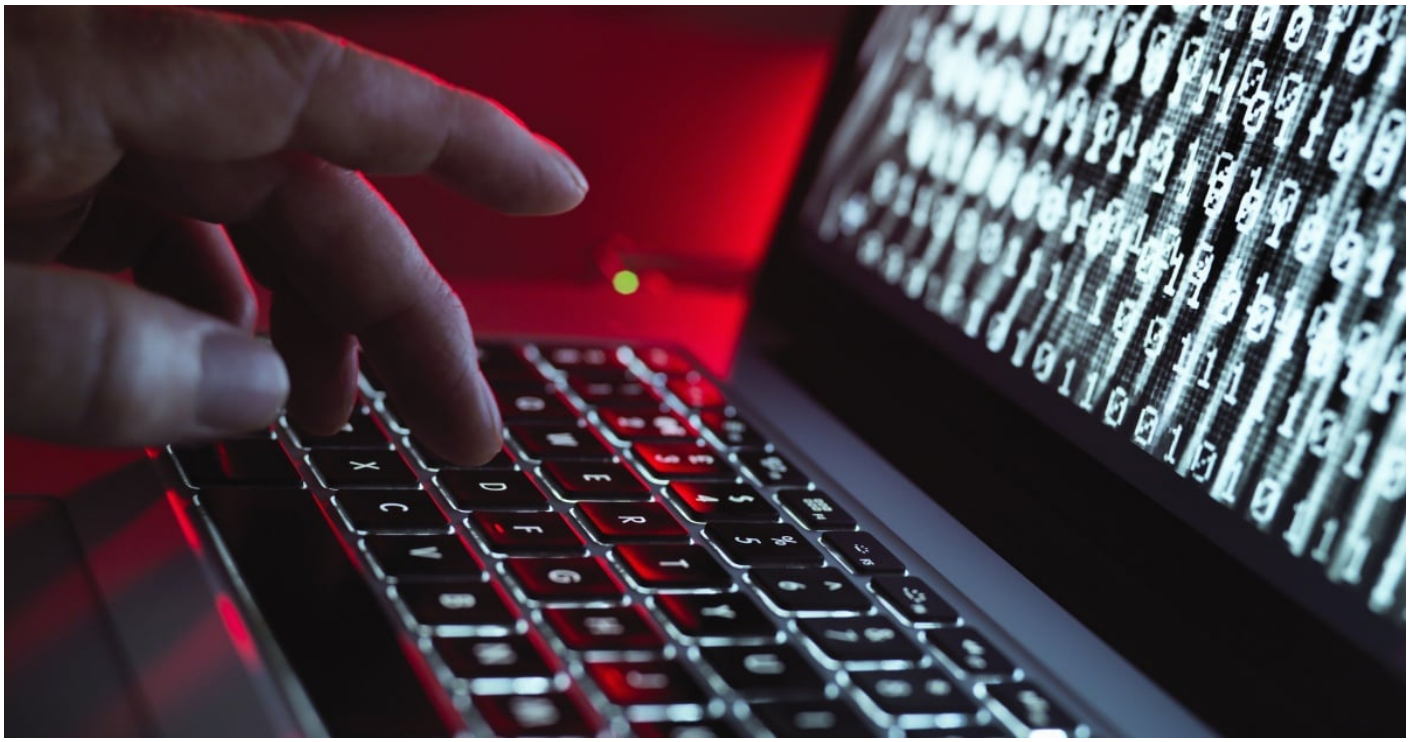
# Bluebottle: Campaign Hits Banks in French-speaking Countries in Africa



Bluebottle, a cyber-crime group that specializes in targeted attacks against the financial sector, is continuing to mount attacks on banks in Francophone countries. The group makes extensive use of living off the land, dual-use tools, and commodity malware, with no custom malware deployed in this campaign.

