NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS HIVATAL

Új Nemzeti Kiválóság Program

Az orosz-ukrán háború egyes kiberbiztonsági tanulságai az energiabiztonság aspektusából

Kiss Adrienn

Az Innovációs és Technológiai Minisztérium ÚNKP-23-3-I-NKE-114 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

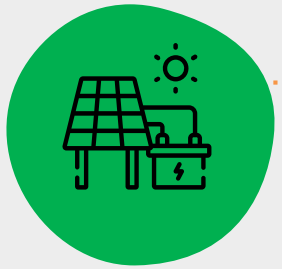
KATONAI MŰSZAKI DOKTORI ISKOLA

ELŐADÁS FELÉPÍTÉSE

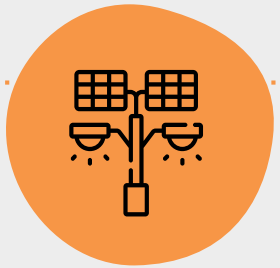
1. BEVEZETÉS
2. MŰVELETEK
3. ESETTANULMÁNYOK
4. HELYZETÉRTÉKELÉS
5. ÖSSZEGZÉS

KRITIKUS INFRASTRUKTÚRÁK

Létszükségletek fenntartása



Kiemelt jelentőségű



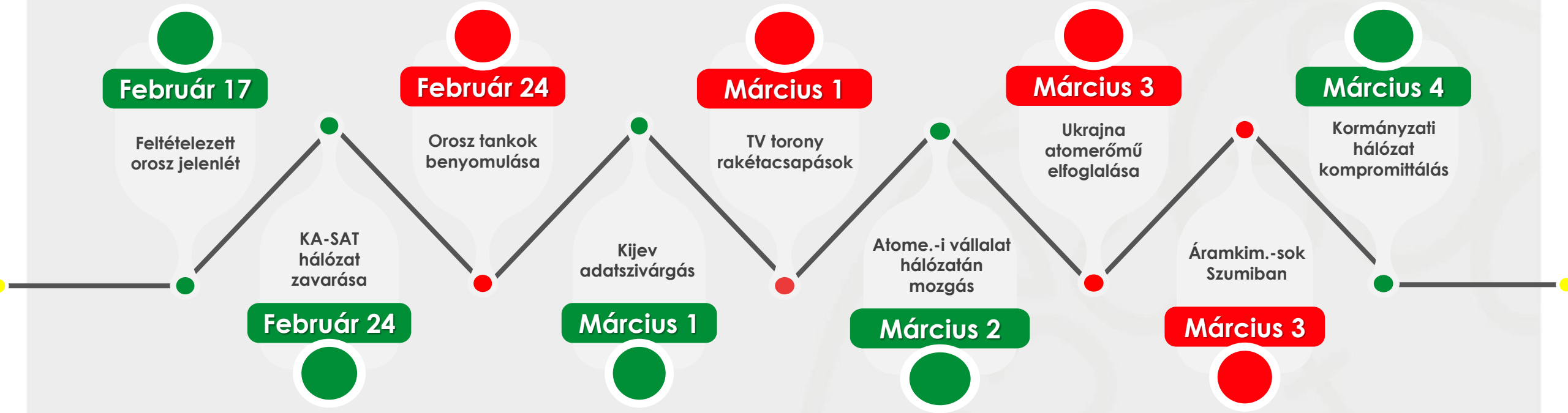
Nem opcionális, hanem szükségszerű

Kölcsönös függőség

OROSZ-UKRÁN HÁBORÚ

2014-től konfliktus
2022. február 24.
fizikai támadások
kibertámadások
kritikus infrastruktúrák
összehangolt
atomerőművek
leterhelése

