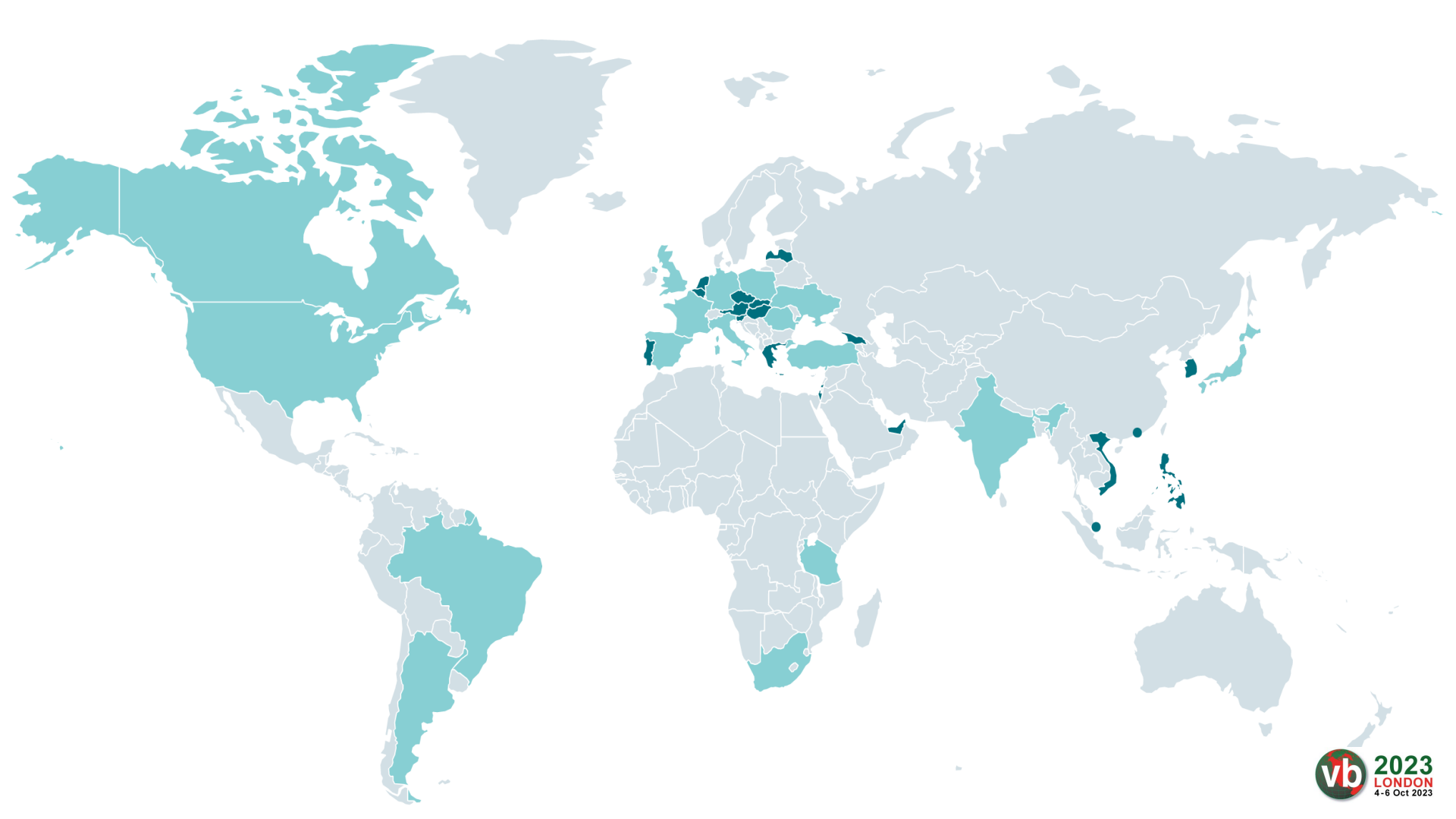
“Lazarus is a North Korea-aligned threat actor that performs cyber activities reflecting the state’s motivations in the physical world.”