The activity observed by Symantec, a division of Broadcom Software, appears to be a continuation of activity documented in a Group-IB report from November 2022. The activity documented by Group-IB spanned from mid-2019 to 2021, and it said that during that period this group, which it called OPERA1ER, stole at least $11 million in the course of 30 targeted attacks.

Similarities in the tactics, techniques, and procedures (TTPs) between the activity documented by Group-IB and the activity seen by Symantec include:

- Same domain seen in both sets of activity: personnel[.]bdm-sa[.]fr
- Some of the same tools used: Ngrok; PsExec; RDPWrap; Revealer Keylogger; Cobalt Strike Beacon
- No custom malware found in either set of activity
- The crossover in targeting of French-speaking nations in Africa
- Both sets of activity also feature the use of industry-specific, and region-specific, domain names

While this does appear to be a continuation of the activity documented by Group-IB, the activity seen by Symantec is more recent, running from at least July 2022 to September 2022, though some of the activity

may have begun as far back as May 2022. Some new TTPs have also been employed in recent attacks, including:

- Some indications the attackers may have used ISO files as an initial infection vector
- The use of the commodity malware GuLoader in the initial stages of the attack
- Indications the attackers have adopted the technique of abusing kernel drivers to disable defenses

## Attack chain

The initial infection vector is unknown, but the earliest malicious files found on victim networks had French-language, job-themed file names. These likely acted as lures. In some cases, the malware was named to trick the user into thinking it was a PDF file, e.g.:

- *fiche de poste.exe ("job description")*
- *fiche de candidature.exe ("application form")*
- *fiche de candidature.pdf.exe ("application form")*

It's most likely these files were delivered to victims via a spear-phishing email, which would align with the initial infection vector documented by Group-IB for the OPERA1ER activity.

Although the majority of the activity observed by Symantec researchers began in July 2022, at least one victim was found to have an infostealer with a similar naming theme on its network as early as mid-May 2022. In that case, the malware arrived in the form of a ZIP file containing an executable SCR file.

- *fiche de candidature(1).zip (ZIP file)*
- *fiche de candidature.scr  (executable SCR file)*

The file is an older, likely commodity, malware. It's difficult to determine when it was used to target the organization. It is, however, consistent with infection vectors reported as used by OPERA1ER in 2021.

However, the job-themed malware in July was observed in paths suggesting it had been mounted as CD-ROMs. This could indicate a genuine disc was inserted, but it could also be that a malicious ISO file was delivered to victims and mounted. An ISO file is an archive file that contains an identical copy or image of the data that would be found on an optical disc. Malicious ISO files have been used as an initial infection vector in other campaigns in 2022, including being used alongside the Bumblebee loader in a campaign where delivering ransomware was the ultimate goal. If the Bluebottle and OPERA1ER actors are indeed one and the same, this would mean that they swapped out their infection techniques between May and July 2022. ISO files were not seen in the activity documented by Group-IB.

In many cases, the job-themed malware delivered to victims was the commodity loader called GuLoader. GuLoader is a shellcode-based downloader with anti-analysis features. In addition to malicious files, the loader deploys some legitimate binaries as a decoy for its malicious activity. GuLoader was distributed to victims in a self-extracting NSIS executable. This NSIS script decrypts and injects obfuscated shellcode into another process. The process most often observed in the July activity was *ieinstal.exe*, the Internet Explorer Add-on Installer, but also included *aspnet_regbrowsers.exe*, the ASP.NET Browser Registration tool.

The process for the Internet Explorer Add-on Installer was likely used to download a malicious .NET downloader from URLs such as *hxxp://178.73.192[.]15/ca1.exe*. Multiple .NET downloaders were found that abused the file transfer service *transfer[.]sh* to download a file named with an RTF extension. This payload is unknown, but the downloaders are designed to load it as a .NET DLL.

