AISA

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

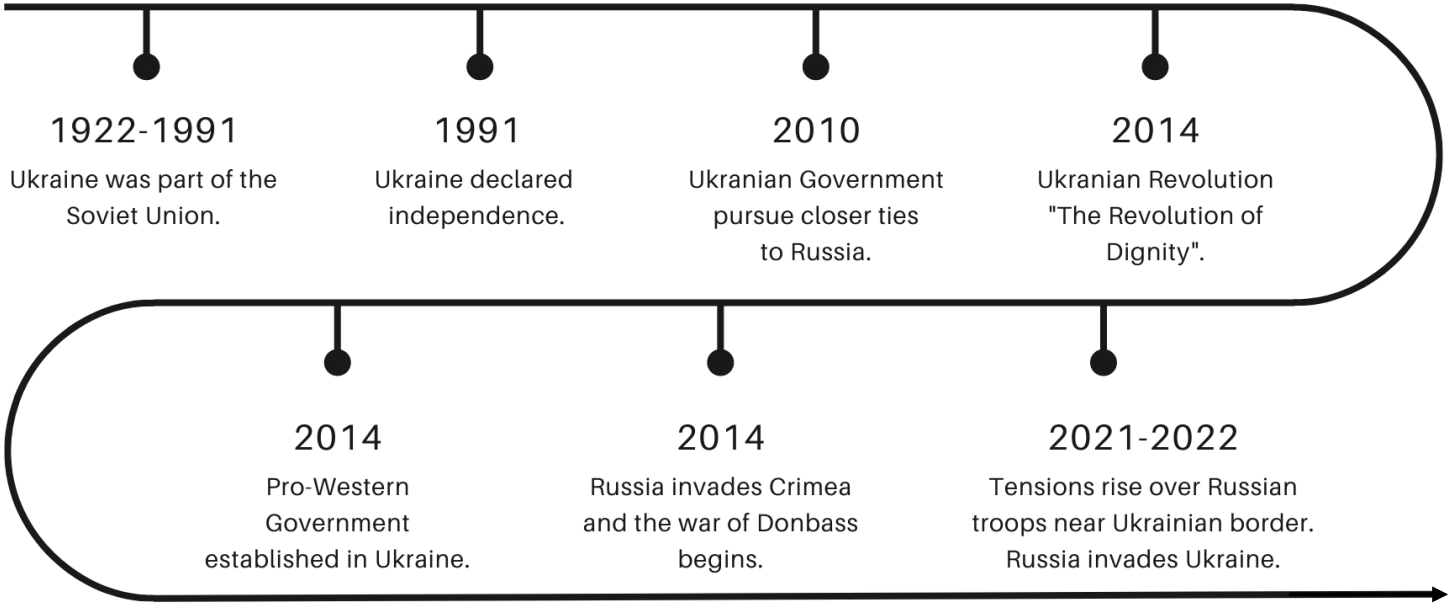
@_eohealy

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 it's power and influence specifically relating to Ukraine?

- Espionage
- Information Operations
- Destruction

Publicly Reported Attribution

FSB
Federal Security Service of the Russian Federation

- **Turla**
  Snake/Uroburos
- **Gameredon**
  Armageddon
- **APT29**
  The Dukes/Cozy Bear

SVR
Foreign Intelligence Service of the Russian Federation

- **APT29**
  The Dukes/Cozy Bear

GRU
Main Intelligence Directorate of the Russian Federation

- **Sandworm**
  BlackEnergy (Group)
- **APT28**
  Sofacy/Fancy Bear

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"

