



# Uncovering the Tactics of RomCom RAT in the Ukraine-Russia Conflict

Eoin Healy  
Senior Security Researcher at BlackBerry

 @\_eohealy



## WHO AM I?



Eoin Healy

Senior Threat Researcher, Threat Intelligence

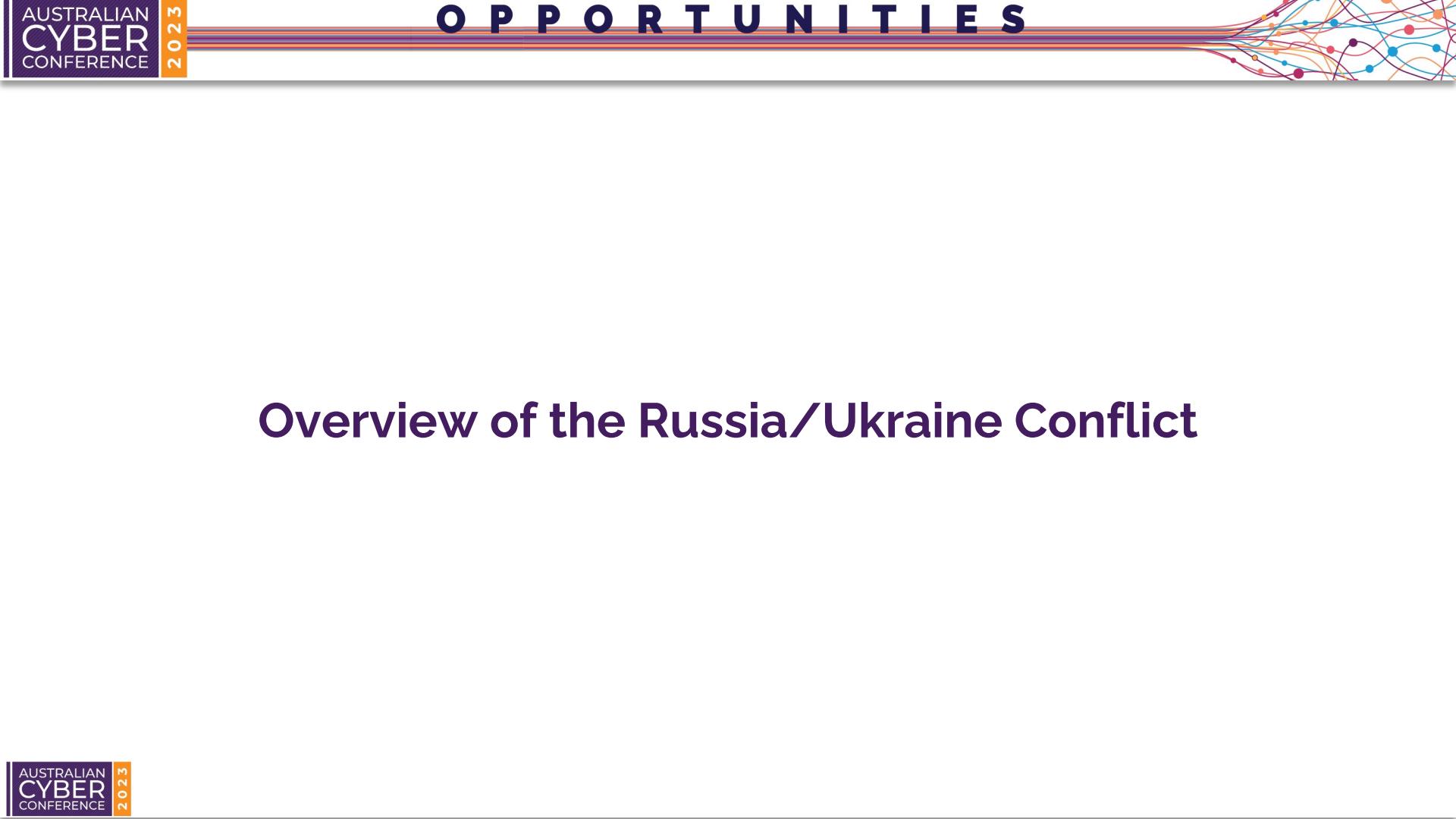
From Cork, Ireland to Sydney, Australia



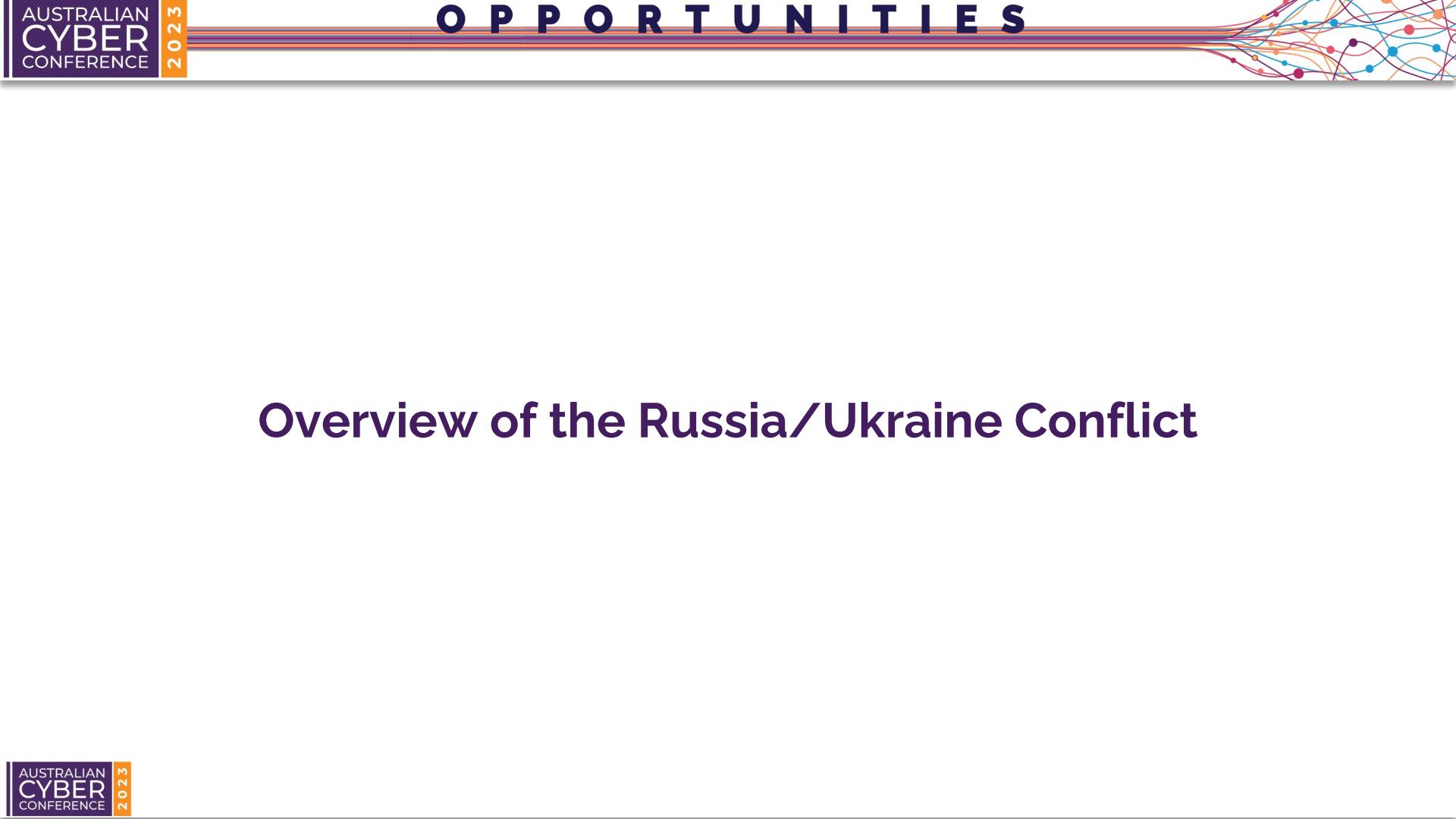