After GuLoader and the .NET loaders were deployed, various other post-compromise tools were seen on victim networks. These include the publicly available Netwire remote access Trojan (RAT) and the open-source Quasar RAT. The attackers also used the commercial post-compromise tool Cobalt Strike Beacon. The Cobalt Strike Beacon variant used by Bluebottle employed an API hammering technique in order to hamper analysis.

## Use of a signed driver to kill processes

A set of malware was also deployed by the attackers that had the likely goal of disabling the security products on victim networks. The malware consisted of two components, a controlling DLL that reads a list of processes from a third file, and a signed 'helper' driver controlled by the first driver and used to terminate the processes in the list.

Attackers used Windows Service Control (sc.exe) to load the driver:

*sc create fgt binPath= %TEMP%\fgt.sys type= kernel*

*sc start fgt*

In August 2022, Symantec observed the same driver being used in suspected pre-ransomware attack activity against a non-profit in Canada. Another tool found on the victim network was Infostealer.Eamfo, a hacktool that has been associated with Cuba, Noberus, and Lockbit ransomware attacks.

The same driver also appears to have been used by multiple groups for similar purposes. Mandiant documented a financially motivated threat group it calls UNC3944 using this same driver to disable defenses. It referred to this driver as POORTRY and the malware that uses it as STONESTOP. However, Mandiant did note at the time that “POORTRY appears across different threat groups and is consistent with malware available for purchase or shared freely between different groups.”

Sophos also documented an instance where Cuba ransomware operators used a loader called BURNTCIGAR to load signed drivers to kill defenses. The loader operates similarly to the malicious DLL seen in this activity.

These drivers were reported to Microsoft by other vendors, and the company suspended the developer accounts and added defenses to address them.

The short-term goal of Bluebottle in this recent activity appears in part to be persistence and credential theft. The actors used credential theft techniques and tools, such as modifying the WDigest setting and deploying Mimikatz, as well as an open-source fake login screen keylogger.

For lateral movement, the attackers deployed the penetration testing tool SharpHound for domain trust enumeration and executed additional files across the victim organizations using PsExec.

For persistence, evidence suggests the attackers added additional accounts using the *'net localgroup /add'* command. They also deployed an open-source RDPWrap script to enable multiple concurrent RDP sessions on victim systems. This script also modifies the registry and opens port 3389 on the firewall to allow RDP traffic through.

Indications are that this activity was likely “hands-on-keyboard” activity rather than automated. While we do not see what further activity is carried out by the attackers, the victims and the crossover with the activity documented by Group-IB all indicate that this activity is likely financially motivated.

## Victims

Three different financial institutions in three African nations were compromised in the activity seen by Symantec, with multiple machines infected in all three organizations.

The activity on one of the infected institution’s networks ran as follows:

The first activity was seen in mid-July 2022, when job-themed malware was spotted on the infected system. A downloader was then deployed, before the Sharphound hacktool was detected and a tool called fakelogonscreen was also deployed.

About three weeks after the initial compromise of the network, the attackers were seen using a command prompt and PsExec for lateral movement. It appears the attackers were “hands on keyboard” at this point of the attack. The attackers used various dual-use and living-off-the-land tools for numerous purposes, including:

- Quser for user discovery
- Ping for checking internet connectivity
- Ngrok for network tunneling
- Net localgroup /add for adding users
- Fortinet VPN client - likely for a secondary access channel
- Xcopy to copy RDP wrapper files
- Netsh to open port 3389 in the firewall
- The Autoupdatebat 'Automatic RDP Wrapper installer and updater' tool to enable multiple concurrent RDP sessions on a system
- SC privs to modify SSH agent permissions - this could have been tampering for key theft or installation of another channel

Malicious tools used included:

- GuLoader
- Mimikatz
- Revealer Keylogger
- Backdoor.Cobalt
- Netwire RAT
- The malicious DLL and driver for killing processes

Multiple other unknown files were also deployed on this network. The last activity seen on this network was in September 2022, but the Ngrok tunneling tool remained on the network until November 2022.