ESET

Lazarus campaigns

Lazarus operations and campaigns

- **Social engineering-based:**
  - Operation In(ter)ception
  - DangerousPassword attacks
  - Operation DreamJob
- **Supply chain:**
  - WIZVERA 2020
  - Trading Technologies & 3CX 2022-2023
- **Exploitation (0-days, n-days):**
  - Campaigns against security researchers
  - South Korean targets



vb 2023 LONDON 4-6 Oct 2023

Operation In(ter)ception

Date	Country	Industry	Theme	Payloads
2022-01	Turkey	**Defense**	BAE SYSTEMS	In(ter)ception backdoor
2022-01	Italy, Spain, India, Slovenia (VT)		Lockheed Martin	
2022-02	Ukraine	**Defense**		In(ter)ception backdoor
2022-03	Turkey	**Defense**	Northrop Grumman	BackbitingTea
2022-03	Brazil		Solana	
2022-07	Argentina, Brazil	**Crypto trading**	Coinbase	
2022-12	USA, Poland	**Finance**	Signature Bank	BackbitingTea

DangerousPasswords attacks

Date	Country	Industry	Theme	Payloads
2022-02	United Kingdom (VT)		New Salary Adjustments	
2022-02	Ukraine	**Digital investment**	JP Morgan Chase	
2022-02	Poland	Defense	Pensja Adiustacja 202202101019	
2022-02	France	Defense	Lettre de veille internationale GICAN n°37 - février 2022	
2022-03	Canada	**Finance**		WebbyTea, BackbitingTea
2022-07	Israel	**Blockchain company**	New Salary Adjustment	
2022-09	Latvia	**Blockchain company**		BackbitingTea, SecondHandTea
2022-09	Tanzania	**Finance**	MUFG	
2022-12	United States	**Finance**	Signature Bank	BackbitingTea
2023-02	Netherlands	**Cryptotrading**	DocuSign - Executed Version (Secured)	SecondhandTea

Operation DreamJob

Date	Country	Industry	Theme	Payloads
2022-03	Spain	Aerospace	Programming challenges	BlindingCan, miniBlindingCan, LightlessCan, NickerLoader
2022-03	South Africa		Airbus	ImprudentCook
2022-10	Portugal, Germany (VT)		Airbus	
2022-11	Netherlands (VT)		IBM	WinInetLoader, NickelLoader
2023-01	India	Tech & Data	Accenture	mini-BlindingCan, BlindingCan. LightlessCan
2023-02	Poland	Defense	Boeing	ScoringMathTea, ImprudentCook
2023-02	SAE (VT)		Bitzlato	WebbyTea
2023-02	(VT)		Comcast	mini-BlindingCan
2023-03	Georgia (VT)		HSBC	SimpleTea for Linux
2023-05	Hungary (VT)	Nuclear energy	IBM + Rosatom	WinInetLoader

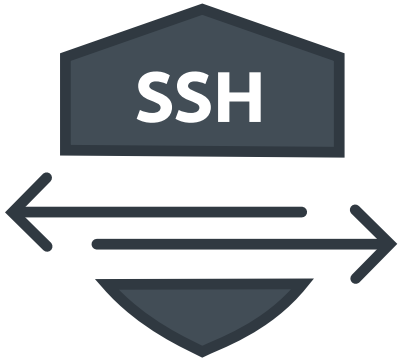
Themes I: Aerospace/Defense targets

Themes II: Finance/Crypto targets

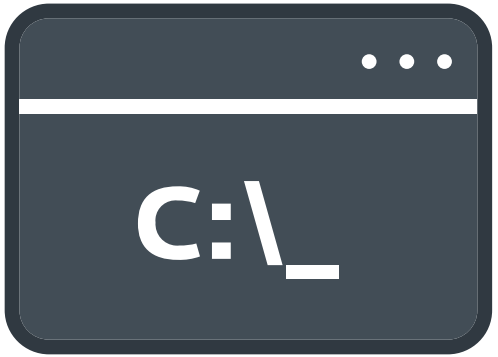
Themes III: Media/Tech targets

Scenarios in Operation DreamJob

Trojanized PDF readers



Trojanized network tools



Trojanized coding challenges

Scenario I: PDF readers

SumatraPDF (Krzysztof Kowalczyk)

