

WithSecure™ Intelligence Research

DUCKTAIL returns: Underneath the ruffled feathers

by Mohammad Kazem Hassan Nejad

Contents

- Introduction 3
- Updates to malware capabilities 4
 - First adaptation 4
 - NativeAOT binaries 5
 - There and back again 6
 - Unused ‘anti-analysis’ code 6
 - Launching a dummy file 7
- The outliers 8
 - Development samples 8
 - Multi-stage variants 9
- The certificate cat-and-mouse game 10
 - C&C and the new affiliates 10
- Fake businesses 11
- Learnings from the incident corner 13
- Conclusion 14
- Recommendations and protection 15
- Acknowledgement 15

Introduction

In late July 2022, WithSecure shed light on a financially motivated malware operation, dubbed DUCKTAIL, that targets individuals and businesses operating on Facebook Ads and Business platform.

In short, the operation consists of an information stealer malware that is delivered to targeted victims that primarily operate in the digital marketing and advertisement space. The malware is designed to steal browser cookies and take advantage of authenticated Facebook sessions to steal information from the victim's Facebook account. The operation ultimately hijacks Facebook Business accounts to which the

victim has sufficient access. The threat actor uses their gained access to run ads for monetary gain.

After a short hiatus, the DUCKTAIL campaign returned with slight changes in their mode of operation. In this report, we'll discuss what we have discovered since our original analysis ¹ was published.

We would like to note that a new campaign was recently discovered and attributed to DUCKTAIL ². However, none of the technical indicators or intelligence gathered on the threat actor behind DUCKTAIL indicate any overlap between these

operations and as such, WithSecure's current assessment is that it is not a new variant or campaign conducted by or related to the operation tracked by WithSecure as DUCKTAIL.

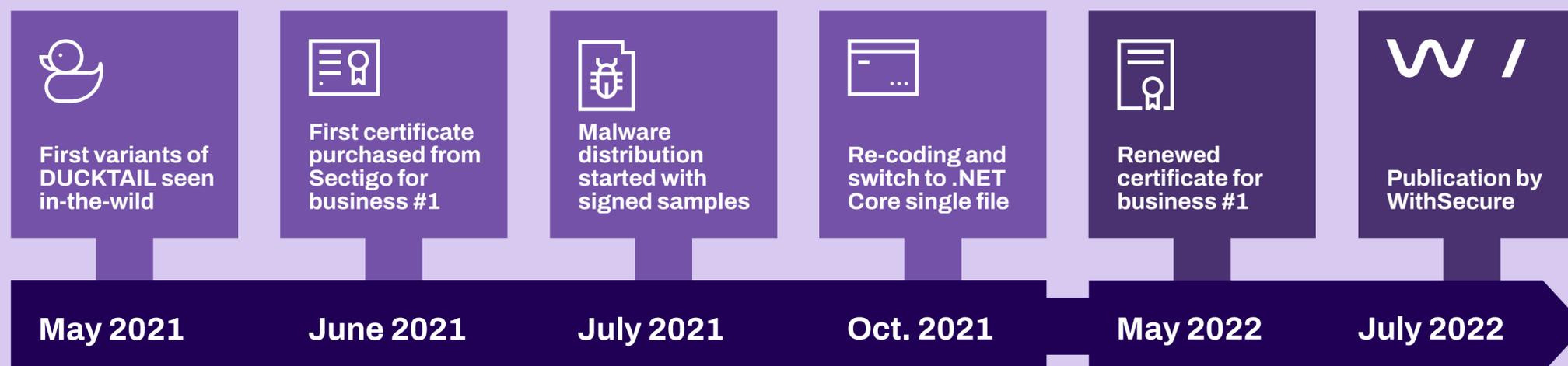


Figure 1. Overview of DUCKTAIL's past

1. <https://labs.withsecure.com/publications/ducktail>
2. <https://www.zscaler.com/blogs/security-research/new-php-variant-ducktail-infostealer-targeting-facebook-business-accounts>

Updates to malware capabilities

First adaptation

After WithSecure’s initial report on DUCKTAIL was published, Sectigo revoked the certificate used to sign the malware, causing the threat actor to try and adapt by signing the information stealer malware with invalid certificates.

However, as they soon realized their attempts were in vain, the campaign was stopped altogether with the last activities being observed on 12th August 2022, shortly after which the Telegram bots were disabled by the threat actor.