Some of the same tools were also deployed on the other victims, with GuLoader seen in all three victims. Other activity linking the activity in all three victims includes:

- Same .NET downloader
- Malicious driver used
- At least one overlapping transfer[.]sh URL

## Conclusion

While Symantec cannot confirm whether or not Bluebottle successfully monetized the campaigns we saw it carrying out, the group's success at monetizing its activity between 2019 and 2021, as documented by Group-IB, indicates that this group has had a significant amount of success in the past.

The effectiveness of its campaigns means that Bluebottle is unlikely to stop this activity. It appears to be very focused on Francophone countries in Africa, so financial institutions in these countries should remain on high alert for the activity documented in this blog. The attackers appear to be French-speaking, so the possibility of them expanding this activity to French-speaking nations in other regions also cannot be ruled out.

## Glossary of tools mentioned

- **Cobalt Strike:** An off-the-shelf tool that can be used to execute commands, inject other processes, elevate current processes, or impersonate other processes, and upload and download files. It ostensibly has legitimate uses as a penetration testing tool but is invariably exploited by malicious actors.
- **GuLoader:** A shellcode-based downloader with anti-analysis features. In addition to malicious files, the loader deploys some legitimate binaries as a decoy for its malicious activity.
- **Mimikatz:** Freely available tool capable of changing privileges, exporting security certificates, and recovering Windows passwords in plaintext depending on the configuration.
- **Netsh:** Windows command-line utility that allows a user to configure and display the status of various network communications server roles and components.
- **Netwire RAT:** A remote access Trojan capable of stealing passwords, keylogging, and includes remote control capabilities.
- **Ngrok:** A tunneling tool that allows a user to open a secure tunnel that allows them to instantly open access to remote systems without touching any network settings or opening any ports on a router.
- **Ping:** A tool that is freely available online that can allow users to determine if a specific location on a network is responding.
- **PsExec:** Microsoft Sysinternals tool for executing processes on other systems. The tool is primarily used by attackers to move laterally on victim networks.
- **Quasar RAT:** A remote access Trojan that primarily targets Windows systems and which allows users to remotely control other computers over a network.

- **Quser:** Displays information about user sessions on a Remote Desktop Session Host server. You can use this command to find out if a specific user is logged on to a specific Remote Desktop Session Host server.
- **RDPWrap:** An open-source tool that enables Remote Desktop Host support and concurrent RDP sessions.
- **Revealer Keylogger:** A free tool that records everything typed into a computer.
- **SharpHound:** Can collect data from domain controllers and domain-joined Windows systems.

## Protection

For the latest protection updates, please visit the Symantec Protection Bulletin.

## Indicators of Compromise

**File hashes (SHA256)**

117c66c0aa3f7a5208b3872806d481fd8d682950573c2a7acaf7c7c7945fe10d — ZIP file

c56c915cd0bc528bdb21d6037917d2e4cde18b2ef27a4b74a0420a5f205869e6 — Infostealer

91b3546dde60776ae3ed84fdf4f6b5fba7d39620f0a6307280265cde3a33206b — .NET downloader

9c4c9fa4d8935df811cae0ce067de54ffdb5cfb4f99b4bc36c5aa2a1ac6f9c8f — .NET downloader

1f6be4c29dfb50f924377444e5ca579d3020985a357533fc052226f0091febf6 — .NET downloader

d5b8009dcb50aac8a889e24f038a52fe09721d142a3f1eaa74ac37fff45e9ba2 — .NET downloader

ae4ff662c959cf24df621a2c0b934ed1fa1c26a270a180f695cd5295579afbbd — .NET downloader

0612ef9d2239edeab05f421e3188e2cfcadacbaeafbc9b8e35e778f7234aaa3b — .NET downloader

4acd4335ca43783ff52c0ccbb7e757ea14fb261c33d08268e85ed0ac34e0abec — .NET downloader

