

An Angry Spark, or a Triangle in Disguise?

By Bill Marczak

Published: 2026-07-27 · Archived: 2026-07-30 02:00:58 UTC



5 min read

1 day ago

--

A Union-Jack-clad triangle angrily emits sparks on the screen of a retro monitor (Source: ChatGPT)

On April 14, 2026, *Gen Digital* published “[Chasing an Angry Spark](#)”, a report about sophisticated Windows spyware that *Gen* saw once in 2022, and never again. Fascinatingly, the payload they found — and its command-and-control (C&C) servers — appeared to be completely novel to the threat intelligence community.

So *how* did *Angry Spark* remain undetected for so long, and precisely *who* is behind it? *Gen* did not directly address these questions, but instead provided an oblique hint: the use of British orthography (“sombrely”) in the payload’s strings.

However, in a strange twist, it turns out that years before, we had unwittingly stumbled upon one of the C&C servers listed in *Gen*’s report while examining what we surmised was spyware activity. Our investigation provides a compelling clue as to the pedigree of the *Angry Spark* spyware and its operators.

A Hit and a Pivot

In the Summer of 2020, we noted a Middle Eastern network communicating with a suspected spyware C&C, **ad43-nxs[.]com**. Our experience mapping spyware tells us that its operators tend to divide their targets among multiple such servers, all with similar behavior. Thus, we set out to find the ones we were missing by *pivoting* on the characteristics of **ad43-nxs[.]com**. But, we ran into a problem: the standard techniques we tried (e.g., searching for comparable response headers, body, and [JARM](#)) yielded no additional servers. Clearly, we had to pivot harder!

Fortunately, the operator of **ad43-nxs[.]com** had made an intriguing—if not altogether unusual—choice: they had set up the server to forward any TCP/IP SYN on port 443 through multiple intermediate hops, before a TCP/IP stack on an endpoint generated a SYN/ACK response (as indicated by lower-than-expected response IP TTL values combined with higher-than-expected round-trip-time). This behavior allowed us not only to *directly measure* the endpoint without the added complexity of laundering probes through (say) a frontend HTTP proxy, but, crucially, also to fingerprint the *forwarding path itself*.

We built such a path fingerprint, which we call **IP-ESSENCE**, based primarily on responses we triggered using the [Record Route IP option](#). As one may expect from the option's name, all intermediate hops that handle an IP packet including *Record Route*—and whose IP stacks have made the (popular) [choice to](#) support it—append their own IP address to the earliest unfilled slot in the option; any filled slots are forwarded unmodified. Furthermore, the Linux Kernel's TCP implementation [copies](#) the *Record Route* option from an incoming SYN into the response SYN/ACK's IP header, though we could not trace this behavior to any RFC.

Press enter or click to view image in full size

hping3 output shows an example of a returned SYN/ACK with a filled Record Route header.

While routers tend to drop packets containing IP options as they traverse the internet, most of this filtering [occurs at network boundaries](#). As [expected](#), we were able to reliably elicit TCP SYN/ACKs with *Record Route* from **ad43-nxs[.]com** by siting our measurement machine within the same network (Amazon) and EC2 [region](#) (*ap-southeast-1*) as the suspected C&C.

Our most recent successful **IP-ESSENCE** scan on EC2 was in 2024. We set up measurement instances within the free tiers of most Amazon EC2 regions and conducted in-region scanning with *Record Route*. We probed approximately 130 million IPs, and nearly 80 matched our fingerprint. When we later presented our methodology at an invite-only threat intelligence conference, **IP-ESSENCE** became far less effective.

From **OBTUSE** to **SCALENE**

While **IP-ESSENCE** was operative, we found two main clusters of suspected spyware activity on Amazon EC2. The first, which we call **OBTUSE**, used proxy chains of length 3 and was dispersed across multiple EC2 regions. Within **OBTUSE**, we noted several sub-clusters, which often tracked geographic regions. Among them were **OBTUSE-RU**, focused on Russia, and **OBTUSE-ME-1**, focused on the Middle East.

It was in 2023 that we learned our **OBTUSE** cluster represented *bona fide* spyware activity: [Operation Triangulation](#)! Kaspersky's report listed IOCs including one of the four **OBTUSE-RU** domains we identified, **ans7tv[.]net**. Leaked *Snort* rules purportedly from Kaspersky Lab that were posted publicly on *BreachForums* included the same domain alongside **ad43-nxs[.]com** (**OBTUSE-ME-1**), both tagged as "EquationGroup-TriangleDB".

We note that the purported leaked Kaspersky IOCs do *not* include any further **OBTUSE** domains, showing that whoever generated the list of IOCs probably did *not* independently find **IP-ESSENCE**. Yet, they knew *just enough* to associate **ad43-nxs[.]com** with **ans7tv[.]net**. We propose that the list's author (perhaps Kaspersky) identified a Middle East deployment of *Operation Triangulation*'s spyware sometime in 2023 or earlier.

Press enter or click to view image in full size

BreachForums user IgrooEagle *offered up purported Kaspersky goodies for sale, but publicized, perhaps, the most interesting ones for free.*

While Kaspersky's report answered the **OBTUSE** question, the second suspected spyware cluster, which we call **SCALENE**, remained a stubborn mystery. In contrast with **OBTUSE**, the **SCALENE** infrastructure used proxy

chains of length 4, TLS certificates with third-level domains, and was exclusively located in the *eu-west-2* EC2 region, sited in London.

The **SCALENE** cluster *also* had uncommon responses that allowed us to pivot to related infrastructure hosted outside of Amazon EC2. The off-EC2 **SCALENE** infrastructure was largely hosted on the UK IP addresses of various cloud providers. Puzzlingly, we were never able to understand the victimology of **SCALENE**, leading us to suspect that any spyware operations were low volume, or confined to specific geographic regions.

SCALENE shifts into focus

On April 14, 2026, *Gen* provided a critical [missing piece](#): the second stage (“Stage 1”) of the novel spyware they observed talked to one of the off-EC2 **SCALENE** servers we had found: **pick.storewebzone[.]net**, hosted on **185.151.31[.]111**. Thus, we learned that not only did our **OBTUSE** cluster represent *actual* spyware, but so too did our **SCALENE** cluster!

Press enter or click to view image in full size

Two spywares, one fingerprint.

Despite *Gen*’s breakthrough, mysteries remain. We were quite surprised that the spyware *Gen* found was not only designed for *Windows*, but also contained (at least) one instance of British spelling. This shows two important contrasts with *Operation Triangulation*, an *iPhone* attack that was (at least partially) US-linked (including via improper OPSEC during procurement of IP address space, a problem that has [long bedeviled](#) the US intelligence community).

Coincidence, or coordination?

So what does it mean that UK-ish Windows spyware overlaps with US-ish iOS spyware? To start, we must entertain the possibility that we pivoted *too hard*. Perhaps our jump from **OBTUSE** to **SCALENE** was a coincidence, and we accidentally found infrastructure for a spyware deployment wholly unrelated to *Operation Triangulation*. On the other hand, both *Angry Spark* and *Triangulation* appear highly targeted, and our pivoting does not seem to have strayed beyond Western-aligned operations. We think a more likely possibility is that both **OBTUSE** and **SCALENE** shared private tooling or, at least, a “playbook” for standing up infrastructure.

Source: <https://medium.com/@billmarczak/an-angry-spark-or-a-triangle-in-disguise-ac32852a1be3>