French-speaking gang OPERA1ER APT in Africa | Group-IB Blog

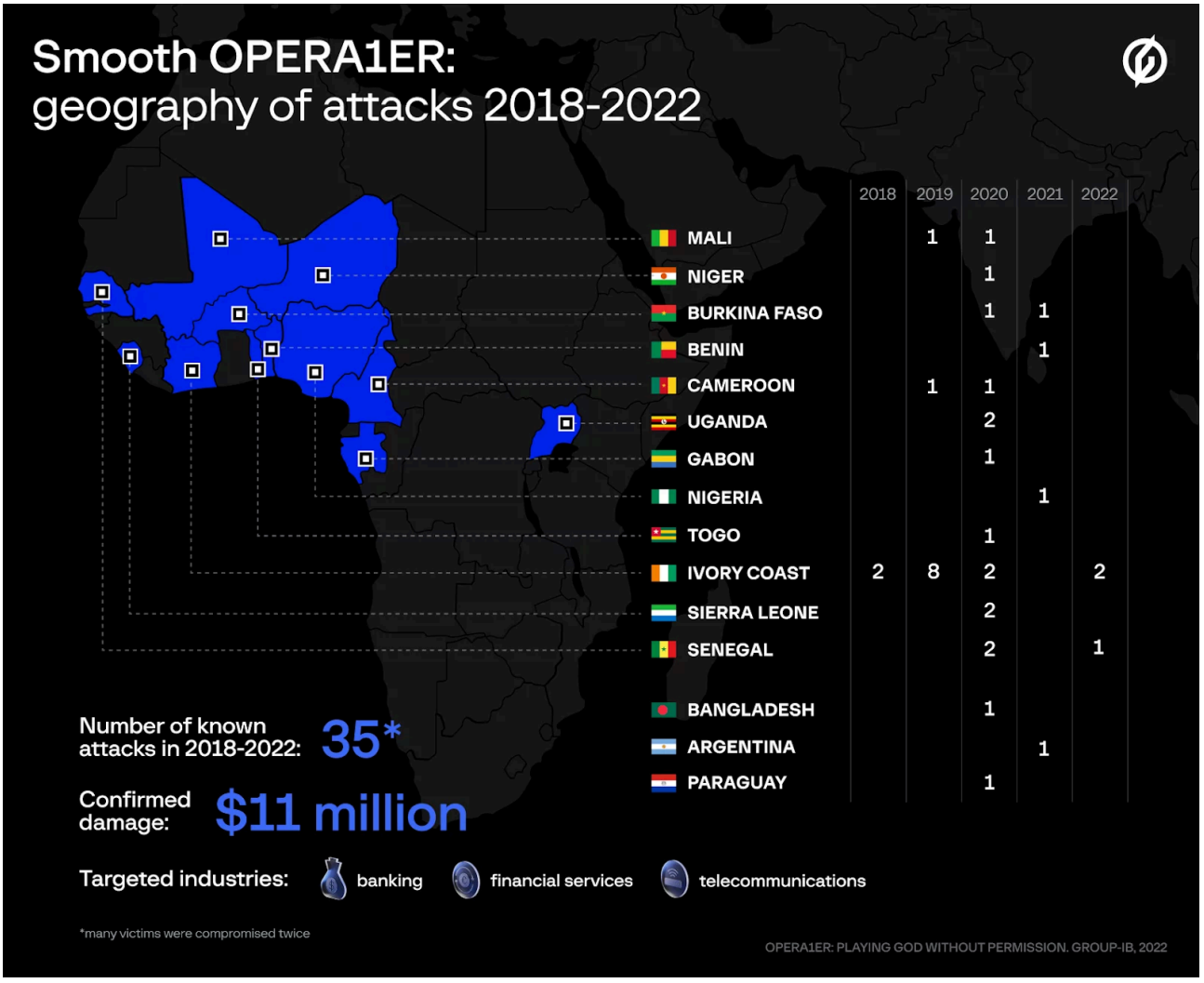
Archived: 2026-05-01 02:04:40 UTC

In 2019, Group-IB Threat Intelligence team detected a series of targeted attacks on financial organizations in Africa. Later in 2020, our professionals in collaboration with Orange, managed to piece together the seemingly disparate attacks into a single timeline and successfully attribute them to **the threat actor codenamed OPERA1ER** (also known as DESKTOP-GROUP, Common Raven, NXSMS).

