Service à la Russia

A tasting menu of intelligence tradecraft and Russia-based threat actor case studies

PwC Threat Intelligence | December 2025 | TLP:CLEAR

Introduction

John Southworth

PwC UK

Technical Russia Lead

john.h.southworth@pwc.com

- 8+ years working in threat intelligence
- Technical analyst focused on threat actor tracking
- Incident response support
- Digital risk intelligence/attack surface management lead

Agenda

1. Hors d’oeuvre: Overview
2. Entrée: Case studies
3. Dessert: Looking ahead

1

Hors d’oeuvre
Overview

Threat actor motivations

Espionage

The “business-as-usual” activity of Russia-based threat actors continues, targeting government, defence, NGOs, etc.

Cyber crime

Overlaps with espionage-focused threat actors and cyber criminal activity continue, such as Blue Dev 11 (a.k.a. RomCom).

Hacktivism

Hacktivist collectives target organisations globally with pro-Ukrainian/anti-Russian sentiment, and influence operations continue.

Sabotage

Wipers continue to be utilised in 2025 by sabotage-focused Russia-based threat actors.

Geopolitical landscape

1

The ongoing war in Ukraine and negotiations for the end of the conflict

Russia-based threat actors continue to heavily target Ukraine, including espionage campaigns against government/defence, and deploying disk wipers to disrupt critical sectors, as well as Kyiv's partners and wider supply chain.

2

Sanctions and pro-Kyiv support informs continued targeting

Russia-based threat actors target European/North American organisations for the purposes of espionage. Hacktivists conduct DDoS campaigns against organisations with a pro-Ukraine and/or anti-Russian stance.

3

Alignment with non-Western partners

Broadening sanctions regimes and lack of access to some export markets have resulted in Russia seeking ever-closer support from countries like China, North Korea and Iran. This has included military support as well as strategic diplomatic relations.

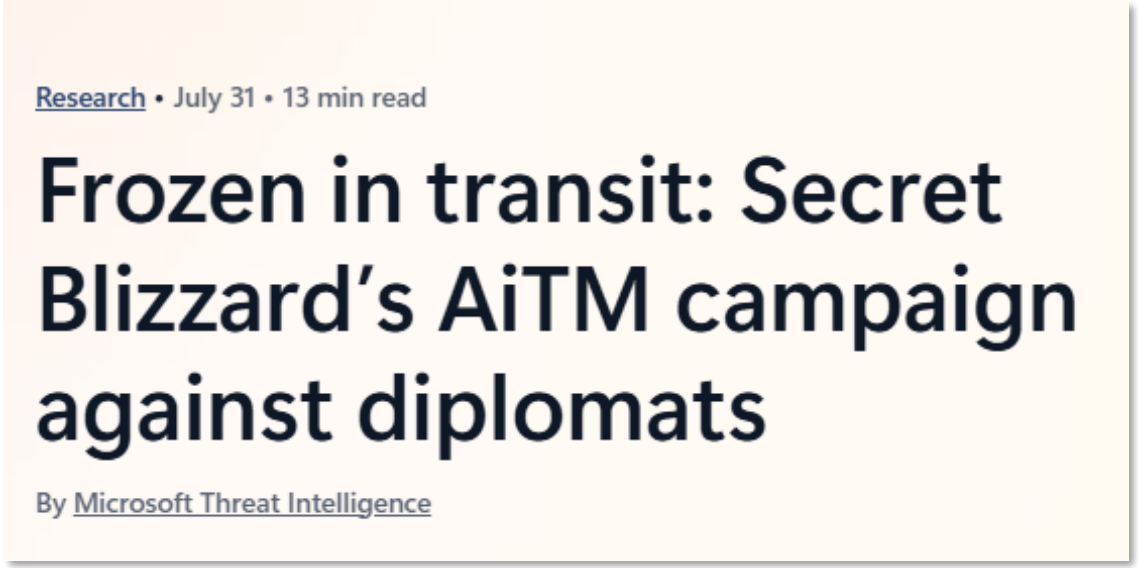
> **"Russia continues to act as a capable and irresponsible threat actor in cyberspace. Russia's most disruptive threat activity continues to be focused on Ukraine, in support of their illegal military campaign."**
> *'NCSC Annual Review 2025', NCSC, October 2025, https://www.ncsc.gov.uk/collection/ncsc-annual-review-2025*