/in/eo-healy



@\_eohealy



## Overview of the Russia/Ukraine Conflict

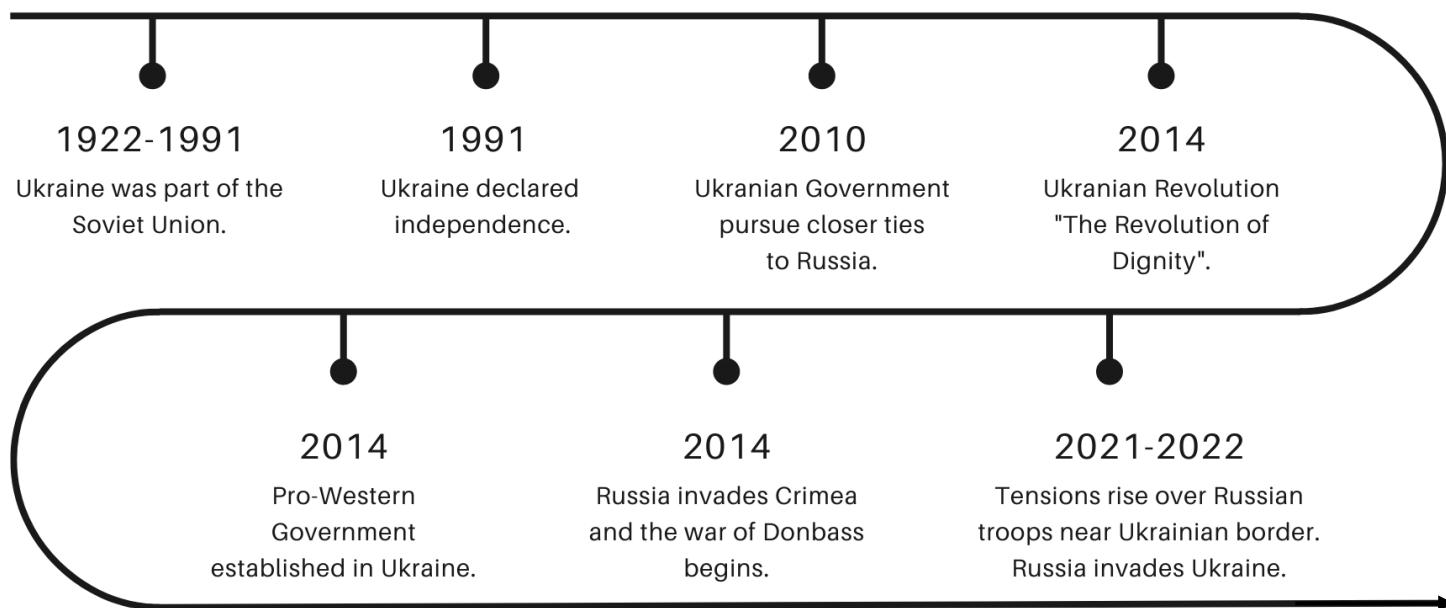


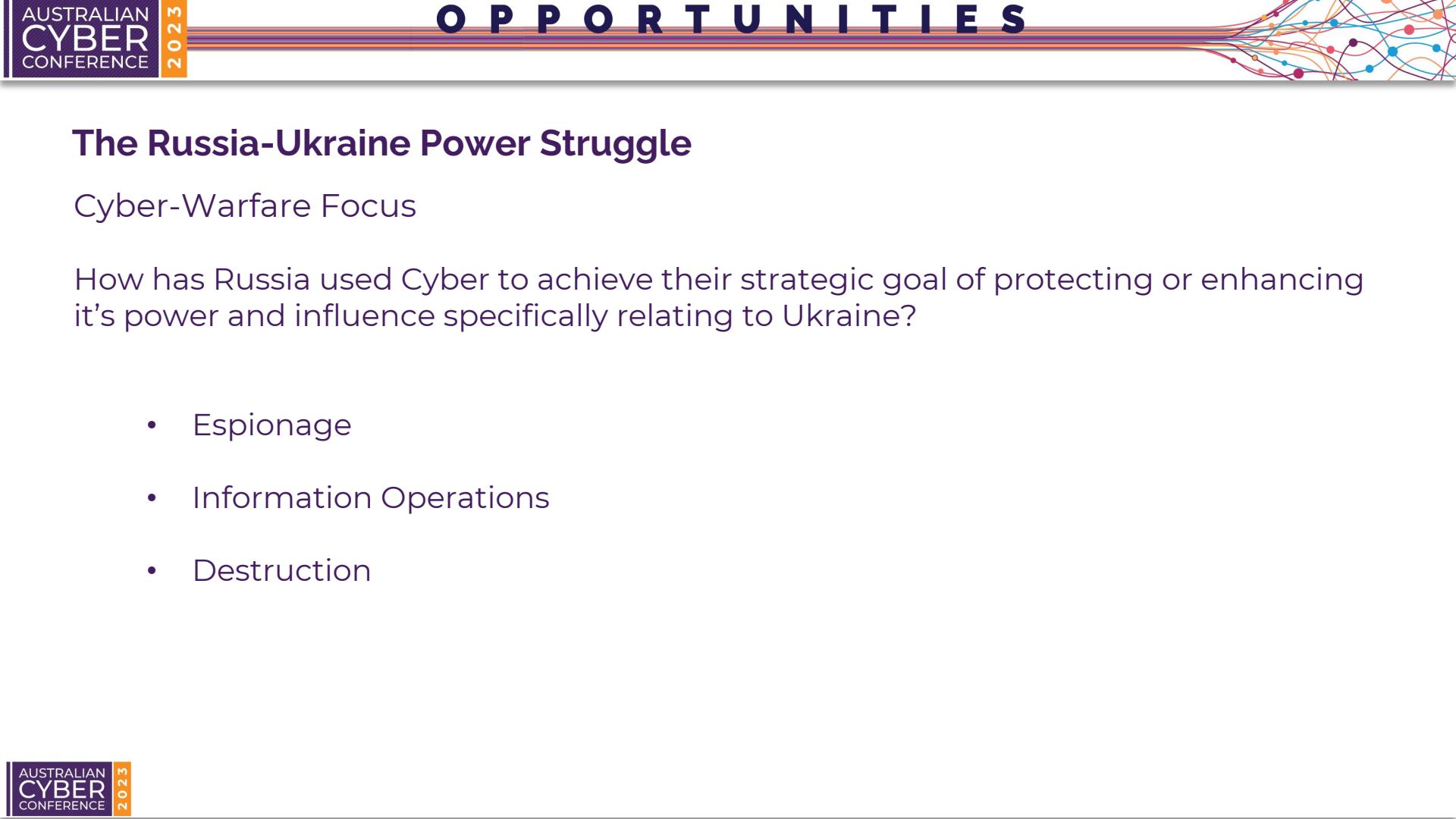


## The Russia-Ukraine Power Struggle

Russia's main goal is to protect or enhance its sphere of influence and control.

Why has Russia pursued conflict with Ukraine throughout the years?