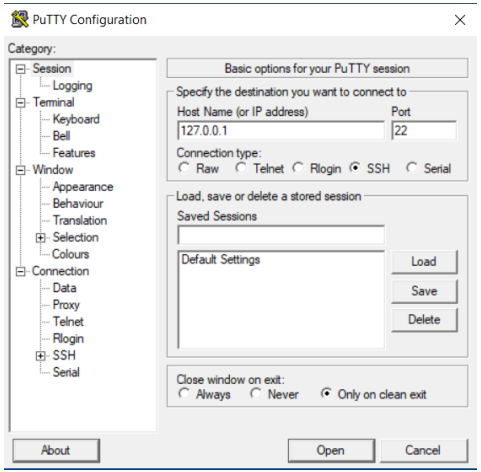
MµPDF (Artifex)

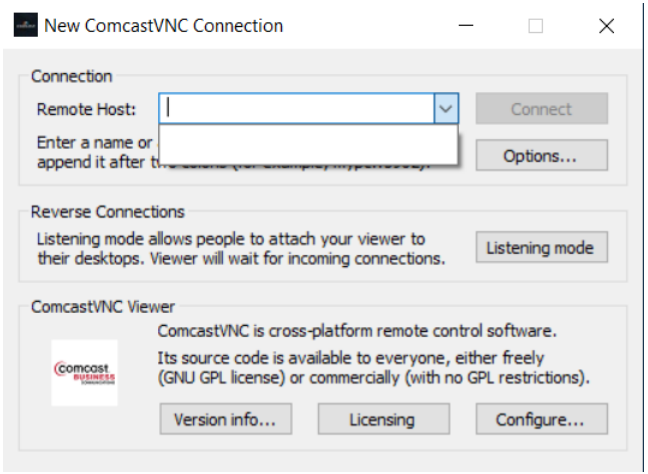
PDF Viewer for WinForms (DevExpress)

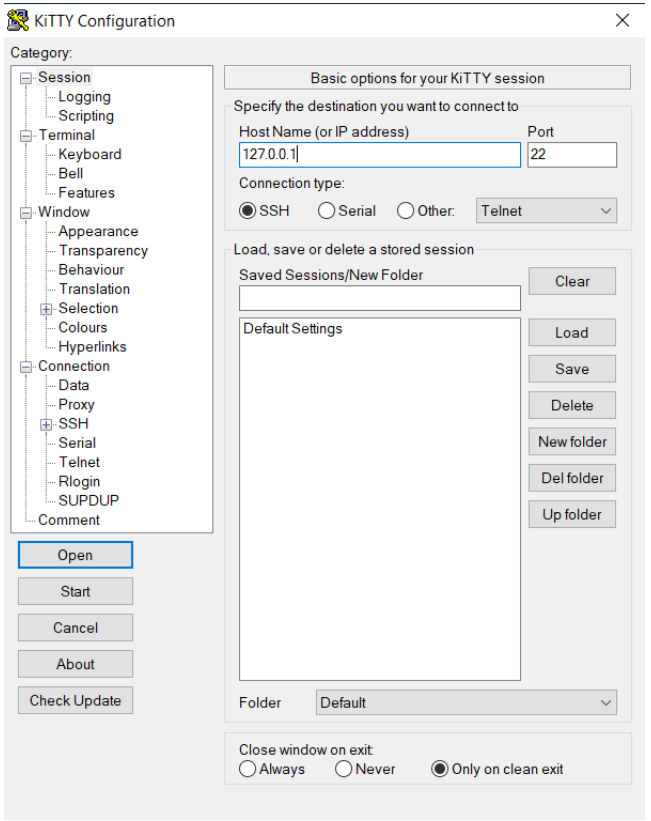
Tinker (Julius Oklamcak)

- The target provided with a trojanized working PDF viewer & an initial PDF data file
- Other PDF viewers display no job description/error message
- The target is left with no option but to execute the provided software
- Full job description downloaded/extracted and displayed
- Malicious action triggered

Scenario II: Network tools







- The target provided with trojanized SSH clients /remote tools & login details (IP + password)
- Malicious action trigged by a specific connection

