

Netógnir á óvissutímum

Ský 29.10.2025

Net- og upplýsingaöryggi á tímum ófriðar

Aðalsteinn Jónsson



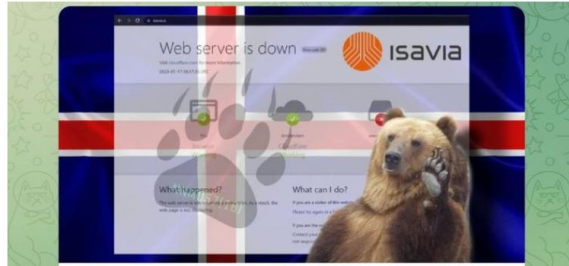
Vefur Alþingis liggur niðri: „Málið er í at-hugun“

Atli Ísleifsson skrifar · 16. maí 2023 09:36



Sami hópur segist hafa tekið niður vef-síðu Isavia

Kjartan Kjartansson skrifar · 17. maí 2023 11:30



CERT-IS
@cert_iceland · Follow



Árásarhópar eru að gera tilraunir til að nýta rafræn skilríki til að komast inn á viðkvæm svæði. Ekki staðfesta rafræn skilríki nema vera viss um að þú hafir beðið um það.

Ekki staðfesta rafræna auðkenningabeðið sem þú kannast ekki við.

11:56 AM · May 16, 2023



91 · Reply · Copy link

[Read more on Twitter](#)



Verið að fremja árásir á íslenska vefi

Verið er að fremja árásir á íslenska vefi að sögn aðstoðaryfirlögregluþjóns hjá greiningardeild ríkislögreglustjóra. Embættið telur sig hafa hugmynd um hvaðan árásirnar koma en ekkert hefur fengist staðfest.

INNLENT · 16.5.2023 10:19

Netárás gerð á Dalvíkurbyggð

Bjarki Sigurðsson skrifar · 15. maí 2023 11:09



Líklegt að árásirnar haldi áfram

Óvissustig Almannavarna var virkjað í dag vegna netárása Rússa í tengslum við fund Evrópuráðsins. Sérfræðingur í netöryggi segir Íslendinga mega eiga von á fleiri árásum og að almenningur þurfi einnig að hafa varan á.

INNLENT · 16.5.2023 19:01

Tölvuþrjótarnir kalla Vesturlönd nasista

Samúel Karl Ólason og Máni Snær Þorláksson skrifa · 16. maí 2023 12:27



Þessi mynd fylgdi yfirlýsingu tölvuþrjótahópsins um netárásina á Íslandi.

Helstu árársaraðilar

	Einyrkjar/Hacktivistar	Skipulagðir hópar	Ógnaraðilar á vegum þjóríkis
Markmið	Tækifærissinnuð	Fjárhagsávinningur	Aukin völd
Geta	- Misgóð þekking - Takmörkuð geta - Lítið fjármagn	- Þekking á UT - Takmarkað fjármagn	- Mikil þekking á UT - Vel fjármagnaðir
			

„Stóru Fjögur“

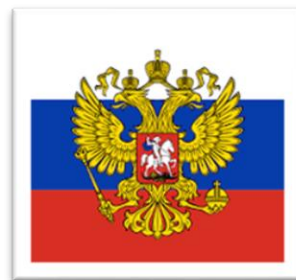
Kína

Rússland

Norður
Kórea

Íran





"CIA"

"FBI"



GRU

APT28 – Fancy Bear
Sandworm (Voodoo Bear)

SVR

APT29 – Cozy Bear

FSB

Center 16
Center 18

NOTPETYA ÁRÁS - 2017

Sandworm (GRU) - ~\$10 Milljarða tjón

FEB-MAR 2017

M.E.Doc brotist inn í - Sandworm kemur sér fyrir

APR-MAÍ 2017

Bakdyrum komið fyrir í uppfærslu

27. JÚNÍ 2017 - 10:30

ÁRÁS HEFST - Skróbb óværa

27. JÚNÍ - SÍÐAR SAMA DAG

ALÞJÓÐLEG ÚTBREIÐSLA

Maersk, Merck, FedEx

2018 - NIÐURSTAÐA

Eignaður Rússlandi (Sandworm/GRU)