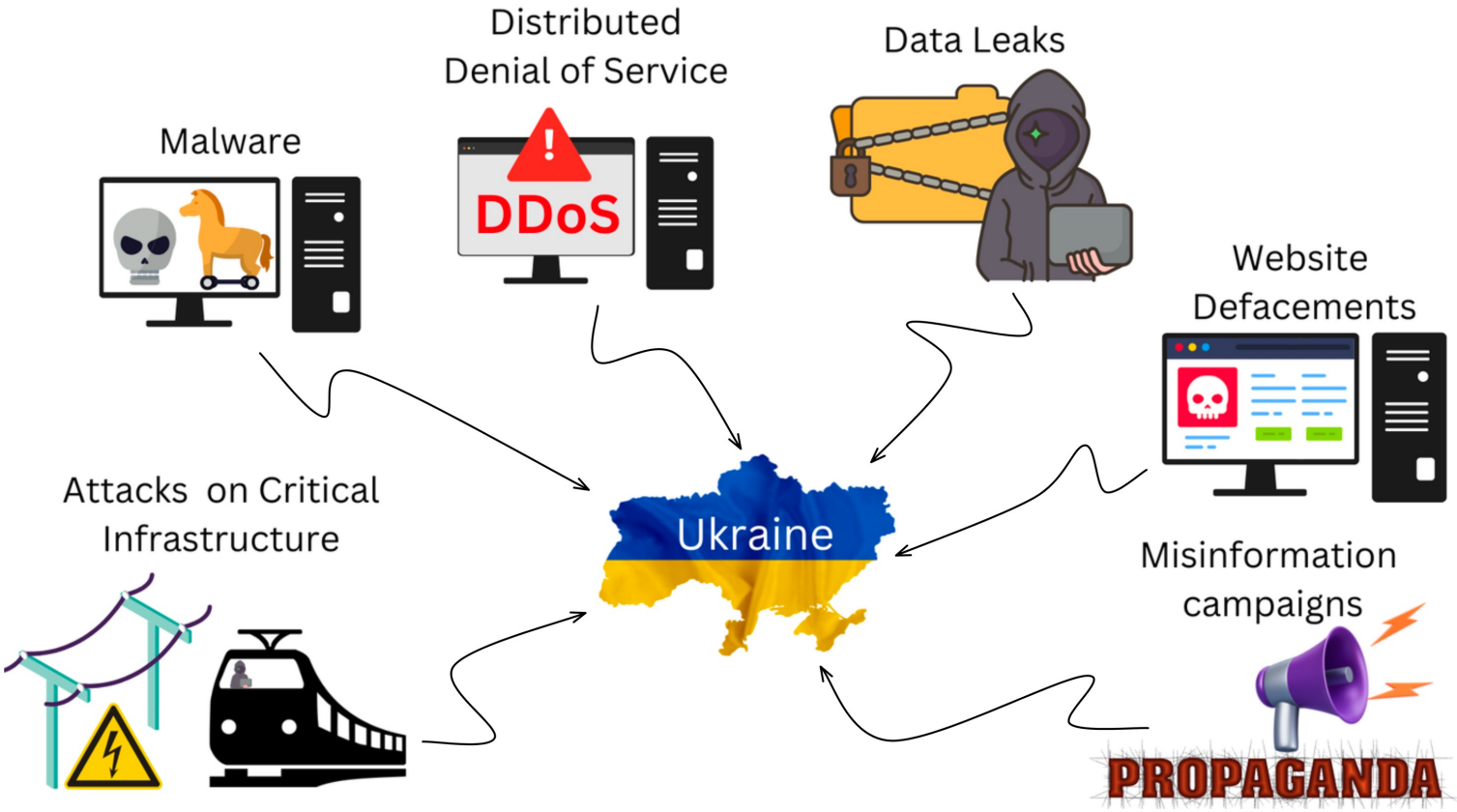
"The Russians had sought to dominate their enemy in every domain of war: land, sea, air, and now the internet."