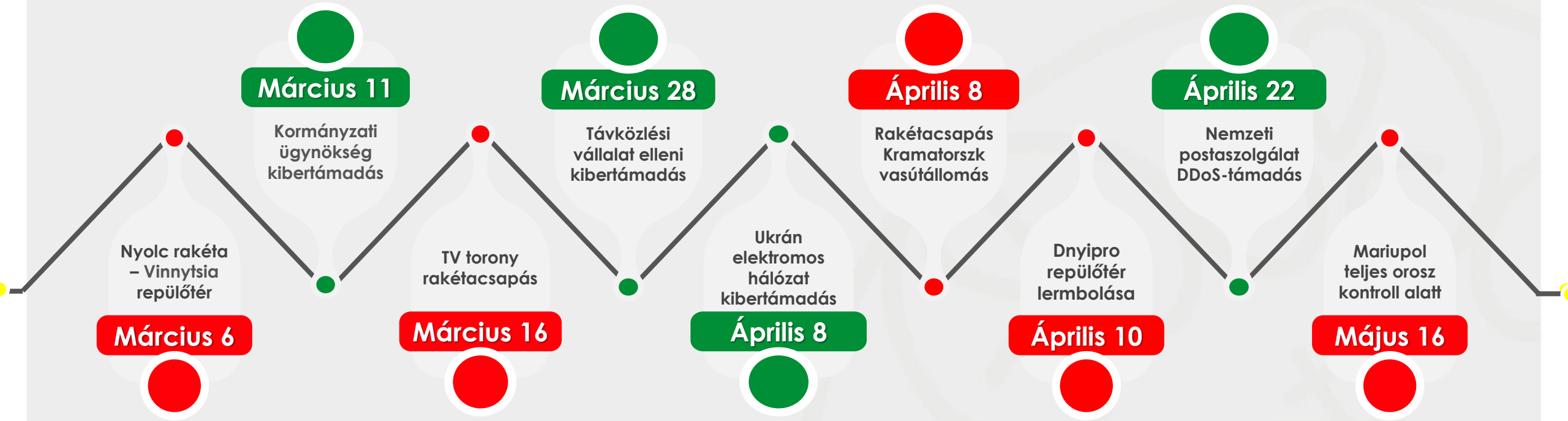
KATONAI TÁMADÁSOK ÉS KIBERMŰVELETEK



Kibertéri műveletek

Fizikai térben zajló műveletek

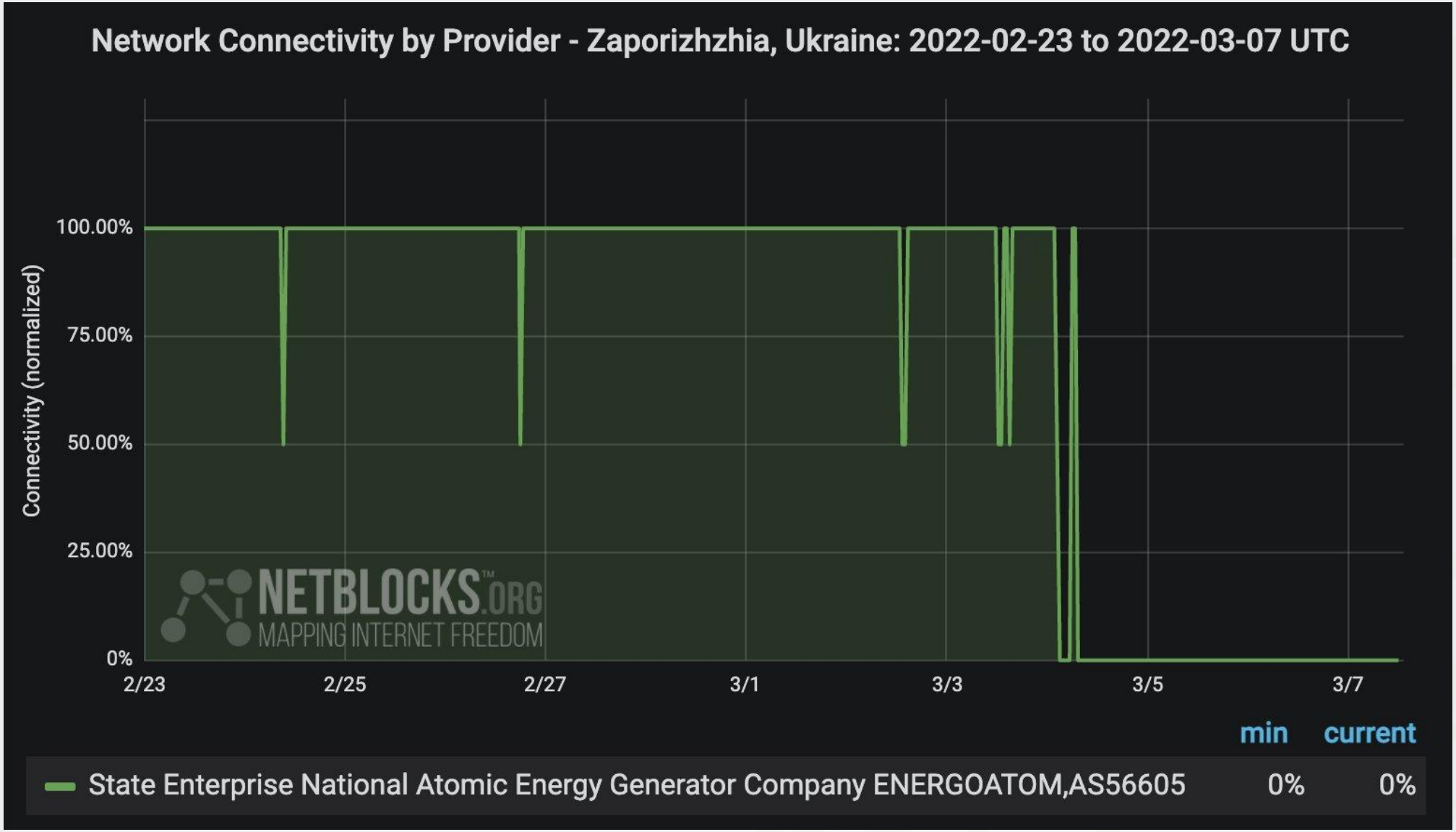
KATONAI TÁMADÁSOK ÉS KIBERMŰVELETEK



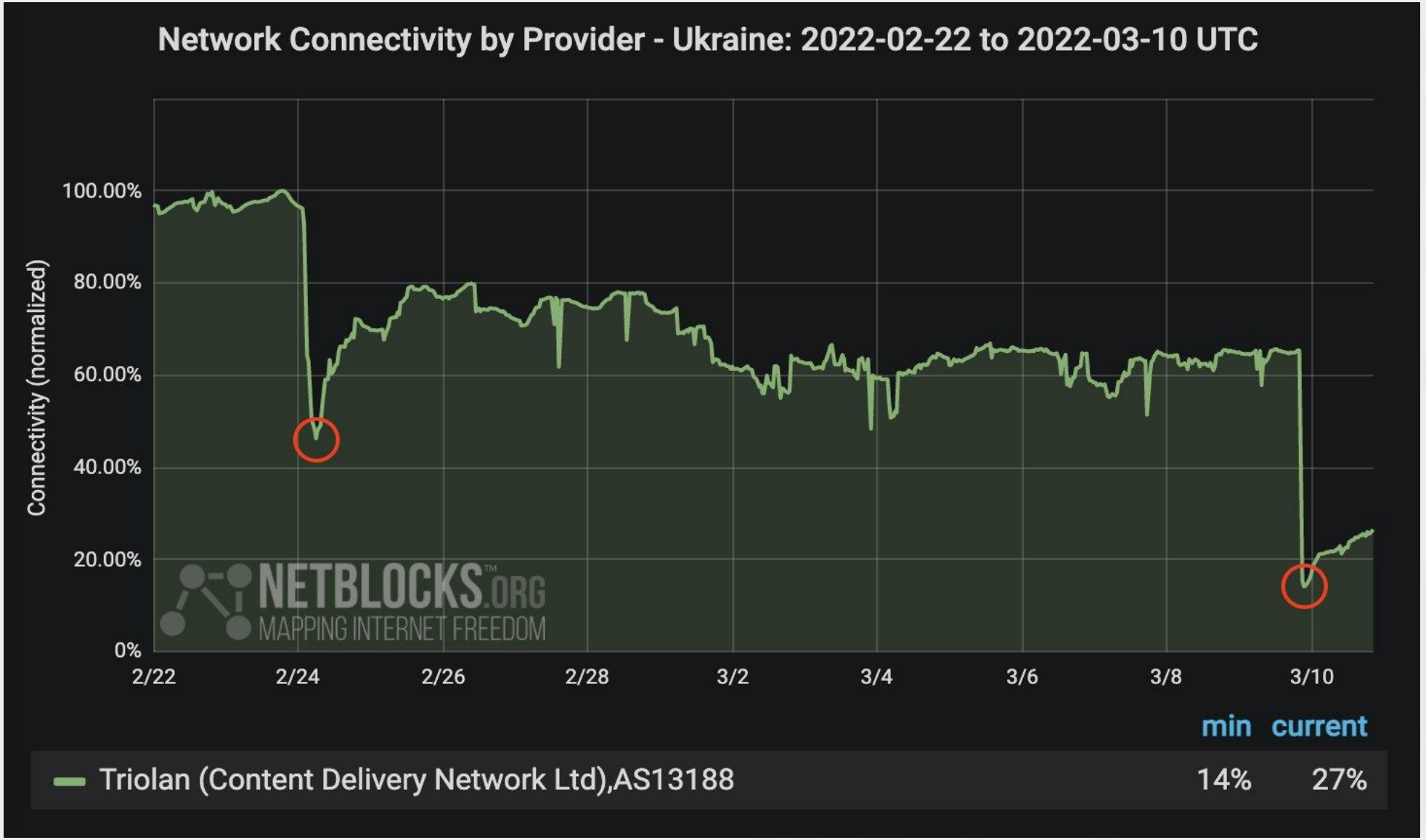
Kibertéri műveletek

Fizikai térben zajló műveletek