Dýrasta netárás sögunnar

SOLARWINDS ÁRÁS - 2019-2021

APT29 (SVR/Cozy Bear) - 9 mánuðir óuppgötvuð

SEPT-OKT 2019

APT29 byrjar að skoða SolarWinds

OKT 2019 - FEB 2020

SUNBURST spillikóði þróaður - Fáguð bakdyr

MARS 2020

SÝKT UPPFÆRSLA SEND ÚT

~18,000 viðskiptavinir fá sýkta uppfærslu

MAÍ-DES 2020 (9 MÁNUÐIR)

❑ NJÓSNIR

~100 skotmörk fyrir hnitmiðaðar árásir - vinna á vinnutíma

8-13. DESEMBER 2020

UPPGÖTVUN & OPINBERUN

FireEye uppgötvar - 9 ríkisstofnanir, Microsoft +

2021 - NIÐURSTAÐA

Árás er eignuð Rússlandi (APT29/SVR)

Ein fáguðasta birgðarkeðjuárás sem sést hefur

Taktískar breytingar

 **14/2**
Ráðist á 70 ríkisstofnanir og birt „Wait for the worst“ á heimasíðum þeirra

 **24/2**
Ráðist á KA-SAT gervihnött

 **25/2**
Ráðist á landamærastöðvar með skrúbb óværu

 **4/3**
Ráðist á hjálparstofnanir innan Úkraínu

 **16/3**
Ráðist á sjónvarpsstöðvar og djúpfölsun af Zelensky

 **8/4**
Ráðist á orkugeira Úkraínu

Netárásir í fyrirrúmi

Margir bjuggust við að innrás Rússlands inn í Úkraínu myndi fylgja ógrynni af netárásum sem myndi lita innrásina mikið

Netárásir fyrir og eftir innrás

Fjöldi netárása gerðist nokkrum dögum fyrir, klukkutímum fyrir og eftir að innrásin átti sér stað, hefur líklega ekki gefið Rússum það hernaðarlega forskot sem búist var við

Forgangur á njósnir og taktískari árásir

Síðan um mitt 2023 var augljós taktísk breyting þegar Rússar fóru að einbeita sér meira að njósnum

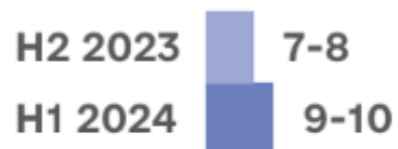
Mikið púður lagt í að komast inn í síma andstæðinganna

Augljóst að farsímar eru áleitnir hernaðarlega mikilvægir í dag

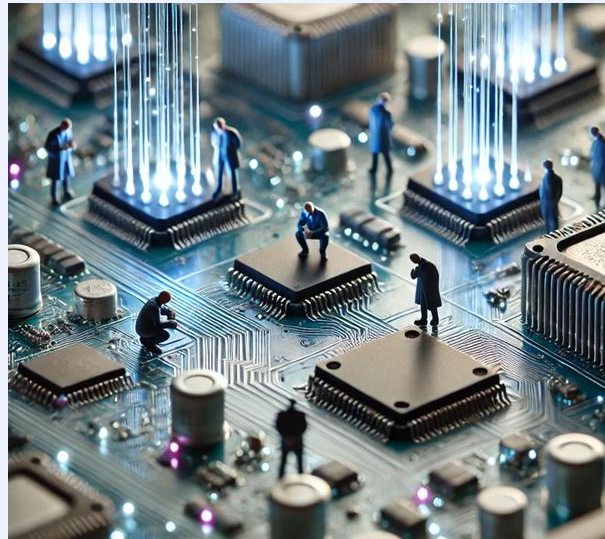
9-10 árásir á dag

Incidents by Severity Level	H2'2023	H1'2024	Change
Critical	31	3	-90%
High	156	45	-71%
Medium	1264	1670	32%
Low	12	21	75%
Total	1463	1739	19%