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

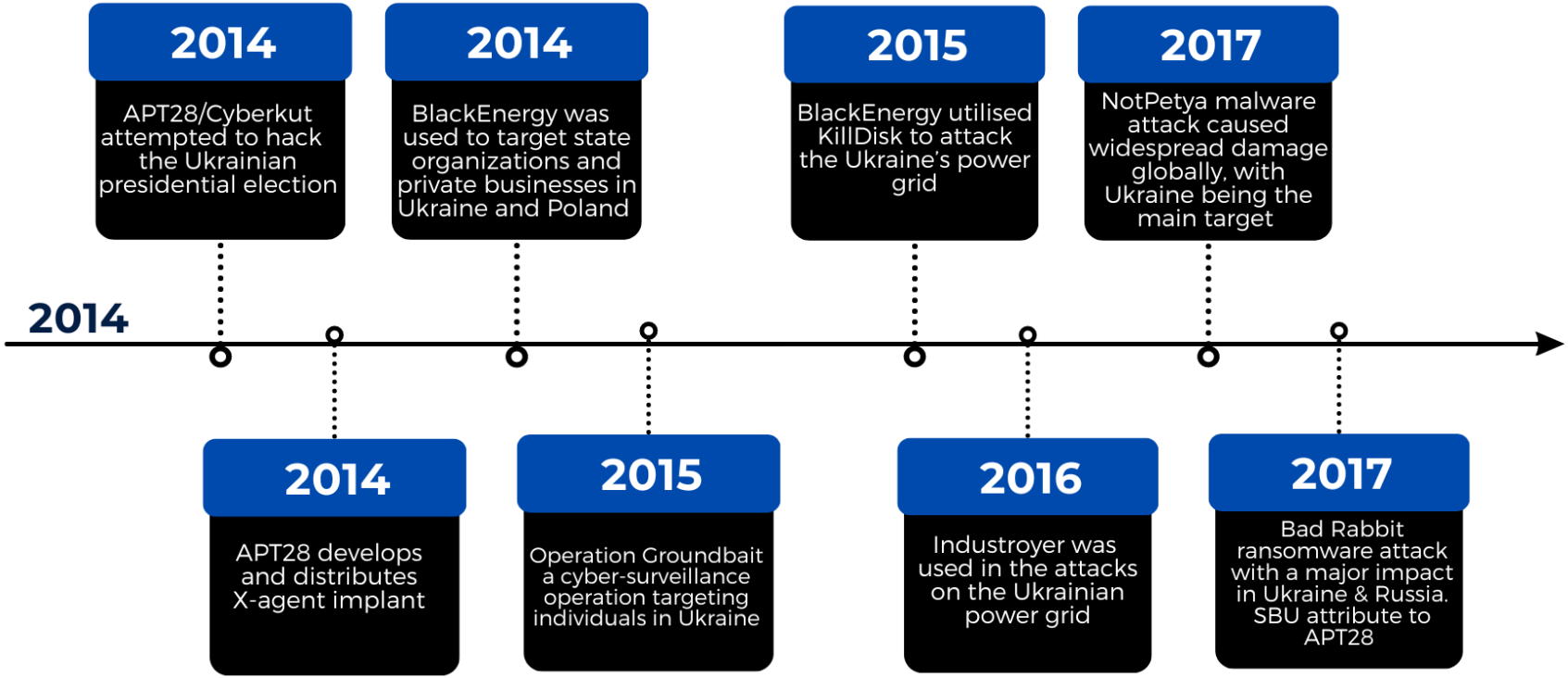
"Russia was trying out basic methods of pairing traditional physical attacks with digital weapons of mass disruption."

- 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



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?

Ref: https://unit42.paloaltonetworks.com/cuba-ransomware-tropical-scorpius/#post-124310-_xnikeicczfm4
Ref: https://www.cisa.gov/uscert/ncas/alerts/aa22-335a

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»