Scenario III: Coding challenges

C:\tools\Quiz1.exe

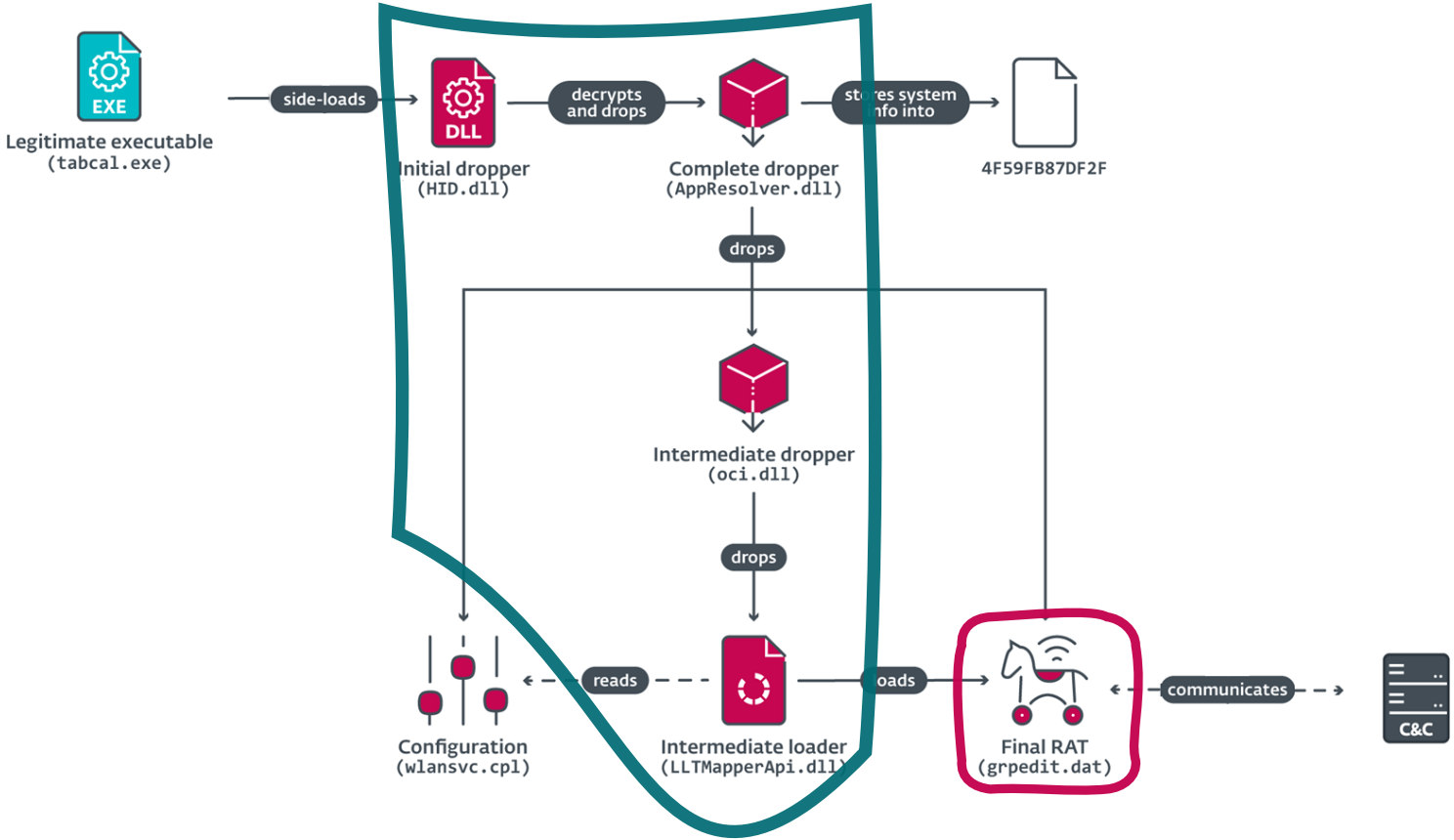
```
Hello_World!
10
0 1 2 3 4 5 6 7 8 9
The End!
```