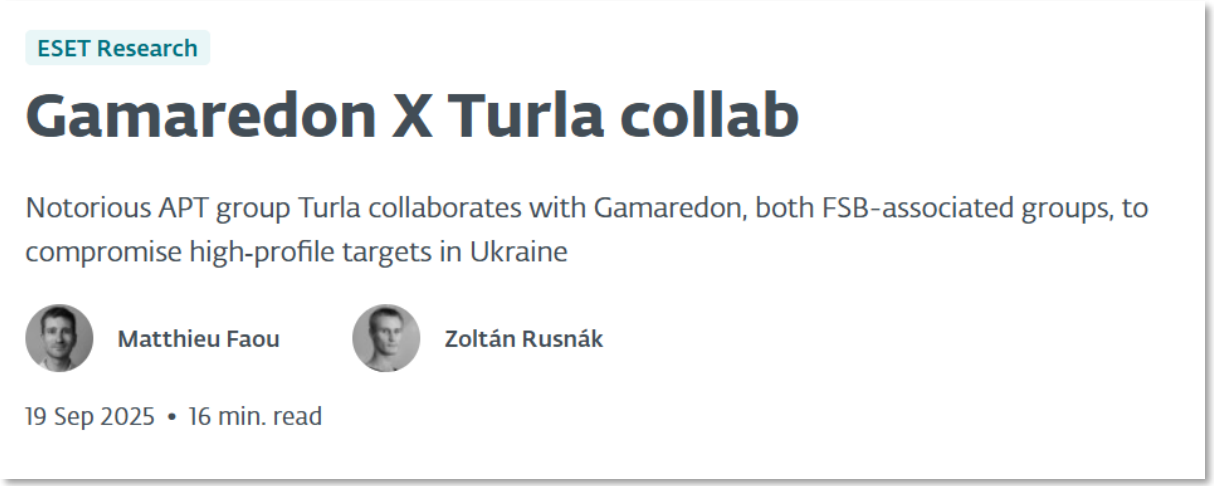
2

Entrée
Case studies

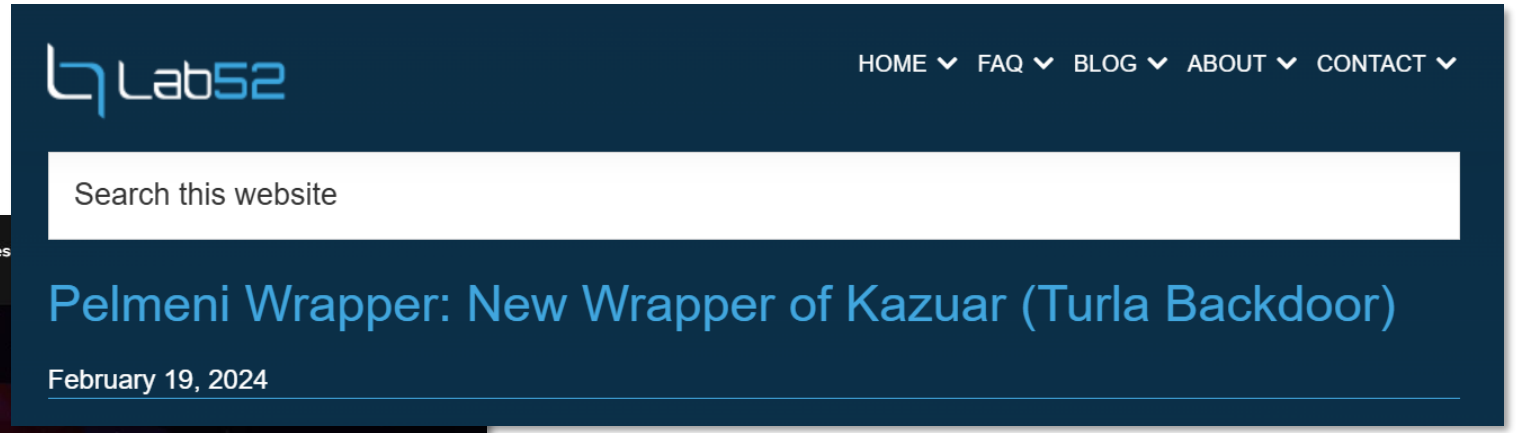
Blue Python

- a.k.a. Turla, Secret Blizzard
- Active since 2004, links to Moonlight Maze from 1996-98
- Target sectors: Government, Defence, Education, NGOs, Pharma





Kazuar backdoor open source research



Kazuar backdoor

- Analysed samples of Kazuar across 2024 showing European targeting.
- Targeting:
  - Military organisations
  - Government departments, including:
    - Ministry of Finance
    - Ministry of Technology
    - Ministry of Foreign Affairs

Loader guardrails

- Uses the hash of the computer name/computer DNS name as an initialisation for the decoding layer.
- Can conduct a known-plaintext attack on the exports of the DLL to derive the key.

