Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Bluebottle Group Continues Attacks on Banks in Francophone Africa

Date of Publication

January 6, 2023

Admiralty Code

A1

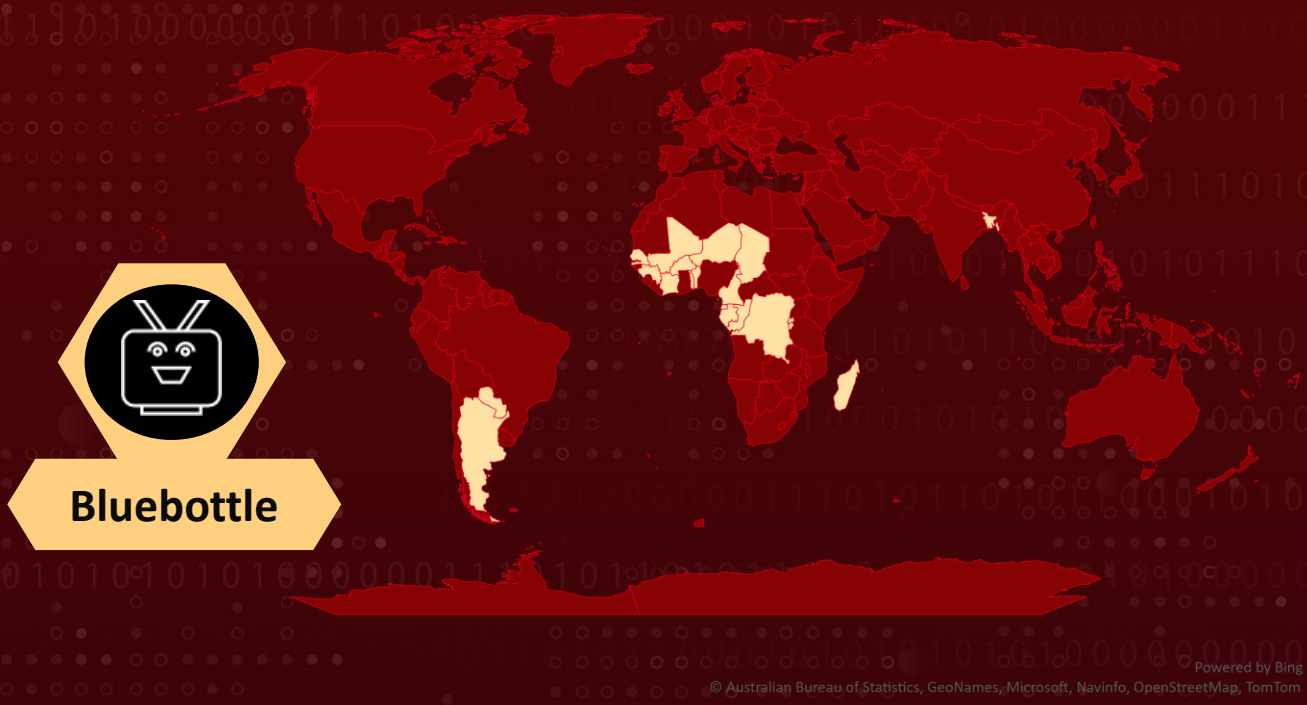
TA Number

TA2023010

Summary

First appeared: 2019
Attack Region: Benin, Burkina Faso, Burundi, Cameroon, Comoros, The Republic of Congo, The Democratic Republic of Congo, The Ivory Coast, The Republic of Djibouti, Gabon, Guinea, Equatorial Guinea, Madagascar, Mali, Niger, The Central African Republic, Rwanda, Senegal, Seychelles, Tchad, Togo, Argentina, Paraguay, Bangladesh
Impacted Sector: Financial
Attack: The Bluebottle group that has been targeting banks in French-speaking countries in Africa and has been using new tactics, techniques, and procedures (TTPs) in its attacks.