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 backdoors

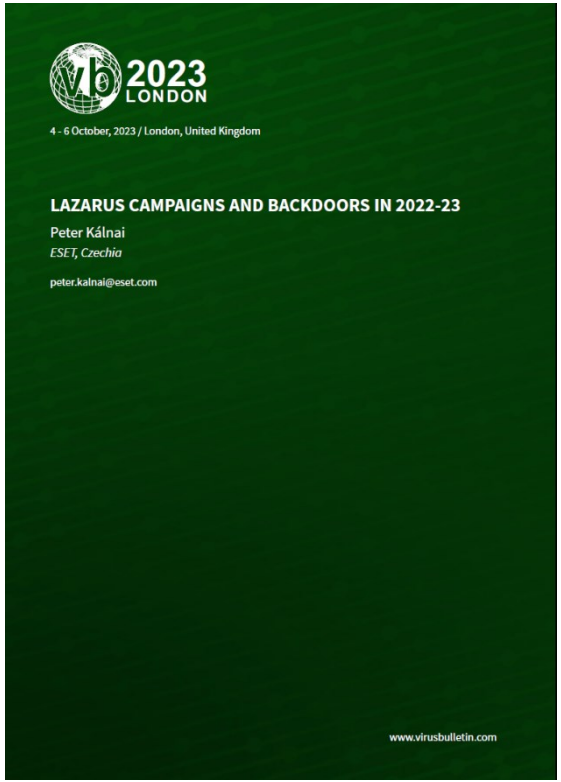
Lazarus: Execution chains



Lazarus: Payloads

- Complex downloaders and fully featured RATs
- Hard to acquire
- Not present on the file system in a plain form
- Protected with VMProtect and Themida
- Binary configuration files
- Multiple compromised servers as C&Cs

- NickelLoader**,** (mini)BlindingCan, **LightlessCan**, ImprudentCook, ScoringMathTea**,** WebbyTea, PostNapTea, BackbitingTea, SecondhandTea, etc.

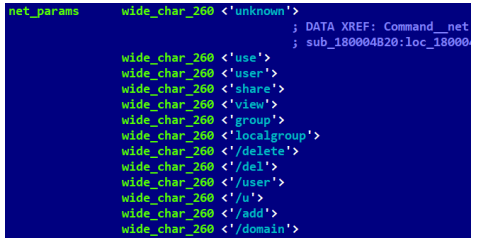


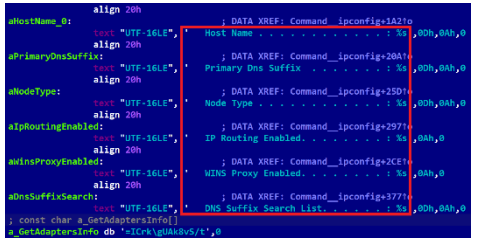
Lazarus: LightlessCan

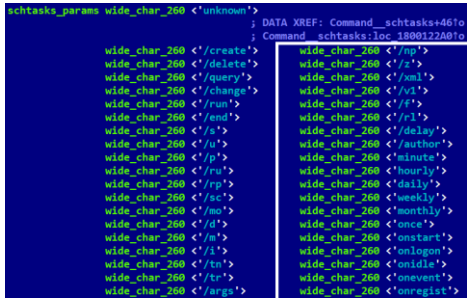
Index	Description
33	Display information about your network configuration and refresh DHCP and DNS.
34	View and configure network resources.
35	Control Windows Firewall behavior.
36	Show network status and protocol statistics.
37	Test the reachability of a host on an Internet Protocol v6 network.
38	Perform operations on registry subkey information and values in registry entries.
39	Configure, query, stop, start, delete, and add system services.
40	Test the reachability of a host on an Internet Protocol v4 network.
41	Displays a list of currently running processes on the local computer or on a remote computer.
42	Execute or create process via WMI.
43	Query the Domain Name System to obtain the mapping between domain name and IP address, or other DNS records.
44	Create, delete, query, change, run, and end scheduled tasks on a local or remote computer.
45	Display detailed configuration information about a computer and its operating system.
46	Display and modify the Internet-to-adapter address translation tables used by the Address in Networks and communication management.
47	Create a directory.