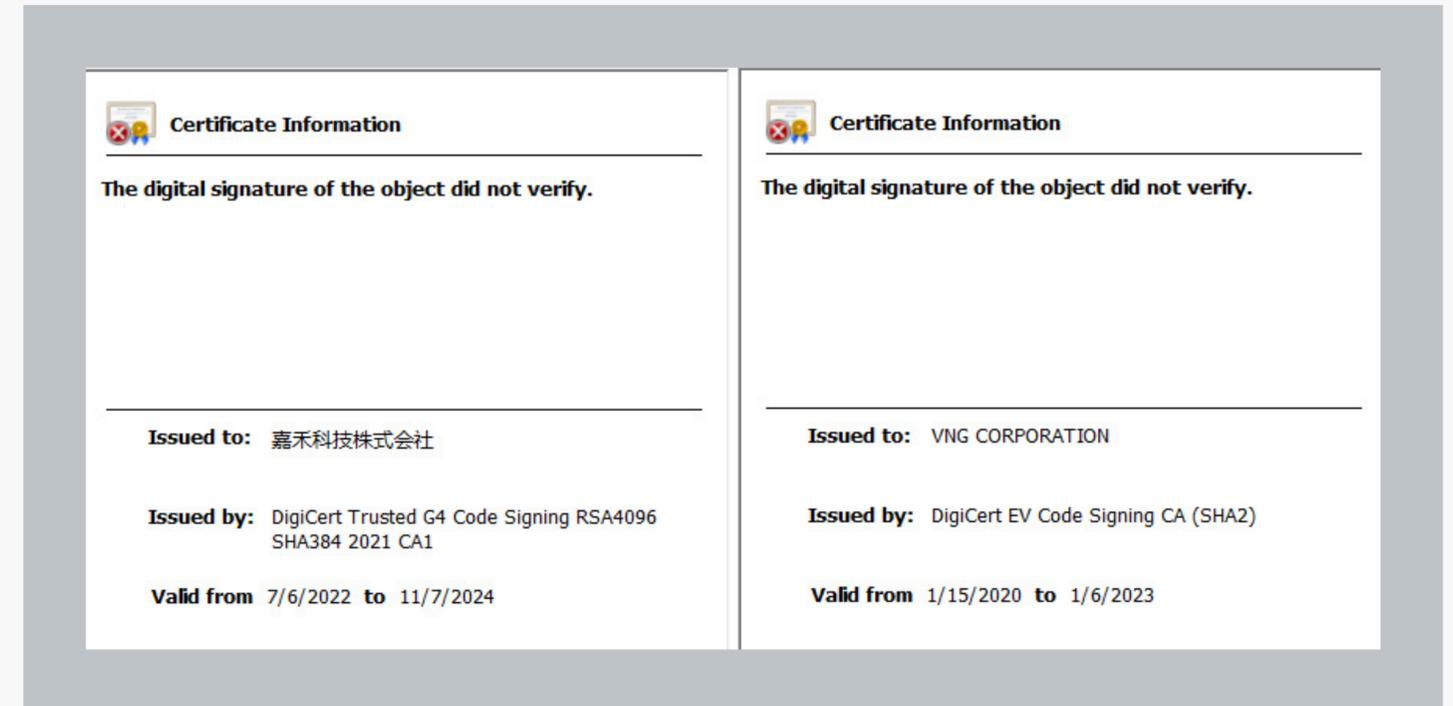


Figure 2. Old samples signed by invalid certificates after revocation

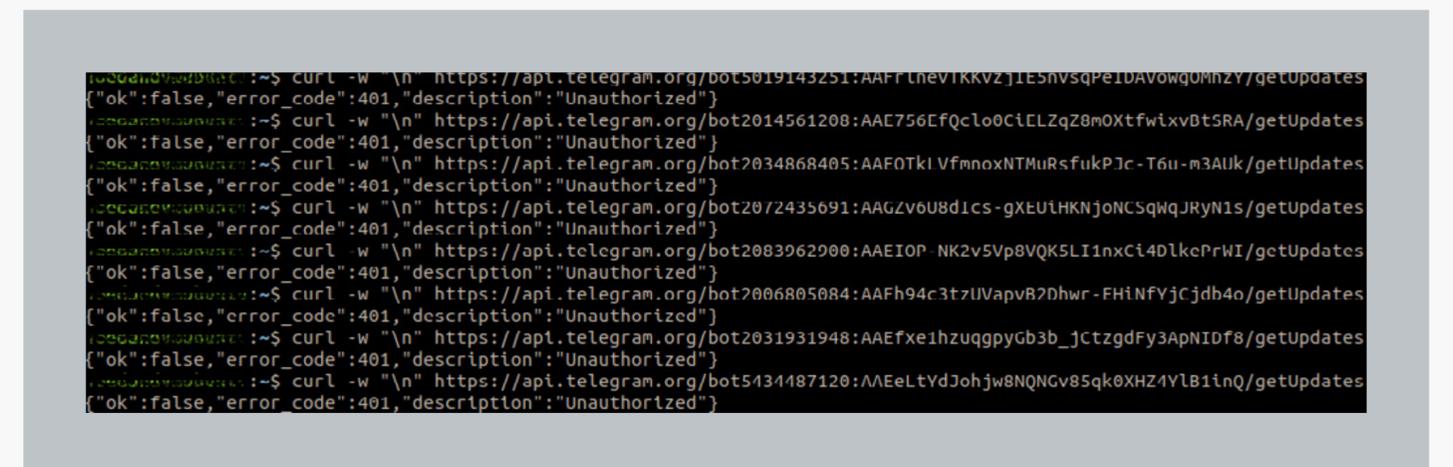


Figure 3. All 8 Telegram bots were disabled

NativeAOT binaries

Almost one month after DUCKTAIL’s last signs of activity, on Tuesday, 6th September 2022, we started receiving alerts from one of our DUCKTAIL hunting rules on new samples observed in-the-wild. In the following days, we observed detection hits across our customer base as our clients were targeted once more.

This new variant utilized the .NET 7 NativeAOT feature which allows binaries to be compiled natively (ahead-of-time) from .NET code. Such binaries differ in format from traditional .NET assemblies.³

NativeAOT offers similar benefits to the .NET single-file feature that previous DUCKTAIL variants used for compilation, especially because they can be compiled as a framework independent binary that doesn’t require .NET runtime to be installed on the victim’s machine.

However, it is worth noting that support for non-native libraries is limited in NativeAOT binaries and could result in crashes. They are also smaller in file size than older variants due to the use of a default trimmed binary setting.⁴

In terms of functionality, the NativeAOT variant was compiled from the same source code base as previous variants, and as such, the behavior of the malware remained largely the same. That being said, there were some slight updates in the code, including:

Complete migration to fetching e-mail list from C&C

- In the initial report, we outlined a feature that was implemented in newer versions of the malware which allowed the threat actor to send a list of e-mail addresses from the C&C channel to be used for business hijacking.

- This is now the default mechanism and e-mail addresses are no longer hardcoded in the binary.
- Additionally, we observed the threat actor experimenting with embedding e-mail addresses inside a text file that would be sent via the C&C, but this was not observed in the samples seen in-the-wild.