Name	Address	Ordinal
Bnjtbm	703DD48C	1
Fimfl	703DAED4	2
Fttvxt	703DD76C	3
Fxicsfqu	703DD478	4
Gfbzv	703DCEA4	5
Gubfsm	703DCF64	6
Hocqivr	703DD8D4	7
Kyakdg	703DD8AC	8
Nplkuq	703DC464	9
Ywsfgww	703DADB0	10
TlsCallback_0	703CBBD0	
TlsCallback_1	703CBC67	
TlsCallback_2	703D1E9C	
DllEntryPoint	**703C2434**	**[main entry]**

```
char *__cdecl sub_68D414F0(char *a1, unsigned int a2)
{
  unsigned int v3; // [esp+4h] [ebp-14h] BYREF
  unsigned int *v4; // [esp+8h] [ebp-10h]
  unsigned int i; // [esp+Ch] [ebp-Ch]

  v4 = &v3;
  v3 = 0x5521D6E2;
  v3 = computer_name_hash() ^ 0x5521D6E2;
  for ( i = 0; i < a2; ++i )
  {
    if ( (i & 3) == 0 )
    {
      *v4 *= 0x19660D;
      *v4 += 0x3C6EF35F;
    }
    a1[i] ^= *(&v3 + (i & 3));
  }
  return a1;
}
```

Obfuscated loader variants

```
char *__cdecl sub_68D414F0(char *a1, unsigned int a2)
{
  unsigned int v3; // [esp+4h] [ebp-14h] BYREF
  unsigned int *v4; // [esp+8h] [ebp-10h]
  unsigned int i; // [esp+Ch] [ebp-Ch]

  v4 = &v3;
  v3 = 0x5521D6E2;
  v3 = computer_name_hash() ^ 0x5521D6E2;
  for ( i = 0; i < a2; ++i )
  {
    if ( (i & 3) == 0 )
    {
      *v4 *= 0x19660D;
      *v4 += 0x3C6EF35F;
    }
    a1[i] ^= *(&v3 + (i & 3));
  }
  return a1;
}
```

```
        }
        if ( qword_70624940 == 42 )
        {
          LODWORD(qword_70624940) = 86;
LABEL_21:
          HIDWORD(qword_70624940) = 0;
        }
      }
    }
    v10[0] = v6 + v4 * v10[0];
LABEL_23:
    GetACP();
    *(a1 + v5) ^= *(v10 + (v5 & 3));
    ++v5;
  }
  if ( dword_7062493C != 127354599 || dword_70624938 != 1584953775 )
    ColorAdjustLuma(0x38ADDB33u, -639731894, 664251866);
  return a1;
}
```

Same decryption routine

String decryption

- Some loaders require extra string decoding – IDA Python can help with this

```
0x703db0d9: v4.0.30319
0x703db125: v2.0.50727
0x703db1ef: mscoree.dll
0x703db44a: wks
0x703dc4d4: SOFTWARE\Microsoft\.NETFramework\v4.0.30319
0x703dc80b: aqclugtvrk.adq
0x703dcb39: amsi.dll
0x703dd6ae: a
0x703dd6de: A
0x703db332: CorBindToRuntimeEx
0x703dc03e: 0
0x703dcaa1: thr == NULL
0x703dcbb2: AmsiScanBuffer
0x703dd3b1: thr == NULL
0x703dd97b: %d:%08X
```

