

THREAT ACTORS PIÙ NOTI

ANALISI CONDOTTA DA MELE
LUISA



Motivazioni

4 Types of Threat Actors

1

Cybercriminals

2

Hacktivist

3

State-Sponsored Attackers

4

Insider Threats

Esistono 4 tipi di Threat Actors:

- I Cybercriminali sono degli individui che forzano sistemi, ne causano la loro indisponibilità, attaccano reti, semplicemente per dimostrare la loro abilità.
- Gli Hacktivist sono gruppi di individui che si organizzano per attaccare istituzioni, banche, governi, in modo tale da "lanciare messaggi".
- Gli State Sponsored Attackers sono attaccanti pagati dai Governi.
- Insider Threats sono coloro che utilizzano impropriamente i loro privilegi per causare danni all'azienda. Possono essere dipendenti dell'azienda stessa, per esempio.

Known Threat Actors

In questa analisi analizzeremo tre tipi di Threat Actors:



Quelli ingaggiati dai governi;



Quelli che agiscono senza un
ingaggio per svariati scopi.



Hacktivist

Government engagement

Nation-state adversaries pose an elevated threat to our national security. These adversaries are engaged in their advanced persistent threat (APT) activity:

- The [Chinese government](#)—officially known as the People's Republic of China (PRC)—engages in malicious cyber activities to pursue its national interests including [infiltrating critical infrastructure networks](#).
- The [Russian government](#)—officially known as the Russian Federation—engages in malicious cyber activities to enable broad-scope cyber espionage, to suppress certain social and political activity, to steal intellectual property, and to harm regional and international adversaries.
- The [North Korean government](#)—officially known as the Democratic People's Republic of Korea (DPRK)—employs malicious cyber activity to collect intelligence, conduct attacks, and generate revenue.
- The [Iranian government](#)—officially known as the Islamic Republic of Iran—has exercised its increasingly sophisticated cyber capabilities to suppress certain social and political activity, and to harm regional and international adversaries.



Sul sito del Governo Americano troviamo I seguenti Stati, che ingaggiano diversi Threat Actors allo scopo di perseguire interessi Nazionali.