- The threat actor currently uses Hotmail and Outlook e-mail addresses, which appear to have been generated using a keyword list. These e-mail addresses appear to be registered before usage, indicating bulk e-mail registration/purchase by the threat actor.

Exfiltrated files are now encrypted

- All files exfiltrated to the C&C are now encrypted with AES-128 algorithm. The key/IV used for encryption are encrypted asymmetrically and sent to the C&C along with the encrypted file.



Figure 4. . Example of exfiltrated file in the latest malware

3. <https://devblogs.microsoft.com/dotnet/announcing-dotnet-7-preview-3/#what-is-native-aot>

4. <https://devblogs.microsoft.com/dotnet/announcing-dotnet-7-preview-7/#trimming-and-nativeaot-all-assemblies-trimmed-by-default>

There and back again

Between 2nd and 4th October 2022, WithSecure spotted yet another batch of new DUCKTAIL samples being submitted to VirusTotal from Vietnam. These were several experimental files that contained a mixture of old and new DUCKTAIL variant code bases, compiled as self-contained .NET Core 3 Windows binaries, indicating an expected shift back to self-contained applications.

On the following day, 5th October 2022, the threat actor started to re-distribute DUCKTAIL malware to victims as self-contained .NET Core Windows binaries, shifting away from NativeAOT and back to using self-contained .NET binaries. The initial shift to NativeAOT could be considered an attempt to stealthily resume their operation after our publication and evade subsequent detection signatures.

Some of the features that were observed in these samples were not seen in the NativeAOT variant and vice versa, indicating that the threat actor is keeping separate development copies of the codebase. This is further evident by the PDB paths, target frameworks, mixture of old and new code, and namespaces that overlap between projects.

Unused ‘anti-analysis’ code

The .NET Core 3 variants contain unused pieces of anti-analysis code that were copied from a GitHub repository.⁵ This is yet another indication of the threat actor’s continuous efforts to evade analysis and detection mechanisms.