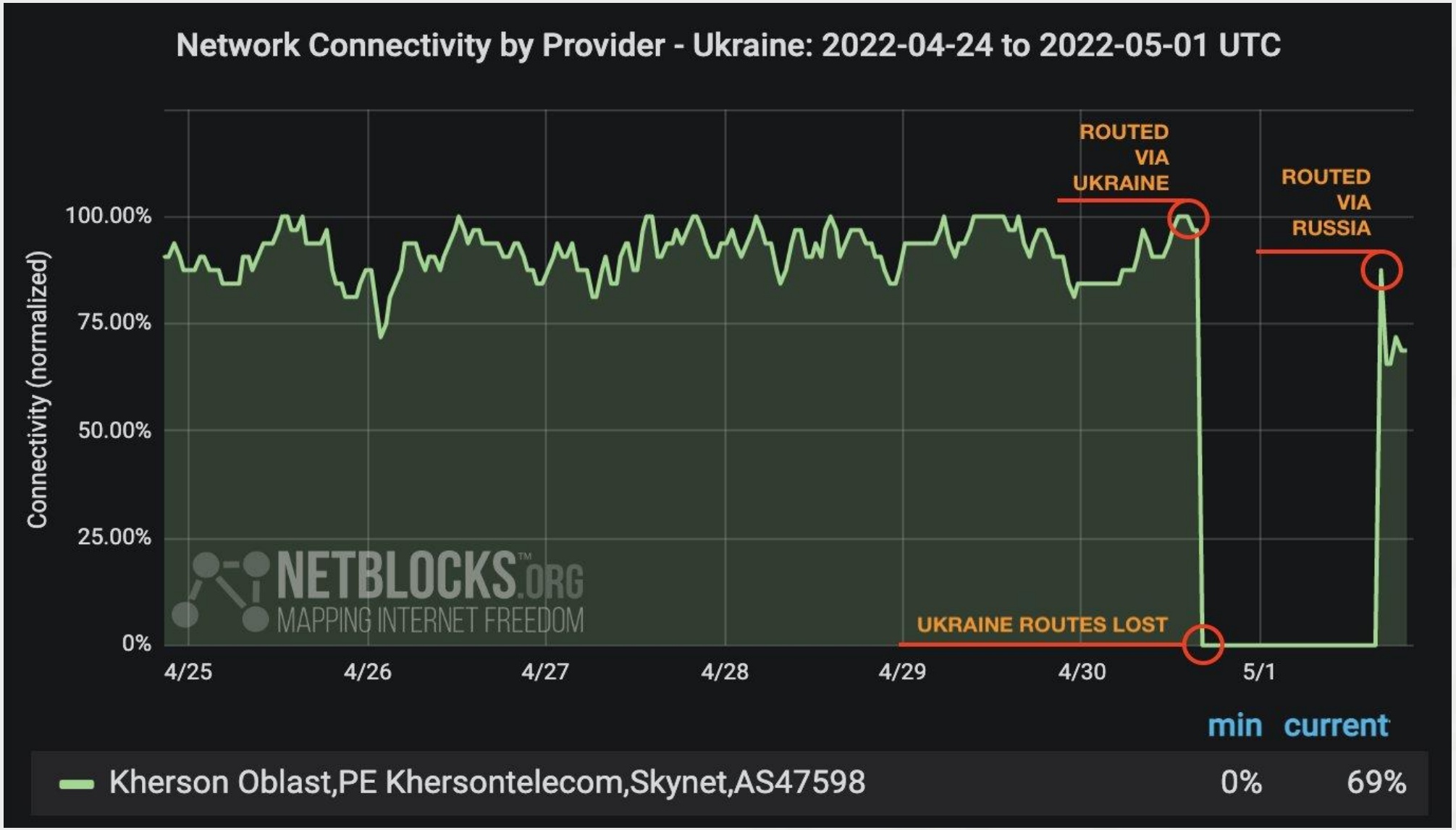
NETBLOCKS


Network Connectivity by Provider - Zaporizhzhia, Ukraine: 2022-02-23 to 2022-03-07 UTC
Connectivity (normalized)
100.00%
75.00%
50.00%
25.00%
0%
2/23
2/25
2/27
3/1
3/3
3/5
3/7
NETBLOCKS.ORG
MAPPING INTERNET FREEDOM
min
current
State Enterprise National Atomic Energy Generator Company ENERGOATOM,AS56605
0%
0%

NETBLOCKS


Network Connectivity by Provider - Ukraine: 2022-02-22 to 2022-03-10 UTC
Connectivity (normalized)
100.00%
80.00%
60.00%
40.00%
20.00%
0%
2/22
2/24
2/26
2/28
3/2
3/4
3/6
3/8
3/10
NETBLOCKS.ORG
MAPPING INTERNET FREEDOM
min
current
Triolan (Content Delivery Network Ltd),AS13188
14%
27%