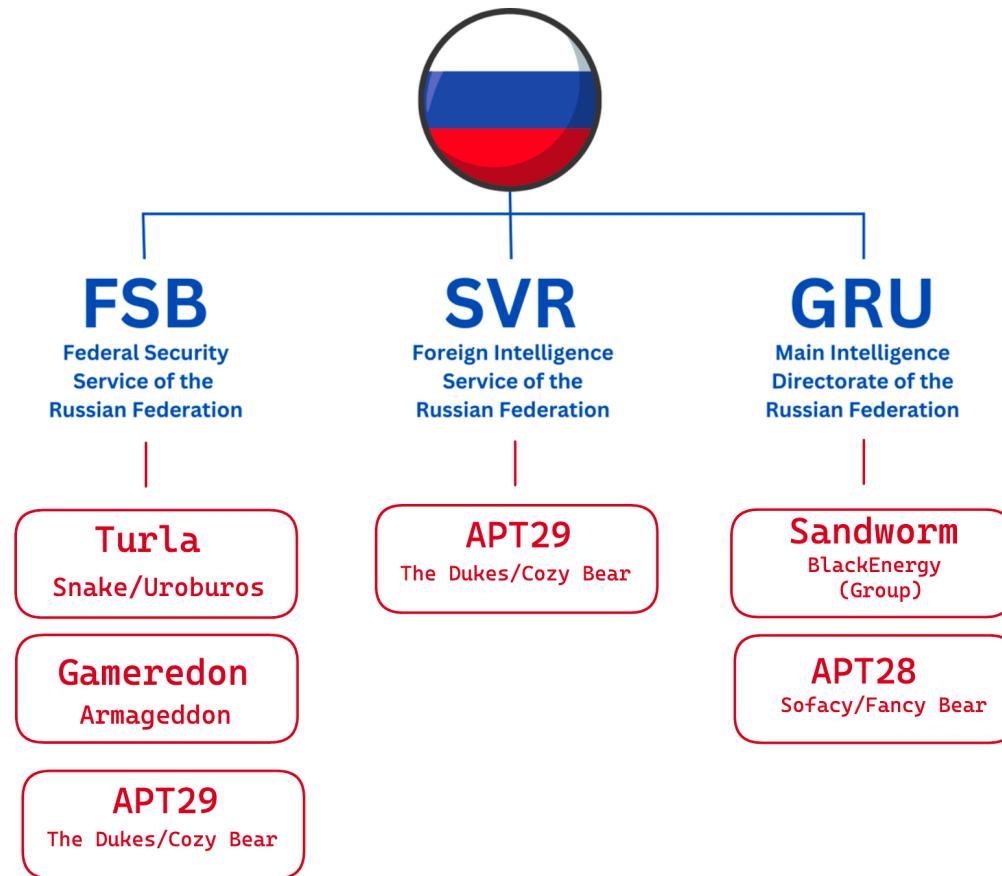
## The Russia-Ukraine Power Struggle

### Cyber-Warfare Focus

How has Russia used Cyber to achieve their strategic goal of protecting or enhancing its power and influence specifically relating to Ukraine?

- Espionage
- Information Operations
- Destruction

## Publicly Reported Attribution





## The Russian Playbook

Russia used Ukraine & Georgia as testbeds to develop their playbook for offensive cyberspace operations

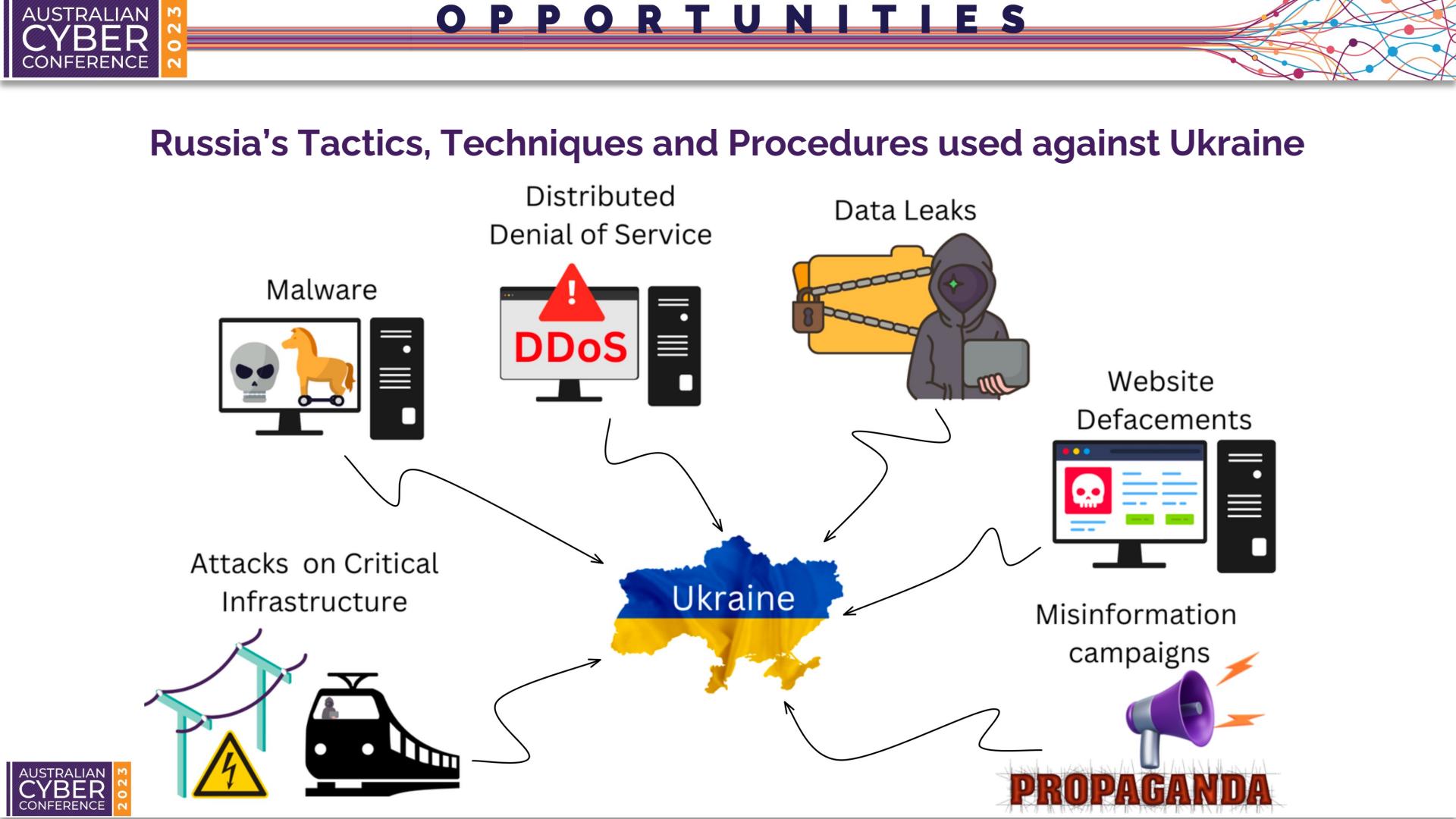
“Russia was turning Ukraine into a test lab for cyberwar innovations”

“The Russians had sought to dominate their enemy in every domain of war: land, sea, air, and now the internet.”