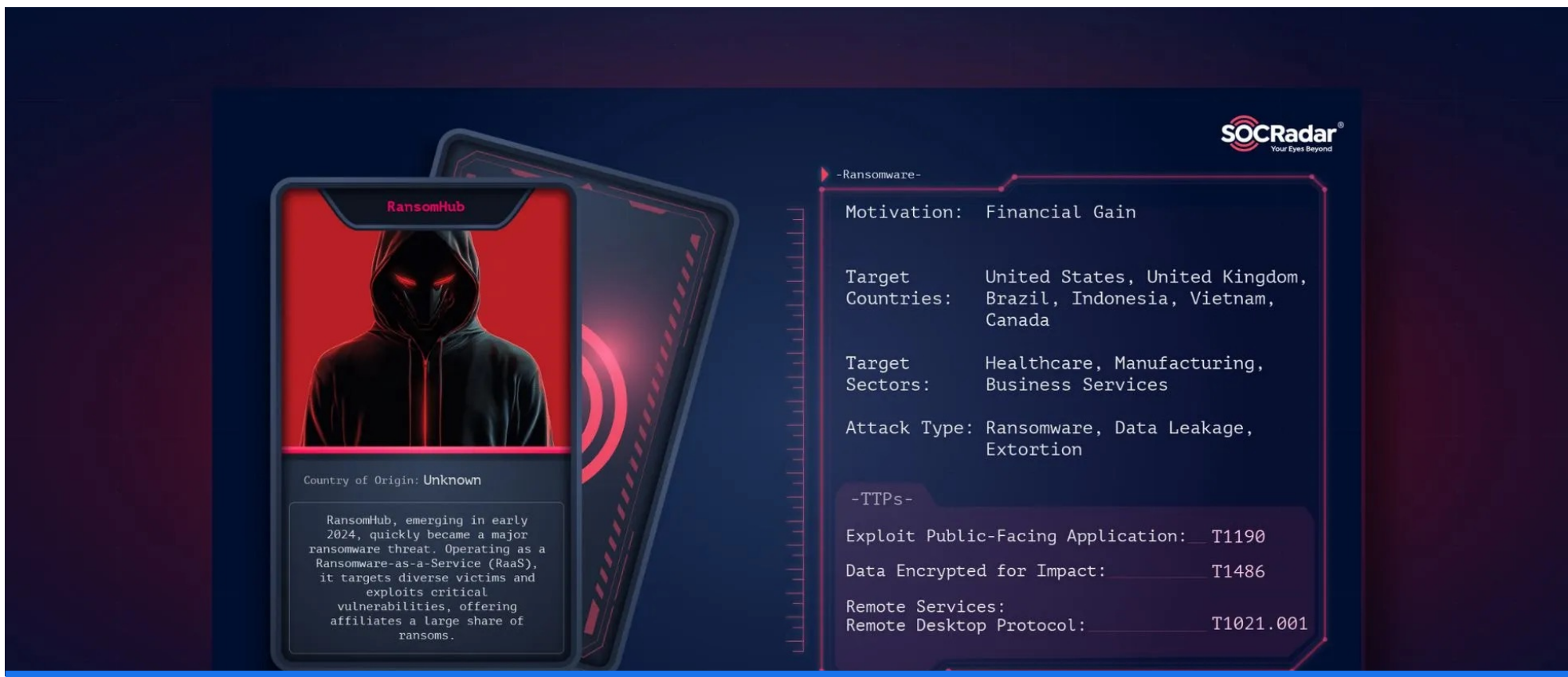
Most known Threat Actors

I secondi, invece, sono quei Threat Actors che agiscono di loro sponte per i più svariati scopi.

SOCRadar (<https://socradar.io/top-10-threat-actors-of-2024-beyond-the-numbers/>), indica i 10 Threat Actors più noti.

Per semplicità analizzeremo i primi 5.

1. **RansomHub**
2. **Qilin Ransomware**
3. **Dark Angels**
4. **LockBit**
5. **Whitewarlock**



1. RansomHub

- Sono un gruppo organizzato che si occupano di 'RaaS', Ransomware As A Service. Ovvero vendono Ransomware ad altri Threat Actors, sotto pagamento.
- Il loro obiettivo è quello di ricevere un compenso finanziario.
- La loro origine non è nota.

RansomHub

RansomHub è nato in preda all'attacco record Change Healthcare all'inizio del 2024.

Quando Change Healthcare è stata attaccata, i suoi dati sanitari sono stati rubati dall'affiliato del ransomware e i suoi sistemi sono stati criptati dal ceppo di ransomware interno di ALPHV.

Fonte: <https://www.checkpoint.com/it/cyber-hub/threat-prevention/ransomware/what-is-ransomhub-ransomware/>

Qilin Ransomware



Country of Origin: Russia 🇷🇺

Qilin, also known as Agenda ransomware, represents a formidable threat in cybercrime. One of the known RaaS groups, is designed with adaptability in mind, allowing it to