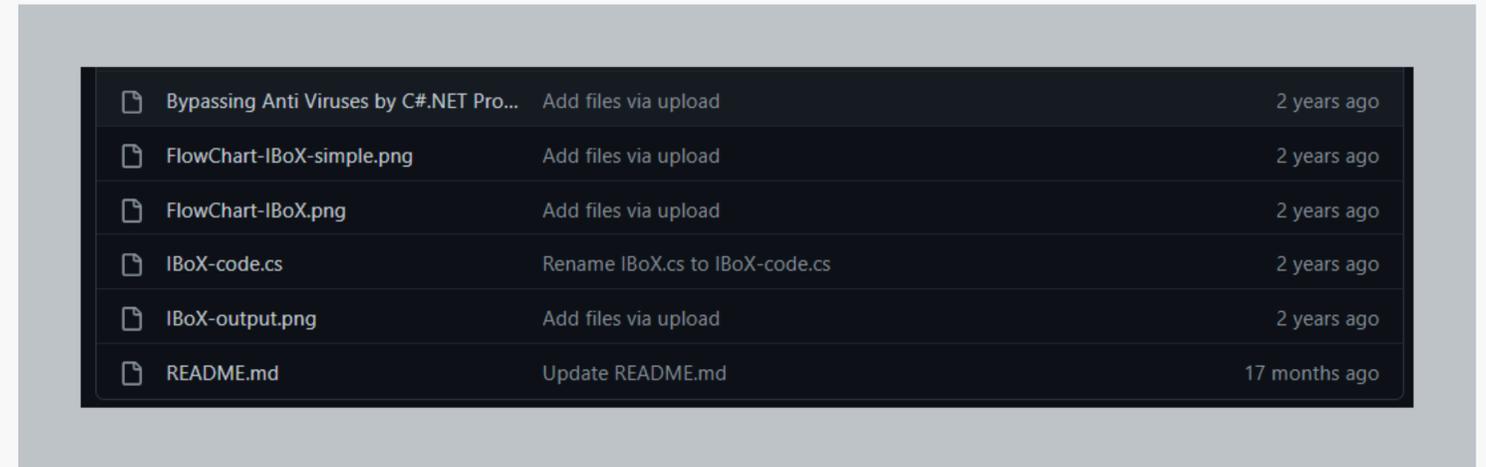


Figure 5. GitHub repo that DUCKTAIL copied



Figure 6. Code comparison between repository and DUCKTAIL

5. <https://github.com/ibo-sec/IBoX>

Launching a dummy file

Previous and current DUCKTAIL samples have used a mixture of double extension, convincing file names, and icons designed to make them look like legitimate video and document files. However, one of the latest additions is the malware launching a dummy file that matches the icon, filename, and extension to further play into this narrative.

The compressed dummy file is embedded into the malware binary, which is decompressed at launch, written to disk in the %TEMP% folder as file_<timestamp>.<ext> and executed via a shell which launches the file with the appropriate application depending on the extension.

At the time of writing, the malware had been seen dropping and launching document (.docx), spreadsheet (.xlsx), and video (.mp4) files.

```

internal class FileOpenHandler
{
    // Token: 0x06000BE5 RID: 3045 RVA: 0x002A2C94 File Offset: 0x002A1894
    public void OpenFile(TelegramHandler telegramHandler)
    {
        bool flag = this._fileData.Length == 0;
        if (!flag)
        {
            string text = Path.Combine(Path.GetTempPath(), "file_" + DateTime.Now.ToString("HHmmssff") + "." + this._extension);
            try
            {
                telegramHandler.Log("Begin open file");
                bool flag2 = !File.Exists(text);
                if (flag2)
                {
                    File.WriteAllBytes(text, FileOpenHandler.Decompress(this._fileData));
                }
                new Process
                {
                    StartInfo = new ProcessStartInfo(text)
                    {
                        UseShellExecute = true
                    }
                }.Start();
                telegramHandler.Log("Begin open success");
            }
            catch (Exception ex)
            {
                telegramHandler.Log(ex.ToString());
            }
        }
    }
}
    
```