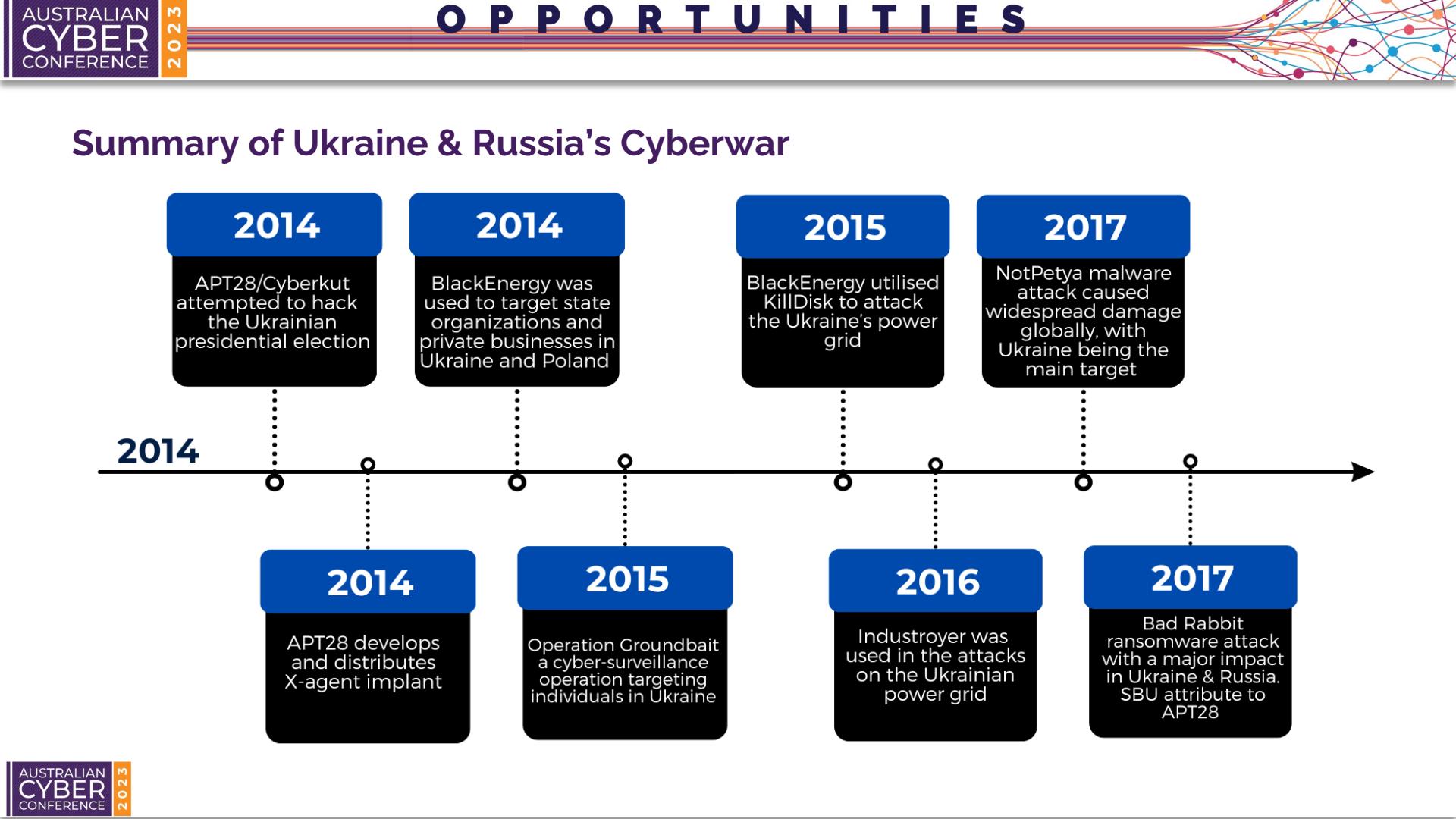
“Georgia was the first crude experiment in a new flavor of hybrid warfare that bridged the digital and the physical.”

“Russia was trying out basic methods of pairing traditional physical attacks with digital weapons of mass disruption.”

- Greenberg, A., 2019. Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers. Anchor.



## Russia's Tactics, Techniques and Procedures used against Ukraine



## Summary of Ukraine & Russia's Cyberwar

**2014**

APT28/Cyberkut attempted to hack the Ukrainian presidential election

**2014**

BlackEnergy was used to target state organizations and private businesses in Ukraine and Poland

**2015**

BlackEnergy utilised KillDisk to attack the Ukraine's power grid

**2017**

NotPetya malware attack caused widespread damage globally, with Ukraine being the main target

**2014**

**2014**

APT28 develops and distributes X-agent implant

**2015**

Operation Groundbait a cyber-surveillance operation targeting individuals in Ukraine

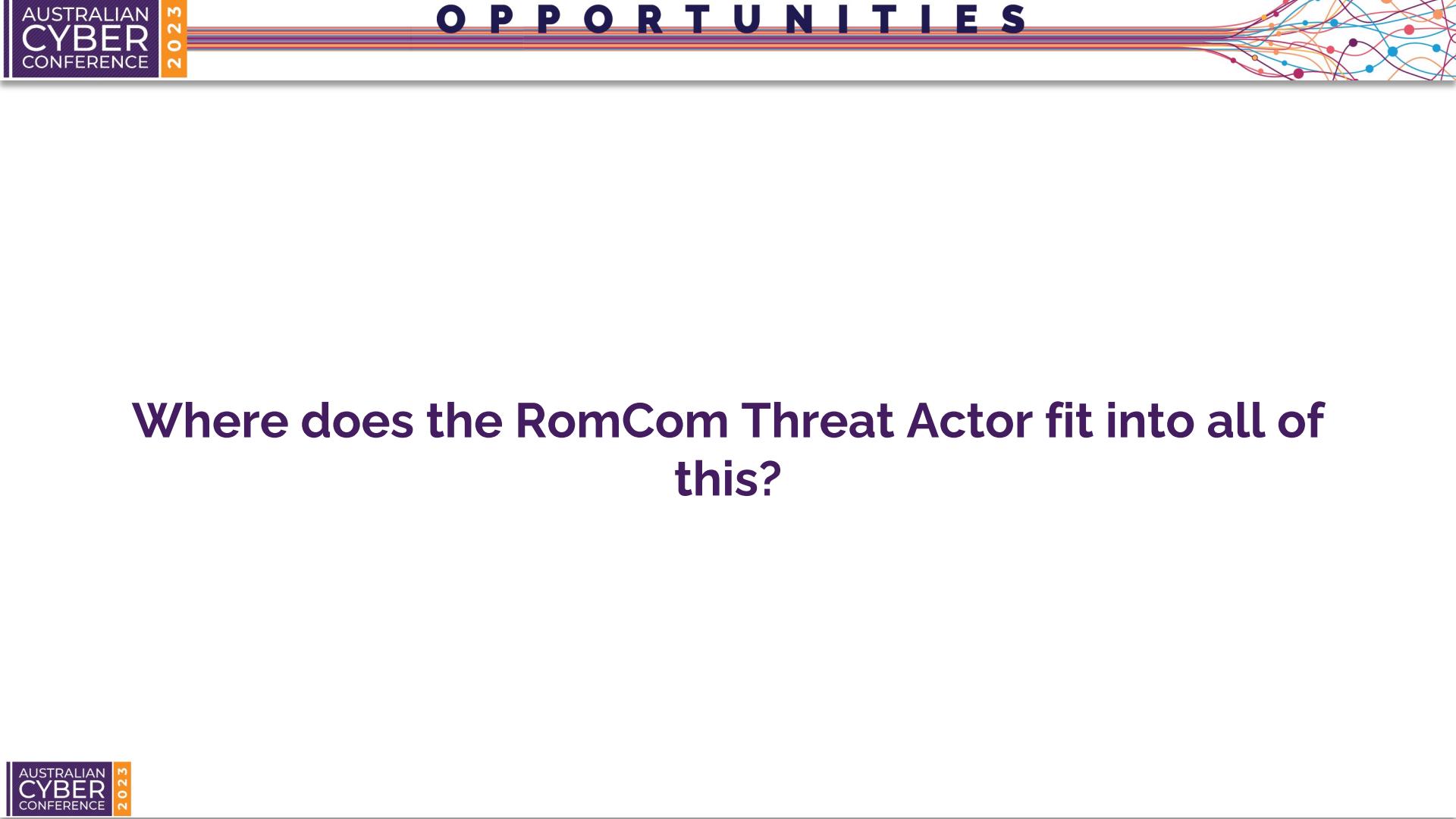
**2016**

Industroyer was used in the attacks on the Ukrainian power grid

**2017**

Bad Rabbit ransomware attack with a major impact in Ukraine & Russia. SBU attribute to APT28





Where does the RomCom Threat Actor fit into all of this?