NETBLOCKS


Network Connectivity by Provider - Ukraine: 2022-04-24 to 2022-05-01 UTC
Connectivity (normalized)
100.00%
75.00%
50.00%
25.00%
0%
4/25
4/26
4/27
4/28
4/29
4/30
5/1
ROUTED VIA UKRAINE
ROUTED VIA RUSSIA
UKRAINE ROUTES LOST
NETBLOCKS.ORG
MAPPING INTERNET FREEDOM
min
current
Kherson Oblast,PE Khersontelecom,Skynet,AS47598
0%
69%

INDUSTROYER VS. INDUSTROYER2

kifejezetten villamosenergia-rendszerre optimalizált	**kifejezetten villamosenergia-rendszerre optimalizált**
fejlett, moduláris felépítésű	fejlett, moduláris felépítésű
nem konfigurálható	**konfigurálható**
a részletes konfigurációt egy külön fájlban tárolja	a részletes konfigurációt önmagában tárolja
kézi	**automatizált**
fizikai károkozás is	vélhetően fizikai károkozás is

INDUSTROYER2

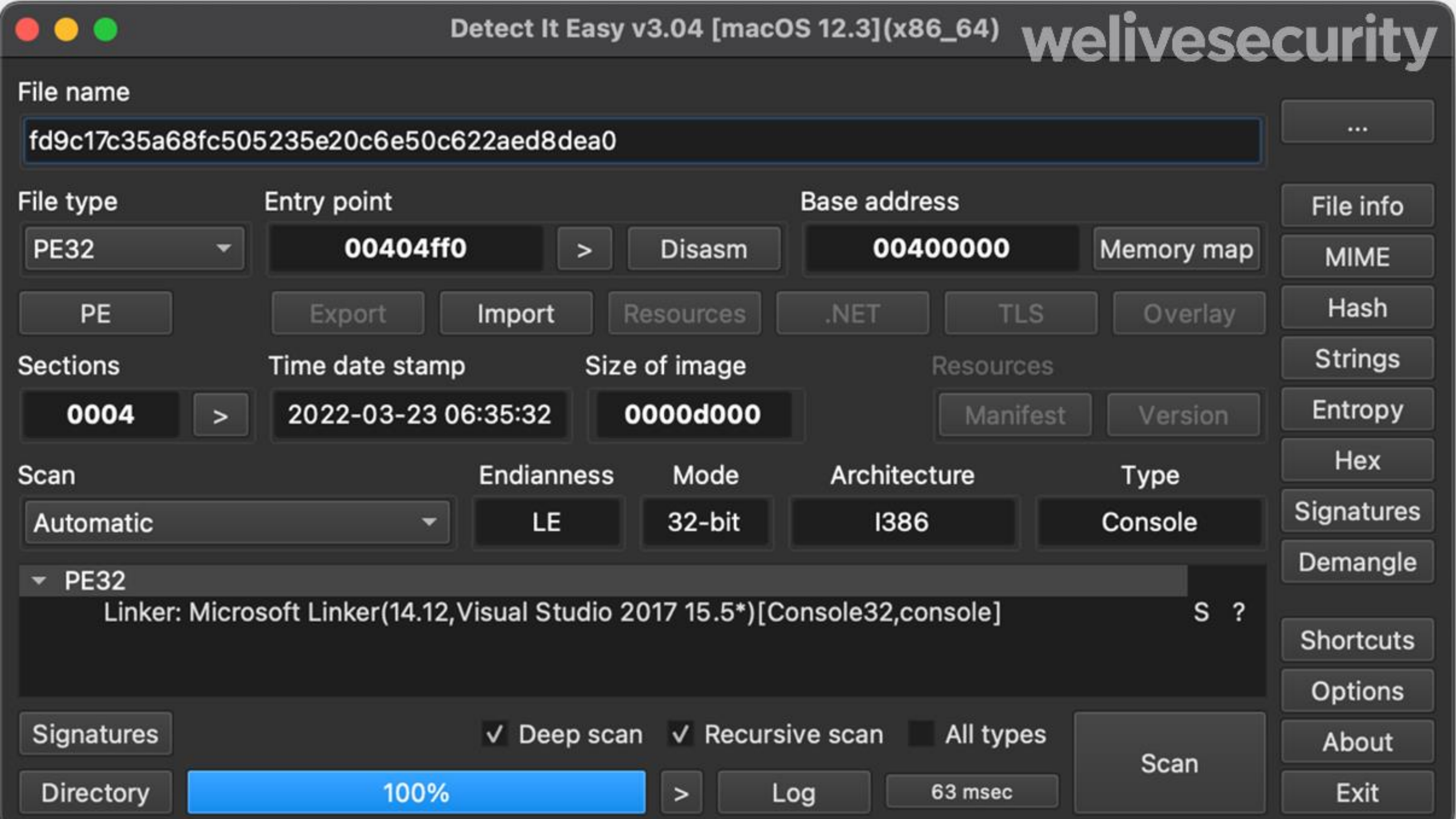
IEC 60870-5-104 protokoll

Konfigurálható

Megszakít

Naplófájl létrehozása

Törléssel való kombinálás


Detect It Easy v3.04 [macOS 12.3](x86_64)
welivesecurity
File name
fd9c17c35a68fc505235e20c6e50c622aed8dea0
...
File type
PE32