Figure 7. Code snippet to launch dummy file

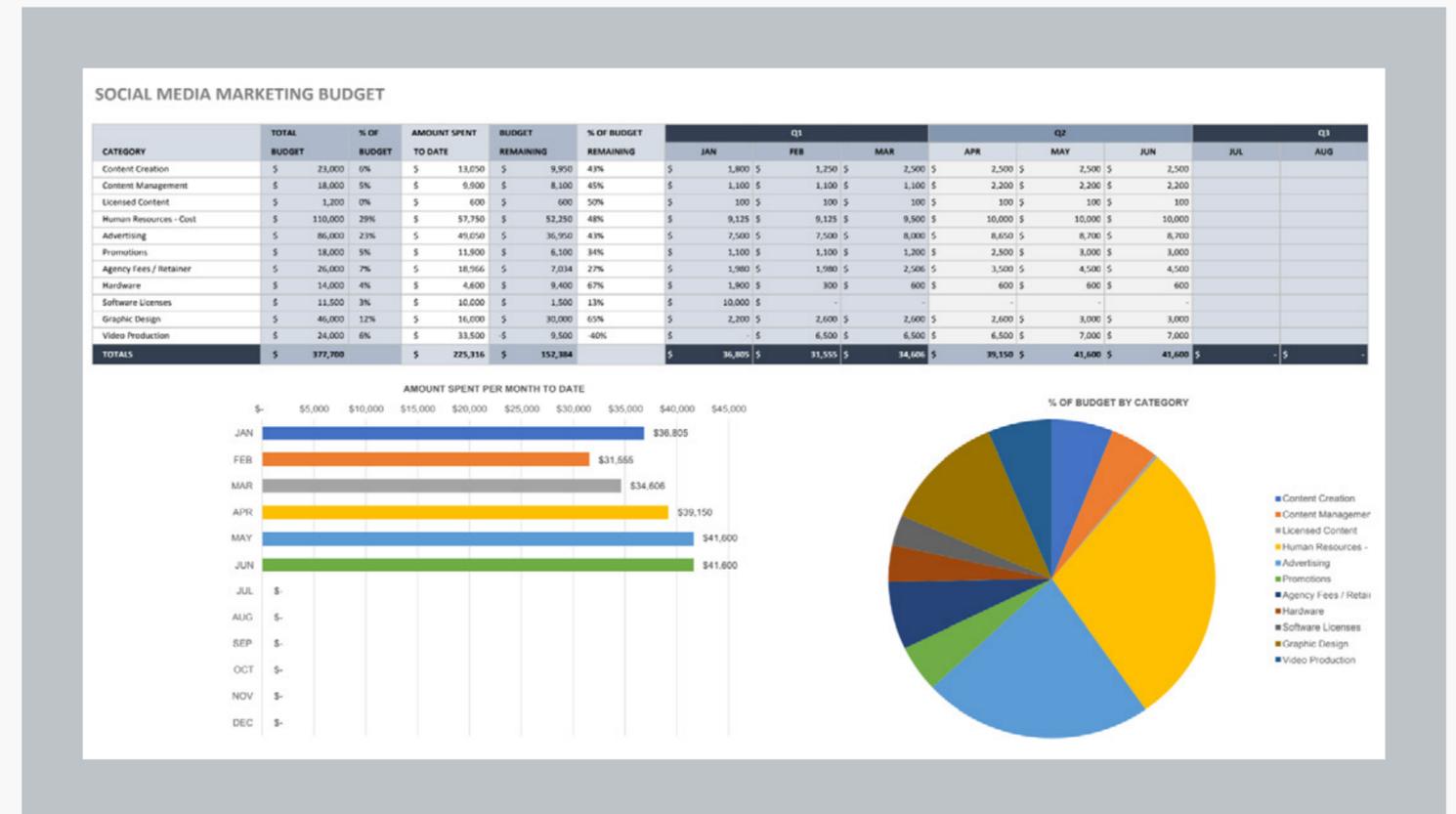


Figure 8. Example of dummy spreadsheet file

The outliers

Aside from the main information stealer malware attributed to the operation, WithSecure has recently identified numerous samples that were either attributed to the threat actor or the operation itself with a high degree of confidence.

Development samples

Between 5th and 10th October 2022, multiple samples were submitted to VirusTotal from Vietnam which were attributable to the threat actor with high confidence.

These samples were all self-contained .NET Core 3 binaries compiled from a project called "WindowsData". The samples appear to have been created for testing purposes and are not malicious samples intended to be distributed to victims. Some of the samples contained code snippets related to the browser scanning functionality found in the main information stealer malware.