## Cuba Ransomware?

### Cuba Ransomware Link to RomCom and Industrial Spy Marketplace

- RomCom RAT was **discovered by Unit42** in May 2022 being delivered alongside Cuba Ransomware
- Data exfiltrated in Cuba ransomware attack posted to the Industrial Spy market
- Industrial Spy ransomware shares a very similar ransom note with Cuba ransomware
- Financially motivated interest?



## RomCom Targeting Ukrainian Military

### A Deeper Look into the RomCom Threat Actor and their Tactics

From Пресслужба Генштабу ЗСУ <s.l.sinkewitch@ukr.net> @  
To [REDACTED].gov.ua @  
Subject **До ознайомлення**

Генеральний штаб ЗСУ

Направляємо наказ Міністерства оборони України № 309 від 20.10.2022 «Про підвищення грошового забезпечення військовослужбовцям Збройних Сил України»

Командирам підрозділів довести наказ до особового складу в частині що стосується.

[https://gov.mil.ua.aspx.io/mail/attachment/Наказ\\_309.pdf](https://gov.mil.ua.aspx.io/mail/attachment/Наказ_309.pdf) Наказ 309.pdf

\* +380 800 500 410  
\* <mailto:press@post.mil.gov.ua> press@post.mil.gov.ua  
\* zsu.gov.ua

The screenshot shows a PDF document titled "Наказ\_309.pdf" with the URL "https://gov.mil.ua.aspx.io/mail/attachment/Наказ\_309.pdf". A large red arrow points from the URL in the email message above to the URL in the browser's address bar. Another red arrow points from the bottom of the PDF viewer window to the download link at the bottom of the slide.

Наказ\_309.pdf

https://gov.mil.ua.aspx.io/mail/attachment/Наказ\_309.pdf

PDF Reader

Доступне оновлення програми перегляду PDF.

Це оновлення містить покращення зручності використання, онлайн-безпеки та стабільності, а також нові функції, які допомагають розробникам контенту надавати багатий і привабливий досвід.

Покращення в цій версії включають....

- Критичні оновлення безпеки
- Покращена продуктивність і сумисність відео
- Нові API для покращення роботи в Інтернеті

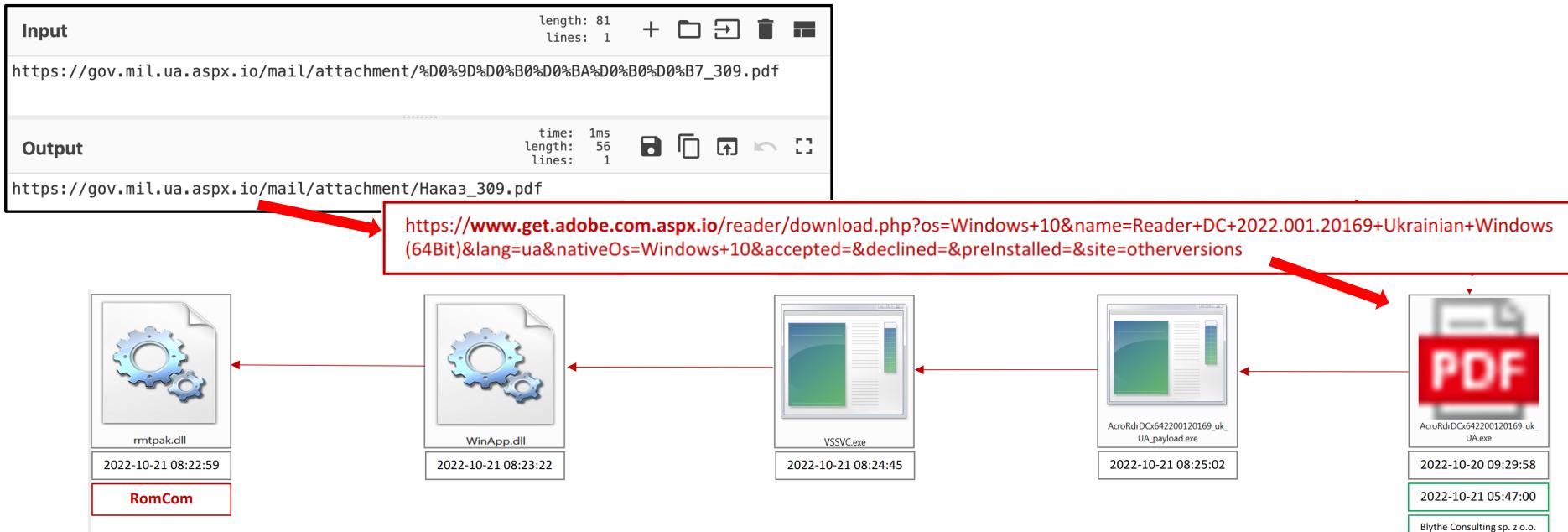
Примітка: якщо ви вибрали встановлення оновлень, це оновлення буде встановлено у вашій системі автоматично протягом 45 днів або ви можете завантажити його зараз.