Attack Regions



Attack Details

#1 Bluebottle is a cybercrime group that has been targeting banks in French-speaking countries in Africa. The group uses a variety of tactics, including living off the land, dual-use tools, and commodity malware, but no custom malware. The group has been active since at least mid-2019, and has stolen at least $11 million in the course of 30 targeted attacks.

#2 More recent activity has been ongoing since at least July 2022, and employs some new tactics, including the use of ISO files as an initial infection vector, the use of the commodity malware GuLoader, and the technique of abusing kernel drivers to disable defenses.

#3 The group uses spear-phishing emails to deliver malware to victims, which is often disguised as a job-themed file or delivered via a ZIP file. The group's ultimate goal is to steal sensitive data from the banks it targets.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0001 Initial Access	TA0003 Persistence	TA0006 Credential Access
TA0004 Privilege Escalation	T1003 OS Credential Dumping	T1055 Process Injection	T1027 Obfuscated Files or Information
T1021 Remote Services	T1056 Input Capture	T1566 Phishing	T1189 Drive-by Compromise
T1562 Impair Defenses	T1127 Trusted Developer Utilities Proxy Execution	T1204 User Execution	T1204.002 Malicious File
T1562.001 Disable or Modify Tools	T1059 Command and Scripting Interpreter		

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxp://files[.]ddrive[.]online:444/load hxxp://85.239.34[.]152/download/XWO_UnBkJ213.bin hxxps://transmissive-basin[.]000webhostapp[.]com hxxps://udapte[.]adesy[.]in 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
IPV4	185.225.73[.]165
SHA256	117c66c0aa3f7a5208b3872806d481fd8d682950573c2a7acaf7c7c7945fe10d c56c915cd0bc528bdb21d6037917d2e4cde18b2ef27a4b74a0420a5f205869e6 1b3546dde60776ae3ed84fdf4f6b5fba7d39620f0a6307280265cde3a33206b 9c4c9fa4d8935df811cae0ce067de54ffdb5cfb4f99b4bc36c5aa2a1ac6f9c8f 1f6be4c29dfb50f924377444e5ca579d3020985a357533fc052226f0091febf6

TYPE	VALUE
SHA256	d5b8009dcb50aac8a889e24f038a52fe09721d142a3f1eaa74ac37ff f45e9ba2 ae4ff662c959cf24df621a2c0b934ed1fa1c26a270a180f695cd5295 579afbbd 0612ef9d2239edeab05f421e3188e2cfcadacbaeafbc9b8e35e778f7 234aaa3b 4acd4335ca43783ff52c0ccbb7e757ea14fb261c33d08268e85ed0a c34e0abec 47718762dc043f84fb641b1e0a8c65401160cc2e558fd38c14d5d35 a114b93cb a539961f80feb689546a2e334b03aed81252a04fae032e2d28ed9a7 000b3afff 07ca6122fde46d48f71bcde356d5eeb89040e4a6e83441968a9dad e98dc36fe5 938f50cb2e2d670497209e8cef5bf1042f752b6bf76d1547d68040b 5a27f618b a257eeebba15afecf76b89a379e066e5ed79a2bb9da349c1fdb5a24 316abc753 f276c6a25d6b865c6202978f1d409e8b74e063263eab517f249cf6d 3ad3fae4a 3d0fd0444a9e295135ecfdc8c87ddc6dcdff63969c745e0218469332 aef18dfe ac98e6bf6d16904355b1c706bc2b79761a8b09044da40f2c8bce351 42ef8bcc8 ca75b0864d8308efe94eb0822de55eb7f5cfd482d2190100dfd00d4 33ee790a0 088110b0ee3588a4822049cf60fff31c67323a9b5993eae3104cc97 37a47ce0c b4adbb5d017d6452c2e1700584261cd3170ee5a14ac658424945f1 5177494ba1 818284e7ea0a4bd64ba0eda664f51877ed8c6d35bf052898559dbf 4ad8030968 fa6ca0a168f3400a00dc43f1be07296f4111d7ad9b275809217a926 9dd613ae8 d5b3b1304739986298ba9b7c3ff8b40b3740233d6bb02437ce61a2 0ee87468bc 8495a328fdd4afd33c3336e964802018d44c1dda15b804560743d6 276e926218 ce2ea1807d984e1392599d05f7ab742bae4f20f8ef80c5a514fbdee de2ff7e55 e933ec0f52cbc60b92134d48b08661b1af25c7d93ff5041fc704559b 45bd85b8 6db5e2bb146b11182f29d03b036af4e195044f0ef7a8f7c4429f5d42 01756b8f