Entry point
00404ff0
>
Disasm
Base address
00400000
Memory map
File info
MIME
Hash
Strings
Entropy
Hex
Signatures
Demangle
PE
Export
Import
Resources
.NET
TLS
Overlay
Sections
0004
>
Time date stamp
2022-03-23 06:35:32
Size of image
0000d000
Resources
Manifest
Version
Scan
Automatic
Endianness
LE
Mode
32-bit
Architecture
I386
Type
Console
PE32
Linker: Microsoft Linker(14.12,Visual Studio 2017 15.5*)[Console32,console]
S
?
Shortcuts
Options
About
Exit
Signatures
Deep scan
Recursive scan
All types
Scan
Directory
100%
>
Log
63 msec

PIPEDREAM

kifejezetten programozható logikai vezérlőkre specializált ismert kártevő

gyártófüggetlenség

az ipari környezetnek, a fizikai folyamatoknak a megzavarására

moduláris, több komponensből áll

különböző funkciókkal, képességekkel rendelkeznek

összetevőit bővíteni is lehet

PIPEDREAM

beszivárgott ukrán és amerikai elektromos és gázipari rendszerekbe

rendszerek lekapcsolása (közel került)

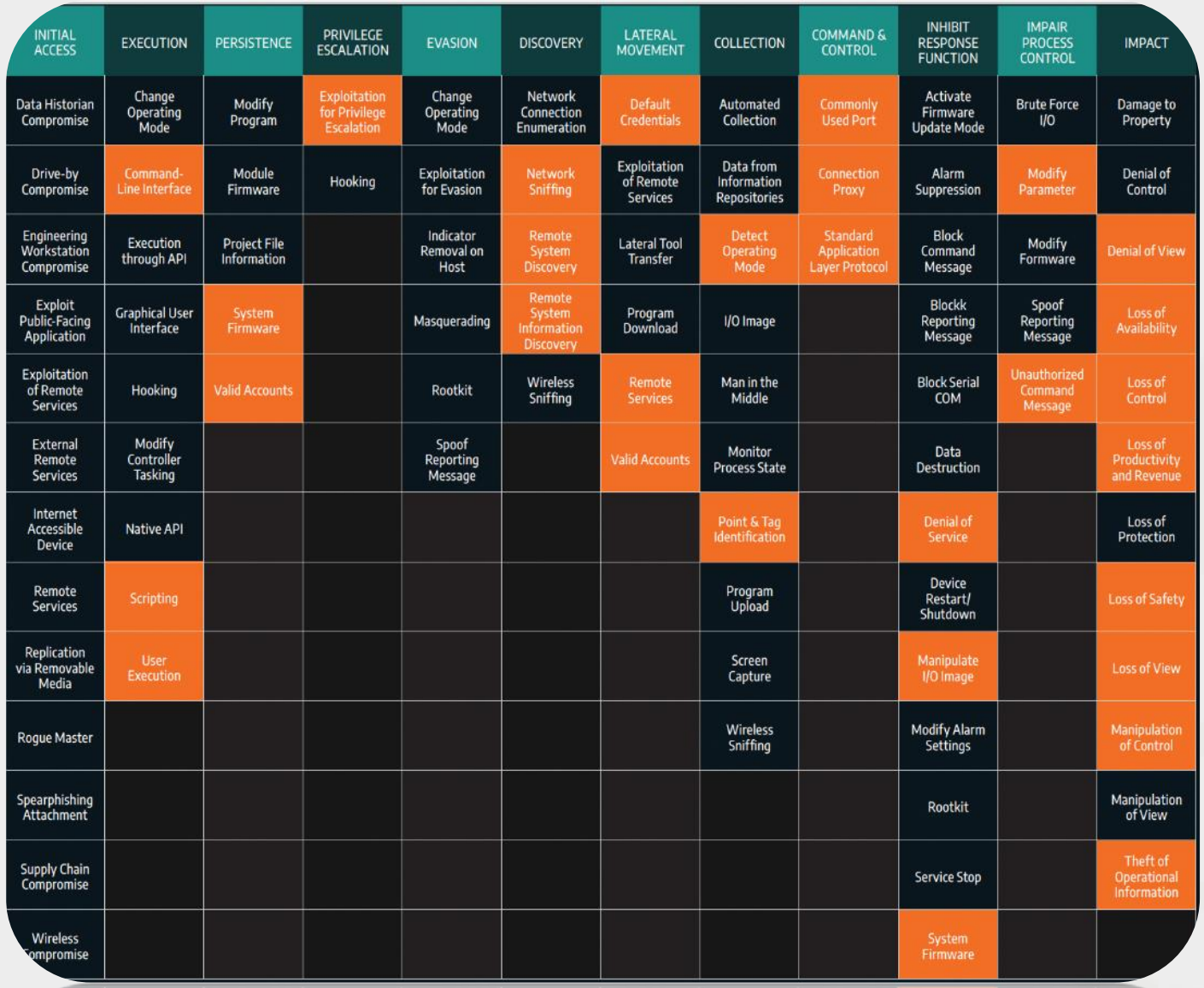
feltételezések (amerikai energiaellátás sérülékenysége)