ЗАВАНТАЖИТИ

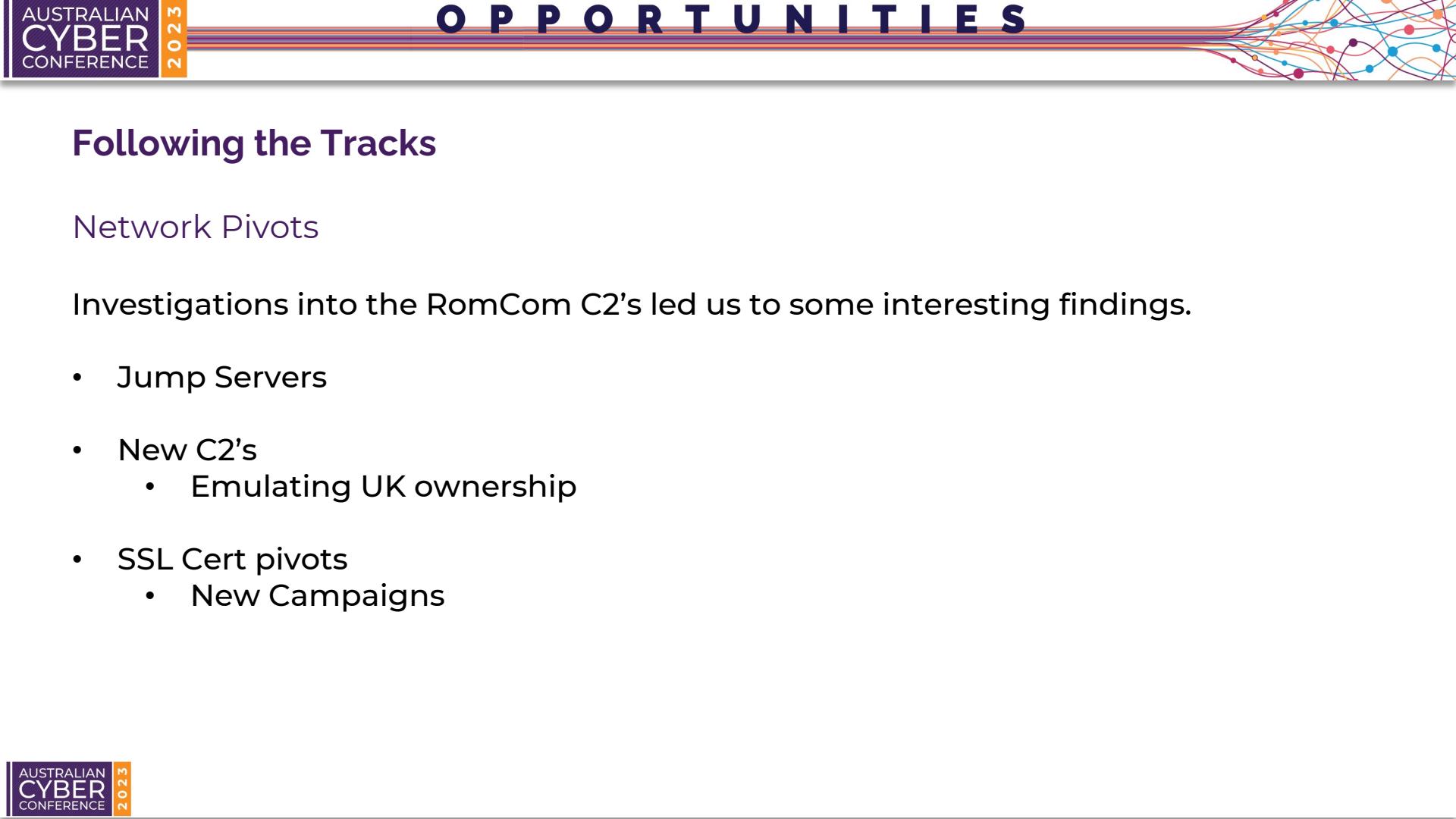
[https://www.get.adobe.com.aspx.io/reader/download.php?os=Windows+10&name=Reader+DC+2022.001.20169+Ukrainian+Windows+\(64Bit\)&lang=ua&nativeOs=Windows+10&accepted=&declined=&preInstalled=&site=otherversions](https://www.get.adobe.com.aspx.io/reader/download.php?os=Windows+10&name=Reader+DC+2022.001.20169+Ukrainian+Windows+(64Bit)&lang=ua&nativeOs=Windows+10&accepted=&declined=&preInstalled=&site=otherversions)

## RomCom Targeting Ukrainian Military

### A Deeper Look into the RomCom Threat Actor and their Tactics







## Following the Tracks

### Network Pivots

Investigations into the RomCom C2's led us to some interesting findings.

- Jump Servers
- New C2's
  - Emulating UK ownership
- SSL Cert pivots
  - New Campaigns

## Following the Tracks

### RomCom Attack Preparations

#### Trojanized SolarWinds NPM Example

1. Scraps legitimate HTML code
2. Registers similar malicious domain
3. Trojanizes legitimate app
4. Uploads malicious bundle to decoy website
5. Deploys targeted phishing emails

Name	File Size	Type	Last Modified
config			
help			
installation			
logs			
mapistub.dll			
mfcore.dll			
mfh264enc.dll			
mpapi.dll			
MSMPEG2ENC.DLL			
scansetting.dat		DAT File	
SearchFolder.dll			
sfc.dll			
Solarwinds-Orion-NPM-Eval	109,283 KB	Application	03/08/2022 18:26
spacebridge.dll	177 KB	Application extension	12/07/2022 08:41
sti.dat	325 KB	DAT File	12/07/2022 08:41
tquery.dll	3,230 KB	Application extension	12/07/2022 08:41
Windows.Media.dll	7,374 KB	Application extension	14/06/2022 04:53
Windows.UI.Core.TextInput.dll	1,016 KB	Application extension	12/07/2022 08:41
WordBreakers.dll	43 KB	Application extension	12/07/2022 08:41
WSManMigrationPlugin.dll	87 KB	Application extension	12/07/2022 08:41
WsmAuto.dll	176 KB	Application extension	12/07/2022 08:41

#### Network Performance Monitor

Multi-vendor network monitoring that scales and expands with the needs of your network

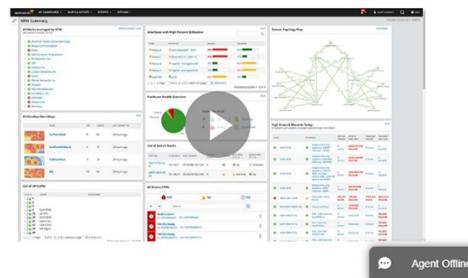
##### Key Features

- Multi-vendor network monitoring
- Network Insights for deeper visibility
- Intelligent maps
- NetPath and PerfStack for easy troubleshooting
- Smarter scalability for large environments
- Advanced alerting

Starts at \$1,638 | [Get a Quote](#)

Subscription and Perpetual Licensing options available

[DOWNLOAD FREE TRIAL](#) [INTERACTIVE DEMO](#)



## Following the Tracks

### RomCom Attack Preparations

RomCom team created a new attack campaign abusing a popular open source password manager called KeePass

The image shows a composite screenshot of a web application. On the left, there is a sidebar with a title 'KeePass' and a sub-section 'ОПИС KEEPASS'. It lists several features under 'ПЛЮСИ' (Pros) such as 'Налаштування є зручним для користувача', 'Двофакторна автентифікація', and 'Можна встановити нагадування про оновлення пароля'. Below this is a section titled 'Початок роботи з KeePass' with instructions on how to download and install it. On the right, the main interface has tabs for 'INFECTION', 'DETAILS', 'RELATIONS' (which is currently selected), 'BEHAVIOR', 'CONTENT', and 'TELEMETRY'. Under 'RELATIONS', it shows 'ITW URLs (1)' with a single entry: 'Scanned 2022-10-31', 'Detections 3 / 90', and 'Status 200'. A URL 'https://keepass.org/KeePass-2.52.zip' is listed under 'URL'. A red arrow points from the left side of the slide towards the 'RELATIONS' tab.

47 / 67

47 security vendors and no sandboxes flagged this file as malicious

596eaef93bdcd00a3aeda6ad6d46db4429eeba61219b7e01b1781ebbf6e321b

KeePass-2.52.zip

zip contains-pe

INFECTION DETAILS RELATIONS BEHAVIOR CONTENT TELEMETRY

ITW URLs (1)

Scanned 2022-10-31

Detections 3 / 90

Status 200

URL

<https://keepass.org/KeePass-2.52.zip>



## Following the Tracks

### RomCom Attack Preparations

Netflow analysis uncovered both spoofed KeePass and PDF Reader Pro sites in Ukrainian language

- PDF Reader Pro had no associated binaries
- PDF Reader Pro Website was discovered on the 01/11/2022
  - The website was dated 02/11/2022
- Likely was in preparation stage





