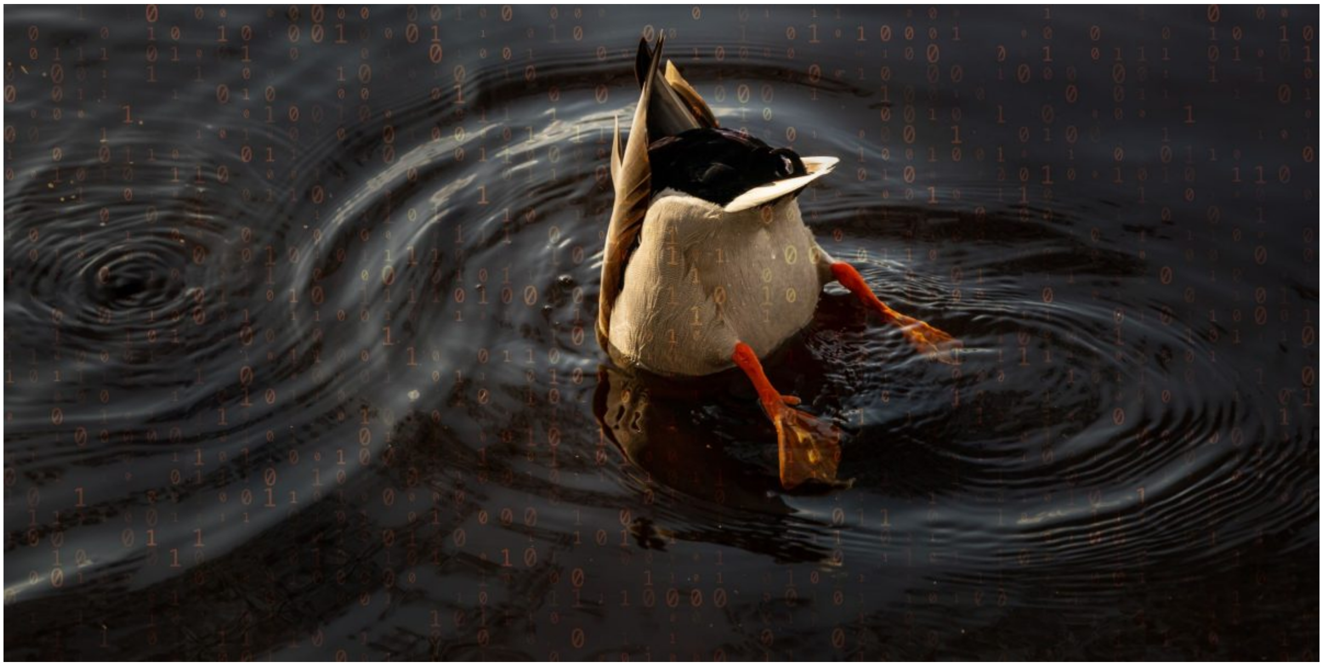
Ducktail fashion week

securelist.com/ducktail-fashion-week/111017/



Authors

Expert AMR

Ducktail is a malware family that has been active since the second half of 2021 and aims to steal Facebook business accounts. WithSecure and GridinSoft have covered Ducktail attacks: the infostealer spread under the guise of documents relating to well-known companies' and brands' projects and products. Both public reports attribute the Ducktail attacks to a group that presumably hails from Vietnam. We have analyzed a recent campaign that ran between March and early October 2023 and targeted marketing professionals. An important feature that sets it apart is that, unlike previous campaigns, which relied on .NET applications, this one used Delphi as the programming language.