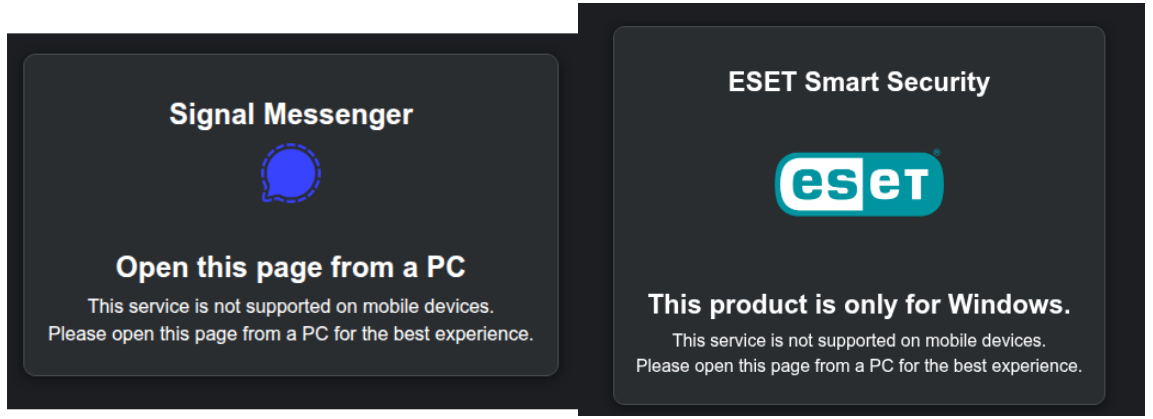
```
unsigned int __cdecl sub_68D61CCC(int a1,
{
  unsigned int result; // eax
  unsigned int j; // [esp+8h] [ebp-Ch]
  unsigned int i; // [esp+Ch] [ebp-8h]

  for ( i = 0; a3 >= i; ++i )
    *(2 * i + a2) = 0;
  for ( j = 0; ; ++j )
  {
    result = j;
    if ( j >= a3 )
      break;
    a6 = a4 * a6 + a5;
    *(2 * j + a2) = a6 ^ *(a1 + j);
    *(2 * j + a2) = *(2 * j + a2);
  }
  return result;
}
```

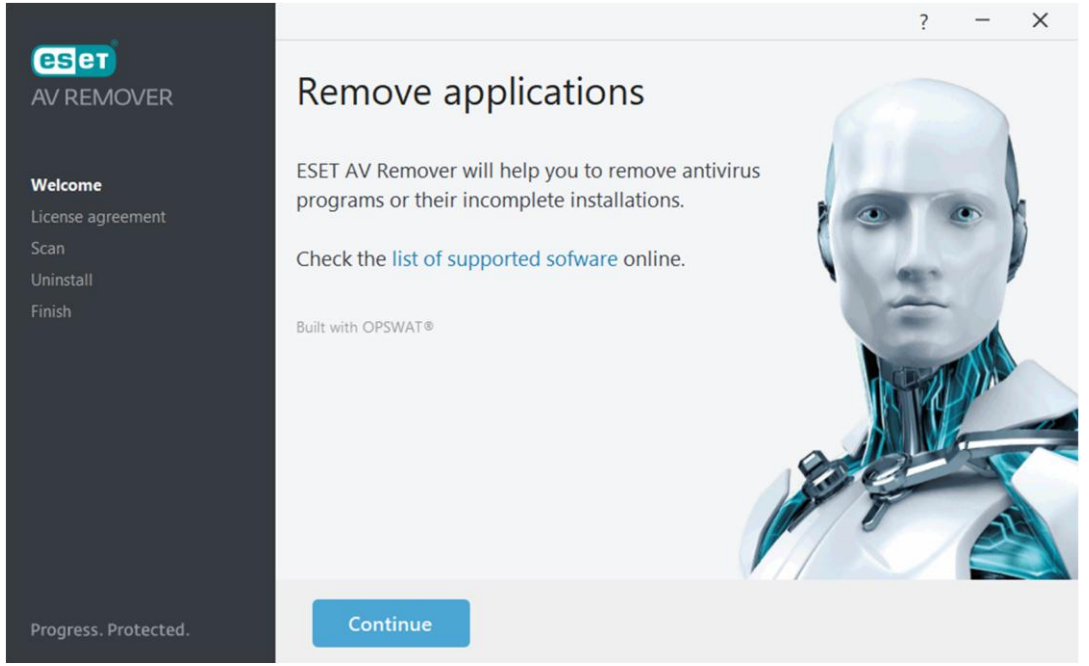
Blue Echidna

- a.k.a. Sandworm, APT44, IRIDIUM, Voodoo Bear
- Known for historically targeting ICS devices in Ukraine, and more recently deploying wipers, but more global targeting for initial access (e.g. BadPilot)
- Kalambur backdoor reported in open source to be used by the threat actor, being loaded by BACKORDER