Lazarus: LightlessCan

Index	Description
33	Mimic the `ipconfig` command from the Windows command prompt
34	Mimic the `net` command from the Windows prompt
35	Mimic the `netsh advfirewall firewall` command from the Windows prompt
36	Mimic the `netstat` command from the Windows prompt.
37	Mimic the `ping -6` command from the Windows prompt.
38	Mimic the `reg` command from the Windows prompt;
39	Mimic the `sc` command from the Windows prompt;
40	Mimic the `ping` command from the Windows prompt.
41	Mimic the `tasklist` command from the Windows prompt.
42	Mimic the `wmic process call create` command from the Windows prompt;
43	Mimic the `nslookup` command from the Windows Server prompt.
44	Mimic the `schstasks` command from the Windows prompt;
45	Mimic the `systeminfo` command from the Windows prompt.
46	Mimic the `arp` command from the Windows prompt.
47	Mimic the `mkdir` command from the Windows prompt.







ESET RESEARCH

Lazarus luring employees with trojanized coding challenges: The case of a Spanish aerospace company

Peter Kálnai • 29 Sep 2023 • 21 min. read

Lazarus TTPs

Lazarus TTPs: Rich Headers

Environment	Linker version	Developed malware
Visual Studio 2010	10.0.30319	NickelLoader, WebbyTea, OfficeCertTea, BackbitingTea, SecondHandTea, LightlessCan, old ThreatNeedleTea
Visual Studio 2010 SP1	10.0.40219	BackbitingTea, ImprudentCook, ScoringMathTea, HTTP(S) uploader, BlindingCan, miniBlindingCan , FudModule, new ThreatNeedleTea
Visual Studio 2015	**14.0.24215** 14.0.24210	**Operation In(ter)ception**
Visual Studio 2017	14.11.25547	wAgentTea
Visual Studio 2019	14.16.27031 14.21.27702 14.29.30146	PostNapTea, WinInetLoader

Lazarus TTPs: Trojanized plugins for Notepad++

Plugin	Developer	Description	Attack
NppExport 0.3.0	chcg	Export plugin for Notepad++	(ASEC Analysis Team, 2021)
NppAStyle 0.2.7	YWX	Artistic Style plugin for Notepad++	VT (Ryu, 2021)
ComparePlus 1.0.0	Pavel Nedev	File comparison plugin for Notepad++	(Ryu, 2021)
FingerText 0.5.60, 0.5.61	erinata	Snippet plugin for Notepad++	Op. DreamJob Netherlands Q4 2021 Op. DreamJob India Q1 2023
GOnpp 1.2.0.0	tike	Go programming language plugin	Op. DreamJob Netherlands Q4 2021
Flashing-Tip	Tipikin Aleksandr	Notepad++ plugin	Op. DreamJob Spain Q2 2022
MZC8051 0.1.1.0	Don HO	MZC8051 C compiler	Op. DreamJob Spain Q2 2022
LuaUtils 1.4.0.0	Charsi 82	Lua plugin for Notepad++	Op. DreamJob Spain Q2 2022
NppyPlugin	Jari Pennanen	General Python plugin for Notepad++	Op. DreamJob Spain Q2 2022
GotoLineCol 2.4.2.0	Shridhar Kumar	Go to line, column plugin for Notepad++	Op. DreamJob in India Q1 2023
Hex Editor 0.9.12	Jens Lorenz	Hex editor plugin for Notepad++	Op. DreamJob April 2023
FWDataViz 2.6.1.0	Shridhar Kumar	Fixed-width data visualizer plugin	(Microsoft, 2022) (Firsh, 2022)

Lazarus TTPs: Encryption

AES	NickelLoader (128-bit), WebbyTea (256-bit), ImprudentCook (128-bit), PostNapTea, wAgentTea (128-bit), SecondhandTea (256-bit); BlindingCan (256-bit + LZ4); miniBlindingCan (256-bit + LZ4); IconicLoader, SimpleTea for Linux (GCM)
A5/1	SimpleTea for Windows and macOS (96-bit)
RC4	In(ter)ception backdoor, BackbitingTea, BlindingCan, miniBlindingCan
RC5	Racket downloader (256-bit)
RC6	LightlessCan (256-bit)
HC	OfficeCertTea (128-bit); ComeBacker (256-bit)
Salsa20	dropper of ScoringMathTea (256-bit)
IDEA	ScoringMathTea
Panama	WinInetLoader (256-bit)
VEST-32	Torisma
DES-like	LPEClientTea