AVERAGE PER DAY



Netárásir



- Erfitt að tímasetja
- Heppnaðist hún?
- Dreifðist hún of víða
- Of mikill tími

	 Rússland	 Kína
Njósir	 Mikil áhersla	 Megináhersla
Þjófnaður á hugverkum	 Tækifærissinnað	 Mikil áhersla
Áhrifaaðgerðir (e. Influence operations)	 Mikil geta – upplýsingaóreiða	 Vaxandi geta
Truflun og skemmdarverk	 Algengt (Úkraína, orkuinnviðir)	 Sjaldan (áhersla á Taívan)
Efnahagslegur ávinningur	 Takmarkað	 Takmarkað
Undirbúningur fyrir átök	 Beinist að kerfum NATO og Úkraínu	 Staðsetning í vestrænum netkerfum
Hefnd / fælingarmáttur	 Algeng viðbrögð við refsiaðgerðum	 Yfirleitt diplómatískar aðgerðir

Aukin áhersla á upplýsingaöflun



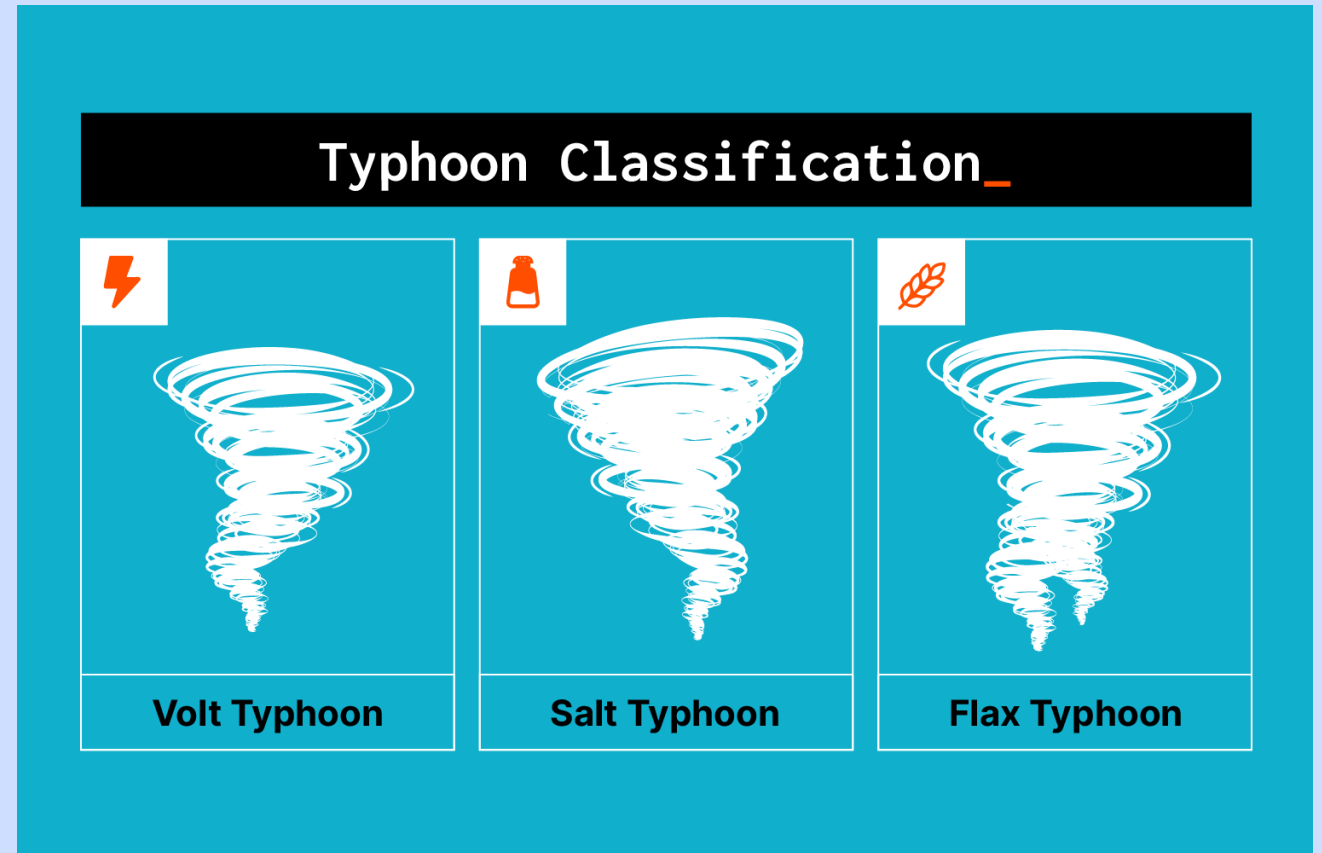
Kína



Notast við skúffufélög til
að fela tengingar við ríkið

- Léttara að neita ábyrgð
- Þekktari fyrir njósnir

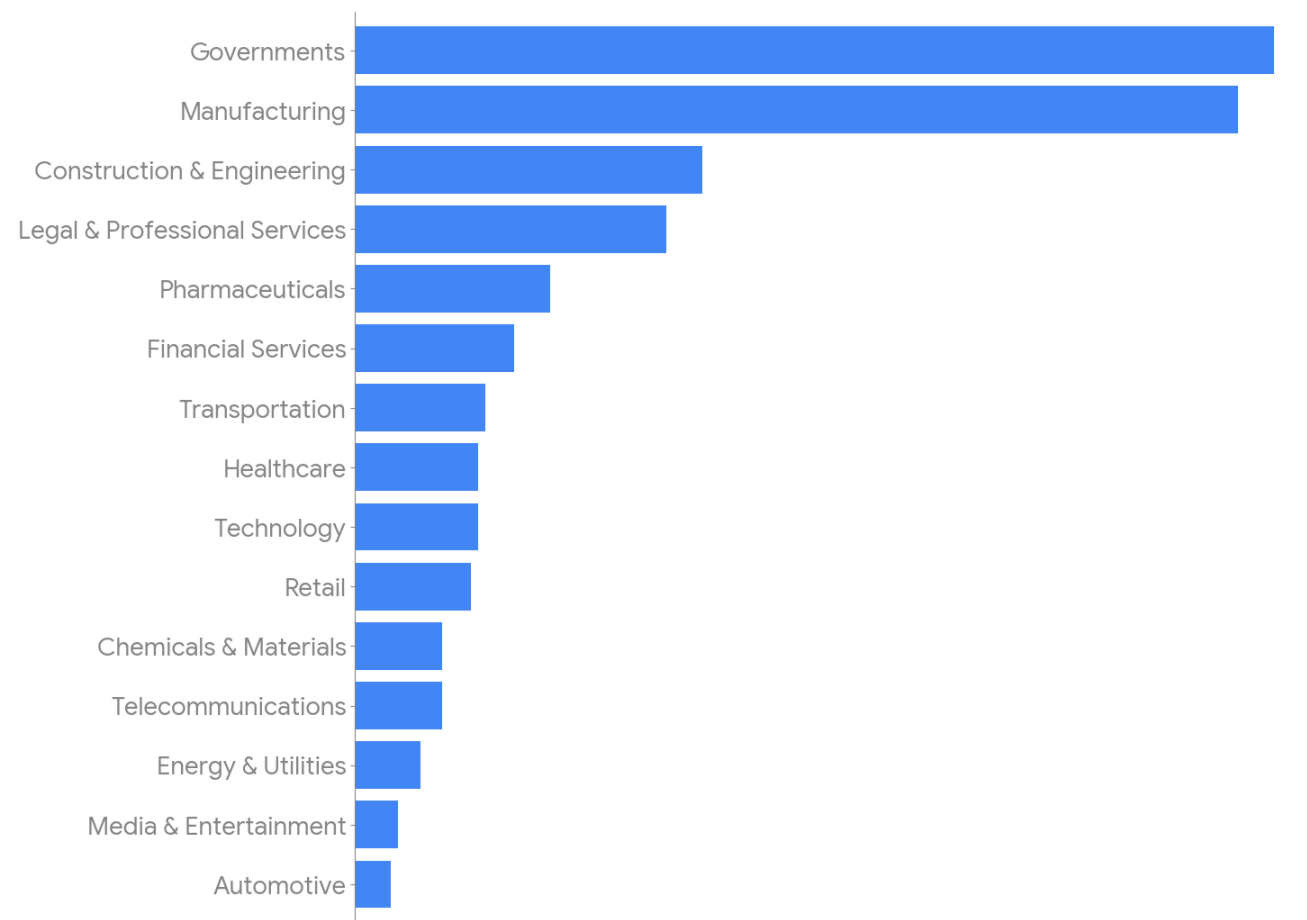
Kínverskir Ógnarhópar



Helstu skotmörk

Q4 2024

TARGETED INDUSTRIES



*Gögn frá Mandiant

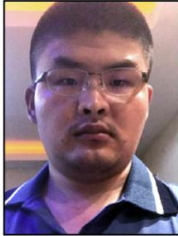
Eftirlýstir



WANTED BY THE FBI

AQUATIC PANDA CYBER THREAT ACTORS

Conspiracy to Commit Computer Fraud; Conspiracy to Commit Wire Fraud

				
Wu Haibo	Chen Cheng	Liang Guodong	Ma Li	Wang Yan
				
Wang Zhe	Zhou Weiwei	Xu Liang	Wang Liyu [MPS]	Sheng Jing [MPS]



WANTED BY THE FBI

DPRK IT FRAUD

Conspiracy to Damage a Protected Computer; Conspiracy to Commit Wire Fraud and Mail Fraud;
Conspiracy to Commit Money Laundering; Conspiracy to Transfer False
Identification Documents; Conspiracy to Violate the International Emergency Economic Powers Act

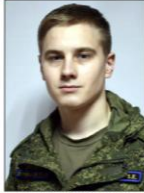
	
Jin Sung-Il	Pak Jin-Song



WANTED BY THE FBI

GRU 29155 CYBER ACTORS

Conspiracy to Commit Computer Intrusion and Damage; Wire Fraud Conspiracy

		
Vladislav Yevgenyevich Borovkov	Denis Igorevich Denisenko	Yury Fedorovich Denisov
		
Dmitriy Yuryevich Goloshubov	Nikolay Aleksandrovich Korchagin	Amin Timovich Stigal