2022. áprilisi bejelentés

számos más rendszerre veszélyes

sebezhetőség több rendszerben is jelen van

MITRE ATT&CK KERETRENDSZER



INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
Data Historian Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Engineering Workstation Compromise	Execution through API	Project File Information		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Modify Formware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Blockk Reporting Message	Spoof Reporting Message	Loss of Availability
Exploitation of Remote Services	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
External Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Internet Accessible Device	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Remote Services	Scripting						Program Upload		Device Restart/ Shutdown		Loss of Safety
Replication via Removable Media	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Rogue Master							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Spearphishing Attachment									Rootkit		Manipulation of View
Supply Chain Compromise									Service Stop		Theft of Operational Information
Wireless Compromise									System Firmware		

mennyire hatékony egy szervezet védekezési és detektálási stratégiája

az ismert ICS támadási technikák 38%-át, és a taktikák 83%-át képes végrehajtani

TÉNYEZŐK

Kiber-szuperhatalom mítosz

Elmaradás attól a pusztítástól, amelyet sokan jósoltak az invázió után.

Nyugati technológia kivonulása

Hogyan lehet fenntartani a lendületet sokkal kevesebből.

Kapkodás

Gyorsabb és piszkosabb módszerek; sokkal kevésbé kifinomultak, és "opportunista viselkedés" különösebb stratégia nélkül.

Nem csak ukrán célpontok

Erőmegosztás más célpontok miatt és az erős intenzitást csak rövid ideig tudják fenntartani.

Kevés haszon

„A kiberműveletek kevés hasznot hoztak" Oroszországnak, és "nem mozdították előre az orosz célokat" a háborúban.

Perspektívák

Külső elemzők alábecsülték Oroszország háborús kibererőfeszítéseit Ukrajna ellen.

KÖVETKEZMÉNYEK

Nagyobb „kiberegyüttműködés”

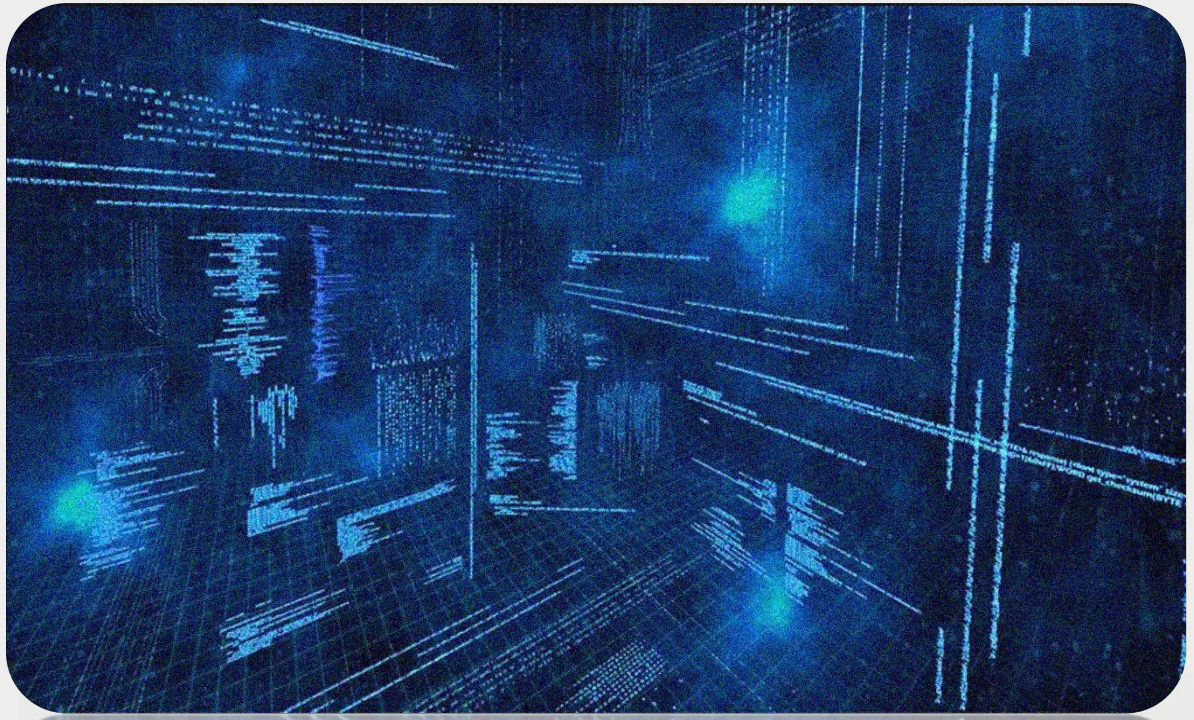
Az orosz invázió nagyobb kiberegyüttműködést váltott ki.