## Continued attacks against Ukraine Military

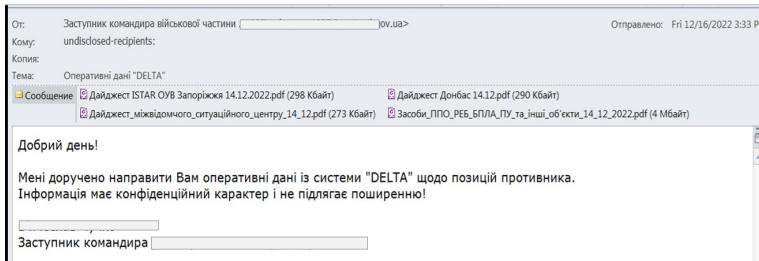
Delta is a situational awareness and battlefield management system

Delta integrates information from a wide range of sensors, intelligence sources, and surveillance streams to provide real-time mapping and analysis of enemy assets

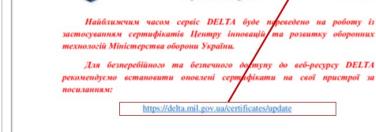
The screenshot shows the official website of the Computer Emergency Response Team of Ukraine (CERT-UA). The header features the Ukrainian trident logo and the text "gov.ua State websites of Ukraine". It also includes links for "People with visual impairments" and a "People with hearing impairments" icon. The main title "CERT-UA" is prominently displayed, along with the subtitle "Computer Emergency Response Team of Ukraine". Below the header, there's a navigation bar with links to "About CERT-UA", "News", "Recommendations", "Contact us", "Contacts", and social media icons for Facebook, Twitter, and RSS. A search bar and a link to "In English" are also present. The main content area displays a news article with the following text:

Cyber attack on DELTA system users using RomCom/FateGrab/StealDeal malware (CERT-UA#5709)

# Phishing Campaign Targeting Delta System Users



14.12.2022



Система ситуаційної обстановки

Fri 12/16/2022 3:33 PM

Отправлено:

Заступник командира військової частини <mailto:...>

Кому:

Копія:

Тема:

Оперативні дані "DELTA"

Сообщение

Дайджест ISTAR ОУВ Запоріжжя\_14.12.2022.pdf (298 Кілобайт)

Дайджест Донбас\_14.12.pdf (290 Кілобайт)

Дайджест\_міжвидового\_ ситуаційного\_центру\_14\_12.pdf (273 Кілобайт)

Засоби\_ППО\_РЕБ\_БПЛА\_ПУ\_та\_інші\_об'єкти\_14\_12\_2022.pdf (4 Мігабайт)

Добрий день!

Мені доручено направити Вам оперативні дані із системи "DELTA" щодо позицій противника.

Інформація має конфіденційний характер і не підлягає поширенню!

Заступник командира

НЕ ДЛЯ РОЗПРОСЮДЖЕННЯ

Піароайл ISTAR ОУВ "Запоріжжя"

МОУ, СБУ, НГУ, ДПСУ та ГО "Аеророндіза"

Дайджест

піароайлу ISTAR в зоні відповідальності ОУВ "Запоріжжя"

\* - в дайджест використано лише об'єкт. Це не координати. Це тільки об'єкт в дайджесті. Коректне ID (т.є. як циклическі об'єкти, про які відсутні в залежності СЦ, можна подивитися на написану попередньо за посиланням: https://delta.mil.gov.ua/dele'

14.12.2022

НЕ ДЛЯ РОЗПРОСЮДЖЕННЯ

ЗАГАЛЬНИЙ ХАРАКТЕР ДІЙ

За оперативною інформацією від 10.12.2022 рОВ обстежили

На інших напрямках підготовки до наступальних (штурмових) дій рОВ не зафіксовано.

Нагадуємо! Більш детальну інформацію ви можете знайти в системі DELTA: <https://delta.mil.gov.ua/>

Найближчим часом сервіс DELTA буде переведено на роботу із застосуванням сертифікатів Центру інновацій та розвитку оборонних технологій Міністерства оборони України.

Для безперебійного та безпечної доступу до веб-ресурсу DELTA рекомендуюмо встановити оновлені сертифікати на свої пристрій за посиланням:

[Установіть сертифікати Центру інновацій та розвитку оборонних технологій Міністерства оборони України](#)

Система розробляється та підтримується Центром інновацій та розвитку оборонних технологій Міністерства оборони України

Технічна підтримка  
E-mail: support@delta.mil.gov.ua  
Signal/WhatsApp: +380 98 297 67 68  
Про систему | Як зареєструватися

[https://delta.mil.gov.ua.delta-storages.com/certificates/windows/certificates\\_rootca.zip](https://delta.mil.gov.ua.delta-storages.com/certificates/windows/certificates_rootca.zip)

C:\asis.exe

Installing certificate(s) in store Root ...

Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

CID Defense Technologies

Windows cannot validate that the certificate is actually from "CID Defense Technologies ". You should confirm its origin by contacting "CID Defense Technologies ". The following will assist you in this process:

Thumbprint (sha1): 0009C804 F4B62052 44D5A3D7 98D2710E 80564C83

Warning:

If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Yes No





## Why are the RomCom attacks against the Ukrainian Military of significant importance?



## A Shift in the Threat Landscape?

### Crossover of Tactics and Targets

Increasingly we are noticing a crossover in TTPs and targets between typically financially motivated cybercrime groups and “state-sponsored” threat groups.

- Initial link to Cuba ransomware & Industrial Spy Marketplace would suggest a financial motivation
- Muddy the waters? False flag?
- Shift of targets to the Ukrainian military



## A Shift in the Threat Landscape?

Blurring the lines between cybercrime and “state-sponsored” groups

Microsoft identified a new ransomware strain "Prestige" in attacks impacting organizations in Ukraine and Poland

- Prestige was targeting organizations in the transportation and related logistics industries in Ukraine and Poland
- Attributed to Iridium (aka Sandworm)
- Difficult to distinguish between state-sponsored and criminal activity