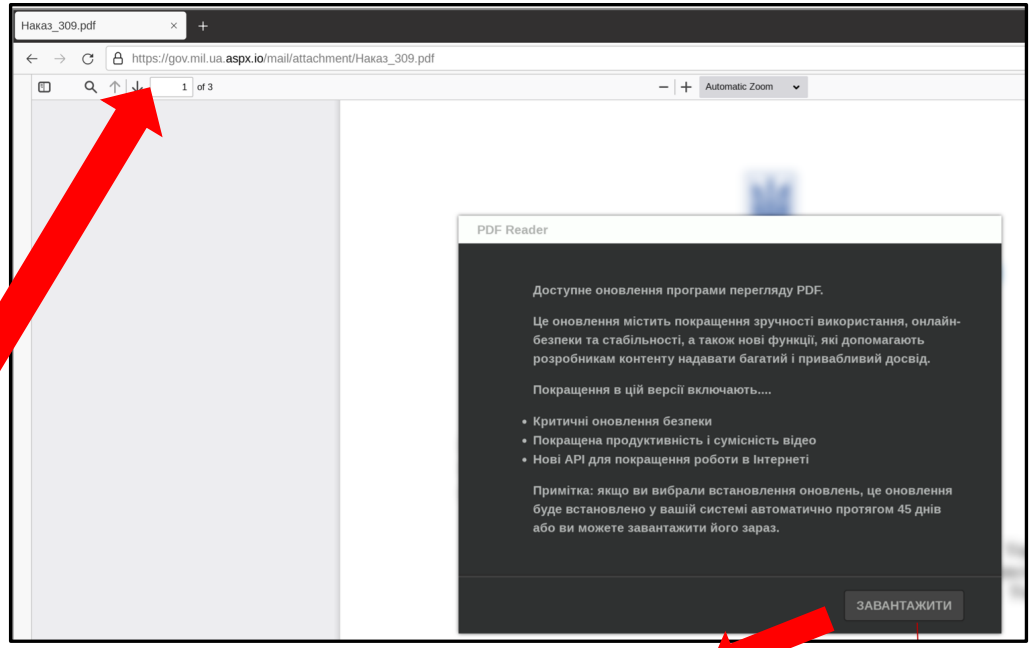
Командирам підрозділів довести наказ до особового складу в частині що стосується.

<https://gov.mil.ua.aspx.io/mail/attachment/Наказ_309.pdf> Наказ_309.pdf

* +380 800 500 410

* <mailto:press@post.mil.gov.ua> press@post.mil.gov.ua

* zsu.gov.ua



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

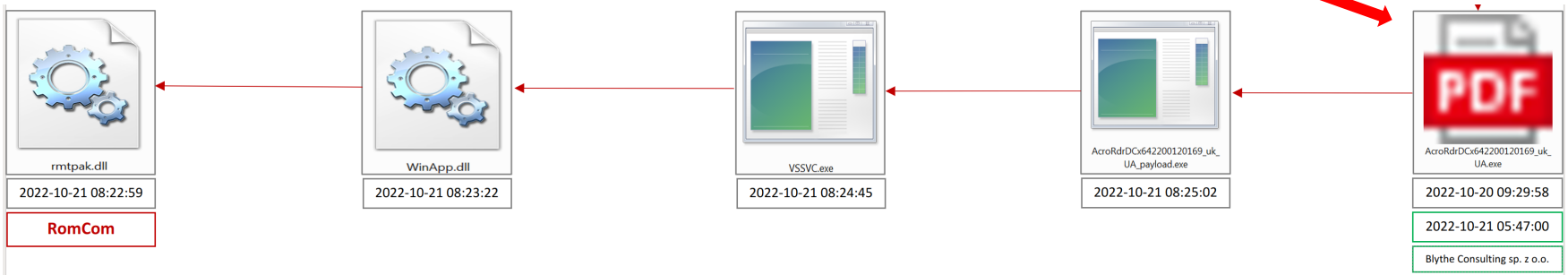
Input length: 81 lines: 1

```
https://gov.mil.ua.aspx.io/mail/attachment/%D0%9D%D0%B0%D0%BA%D0%B0%D0%B7_309.pdf
```