Blue Echidna spoofing ESET

- Spoofing ESET domains/installers to deploy Kalambur:
  - hxxps://esetpremium[.]com/Antivirus/
  - hxxps://esetscanner[.]com/Antivirus/
  - hxxps://esetremover[.]com/Antivirus/
  - hxxps://esetsmart[.]com/Antivirus/
  - hxxps://eset-review[.]com/eset/download/





Tambur: successor to Kalambur

- Hunting for domain registration patterns (onionmail.org registration + Cloudflare) uncovered infrastructure serving ISO files
- Acts as a trojanised, pirated Windows installer, which loads BACKORDER
- Other related infrastructure uncovered a .NET downloader hosted using GitHub attachments, loading a Golang payload referring to itself as “Tambur”
- Used to set up SSH/RDP connections to an infected device. Still a work in progress based on strings in the sample (e.g. references Tor, but doesn’t use)

```
Issuer: C=UA, L=Kyiv, OU=OVA, CN=OVA
Validity
Not Before: Oct 20 07:03:57 2025 GMT
Not After : Oct 20 07:03:57 2026 GMT
Subject: C=UA, L=Kyiv, OU=OVA, CN=OVA
```

Blue Dev 17

- Void Blizzard (which we track as Blue Dev 17) disclosed by Microsoft, following public attribution by Dutch intel agencies
- Active since at least April 2024
- Country targets: NATO members, Ukraine
- Sector targets: Defence, Education, Government, Healthcare, Media, NGO, Technology, Telecommunications, Transport

Tactical Intelligence Bulletin

CTO-TIB-20250530-03A

pwc

Tags: Espionage, APT, Blue Dev 17, Void Blizzard, LAUNDRY BEAR, NATO, Spear Phishing, Evilginx, United States, Ukraine, Netherlands

Sectors: Defence, Education, Government, Healthcare, Media, NGO, Technology, Telecommunications, Transport

TLP: AMBER+STRICT

No third party distribution

Void Blizzard has no chill

Russia-based threat actor referred to as Void Blizzard/LAUNDRY BEAR targets organisations within Europe and North America using spear-phishing emails

Executive summary

The Russia-based threat actor Void Blizzard/LAUNDRY BEAR was publicly reported on in May 2025 by Microsoft,[1] the Netherlands General Intelligence and Security Service (AIVD),[2] and the Netherlands Defence Intelligence and Security Service (MIVD).[3] The threat actor has been targeting organisations in line with the Russian government's strategic objectives across a wide variety of sectors, including Defence, Education, Government, Healthcare, Media, NGO, Technology, Telecommunications, and Transport. In April 2025, Void Blizzard targeted 20 NGOs in Europe and the US with spear-phishing campaigns. Using the domain identified in Microsoft's analysis, we were subsequently able to identify additional infrastructure owned by the threat actor, which we are tracking as Blue Dev 17.

Background

Microsoft identified a new Russia-based threat actor with the help of the Netherlands AIVD, MIVD, and the US Federal Bureau of Investigation (FBI).[4,5] The threat actor, which Microsoft labelled Void Blizzard and which AIVD refers to as LAUNDRY BEAR, has been observed conducting espionage operations aligned to strategic Russian government objectives. We are tracking this threat actor as Blue Dev 17.

Microsoft reported that the threat actor has been active since April 2024 and its operations have largely targeted organisations within Ukraine and NATO member states. The organisations successfully compromised have come from sectors including:

- Defence;
- Education;
- Government;
- Healthcare;
- Media;
- NGOs;
- Technology;
- Telecommunications; and,
- Transport.

Impersonated events/conferences

April

European Defense & Security Summit

Via `micsrosoftonline[.]com`, according to OSINT reporting targeting a wide range of organizations in the NGO sector

June

NATO Summit 2025

NATO impersonation domains, `nato-summit-2025[.]info /org/com`

August

SIDEC Expo

New domain registration impersonating SIDEC, a Slovenian conference around cyber security, R&D, energy efficiency and artificial intelligence: `sidec-expo[.]org`

Agriculture Forum

Agriculture-themed domain which overlaps with typical Blue Dev 17 registration patterns: `agriculture-forum[.]org`

Impersonation target **not confirmed**, potential related events could be:

World Agriculture Forum (webinars on 15th October 2025)

Global Security Chronicle

Domains hosting the fake news portal “Global Security Chronicle”, displaying an article with the heading “The Anchorage Accord: Leaked Details Reveal Secret Plan to Redraw Ukraine's Map”.