HEFÐBUNDIÐ ÖRYGGI

- Lögregla
- Leynirþjónusta
- Landhelgisgæsla
- Herlið

NETÖRYGGI

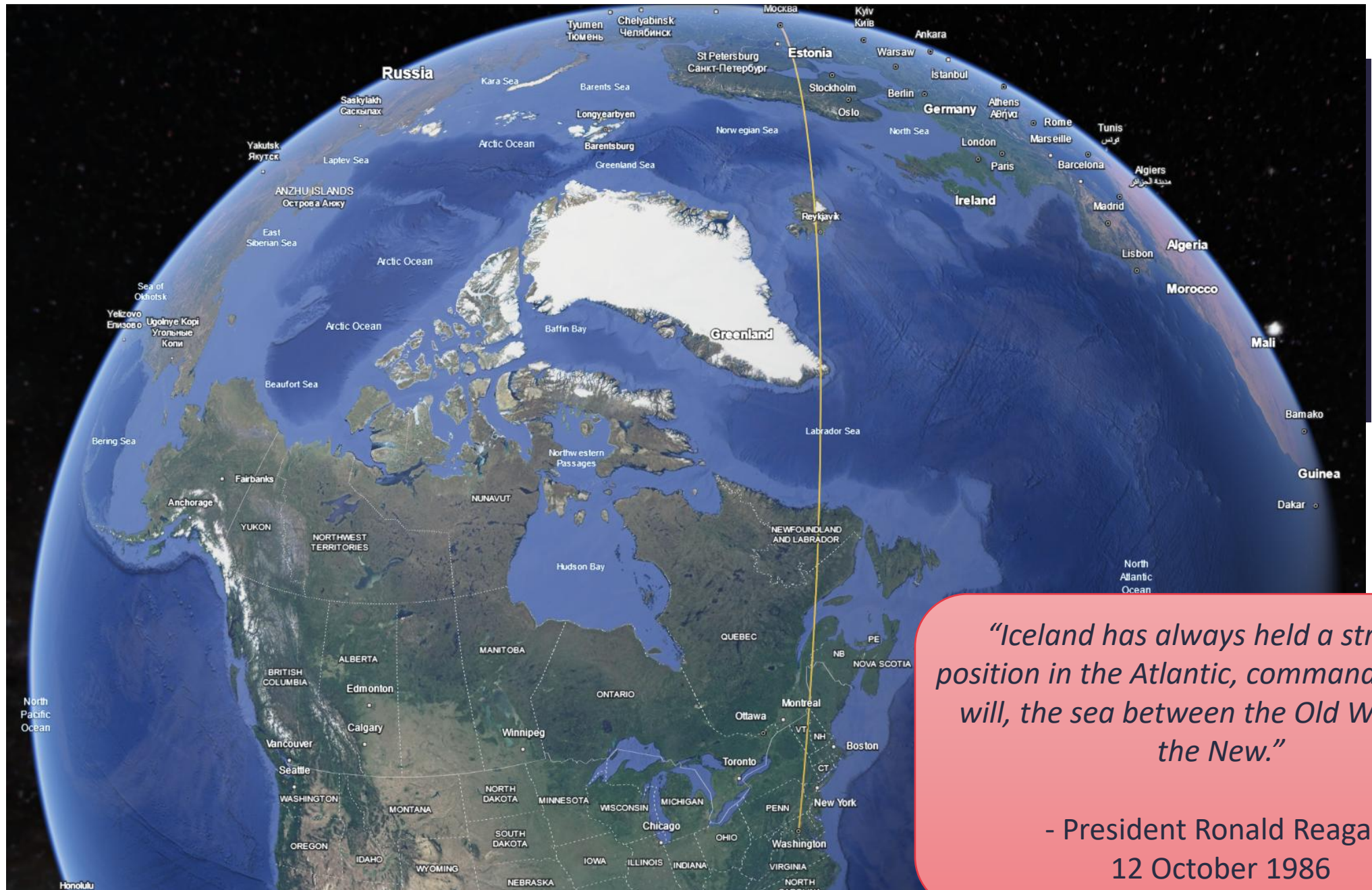
- Mikilvægir innviðir
- Fyrirtæki
- Einstaklingar

"Við erum öll netvarnir"

The logo is a circular emblem. The top half features a globe with binary code (0s and 1s) overlaid on it. The bottom half is divided into two quadrants: the left quadrant contains a white compass rose on a blue background, and the right quadrant contains the text 'NATO' and 'OTAN' stacked vertically on a black background. The words 'CYBER COALITION' are written in a white arc across the top, and 'EXERCISE' is written in a white arc across the bottom.

Markmið: Auka áfallapol og viðbragðsgetu NATO við ógnarhópum





"Iceland has always held a strategic position in the Atlantic, commanding, if you will, the sea between the Old World and the New."

- President Ronald Reagan,
12 October 1986



Takk fyrir

adalsteinn@cert.is

HLIÐARRÁSARÁRÁSIR (E. SIDE CHANNEL ATTACKS)

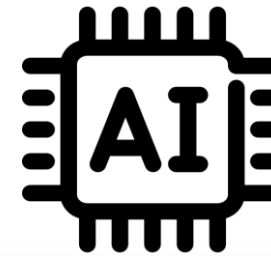
Skrifa á lyklaborð



Gagnaleki



Hljóð



Texti



- 95% Nákvæmni
 - 93% í gegnum fjarfundarbúnað
- Þróaðir hljóðnemar gera árás enn skilvirkari



Zero Click Njósniir



CVE-2025-43300 (CVSS 8.8) // Apple

-> Patched in iOS 18.6.2 (Aug. 20th)



CVE-2025-55177 (CVSS 5.4) // Whatsapp

-> 2.25.21.73 (patched July 28, 2025)

Chained together for zero-click spyware



ALERT: State-sponsored attackers may be targeting your iPhone

Apple is contacting you because this email address [REDACTED] is associated with your Apple ID, [REDACTED]

Apple believes you are being targeted by state-sponsored attackers who are trying to remotely compromise the iPhone associated with your Apple ID

These attackers are likely targeting you individually because of who you are or what you do. If your device is compromised by a state-sponsored attacker, they may be able to remotely access even the camera and microphone. While it's this warning seriously.

Apple recommends that you immediately