47718762dc043f84fb641b1e0a8c65401160cc2e558fd38c14d5d35a114b93cb — .NET downloader

a539961f80feb689546a2e334b03aed81252a04fae032e2d28ed9a7000b3afff — .NET downloader

07ca6122fde46d48f71bcde356d5eeb89040e4a6e83441968a9dade98dc36fe5 — .NET loader

938f50cb2e2d670497209e8cef5bf1042f752b6bf76d1547d68040b5a27f618b — .NET loader

a257eeebba15afecf76b89a379e066e5ed79a2bb9da349c1fdb5a24316abc753 — GuLoader

f276c6a25d6b865c6202978f1d409e8b74e063263eab517f249cf6d3ad3fae4a — GuLoader

3d0fd0444a9e295135ecfdc8c87ddc6dcdff63969c745e0218469332aef18dfe — GuLoader

ac98e6bf6d16904355b1c706bc2b79761a8b09044da40f2c8bce35142ef8bcc8 — GuLoader

ca75b0864d8308efe94eb0822de55eb7f5cfd482d2190100dfd00d433ee790a0 — GuLoader

088110b0ee3588a4822049cf60fff31c67323a9b5993eae3104cc9737a47ce0c — GuLoader

b4adbb5d017d6452c2e1700584261cd3170ee5a14ac658424945f15177494ba1 — GuLoader

818284e7ea0a4bd64ba0eda664f51877ed8c6d35bf052898559dbf4ad8030968 — GuLoader

fa6ca0a168f3400a00dc43f1be07296f4111d7ad9b275809217a9269dd613ae8 — GuLoader

d5b3b1304739986298ba9b7c3ff8b40b3740233d6bb02437ce61a20ee87468bc — GuLoader

8495a328fdd4afd33c3336e964802018d44c1dda15b804560743d6276e926218 — GuLoader

ce2ea1807d984e1392599d05f7ab742bae4f20f8ef80c5a514fbdeede2ff7e55 — Quasar RAT

e933ec0f52cbc60b92134d48b08661b1af25c7d93ff5041fc704559b45bd85b8 — Netwire RAT

6db5e2bb146b11182f29d03b036af4e195044f0ef7a8f7c4429f5d4201756b8f — Cobalt Strike

f4fba2181668f766fdfbd1362420a53ac0b987f999c95baf5dbe235fd3bad4b8 — Cobalt Strike

ec2146655e2c04bf87b8db754dd2e92b8c48c4df47b64a9adc1252efd8618e62 — Fakelogonscreen

e5633d656dea530a62f5ad2792f253e74453712be34d2eadfb49190f7a9ee10b — Malicious DLL used to register Helper Driver

0440ef40c46fdd2b5d86e7feef8577a8591de862cfd7928cdbcc8f47b8fa3ffc — Signed Helper driver

5090f311b37309767fb41fa9839d2770ab382326f38bab8c976b83ec727e6796 — Sharphound

5e245281f4924c139dd90c581fc79105ea19980baa68eeccf5bf36ae613399b9 — PsExec

31eb1de7e840a342fd468e558e5ab627bcb4c542a8fe01aec4d5ba01d539a0fc — Mimikatz

**Network Indicators**

hxxp://files[.]ddrive[.]online:444/load

hxxp://85.239.34[.]152/download/XWO_UnBkJ213.bin

hxxps://transmissive-basin[.]000webhostapp[.]com

hxxps://udapte[.]adesy[.]in

banqueislamik[.]ddrive[.]online

hxxps://transfer[.]sh/get/mKwvWI/NHmZJu.rtf

hxxps://transfer[.]sh/get/RTPlqa/oISxUP.rtf

hxxp://files[.]ddrive[.]online:4448/a

hxxp://banqueislamik[.]ddrive[.]online:4448/ZPjH

hxxp://46.246.86[.]12/ca3.exe

hxxp://178.73.192[.]15/ca1.exe

personnel[.]bdm-sa[.]fr

185.225.73[.]165