Likely referring to the meeting between Trump and Putin in Anchorage, Alaska.

`gl-security[.]eu, gl-ses[.]com`

Impersonated events/conferences

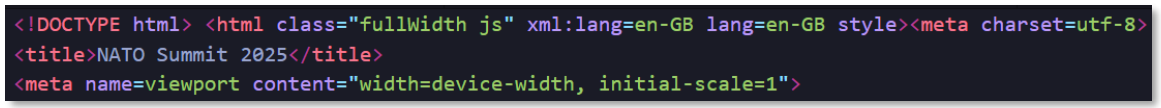
Munich Security Conference

On 22nd September, Blue Dev 17 registered the domain `securityconference[.]org[.]in`, hosting a Munich Security Conference related website.

September | **October-onwards**

NATO Summit 2025

Blue Dev 17 registered another domain in September, hosting a NATO summit website. The domain itself contains no typical NATO terms: `gl-ses[.]com`



Future targeting

Likely further conference/summit themed domains, targeting defence, and wider sectors

Misattribution woes

- Pivots possible on “unique” HTML response with SHA-1: `38c47d338a9c5ab7ccef7413edb7b2112bdfc56f`
- At the time of analysis this gave four unique domains:
  - `micsrosoftonline[.]com` (in Microsoft blog)
  - `miscrsosoft[.]com`
  - `remerelli[.]com`
  - `weblogmail[.]live`
- The domain `weblogmail[.]live` resolved to an IP address hosted using AS12586 in Germany, by GHOSTnet GmbH/ASGHOSTNET.

```
<html><head><meta name='referrer'
content='no-referrer'><script>top.location.
href='https://outlook.live.com';</script></
head><body></body></html>
```

Misattribution woes

- Pivoting to further domains using the following heuristic:
  - Mail and name server being registrar-servers.com (i.e. Namecheap);
  - The domain registrar being Namecheap; and,
  - The resolving IP address being hosted by AS12586.
- This yielded domains which also spoofed Microsoft login pages, and were registered across the same timeframe as the threat actor.
- However, further understanding has led us to attribute this cluster to Egypt-based Indigo Dev 1.
- Infrastructure pivots are more focused on server heuristics + domain themes at this stage.