- Embedded next stage in droppers
- Configuration
- Character strings
- Network traffic (protocol)

Lazarus TTPs: Certificates 2019-2022 (Windows)

Subject name	Country	Email	Type of activity
SAMOYAJ	West Yorkshire, GB	N/A	Operation In(ter)ception
16:20 Software, LLC	Pennsylvania, US	N/A	Operation In(ter)ception
726 Lucile Development LLC	New Mexico, US	harryifrost@yahoo[.]com	Operation In(ter)ception
BRAIN Technology INC	Oklahoma, US	lucasvcastillo.x@gmail[.]com	Operation In(ter)ception
Alexis Security Group LLC	Arizona, US	RaymondJBurkett@protonmail[.]com	WIZVERA supply chain 2020
DREAM SECURITY USA INC	California, US	N/A	WIZVERA supply chain 2020
"A" MEDICAL OFFICE, PLLC,	New York, US	N/A	Operation DreamJob
2 TOY GUYS	Florida, US	N/A	Operation DreamJob
DOCTER USA, INC.	Florida, US	bernardmking@tutanota.com	Exploited INITECH software
MATCH CONSULTANTS LTD	Tackley, GB	N/A	From VirusTotal, unreported

Lazarus TTPs: Certificates 2022-2023 (Windows)

Subject name	Country	Email	Type of activity
Baltkot	Saint-Petersburg, RU	baltkod@yandex.ru	Operation In(ter)ception
Scan-trader ApS	Midtjylland, DK	scan-trader@mail.ee	Operation In(ter)ception
Dmitry Raykhman	New York, US	alexander132@protonmail.com	DangerousPassword attacks
Damion Spencer	Merseyside, UK	damions112@proton.me	DangerousPassword attacks
Cold Air Systems	Ontario, CA	rezulbrown@protonmail.com	DangerousPassword attacks

Lazarus TTPs: Certificates 2019-2023 (macOS)

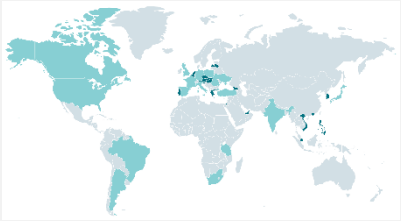
Developer ID	Team Identifier	Email	Type of activity
Golden Book	H5YL5668C7	goldenbook2021@icloud.com	Op. DreamJob
Shankey Nohria	264HFWQH63	N/A	Op.Interception
Esma Sessiz	36PUQV4CN5	N/A	Op.Interception
DPS EXPRESS COMPANY LIMITED	PN6L92RH7B	N/A	DangerousPassword
BBQ BAZAAR PRIVATE LIMITED	7L2UQTVP6F	N/A	DangerousPassword

Wrapping up…

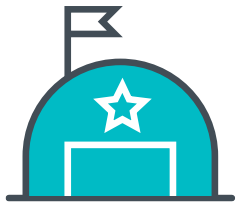
Digital Security
Progress. Protected.

Lazarus

-aligned

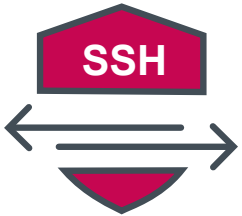


Targeting



Conclusion

Social engineering tactics

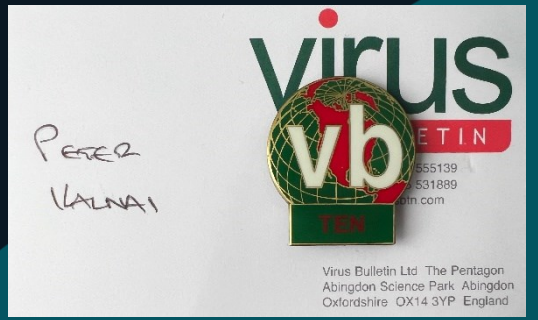


Advanced malware

Peter Kálnai

Senior Malware Researcher

@pkalnai



Thank you!

@pkalnai

@ESETResearch

ESET
Digital Security
Progress. Protected.