-Ransomware Group-

Motivation: Financial

Target Countries: US, UK, Brazil, Argentina

Target Sectors: Public Administration, Healthcare, Education

Attack Type: Encryption, Data Theft, Double Extortion

-TTPs-

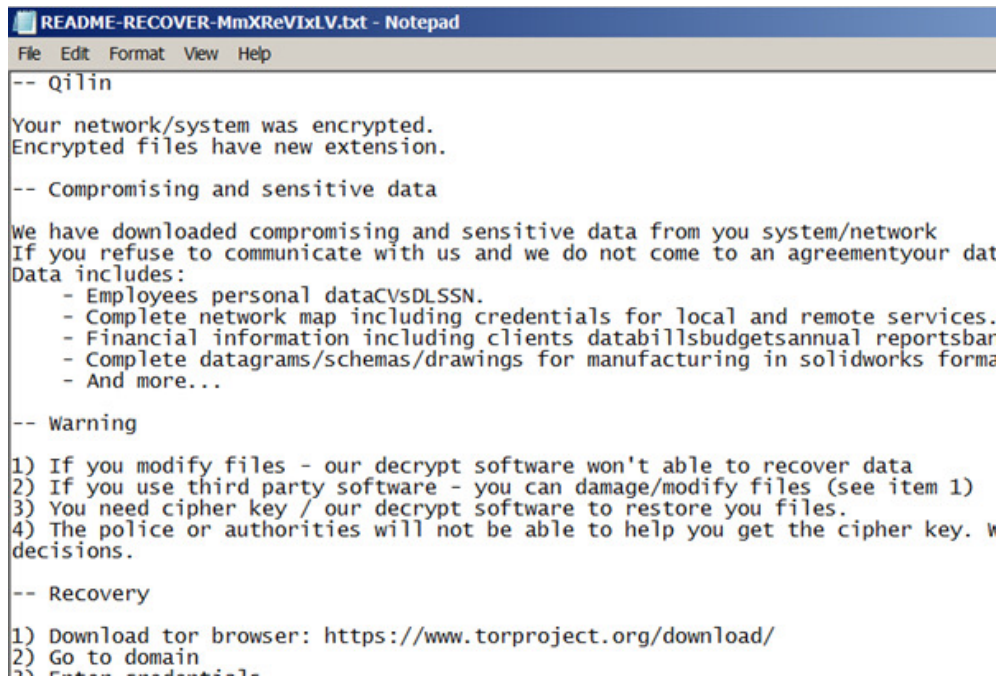
Phishing: T1566

System Services: Service Execution: T1569.002

2. Qilin Ransomware

- Questo gruppo di hackers russi attaccano amministrazioni pubbliche, il settore medico e educativo.
- Il loro obiettivo è quello di ottenere un compenso economico.

Qilin Ransomware

A screenshot of a Notepad window titled 'README-RECOVER-MmXReVixLV.txt - Notepad'. The window contains a ransomware message in a monospaced font. The message is structured with sections separated by double dashes. It starts with a greeting, states that the network/system was encrypted and files have a new extension. It then lists compromised and sensitive data, including employee personal data, network maps, financial information, and manufacturing data. A warning section follows, listing four points: 1) Modifying files prevents decryption, 2) Third-party software can damage files, 3) A cipher key is needed for decryption, and 4) Police cannot help without the key. Finally, a recovery section provides instructions to download a Tor browser and visit a specific domain.

```
-- Qilin

Your network/system was encrypted.
Encrypted files have new extension.

-- Compromising and sensitive data

We have downloaded compromising and sensitive data from you system/network
If you refuse to communicate with us and we do not come to an agreement your data
Data includes:
- Employees personal dataCVsDLSSN.
- Complete network map including credentials for local and remote services.
- Financial information including clients databillsbudgetsannual reportsbar
- Complete datagrams/schemas/drawings for manufacturing in solidworks forma
- And more...

-- Warning

1) If you modify files - our decrypt software won't able to recover data
2) If you use third party software - you can damage/modify files (see item 1)
3) You need cipher key / our decrypt software to restore you files.
4) The police or authorities will not be able to help you get the cipher key. W
decisions.

-- Recovery

1) Download tor browser: https://www.torproject.org/download/
2) Go to domain
3) Enter credentials
```

- Si occupano, come il Threat Actor precedente, di vendere Ransomware As A Service.
- Qilin ha pubblicato per la prima volta informazioni su una vittima nel suo sito di leak nel darknet nell'ottobre 2022 e da allora ha aumentato le sue attività. Tra le vittime ci sono il giornale *The Big Issue*, il gigante dei ricambi per auto Yanfeng e il servizio giudiziario australiano.

Fonte: <https://www.tripwire.com/state-of-security/qilin-ransomware-what-you-need-know>

3. Dark Angels

- I Dark Angels sono un gruppo di criminali specializzato in attacchi ransomware, emerso nel 2022. A differenza di altri gruppi ransomware, i Dark Angels preferiscono evitare interruzioni operative significative nelle organizzazioni vittime, privilegiando l'esfiltrazione di grandi quantità di dati sensibili.
- Nel 2024, i Dark Angels hanno ricevuto un pagamento di riscatto record di 75 milioni di dollari da una società Fortune 50, il più alto mai registrato. (Fonte: <https://www.scworld.com/brief/all-time-high-ransom-paid-to-dark-angels-ransomware-gang>).
- Si sospetta che la vittima possa essere stata la multinazionale farmaceutica Cencora, precedentemente nota come AmerisourceBergen, che ha subito un attacco informatico nel febbraio 2024 (Fonte: <https://www.techtarget.com/searchsecurity/feature/The-mystery-of-the-75M-ransom-payment-to-Dark-Angels>).
- La loro origine è sconosciuta.