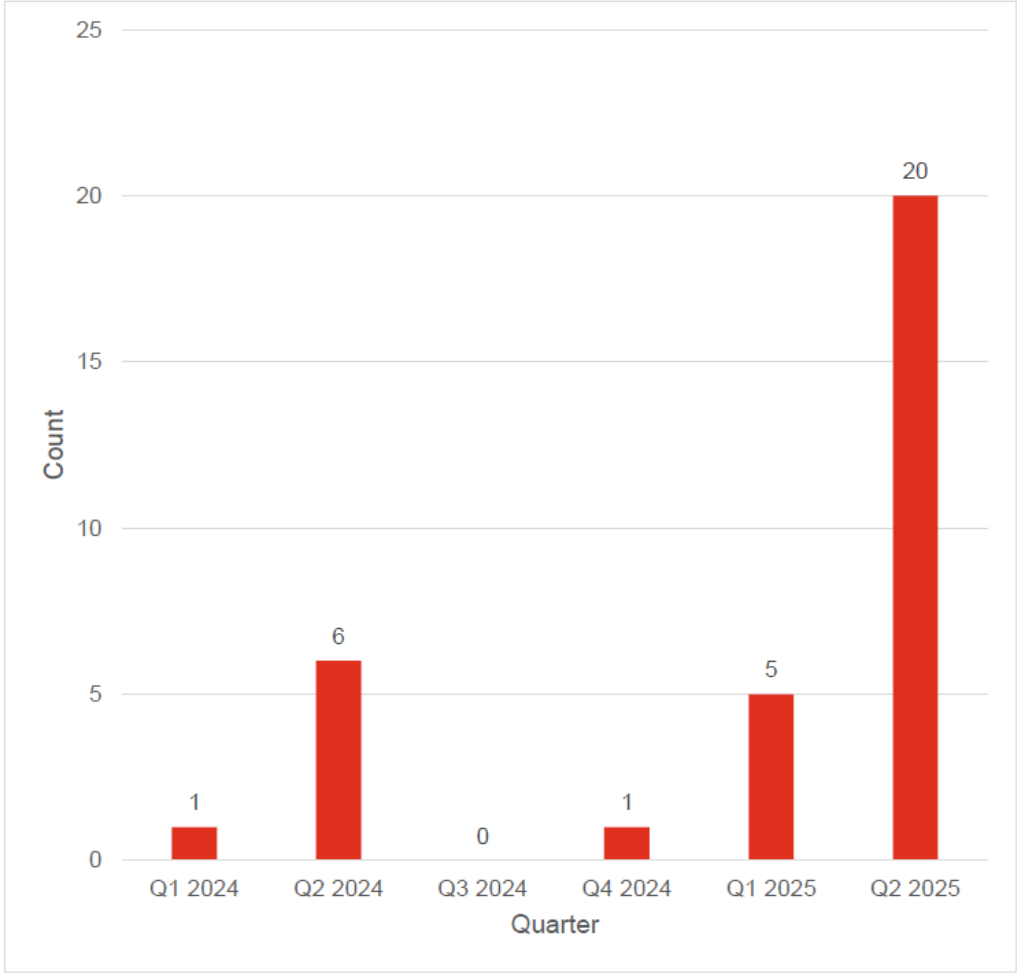


Figure 2 – Number of Blue Dev 17 registered domains per quarter

- **Takeaway:** be careful of confirmation bias when doing infrastructure pivots, and use estimative language.

White Dev 229

- Suspected Russia-based threat actor targeting NGOs and academics in September/October 2025
- Observed targeting: United Kingdom, Australia
- Suspected wider targeting: Africa, South East Asia, South America
- Targeting individuals conducting research into Russia, defence, NATO
- Uses Cloudflare Workers for its campaign infrastructure
- Known to send emails from compromised accounts

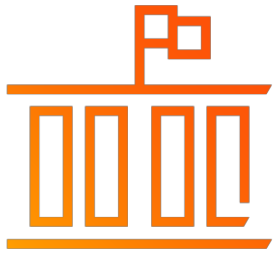
White Dev 229 – URL structure

```
hxxps://onedrive[.]{SPOOFED_ORG}[.]workers[.]dev
/drive/shared?file=topics_[REDACTED].docx
```

- Subdomain `onedrive` consistently used (also spoofing Teams, Yahoo, Google, SharePoint, etc.)
- Created for a `{SPOOFED_ORG}` to make the domain look legitimate
- Using Cloudflare Workers (i.e. `workers[.]dev`) for hosting
- Hosting a benign Word document for a specific topic related to the target named `topics_[REDACTED].docx`

White Dev 229 – Hunting

- Hunting for Cloudflare Workers domains of the structure `onedrive.*.workers.dev`, and manually triaging to look for spoofed organisations leads to likely White Dev 229 domains spoofing organisations across:



Government

Education

Defence

Mining

3

Dessert
Looking ahead

Other Russia-based threat actors not referenced

01
Blue Athena (a.k.a. APT28, Fancy Bear, Forest Blizzard)

02
Blue Dev 11 (a.k.a. RomCom)

03
Blue Dev 13 (a.k.a. UAC-0063)

04
Blue Callisto (a.k.a. Callisto Group, Star Blizzard, COLDRIVER)

05
Blue Otso (a.k.a. Gamaredon Group)

06
Blue Dev 5 (a.k.a. APT29, Midnight Blizzard)

07
Blue Dev 3 (a.k.a. InvisiMole)

Forecasting Russia-based threat actor activity

Less malware, more infrastructure

Less instances of malware observed, need to prioritise the tracking of infrastructure (dedicated, or third party hosted) used by Russia-based threat actors.

Innovating approaches to target identity

Iterating on approaches to steal credentials, or abuse authentication workflows.

Retasking post-conflict

As/when the conflict in Ukraine draws to a close, threat actors that have previously focused on Ukraine may have a wider targeting remit.

AI and cloud threats

Continued targeting of cloud environments by Russia-based threat actors, and developing usage of AI in the near future.

Thank you