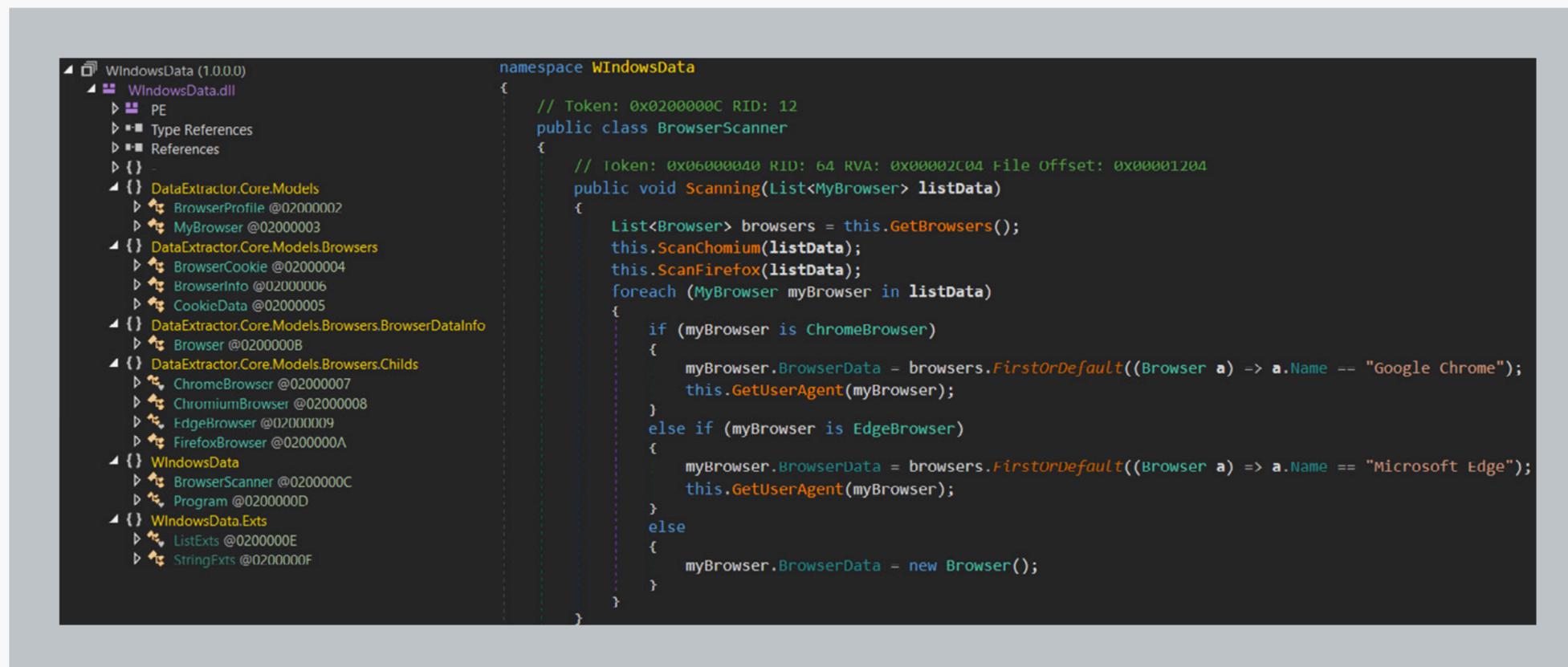


Figure 8. Classes and code snippets found in original infostealer

The certificate cat-and-mouse game

The threat actor has relied on signing their binaries with EV (extended validation) certificates since mid-2021 in what we believe is an attempt to evade Microsoft's SmartScreen prompt designed to raise suspicion among victims as the samples are meant to mimic document/video files.

The threat actor has continued with this trend in their latest campaign, replacing certificates after each revocation. In the middle of the latest campaign,

the threat actor switched their certificate authority from Sectigo to GlobalSign. In each new instance, WithSecure reported the certificate to the relevant certificate authority, and this caused setbacks to the operation as signaled by pauses in the campaigns between each revocation.

At the time of writing, the threat actor has adapted to certificate revocations by utilizing timestamping⁷ as a countersignature method through DigiCert.

C&C and the new affiliates

The malware still relies on Telegram as its C&C channel. At the time of writing, three active Telegram bots and channels were observed in the latest campaign, with the threat actor re-using the same Telegram chats that were initially discovered, indicating that only the bots (and access tokens) were refreshed with stricter administrator rights. The previous access tokens granted full administrator rights to the bots, such as generating invite links for the chats.

An interesting shift that was observed with the latest campaign is that C&C channels now include multiple administrator accounts, indicating that the adversary may be running an affiliate program. This is further strengthened by increased chat activity and the new file encryption mechanism that ensures only certain users will be able to decrypt certain exfiltrated files. WithSecure has also observed decrypted versions of exfiltrated data being shared in some of the C&C channels.

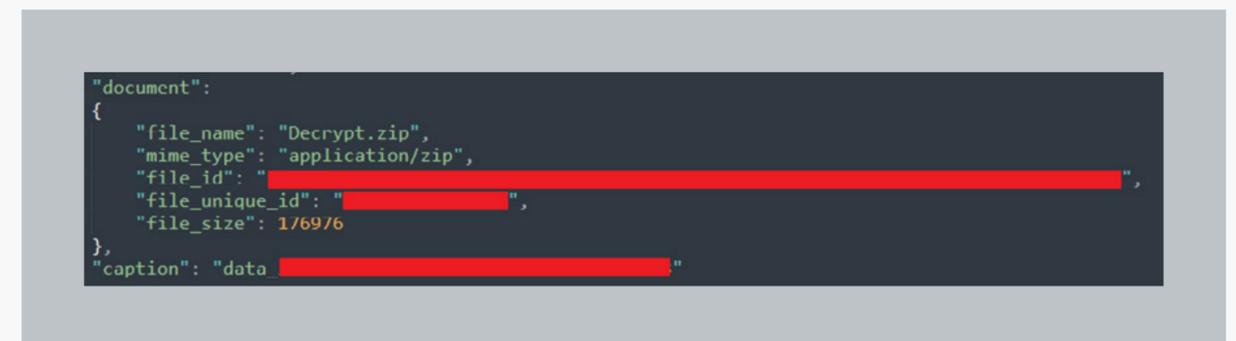


Figure 12. Example of decrypted exfiltrated files sent to the channels

7. <https://learn.microsoft.com/en-us/windows/win32/seccrypto/time-stamping-authenticode-signatures>