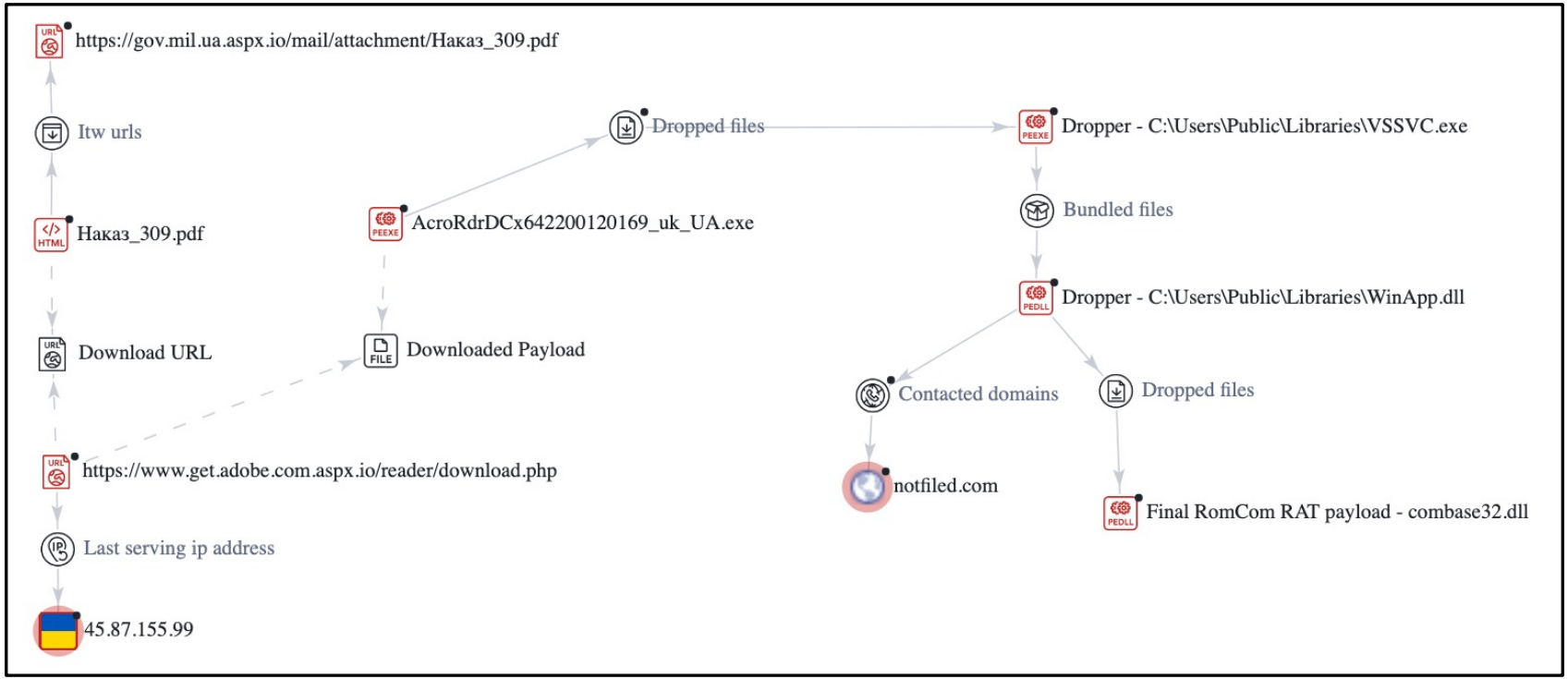
Output time: 1ms length: 56 lines: 1

```
https://gov.mil.ua.aspx.io/mail/attachment/Наказ_309.pdf
```

