#OpAPT28 by Anonymous - APT28 - Fancy Bear

@anonymous · May 1, 2025

Operation APT28.

GRU-Linked Infrastructure :

Primary Domains :

- `mil.ru`
- `sso.mil.ru (Official portal of the Russian Ministry of Defens`

C2 - Phishing Domain :

- frge.io (Phishing and Command & Control infrastructure)

Subdomains :

- https://setnewcreds.ukr.net.frge.io
  http://setnewcreds.ukr.net.frge.io
  https://re-authentication-702.frge.io
  https://moneypath65.frge.io
  https://setnewcred.ukr.net.frge.io
  http://re-authenticate-647.frge.io
  http://kitten-948.frge.io:443
  https://kitten-604.frge.io
  http://moneypath65.frge.io

http://panelunregistertle-348.frge.io
http://sharepointo365voicemails.frge.io
https://sharepointo365voicemails.frge.io
https://smtp-relay.frge.io
http://smtp-relay.frge.io
http://suspectpractice29.frge.io
http://kitten-396.frge.io:443
http://ponelunregistertle-348.frge.io:443
http://robot-876.frge.io
https://suspectpractice29.frge.io
http://monkey-76.frge.io
http://shark-387.frge.io
http://office-3-docturtle-302.frge.io
https://service-panel-inc.frge.io
http://office-3-docturtle-302.frge.io:443
http://robot-876.frge.io:443
http://shark-354.frge.io
http://ua-consumerpanel.frge.io:443
http://moneypath40.frge.io:443
http://poczta.exalo.pl.frge.io:443
http://moneypath59.frge.io
https://monkey-76.frge.io
http://tellcourse2.frge.io
http://ua-consumerspanel.frge.io
http://shark-549.frge.io:443
http://kitten-604.frge.io
http://net.frge.io
http://moneypath20.frge.io:443

http://shark-549.frge.io
https://partsbinord-215.frge.io
http://service-panel-inc.frge.io
http://uaconsumerpanel.frge.io:443
http://setnewcred.ukr.net.frge.io
http://moneypath64.frge.io
http://sugarsgames.frge.io
http://ponelunregistertle-348.frge.io
http://moneypath66.frge.io
http://net.frge.io:443
http://moneypath59.frge.io:443
http://re-authentication-702.frge.io
http://sberbank-vyplaty-detyam-do-18-let.frge.io:443
http://panelunregistertle-348.frge.io:443
http://settings-panel.frge.io
http://settings-panel.frge.io:443
http://moneypath40.frge.io
http://poczta.exalo.pl.frge.io
http://ukr.net.frge.io:443
http://sharkk-406.frge.io
http://moneypath20.frge.io
http://mail-gov-ua.frge.io:443
https://shark-387.frge.io
http://re-authenticate-647.frge.io:443
http://monkey-31.frge.io
http://moneypath67.frge.io:443
https://ua-consumerspanel.frge.io
http://sberbank-vyplaty-detyam-do-18-let.frge.io

http://lightpixel-360.frge.io:443
http://moneypath66.frge.io:443
http://ukr.net.frge.io
http://uaconsumerpppanel.frge.io:443
https://ukrsettingspanel.frge.io
http://monkey-31.frge.io:443
http://moneypath67.frge.io
https://ukrprivacysite.frge.io
https://wetransf-022022.frge.io
http://moneypath64.frge.io:443
http://ukrsettingspanel.frge.io
http://xn--panelunregistertle348-dun.frge.io
http://www.kitten-396.frge.io
http://wetransfr-022022.frge.io:443
https://ukrprivatesite.frge.io
http://lightpixel-360.frge.io
http://usersettingspanel.frge.io:443
http://ukrprivacysite.frge.io
https://xgfdstu6k.frge.io
https://www.kitten-396.frge.io
http://xcfhgxcfjhghjhgk.frge.io
http://uaconsumerpppanel.frge.io
http://xgfdstu6k.frge.io
http://ukrprivatesite.frge.io
http://usersettingspanel.frge.io
http://wetransfr-022022.frge.io
https://xn--panelunregistertle348-dun.frge.io

https://xcfhgxcfjhghjhgk.frge.io
http://wetransf-022022.frge.io

Sample C2 Infrastructure :

```
IP Address : 3.8.198.160
ASN : AS16509 (Amazon.com, Inc.)
Hostname : ec2-3-8-198-160.eu-west-2.compute.amazonaws
IP Range : 3.8.0.0/14
Company : Amazon Data Services UK
Privacy Proxy : True
Anycast : False
Hosting Type : Cloud Infrastructure (AWS EC2)
```

APT28 Members (Unit 26165 / Unit 74455) :

1. Dmitriy Sergeyevich Badin — Officer, Unit 26165 — Involved in DNC hack and WADA intrusion
2. Ivan Sergeyevich Yermakov — Officer, Unit 26165 — Specialist in phishing infrastructure
3. Artem Andreyevich Malyshev — Developer, Unit 26165 — X-Agent malware developer
4. Aleksei Valeryevich Minin — Support staff, Unit 26165 — Logistics and ops coordination

5. Aleksei Sergeyevich Morenets — Operative, Unit 26165 — Field ops in The Hague (OPCW)
6. Evgenii Mikhaylovich Serebriakov — Operative, Unit 26165 — Participated in OPCW cyber ops
7. Oleg Mikhaylovich Sotnikov — Field Agent, Unit 26165 — Surveillance in cyber missions
8. Viktor Borisovich Netyksho — Commander, Unit 26165 — Senior leadership of GRU cyber ops
9. Boris Alekseyevich Antonov — Deputy Commander, Unit 26165 — Strategic coordination
10. Aleksey Viktorovich Lukashev — Operator, Unit 26165 — Spearphishing and email targeting
11. Sergey Aleksandrovich Morgachev — Officer, Unit 26165 — Lead planner in DNC breach
12. Nikolay Yuryevich Kozachek — Developer, Unit 26165 — Malware engineering
13. Pavel Vyacheslavovich Yershov — Operator, Unit 26165 — Targeting U.S. infrastructure
14. Aleksandr Vladimirovich Osadchuk — Director, Unit 26165 — Oversight of operations
15. Aleksey Aleksandrovich Potemkin — Analyst, Unit 26165 — Vulnerability and network research
16. Anatoliy Sergeyevich Kovalev — Operator, Unit 26165 — Spam, DDoS, and disinfo operations
17. Vladislav Yevgenyevich Borovkov — Unknown assignment — Possibly new operator
18. Yuriy Fedorovich Denisov — Unknown assignment — Possibly new operator

Summary :

APT28, also known as Fancy Bear or Sofacy, is a Russian military intelligence threat group attributed to GRU units 26165 and 74455. This group is responsible for a wide range of cyber espionage and influence operations, including :

- The 2016 DNC and U.S. election interference
- Attacks on NATO, Eastern European states, and anti-doping agencies
- Deployment of malware families like X-Agent, CHOPSTICK, and Sednit
- Use of spearphishing, credential harvesting, and advanced persistence techniques

Many of the individuals listed above have been indicted by USA federal authorities for their roles in these activities, including conspiracy to commit computer fraud, identity theft, and wire fraud.

To APT28 : You started this cyberwar, we will finish it.

We are Anonymous.
We are Legion.
We do not Forgive.
We do not Forget.
Expect us.

x.com/YourAnonFrench_
x.com/Anonymousbsns
x.com/YourAnonMajor_
x.com/YourAnonCN
x.com/YourAnonSurge_