New 'OtterCookie' malware used to backdoor devs in fake job offers

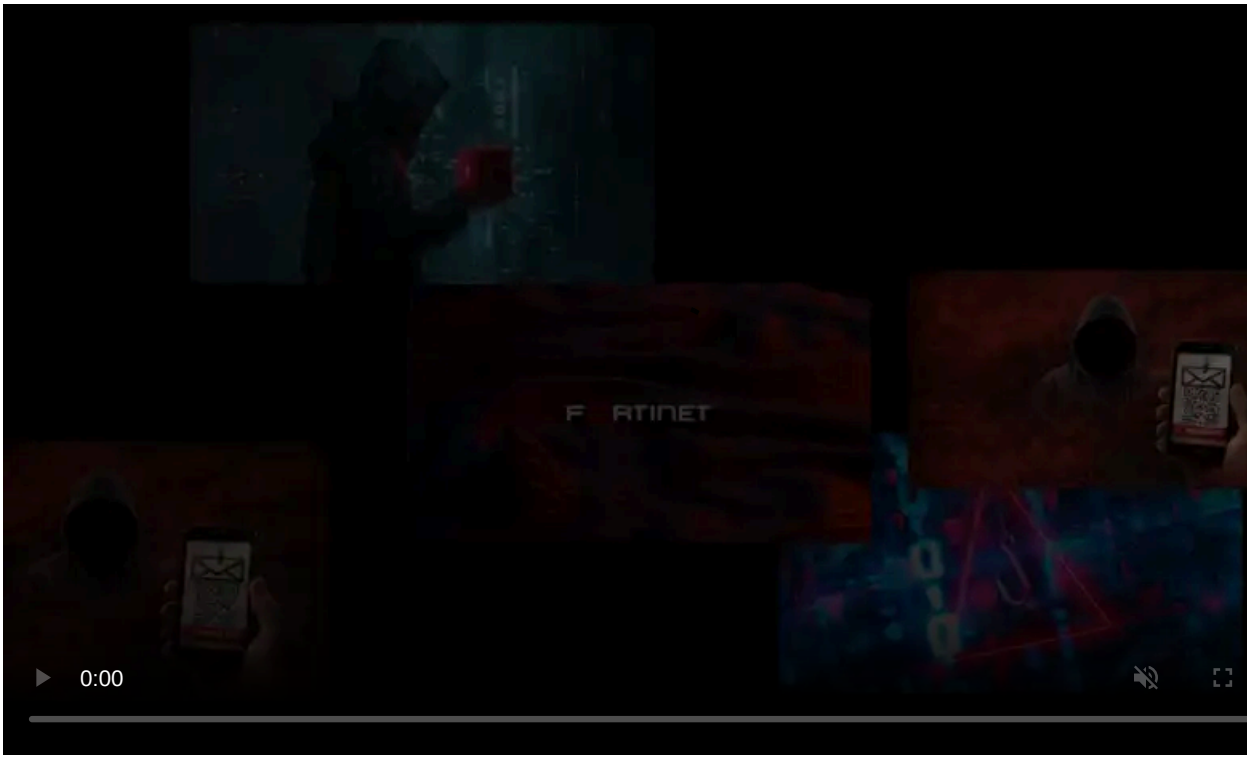
By Bill Toulas

Published: 2024-12-26 · Archived: 2026-04-06 03:09:35 UTC

North Korean threat actors are using new malware called OtterCookie in the Contagious Interview campaign that is targeting software developers.

Contagious Interview has been active since at least December 2022, according to researchers at cybersecurity company Palo Alto Networks. The campaign targets software developers with fake job offers to deliver malware such as BeaverTail and InvisibleFerret.

A report from NTT Security Japan notes that the Contagious Interview operation is now using a new piece of malware called OtterCookie, which was likely introduced in September and with a new variant appearing in the wild in November.