TYPE	VALUE
SHA256	f4fba2181668f766fdfbd1362420a53ac0b987f999c95baf5dbe235fd3bad4b8 ec2146655e2c04bf87b8db754dd2e92b8c48c4df47b64a9adc1252efd8618e62 e5633d656dea530a62f5ad2792f253e74453712be34d2eadfb49190f7a9ee10b 0440ef40c46fdd2b5d86e7feef8577a8591de862cfd7928cdbcc8f47b8fa3ffc 5090f311b37309767fb41fa9839d2770ab382326f38bab8c976b83ec727e6796 5e245281f4924c139dd90c581fc79105ea19980baa68eeccf5bf36ae613399b9 31eb1de7e840a342fd468e558e5ab627bcb4c542a8fe01aec4d5ba01d539a0fc

References

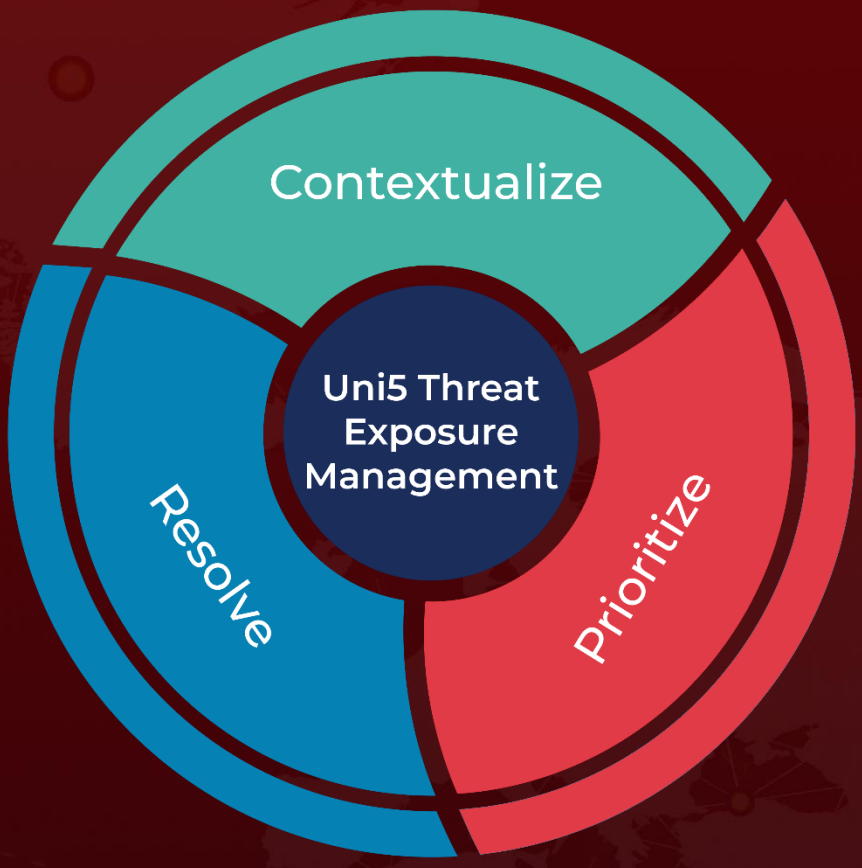
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bluebottle-banks-targeted-africa

https://www.bleepingcomputer.com/news/security/bluebottle-hackers-used-signed-windows-driver-in-attacks-on-banks/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 6, 2023 . 6:40 AM

More at www.hivepro.com