Infection

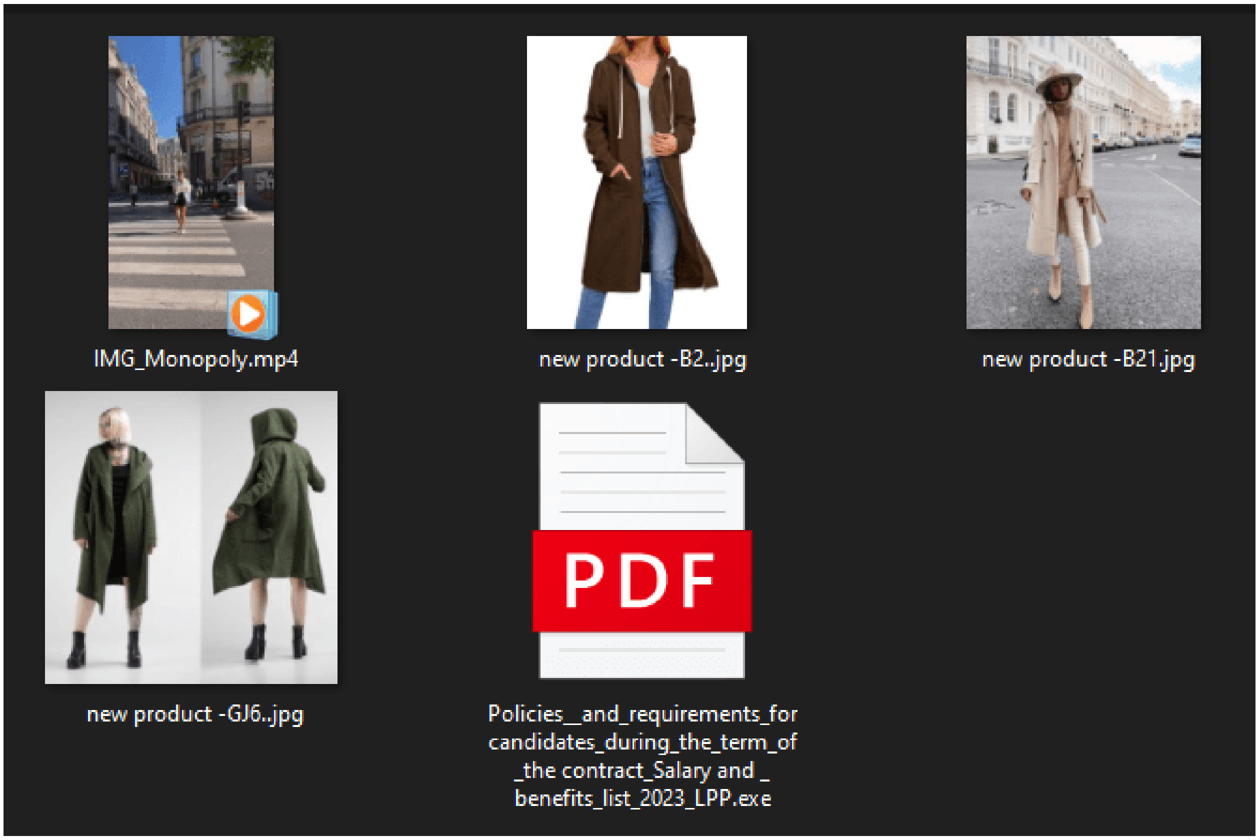
The campaign saw the bad actor send out an archive containing images of new products by bona fide companies along with a malicious executable disguised with a PDF icon. When started, the malware would open a real, embedded PDF file that contained the job details.

The attack was tailored to target marketing professionals looking for a career change. The choice of victims and the distinctive means used by the threat actor led us to assume early on that the campaign was about spreading a new version of Ducktail.

The malware would install a browser extension capable of stealing Facebook business and ads accounts, likely for subsequent sale.

Ducktail and the malicious extension

We examined a large number of archives from the latest campaign: in each case, a copy of Ducktail was emailed in the name of a major clothing company.


IMG_Monopoly.mp4
new product -B2..jpg
new product -B21.jpg
new product -GJ6..jpg
PDF
Policies_and_requirements_for candidates_during_the_term_of _the contract_Salary and _ benefits_list_2023_LPP.exe

The contents of the malicious archive

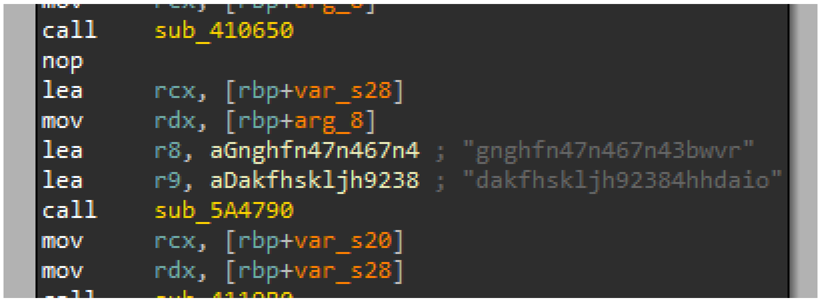
If opened by an interested victim, the malicious file saves a PowerShell script named param.ps1 and a PDF decoy locally to C:\Users\Public. The script uses the default PDF viewer on the device to open the decoy, pauses for five minutes, and then terminates the Chrome browser process.