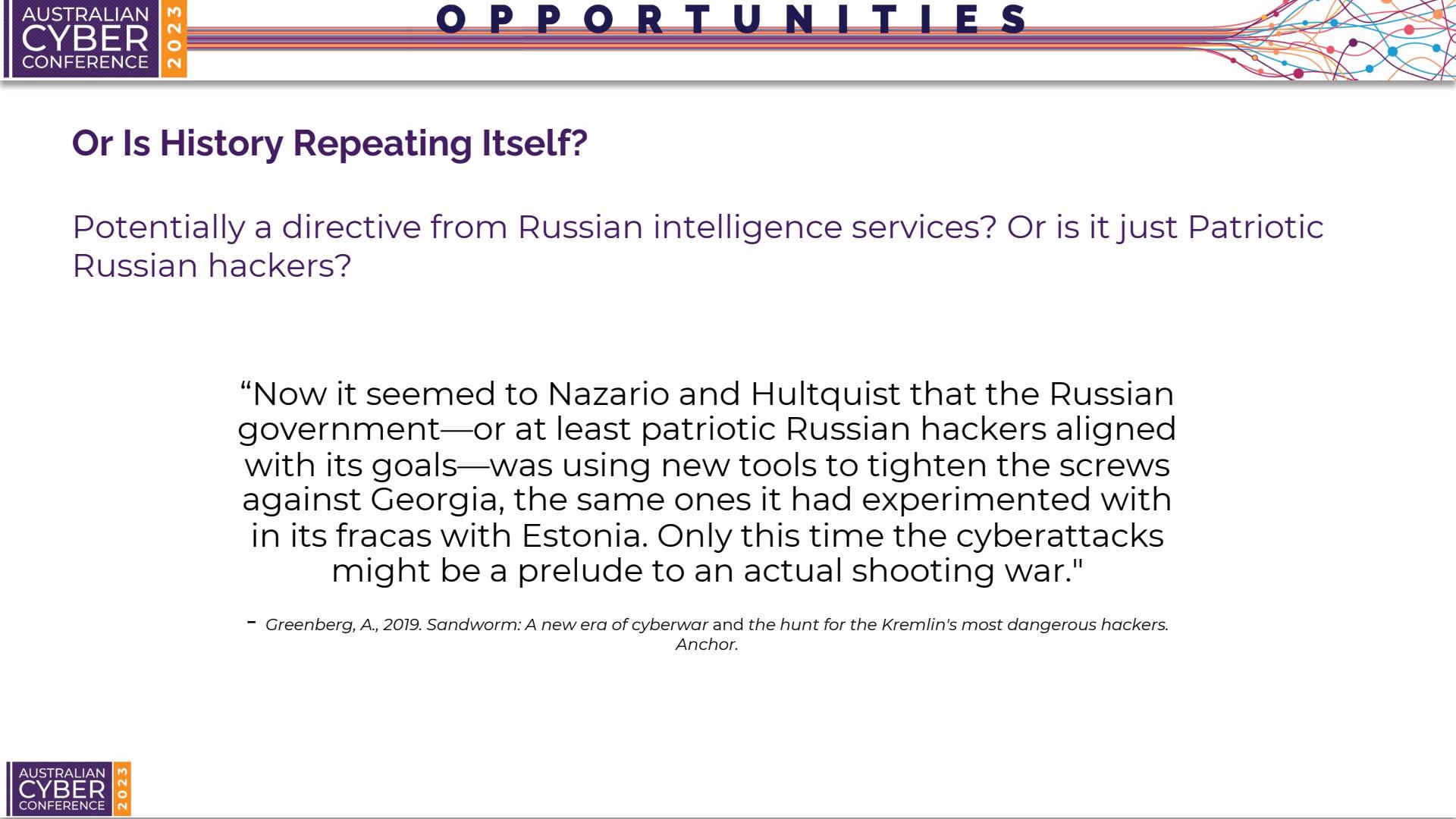


## A Shift in the Threat Landscape?

Blurring the lines between cybercrime and “state-sponsored” groups

Google TAG identified overlaps between financially motivated and government-backed threat actors

- UAC-0098 historically delivered IcedID acting as an initial access broker for ransomware groups.
- Shifted their focus to targeting Ukrainian organizations, the Ukrainian government, and European humanitarian and non-profit organizations
- UAC-0098 is believed to be former Conti members repurposing techniques to target Ukraine.

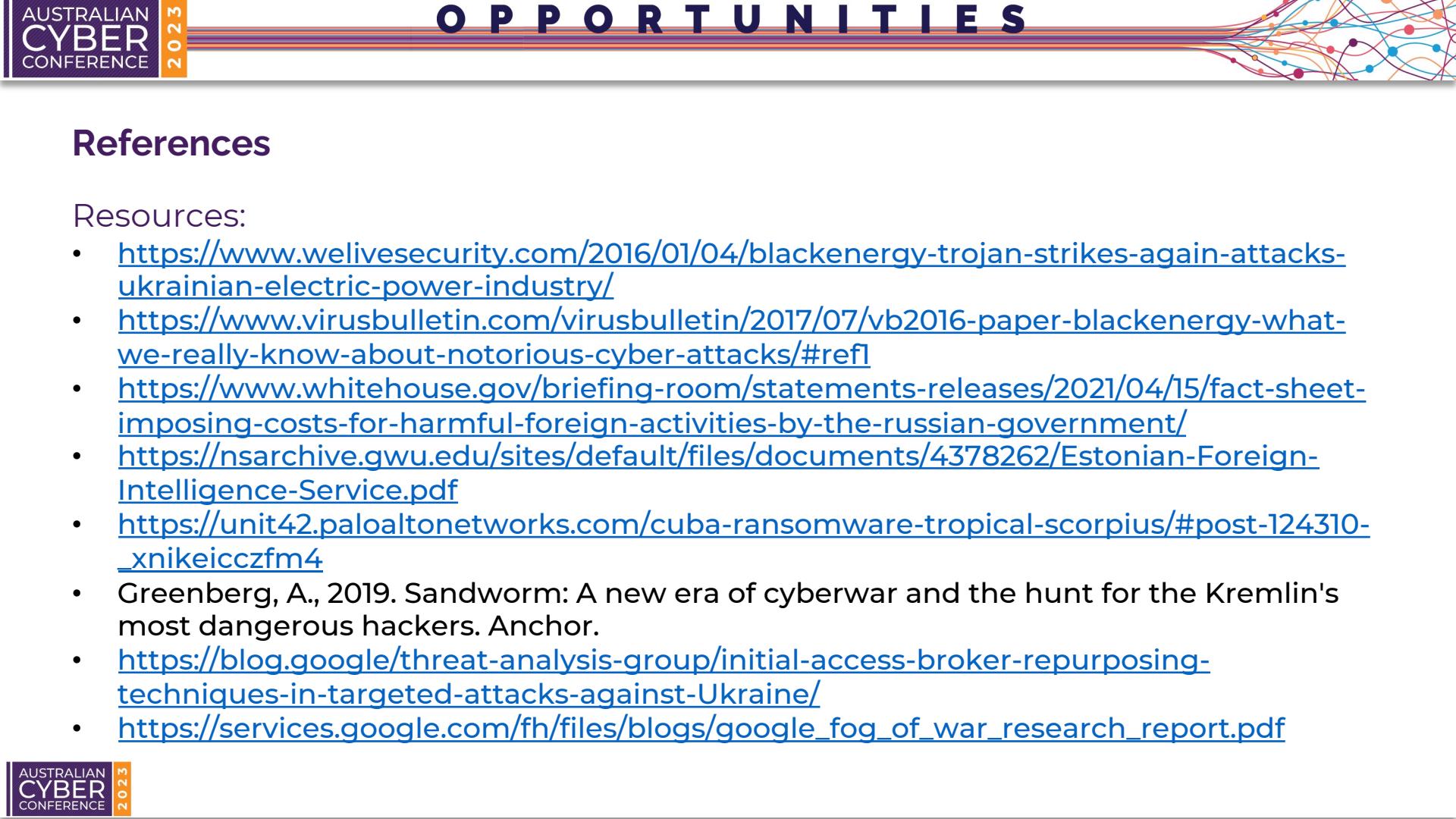


## Or Is History Repeating Itself?

Potentially a directive from Russian intelligence services? Or is it just Patriotic Russian hackers?

“Now it seemed to Nazario and Hultquist that the Russian government—or at least patriotic Russian hackers aligned with its goals—was using new tools to tighten the screws against Georgia, the same ones it had experimented with in its fracas with Estonia. Only this time the cyberattacks might be a prelude to an actual shooting war.”

- Greenberg, A., 2019. *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers.* Anchor.



## References

Resources:

- <https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/>
- <https://www.virusbulletin.com/virusbulletin/2017/07/vb2016-paper-blackenergy-what-we-really-know-about-notorious-cyber-attacks/#ref1>
- <https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/>
- <https://nsarchive.gwu.edu/sites/default/files/documents/4378262/Estonian-Foreign-Intelligence-Service.pdf>
- <https://unit42.paloaltonetworks.com/cuba-ransomware-tropical-scorpius/#post-124310-xnikeicczfm4>
- Greenberg, A., 2019. Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers. Anchor.
- <https://blog.google/threat-analysis-group/initial-access-broker-repurposing-techniques-in-targeted-attacks-against-Ukraine/>
- [https://services.google.com/fh/files/blogs/google\\_fog\\_of\\_war\\_research\\_report.pdf](https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf)



## Questions?

Thank you!