Magánszektor szerepe

A háború rávilágított a magánszektor hatalmas szerepére a védelemben.

Háborús „kiberköd”

Nyilvános jelentések és egységes álláspontok hiánya.



TANULSÁG?

védelmi intézkedések újra gondolása
kritikus infrastruktúrák kölcsönös függősége
ukrán kibervédelmi képességek fejlődtek
automatizált támadások
7-8 éves fejlődés támadói oldalról
sikerráta mértékének becslése
hamis biztonságérzet veszélye

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS HIVATAL

Új Nemzeti Kiválóság Program

Köszönöm szépen a megtisztelő figyelmet!

Kiss Adrienn

Az Innovációs és Technológiai Minisztérium ÚNKP-23-3-I-NKE-114 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

KATONAI MŰSZAKI DOKTORI ISKOLA

FELHASZNÁLT IRODALOM

[1] **Canadian Centre for Cybersecurity:** *CYBER THREAT BULLETIN: Cyber Threat Activity Related to the Russian Invasion of Ukraine*, pp. 1-9., cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf, 2022.

[2] **Görgey P.:** *Kibertámadások Ukrajnában: áramszünetek és tanulságok (II. rész),* Elektrotechnika 110.évf. pp. 22-24., https://www.mee.hu/files/files/et2020-11.pdf, 2020.

[3] **Wright R.: Industroyer2:** *How Ukraine avoided another blackout attack., TechTarget,* https://www.techtarget.com/searchsecurity/news/252523694/Industroyer2-How-Ukraine-avoided-another-blackout-attack, 2022.

[4] **ESET Research.:** *Industroyer2: Industroyer reloaded.,* Welivesecurity, https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/, 2022.

[5] **Miller M..:** *Russian-linked malware was close to putting U.S. electric, gas facilities 'offline' last year.,* Politico, https://www.politico.com/news/2023/02/14/russia-malware-electric-gas-facilities-00082675, 2023.

[6] **Dragos.:** *PIPEDREAM: CHERNOVITE'S EMERGING MALWARE TARGETING INDUSTRIAL CONTROL SYSTEMS.,* https://www.dragos.com/blog/industry-news/CHERNOVITE-pipedream-malware-targeting-industrial-control-systems/, 2022.

[7] **Jones S.:** *Russian-Linked Malware Targets U.S. Critical Infrastructure.,* Ankura CTIX https://angle.ankura.com/post/102icqx/russian-linked-malware-targets-u-s-critical-infrastructure, 2023.

[8] **ESET.:** *Threat Report.,* https://web-assets.esetstatic.com/wls/2023/07/eset_threat_report_h12023.pdf, 2023.

[9] **Scroxton A.:** *Sandworm rolls out Industroyer2 malware against Ukraine.,* h https://www.computerweekly.com/news/252515855/Sandworm-rolls-out-Industroyer2-malware-against-Ukraine, 2022.

[10] ***Butler N.:*** *The impact of the Ukraine war on global energy markets,* Centre for European Reform, pp.1-4. 2022.

[11] **Nerlinger M., Utz S.:** *The impact of the Russia-Ukraine conflict on the green energy transition – A capital market perspective,* Swiss Finance Institute Research Paper pp. 22-49, http://dx.doi.org/10.2139/ssrn.4132666, 2022.

[12] **Umar M., Riaz Y., Yousaf I.:** *Impact of Russian-Ukraine war on clean energy, conventional energy, and metal markets: Evidence from event study approach,* Resources Policy,Volume 79, pp. 1-8. ISSN 0301-4207, https://doi.org/10.1016/j.resourpol.2022.102966, 2022.

[13] **Baranowski M.:** *Welfare over Warfare? Russia's payloadsWar on Ukraine through the Prism of Europe's Energy Security.* International Journal of Energy Economics and Policy. 12. pp. 226-231.,10.32479/ijeep.13415., 2022.