4. LockBit



LockBit

Country of Origin: Russia 🇷🇺

The most successful RaaS group operating since 2019. The group is continuously evolving and is highly active in deploying models such as double-extortion and initial access broker affiliates.

-Ransomware Group-

Motivation: Financial Gain

Target Countries: United States, United Kingdom, Canada, Europe, Thailand, Taiwan

Target Sectors: Manufacturing, Professional Services, IT, Healthcare, Finance, Education, Legal Services

Attack Type: Phishing, RDP and VPN access Exploitation, Ransomware, Data Exfiltration, Double-extortion

-TTPs-

Exploit Public-Facing Application: T1190

Remote Desktop Protocol: T1021.001

Data Encrypted for Impact: T1486

socradar.io

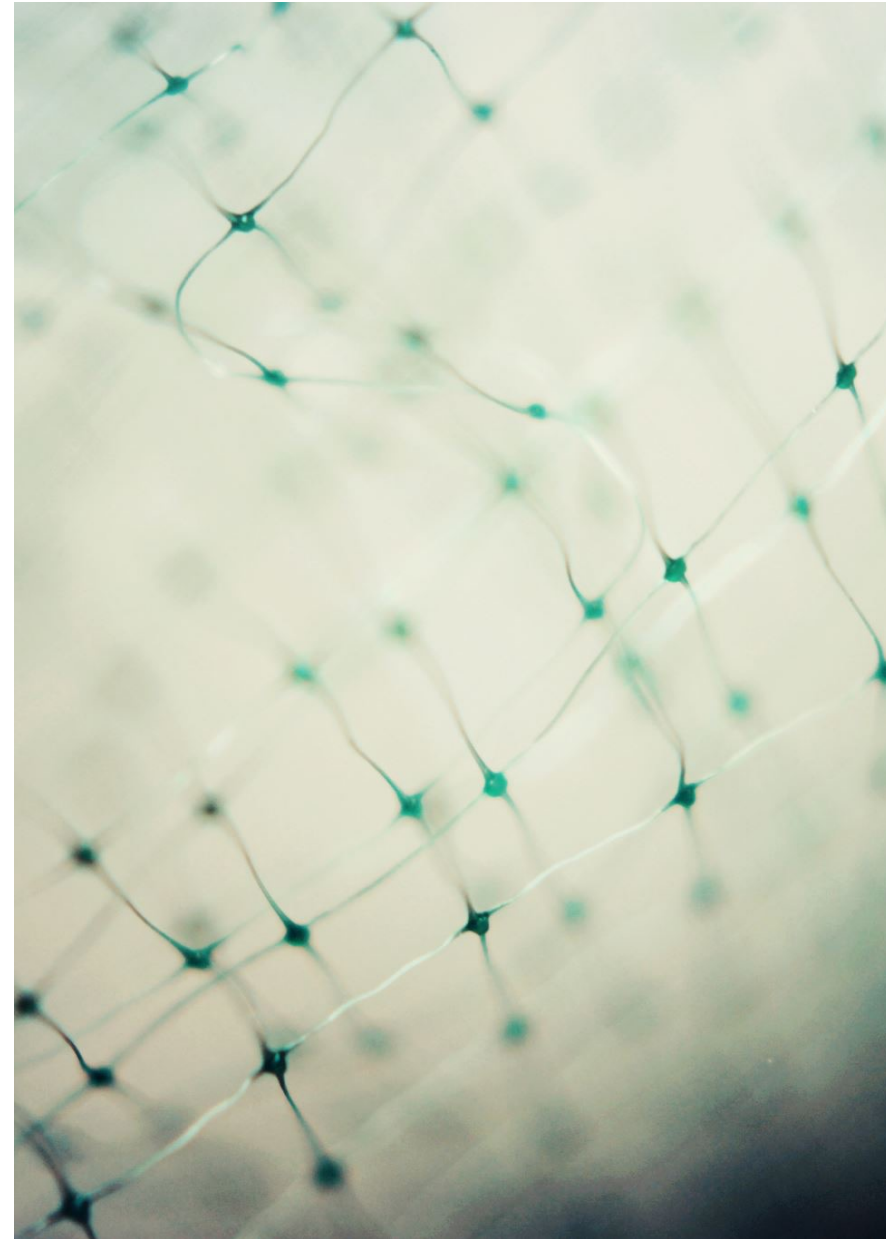
SONO UN GRUPPO DI HACKERS RUSSI CHE SI OCCUPA, ANCHE ESSO DI RANSOMWARE-AS-A-SERVICE.