Fake businesses

The threat actor has been relying on businesses registered in Vietnam to purchase code signing certificates. At the time of writing, WithSecure has identified seven businesses linked to the operation for this purpose.

The first business linked to DUCKTAIL was registered in 2017 and online activity related to the business had been briefly observed in 2017. The earliest code signing certificate purchased for the business was seen in 2021 as outlined in our initial report, which was used exclusively by the threat actor. The threat actor has continued to rely on purchasing code signing certificates for this business through multiple certificate authorities, even in the latest campaign. We have linked this business to DUCKTAIL with low confidence.

WithSecure observed six other businesses that were registered after our initial report was published, all of which have been linked to DUCKTAIL with medium confidence. Three of these have already been used to purchase certificates in the latest campaign. These registered businesses do not seem operational and gathered intelligence suggest that they are fake.

It is worth noting that the websites associated with all seven businesses have been replicated from a single legitimate business's website.

```
<!-- Mirrored from hackerone.com / by HTTrack Website Copier/3.x [XR&CO'2014], Fri, 20 May 2022 05:51:56 GMT -->
</html>
```

Figure 13. Watermark comment found in HTML content of all businesses' websites

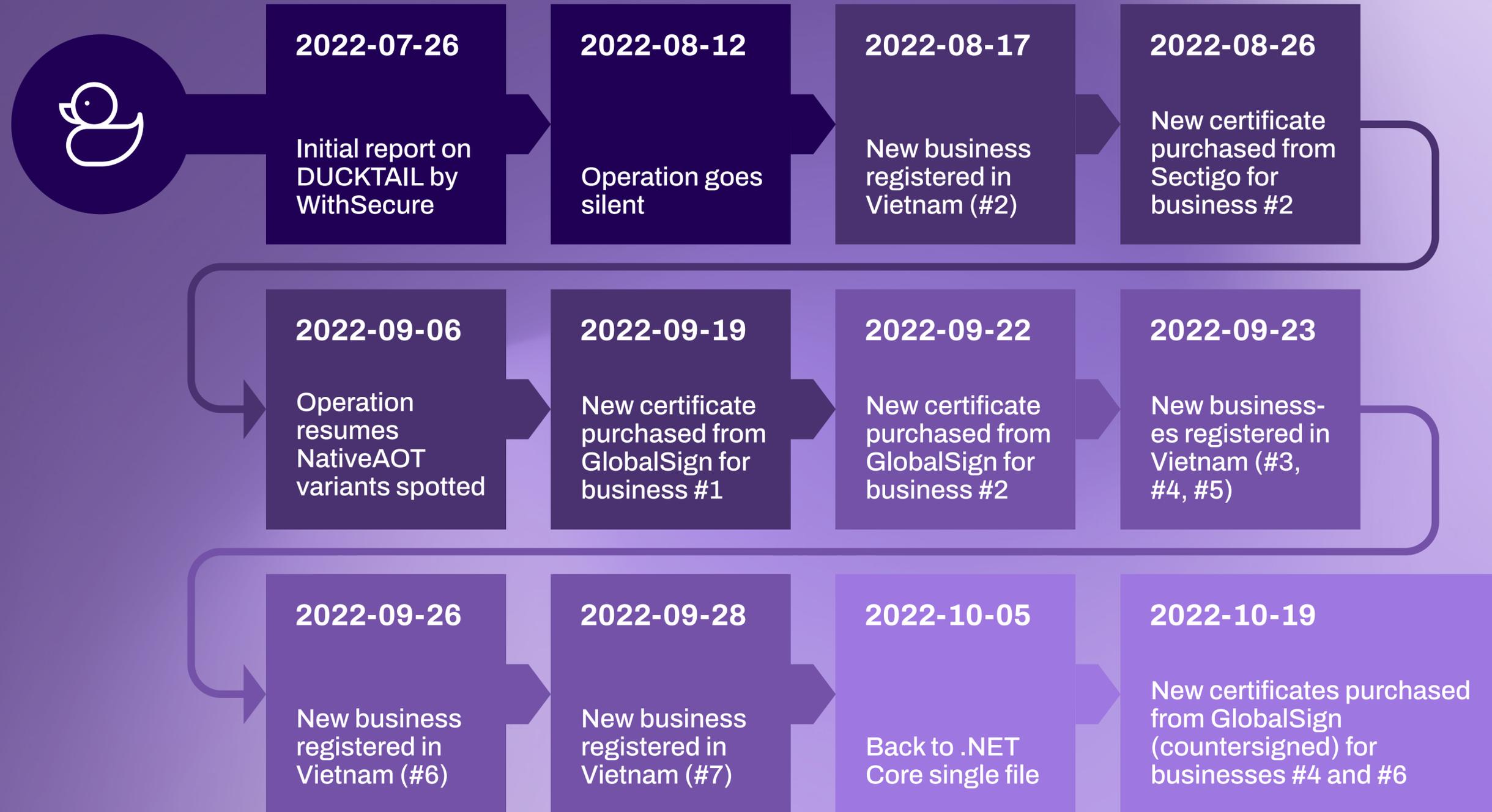


Figure 14. Overview of DUCKTAIL's current activities

Learnings from the incident corner

Based on incidents WithSecure's Incident Response team recently engaged in, some DUCKTAIL victims were targeted through WhatsApp, receiving archive files like those outlined in the initial report, designed to be downloaded and executed on a Windows machine.

In instances where the targeted victims did not have sufficient access to allow the malware to add the threat actor's email addresses into the intended business accounts, the threat actor relied on the information that was exfiltrated from the victims' machines and Facebook accounts to impersonate them and achieve their post-compromise objectives via hands-on activity.

One of these hands-on incidents involved a victim operating entirely within the Apple ecosystem that had not logged on to their Facebook account from any Windows machine. The initial vector for this incident has been left undetermined due to insufficient evidence. The investigation found no sign of malware usage or host compromise across user devices. No clear links could be found between this incident and the DUCKTAIL operation, however it's worth noting that the operators behind this incident were likely from and/or operated

in Vietnam as well. This is indicative of the lucrative vector that the platform provides threat actors.

In these incidents, the companies targeted operated in the advertisement vertical, and the reported direct financial damage fluctuated between \$100,000 to \$600,000.