While the script stands by, the parent executable saves a malicious library named libEGL.dll to C:\Users\Public\Libraries\ and then loads it. When launched, the library goes over every LNK file that it finds in:

- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\,
- C:\ProgramData\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\,

and on the desktop, altering the launch string for all Chromium-based browsers (Google Chrome, Edge, Vivaldi, Brave) by adding the following code: `--load-extension="C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\fjoaledfpmneenckfbpdfhkmimnjocfa"`

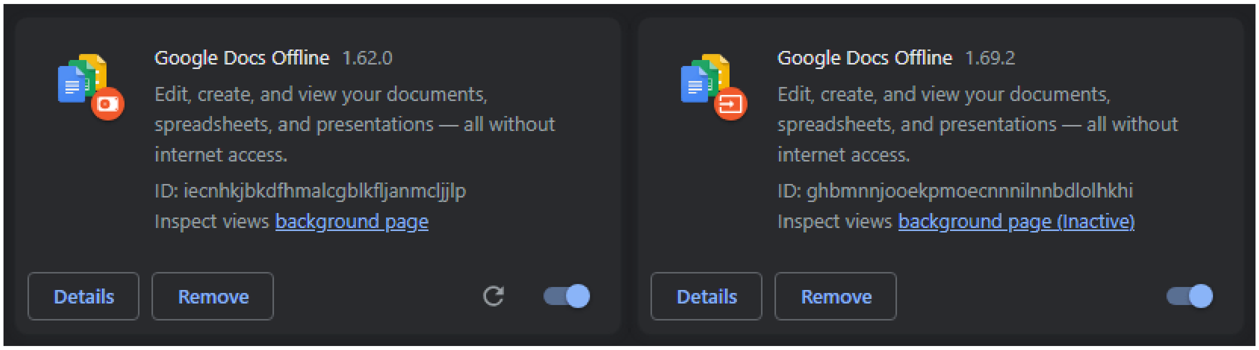
Some of the library strings required for the malicious code to run are encrypted with the AES-CBC key “gnghfn47n467n43b” and the initialization vector “dakfhskljh92384h”.



```
call    sub_410650
nop
lea     rcx, [rbp+var_s28]
mov     rdx, [rbp+arg_8]
lea     r8, aGnghfn47n467n4 ; "gnghfn47n467n43bwvr"
lea     r9, aDakfhskljh9238 ; "dakfhskljh92384hhdaio"
call    sub_5A4790
mov     rcx, [rbp+var_s20]
mov     rdx, [rbp+var_s28]
```

The use of the strings containing the AES key and initialization vector as featured in the code

In addition to launching the library, the parent file saves malicious browser extension files to C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\fjoaledfpmneenckfbpdfhkmimnjocfa. The extension disguises itself with the Google Docs Offline icon and description text, while the directory that features in the path (fjoaledfpmneenckfbpdfhkmimnjocfa) is used by the bona fide extension NordVPN. It is worth noting that other variants of the malware may use different paths to host the extension.



Google Docs Offline 1.62.0

Edit, create, and view your documents, spreadsheets, and presentations — all without internet access.

ID: iecnhkjbkdfhmalcgblkfljanmcljjlp

Inspect views background page

Google Docs Offline 1.69.2

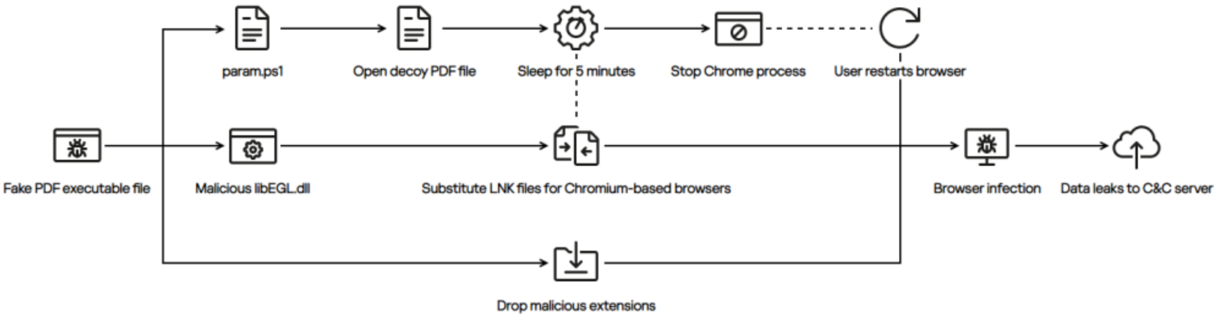
Edit, create, and view your documents, spreadsheets, and presentations — all without internet access.