IL LORO SCOPO È SEMPRE ECONOMICO.

SOLITAMENTE I LORO OBIETTIVI SONO PARTE DEL SETTORE MANUFATTURIERO, IT, MEDICO, EDUCATIVO E LEGALE.

Lockbit

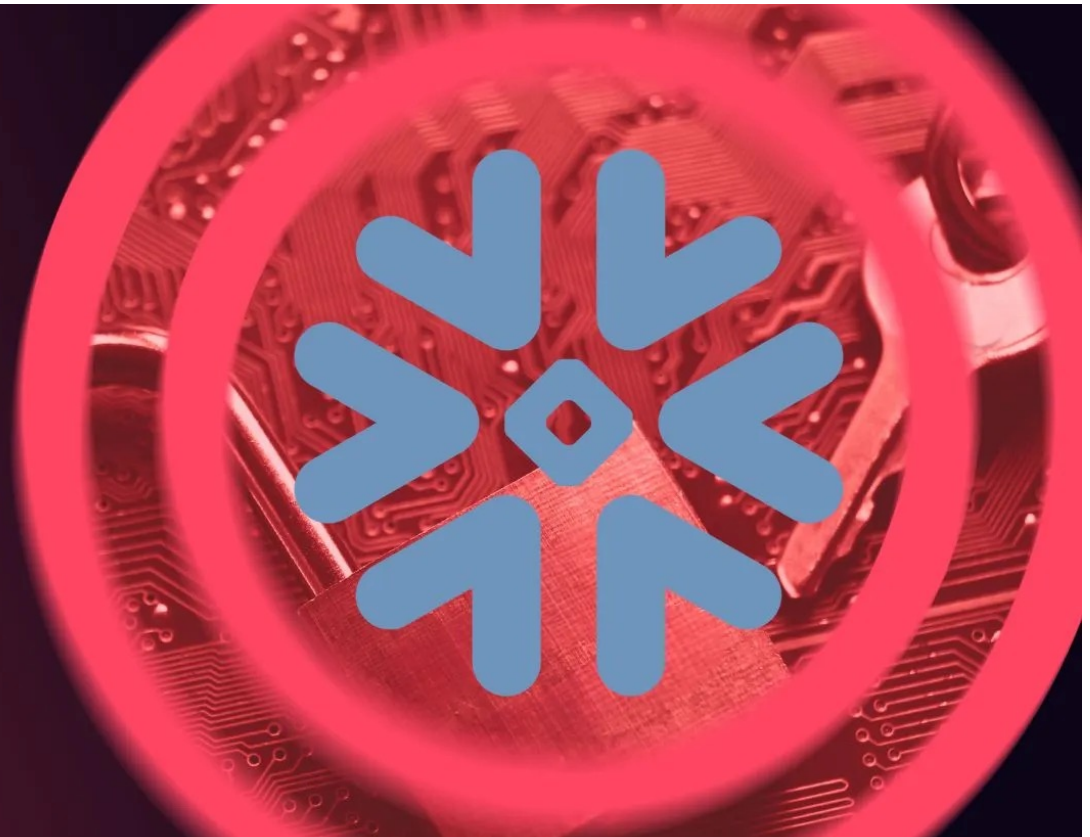
- Il modus operandi di LockBit prevede l'infiltrazione nelle reti delle vittime, la crittografia dei dati e la richiesta di un riscatto per il ripristino dell'accesso. Inoltre, minacciano di divulgare pubblicamente i dati rubati se le richieste non vengono soddisfatte.
- LockBit è stato collegato a numerosi attacchi di alto profilo, tra cui quelli contro Boeing, la Industrial Commercial Bank of China, il servizio postale britannico Royal Mail e il National Health Service del Regno Unito. (Fonte: <https://apnews.com/article/361e788f5482bfd787af01002af2ff4c>)