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



Following the Tracks

Network Pivots

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

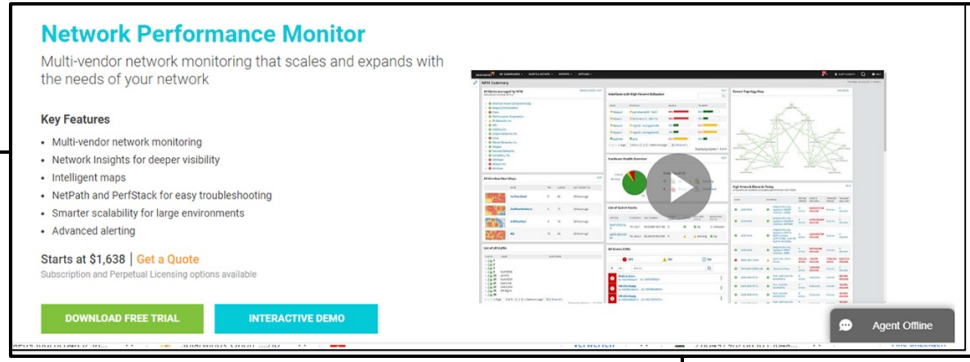
- Jump Servers
- New C2's
  - Emulating UK ownership
- SSL Cert pivots
  - New Campaigns