Across our investigations, WithSecure Incident Response team found that business history logs⁸ and targeted individual's Facebook data⁹ were relevant to analysis of the incident. However, for logs relating to the individuals Facebook account, inconsistencies are widely present between what is visible on the web portal compared to what you would get if you were to download a copy of your data. As recommendation to other investigators, WithSecure Incident Response team strongly recommends capturing a local copy of business history logs as soon as possible and requesting a copy of user data for their account.

8. <https://www.facebook.com/business/help/2512887368958412>

9. <https://www.facebook.com/help/212802592074644>

Conclusion

Facebook advertising revenues continue to rise year-over-year indicating that more brands and businesses are taking advantage of their platform to reach a wider customer base. As such, Facebook's Ads & Business platform remains a lucrative vector particularly for financially motivated cyber criminals. The history and emergence of other similar threats targeting social media ecosystems also indicates an evolving trend among threat actors, which we believe will continue.

The DUCKTAIL operation has shown relentless willingness to persist in the face of multiple setbacks. The operation continues to evolve and has made many attempts to evade detection. The fact that the operation seems to be expanding

through a possible affiliate program indicates that the adversary clearly sees enough financial motivation to continue and as such will remain active for the time being.

Given the cross-platform capabilities of .NET Core and the popularity of other devices (mobile phones) and OS platforms (Android, iOS, MacOS) likely used by potential victims that work in digital marketing/media and advertisement, it is possible that the DUCKTAIL operation may eventually expand by targeting victims across other devices and OS platforms either by re-targeting the codebase or through other attack vectors such as phishing.

Recommendations and protection

WithSecure Elements¹⁰ Endpoint Detection and Response, Endpoint Protection as well as WithSecure Countercept Detection and Response¹¹ continue to provide full protection and detection coverage across the attack lifecycle of the malware.

If you believe your business has been targeted or fallen victim to the same or similar attack and require assistance, you can reach out to our 24/7 incident hotline.¹²

Additionally, you can find an updated list of IOCs as well as YARA rules in WithSecure Lab's GitHub.¹³

Acknowledgement

This report would not have been complete without contributions from WithSecure Intelligence, WithSecure Countercept Detection and Response team, and WithSecure Incident Response team.

10. <https://www.withsecure.com/en/solutions/software-and-services/elements#trial>

11. <https://www.withsecure.com/en/solutions/managed-services/countercept>

12. <https://www.withsecure.com/en/about-us/company-contacts/24-7-incident-hotline>

13. <https://github.com/WithSecureLabs/iocs/tree/master/DUCKTAIL/>

Who We Are

WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.