Snowflake Breach

Threat Actor Offers Data of Cloud Company's Customers



5. Whitewarlock

- 'Whitewarlock' è emerso nel maggio 2024, noto per aver rivendicato attacchi informatici significativi.
- Il 23 maggio 2024, 'Whitewarlock' ha pubblicato su un forum del dark web in lingua russa, 'Exploit.in', affermando di aver violato il gruppo bancario Santander e offrendo in vendita dati sensibili per 30 Bitcoin.
- Il loro obiettivo è finanziario.
- La loro origine è sconosciuta.



Anonymous – Hacktivist

Come Hacktivist troviamo Anonymous.

- Origine: Stati Uniti, Regno Unito, Francia, Italia, Russia, Brasile.
- Il collettivo si oppone alla censura, alla corruzione e alle ingiustizie sociali, promuovendo la libertà di espressione e la trasparenza. Le loro azioni mirano a colpire governi, istituzioni e aziende percepite come oppressive o corrotte (Fonte: <https://www.geopop.it/chi-e-e-che-scopo-ha-anonymous-il-collettivo-di-hacker-con-la-maschera-di-guy-fawkes-come-simbolo/>).

APT 28 – Government Engagement

APT28, noto anche come Fancy Bear, è un gruppo di cyber spionaggio attribuito all'intelligence militare russa (GRU).

Le sue attività sono state rilevate sin dal 2008, con operazioni mirate a governi e organizzazioni internazionali.

Il gruppo si concentra su operazioni di spionaggio cibernetico, prendendo di mira istituzioni governative, militari e organizzazioni internazionali per raccogliere informazioni strategiche a favore della Russia.



Associated APT designations

- APT28 (FireEye/Mandiant)
- Fancy Bear (CrowdStrike)
- SOFACY (Kaspersky)
- STRONTIUM (Microsoft)
- PawnStorm (Trend Micro)
- IRON TWILIGHT (SecureWorks)
- Sednit (ESET)
- Snakemackerel (iDefense)
- Tsar Team (Sight)
- G0007 (MITRE ATT&CK)

Sources [3], [2], [3], [4], [5], [32]

Country of origin



Time period of activity

2004 today

Sources [2], [10]

Political affiliations

Today, APT28 is consistently attributed to GRU Unit 26165, 85th Main Special Service Centre (GTSSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU). This attribution is mainly based on an indictment unsealed by the US Department of Justice (DoJ) in 2018. A report by the US Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) from 2016 had previously attributed APT28 with high confidence to the Russian military or civilian intelligence services without specifying the agency. In its 2018 security environment assessment, the Estonian Intelligence Service affirmed that APT28 is consistent with observations for GRU Unit 26165. Later in 2018, the UK National Cyber Security Center (NCSC) assessed with "almost certainty" that APT28 operates as part of the GRU. Industry sources, such as FireEye, had already attributed APT28 as a Russian state sponsored actor in 2014 without identifying any specific links to state institutions or agencies. In 2016, CrowdStrike was the first to publicly identify the GRU as the responsible state agency as a product of its investigations into the intrusions into the networks of the Democratic National Committee (DNC).

Sources [6], [7], [8], [9], [5], [34]

By Kerstin Zettl Schabath, Timothy Gschwend and Camille Barrett

<https://www.google.com/url?sa=i&url=https%3A%2F%2Feurepoc.eu%2Fpublication%2Fapt-profile-apt-28%2F&psig=AOvVaw0SiAFB7CuWwZuvuqyp0goN&ust=1741015651924000&source=images&cd=vfe&ei=89978449&ved=0CBYQjRxqFwoTCPjIue3a64sDFQAAAAAdAAAAABAI>

Grazie!