Our latest threat research

In 2021, together with Orange CERT-CC, we've got an idea to release a comprehensive report (now known as **"OPERA1ER. Playing God without permission"**) which would thoroughly describe this persistent threat, map out all TTPs and methods this criminal syndicate leverages that remained unnoticed in the network for years.

Active and dangerous throughout 2018 – 2022, **the French-speaking gang managed to carry out over 30 successful attacks on banks, financial services and telecommunications companies**, mainly located in Africa. **During this period OPERA1ER is confirmed to have stolen at least $11 million.**



Seasoned threat actors rarely lack street smarts, and **OPERA1ER** clearly noticed a growing interest in their activity and reacted by deleting their accounts and changing some TTPs to cover their tracks. When this happened, we risked losing sight of them. To avoid being outfoxed, the Group-IB team postponed publishing our findings until they revealed themselves again.

You can find **the Blog in French** here: [L'APT OPERA1ER en Afrique]

The moment has come

We are pleased to finally release this report, OPERA1ER: Playing God without permission, in tight cooperation with Orange CERT-CC. This report is truly unique: it covers **several years of research and illustrates a perfect outcome of international collaboration** along with the impactful contributions of numerous organizations and experts. We are incredibly grateful for their support; please find a complete list of contributors in the report.

New discoveries

Threat actors are constantly developing new TTPs and in August 2022, with the help of Przemyslaw Skowron, **Group-IB identified new Cobalt Strike servers used by OPERA1ER.**

Our teams analyzed the newly detected infrastructure, revealing that **attacker had carried out 5 more attacks in the time after we finished having targeted:**

- A bank in Burkina Faso in 2021
- A bank in Benin in 2021
- 2 banks in Ivory Coast in 2022
- A bank in Senegal in 2022

Keep in mind that the IOCs and hunting tips presented in the report were collected over several years and may no longer be relevant, however in this article we provide some important updates. The report's MITRE matrix is in a similar position and we recommend that reads utilize the updated information for the 5 new attacks below.

This article shares the latest network indicators and extra hunting techniques. These extra findings are supposed to **fill in the gaps in the narrative about this APT** so that the cybersecurity community can better track OPERA1ER's activity, but please download the full report to get a holistic view.

Extra findings: hunting new infrastructure

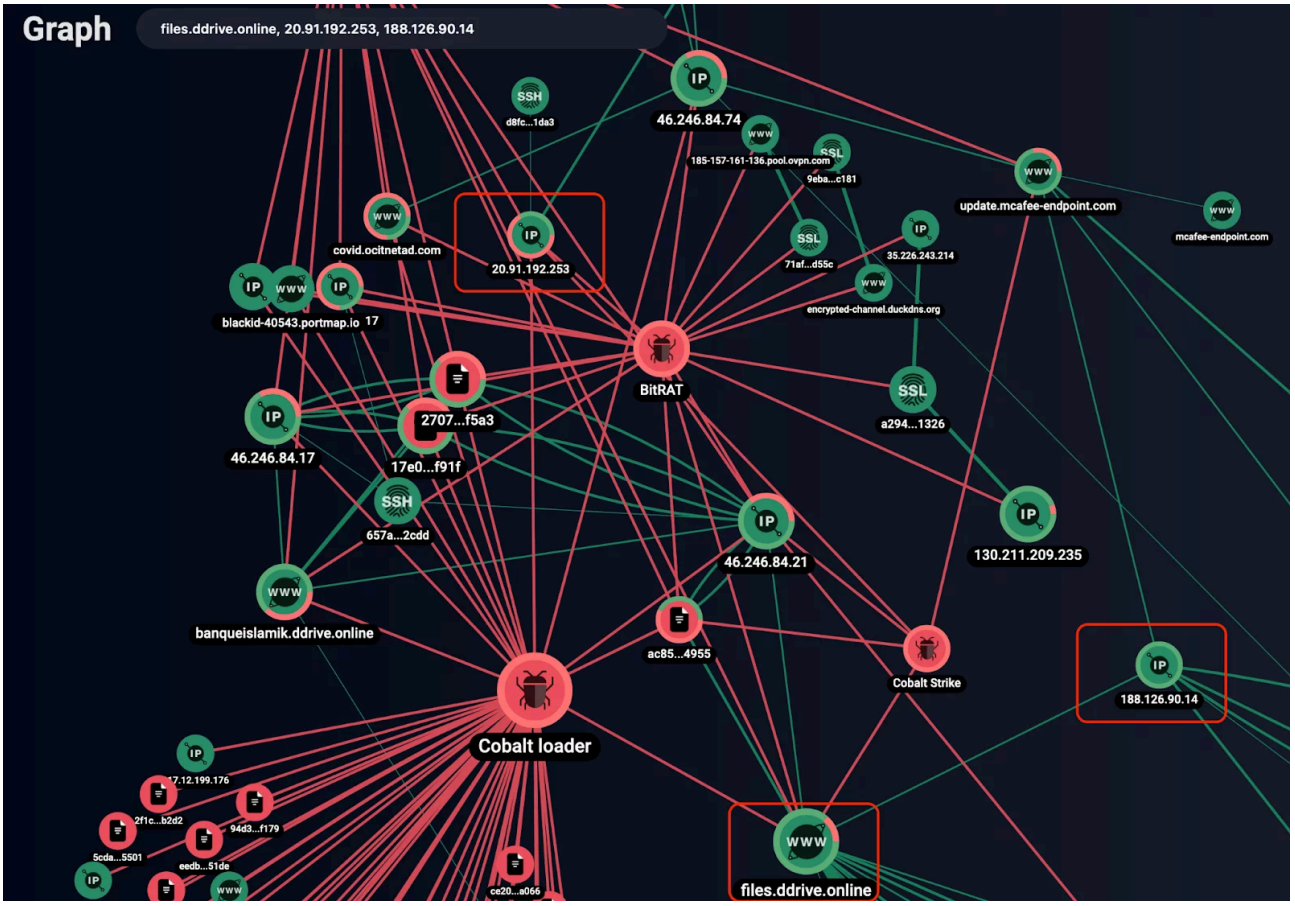
First, Mr Skowron, an Organised Crime Lead, noticed that the attacker uses a specific Public Key on their Cobalt Strike servers:

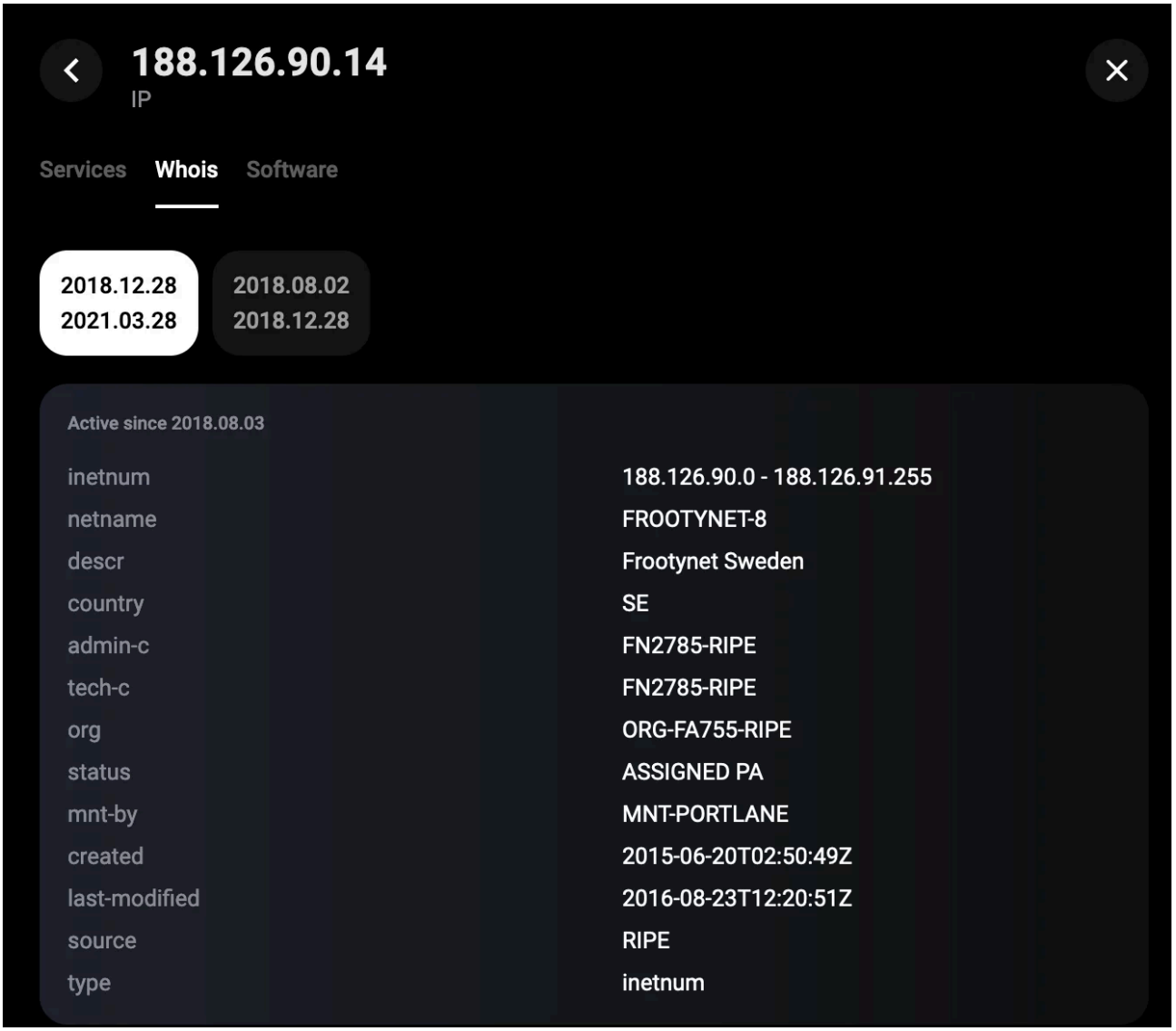
"PublicKey_MD5":"52c66274994172447b21054744cc5b69".