Following the Tracks

RomCom Attack Preparations

Trojanized SolarWinds NPM Example

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

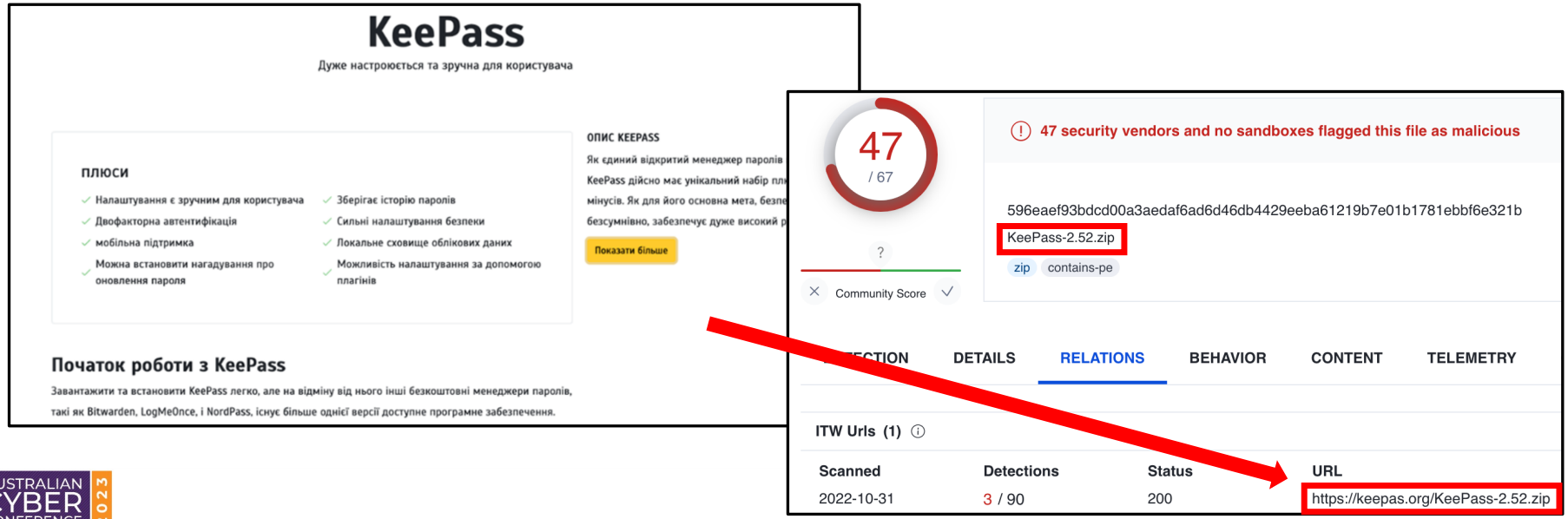


Name			
config			
help			
installation			
logs			
mapistub.dll			
mfcore.dll			
mfh264enc.dll	12/07/2022 08:41	Application extension	568 KB
mprapi.dll	14/06/2022 04:53	Application extension	514 KB
MSMPEG2ENC.DLL	14/06/2022 04:53	Application extension	922 KB
scansetting.dat	12/07/2022 08:41	DAT File	291 KB
SearchFolder.dll	14/06/2022 04:53	Application extension	403 KB
sfc.dll	14/06/2022 04:53	Application extension	13 KB
Solarwinds-Orion-NPM-Eval	03/08/2022 18:26	Application	109,283 KB
spacebridge.dll	12/07/2022 08:41	Application extension	177 KB
sti.dat	12/07/2022 08:41	DAT File	325 KB
tquery.dll	12/07/2022 08:41	Application extension	3,230 KB
Windows.Media.dll	14/06/2022 04:53	Application extension	7,374 KB
Windows.UI.Core.TextInput.dll	12/07/2022 08:41	Application extension	1,016 KB
WordBreakers.dll	12/07/2022 08:41	Application extension	43 KB
WSManMigrationPlugin.dll	12/07/2022 08:41	Application extension	87 KB
WsmAuto.dll	12/07/2022 08:41	Application extension	176 KB

Following the Tracks

RomCom Attack Preparations

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



Following the Tracks

RomCom Attack Preparations

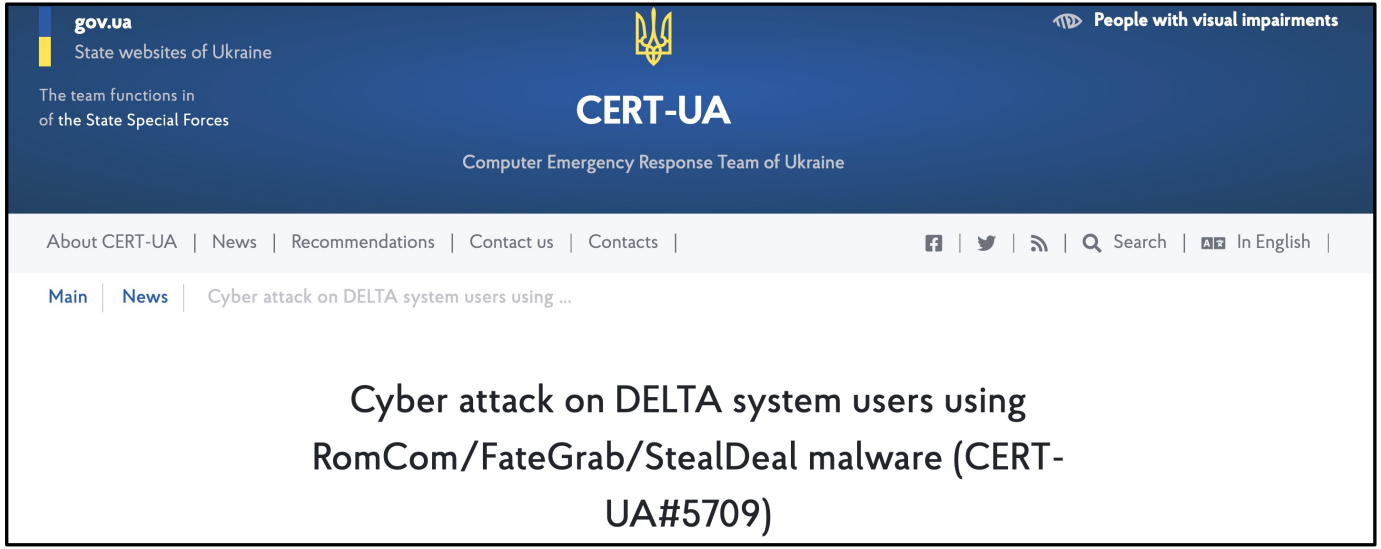
Netflow analysis uncovered both spoofed KeePass and PDF Reader Pro sites in Ukrainian language