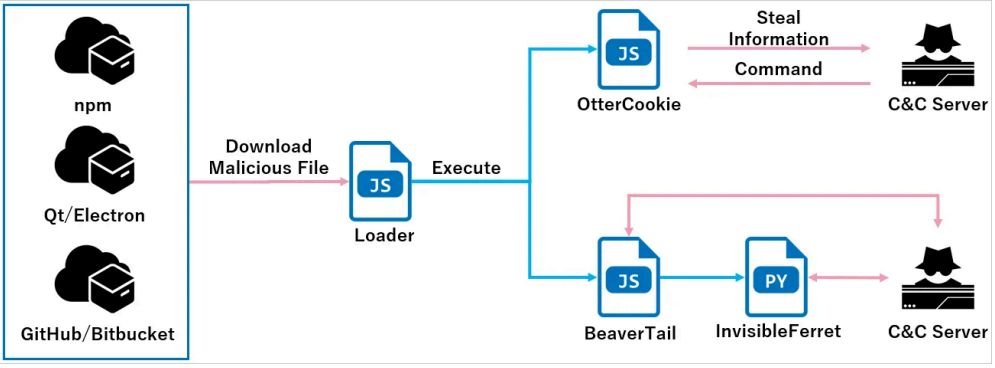

F RTINET
0:00

OtterCookie attack chain

Just like in the attacks documented by Palo Alto Networks' Unit42 researchers, OtterCookie is delivered via a loader that fetches JSON data and executes the 'cookie' property as JavaScript code.

NTT says that, even though BeaverTail remains the most common payload, OtterCookie has been seen in some cases either deployed alongside BeaverTail or on its own.

The loader infects targets through Node.js projects or npm packages downloaded from GitHub or Bitbucket. However, files built as Qt or Electron applications were also used recently.



Overview of the latest Contagious Interview attacks

Source: NTT Japan

Once active on the target device, OtterCookie establishes secure communications with its command and control (C2) infrastructure using the Socket.IO WebSocket tool, and awaits for commands.

The researchers observed shell commands that perform data theft (e.g. collecting cryptocurrency wallet keys, documents, images, and other valuable information).

"The September version of OtterCookie already included a built-in functionality to steal keys related to cryptocurrency wallets," NTT explains.

"For example, the checkForSensitiveData function used regular expressions to check for Ethereum private keys," the researchers note, adding that this was changed with the November variant of the malware where this is achieved through remote shell commands.

```
const regexPatterns = {
    bitcoinPrivateKey: /^[5KL][1-9A-HJ-NP-Za-km-z]{50,51}$/, // Matches Bitcoin private keys
    ethereumPrivateKey: /([a-fA-F0-9]{64})/, // Matches Ethereum private keys (with 0x prefix)
    seedPhrase: /"([a-zA-Z]+ ){11,23}[a-zA-Z]+"/, // Matches possible seed phrases (12-24 words)
};

function checkForSensitiveData(filePath) {
    try {
        // Read the file content
        const fileContent = fs.readFileSync(filePath, 'utf8');

        if (regexPatterns.bitcoinPrivateKey.test(fileContent)) {
            return true;
        }

        if (regexPatterns.ethereumPrivateKey.test(fileContent)) {
            return true;
        }

        const words = fileContent.split(/s+/).filter(Boolean);
        if (
            regexPatterns.seedPhrase.test(fileContent) &&
            words.length >= 12 &&
            words.length <= 24
        ) {
            return true;
        }
        return false;
    } catch (err) { }
}
```

Targeting cryptocurrency information

Source: NTT Japan

The latest version of OtterCookie can also exfiltrate clipboard data to the threat actors, which may contain sensitive information.

Commands typically used for reconnaissance, like ‘ls’ and ‘cat’, were also detected, indicating the attacker’s intention to explore the environment and stage it for deeper infiltration or lateral movement.

The appearance of new malware and the diversification of the infection methods indicate that the threat actors behind the Contagious Interview campaign experiment with new tactics.

Software developers should try to verify information about a potential employer and be wary of running code on personal or work computers as part of a job offer that require coding tests.