Using that fingerprint, we were able to conduct additional investigations, as described below. Beginning with the PublicKey we identified the following servers:

- *files[.]ddrive[.]online*
- *20[.]91[.]192[.]253*
- *188[.]126[.]90[.]14*

Using Group-IB Threat Intelligence Graph tool we can investigate these servers in depth:


Graph
files.ddrive.online, 20.91.192.253, 188.126.90.14
SSH
d8fc...1da3
IP
46.246.84.74
www
185-157-161-136.pool.ovpn.com
SSL
9eba...c181
www
update.mcafee-endpoint.com
www
mcafee-endpoint.com
www
covid.ocitnetad.com
IP
20.91.192.253
SSL
71af...d55c
IP
35.226.243.214
www
encrypted-channel.duckdns.org
IP
www
IP
blackid-40543.portmap.io
17
BitRAT
SSL
a294...1326
2707...f5a3
IP
46.246.84.17
17e0...f91f
SSH
657a...2cdd
IP
46.246.84.21
IP
130.211.209.235
www
banqueislamik.ddrive.online
ac85...4955
Cobalt Strike
IP
188.126.90.14
Cobalt loader
IP
2f1c...b2d2
94d3...f179
5cda...5501
eedb...51de
ce20...a066
www
files.ddrive.online



According to the Graph, all three servers are connected to infrastructure described in the OPERA1ER report. We identified the following fingerprints on the servers:

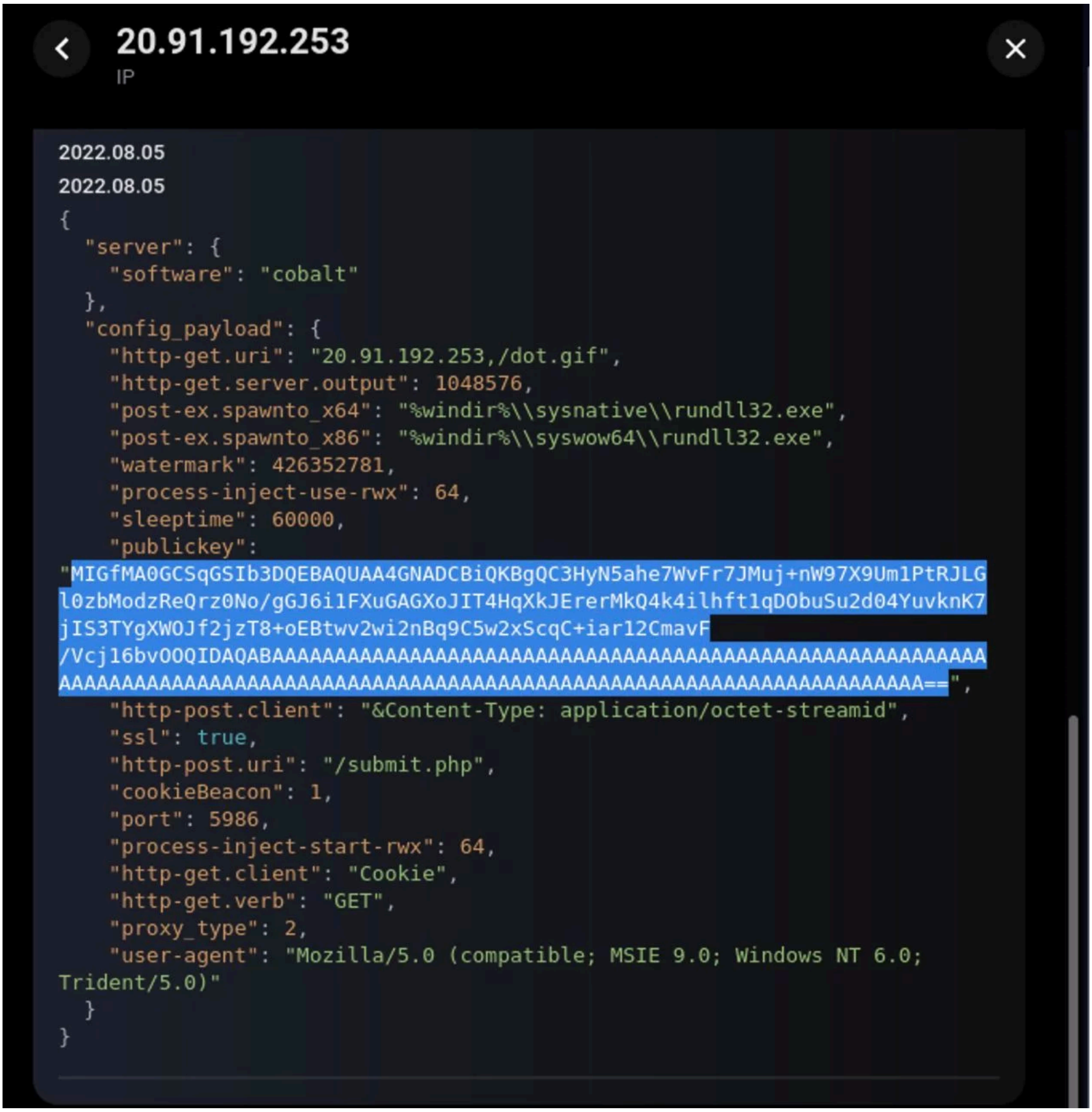
- Usage of *BitRAT*
- Usage of VPN infrastructure like *FrootVPN*
- Usage of *DynDNS* services

The only missing part here is a Cobalt Strike Listener on port *777*, which we know exists because OPERA1ER has been observed deploying *Cobalt Strike Beacon*. Analyzing further, **Group-IB was able to identify a new heuristic to hunt for OPERA1ER's malicious infrastructure.**

With the Graph we were also able to identify the following:

- *banqueislamik[.]ddrive[.]online*
- *178[.]73[.]192[.]17*
- *46[.]246[.]84[.]17*
- *46[.]246[.]84[.]21*

One of these servers contains another *PublicKey*, shown below:



With that *PublicKey*, the following servers were identified:

- 43[.]205[.]33[.]202
- 46[.]246[.]84[.]74
- 72[.]11[.]142[.]240
- 178[.]73[.]192[.]17

While analyzing the servers above, we found another heuristic to identify other ones:

SSH fingerprint :"657a78dcd2c190f00b2f4ef745dd2cdd"

To learn more don’t hesitate to sink your teeth into **the full report, OPERA1ER: Playing God without permission**, to get exhaustive information about OPERA1ER operations. To learn more about the Threat Intelligence Graph reach out to one of our experts.

IOCs

43[.]205[.]33[.]202
46[.]246[.]84[.]74
72[.]11[.]142[.]240
178[.]73[.]192[.]17
banqueislamik[.]ddrive[.]online
46[.]246[.]84[.]17
46[.]246[.]84[.]21
files[.]ddrive[.]online
20[.]91[.]192[.]253
188[.]126[.]90[.]14
2707299e9ec7fb2173f6afb2e23a4d74865cf5a3
17e0b8fe9acfd1776a1566ce5ed6f051f7e0f91f
ac85af8395d1b97a8cbcbd16f995ce119e3c4955