- 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

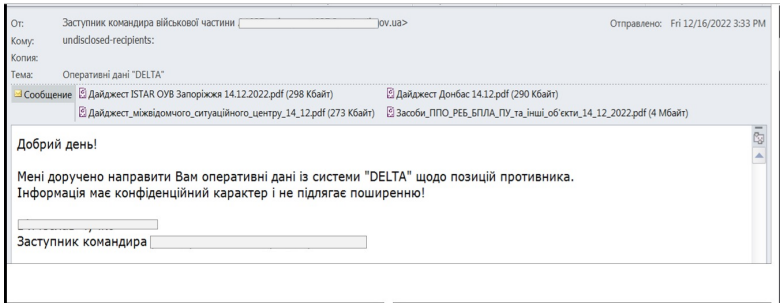
Continued attacks against Ukraine Military

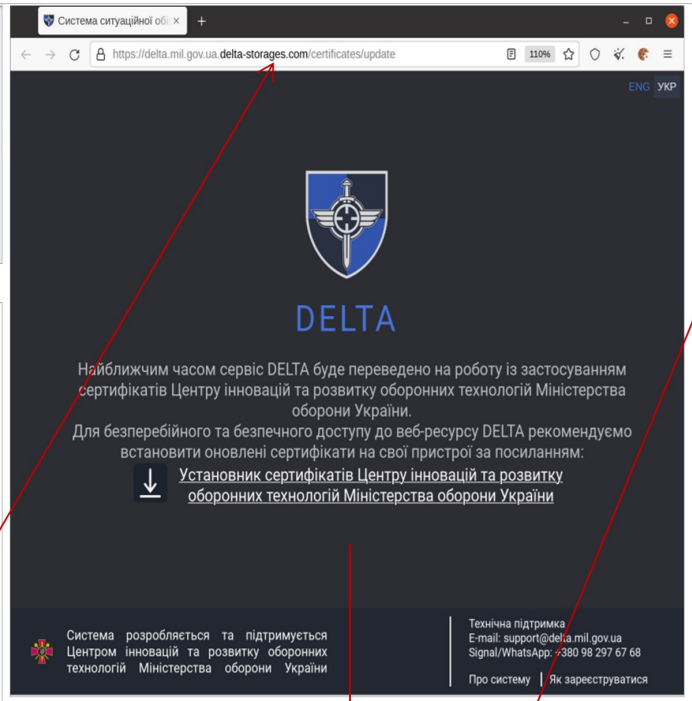
Delta is a situational awareness and battlefield management system

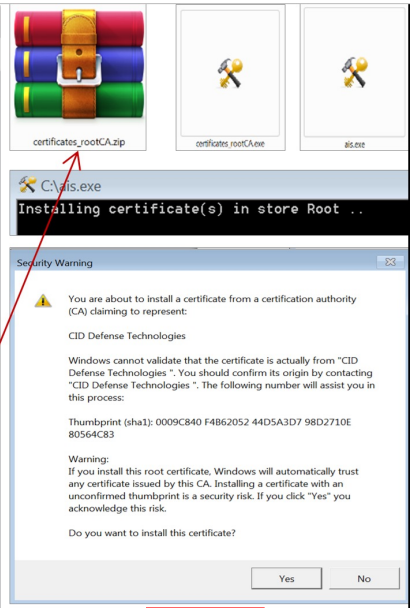
Delta integrates information from a wide range of sensors, intelligence sources, and surveillance streams to provide real-time mapping and analysis of enemy assets



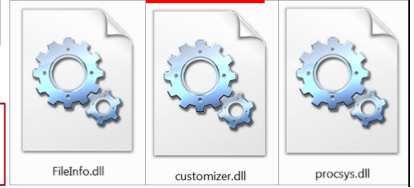
Phishing Campaign Targeting Delta System Users







FateGrab **RomCom** **StealDeal**



https://delta.mil.gov.ua.**delta-storages.com**/
certificates/windows/**certificates_rootca.zip**

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

Ref: https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/

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.

Ref: https://kcm.trellix.com/corporate/index?page=content&id=KB96150&locale=en_US

Ref: https://blog.google/threat-analysis-group/initial-access-broker-repurposing-techniques-in-targeted-attacks-against-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

Questions?

Thank you!