ID: ghbmnnjooekpmoecnnnilnnbdlolhkhi

Inspect views background page (Inactive)

The malicious extension as seen in Google Chrome (left) and the authentic Google Docs Offline extension (right)

The core exception script is obfuscated. It constantly sends the details of all open browser tabs to the command-and-control (C&C) server, and if detecting Facebook-related URLs, checks for ads and business accounts to try and steal them. In particular, the extension snatches cookies and details of accounts that the victim is signed in to on the device. To bypass two-factor authentication, the extension uses Facebook API requests and Vietnam’s 2fa[.]live service, which offers various auxiliaries for generating one-time access codes, among other things. This is probably how the hackers log in after the user’s authentication session has expired. Stolen credentials and cookies are forwarded to a C&C server registered in Vietnam.



Malicious file usage flowchart

In this campaign, in addition to the main script, the malware would save to the extension folder a script named jquery-3.3.1.min.js, a corrupted version of the core script from prior attacks.

DuckTail attack geography

According to our telemetry, cybercriminals most often attacked users in India. Our solutions also stopped infection attempts on devices of users in Kazakhstan, Ukraine, Germany, Portugal, Ireland, Greece, Jordan, Pakistan, Vietnam, UAE, USA, Peru and Chile.

MITRE ATT&CK Matrix

Tactic	Technique ID	Technique
Initial Access	T1566.001	Phishing: Spearphishing Attachment
Persistence	T1176	Browser Extensions
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
	T1129	Shared Modules
	T1204.002	User Execution: Malicious File
Enterprise	T1539	Steal Web Session Cookie
Resource Development	T1583.001	Acquire Infrastructure: Domains
Reconnaissance	T1589	Gather Victim Identity Information
	T1598.002	Phishing for Information: Spearphishing Attachment
Defense Evasion	T1027	Obfuscated Files or Information

Command and Control	T1071.001	Application Layer Protocol: Web Protocols
	T1132.001	Data Encoding: Standard Encoding
Exfiltration	T1041	Exfiltration Over C2 Channel

Indicators of compromise

c82b959d43789d3dbf5115629c3c01fa8dd599fbec36df0f4bc5d0371296545a
2b3decf08bf9223fb3e3057b5a477d35e62c0b5795a883ceaa9555ca7c28252f
69257876e2ec5bdbe7114d6ce209f13afbfddb2af0006a6d17e6e91578966870
da13db80b0f3c25b512a1692494f303eff1ff1778a837208f79e2f3c81f8192e
bde696a0ae901864716320e3111d5aa49cba3b1d9375dce2903f7433a287b2f2
04dd228d0b088c4116b503c31de22c1746054226a533286bec3a3d0606d73119
89f016d32707f096cc8daf674e5a9fc2ba6cf731d610f5303d997fc848645788
7da7ca7fcbc6e8bc22b420f82ae5756ecd3ad094b8ebcbd5a78a2362eb87b226
655a8ea3bc1baff01639dcdc43a294f8a5dc622e543d8f51e9d51c6eaaae6f6e
1117a93b4b4b78e4d5d6bd79f5f0e04926759558218df30e868464f05bf1bd3d
554353cda0989c3a141c2ab0d0db06393e4f3fd201727e8cf2ed8d136f87d144
b9a984383a5825868c23bc3afdc70e3af2a56d26d002431940d2429c8e88ace9
c6ae36e28668c6132da4d08bca7ceb13adf576fa1dbdb0a708d9b3b0f140dd03
d03e1a0fce0b112bba4d56380c8d1be671845dd3ed90ec847635ba6015bad84d
ab95f377bf7ae66d26ae7d0d56b71dec096b026b8090f4c5a19ac677a9ffe047
f59e2672f43f327c9c84c057ad3840300a2cd1db1c536834f9e2531c74e5fd1c
ba8eb1a7f18e4cfca7dd178de1546d42ffb50028c8f3f7ba6551f88c11be75db
06afd110d91419ece0114a7fdeaeba4e79fbc9f2a0450da8b4f264e4ae073a26
64f6cbe9adf91bc4ed457c79643d764a130b0d25364817c8b6da17b03ff91aa7
bdf8dea28f91adcba7780a26951abc9c32a4a8c205f3207fd4f349f6db290da7
d4f10bd162ee77f4778ecc156921f5949cd2d64aab45b31d6050f446e59aed5a
bdf8dea28f91adcba7780a26951abc9c32a4a8c205f3207fd4f349f6db290da7

C&C
dauhetdau[.]com
motdanvoi20232023[.]com
voiconprivatesv2083[.]com
cavoisatthu2023asd[.]com

Ducktail fashion week

Your email address will not be published. Required fields are marked *