



DESKTOP-Group or OPERA1ER

BOTCONF 2023 – LIGHTNING TALK

```
C:> whoami /all
```

- Tom Ueltschi
- Swiss Post CERT / SOC / CSIRT since 2007 (*soon 16 years!*)
- Focus & Interests: **Malware Analysis, Threat Intel**, Threat Hunting, **Red / Purple** Teaming
- Member of many trust groups & infosec communities
- FIRST SIG member (malware analysis, red teaming, CTI)
- Twitter: @c_APT_ure || @SwissPost_CERT

Swiss Post CERT

@SwissPost_CERT

CERT-Team @swisspost / @postschweiz
Cyber Defence for post.ch / AS12511
FIRST member @FIRSTdotOrg

BotConf speaker history

- 2013 - My Name is Hunter, **Ponmocup** Hunter
- 2014 - **Ponmocup** Hunter 2.0 – The Sequel
- 2015 - LT: Creating your own CTI (in 3 minutes.. or 5 😊)
- 2016 - Advanced Incident Detection and Threat Hunting using **Sysmon** (and Splunk)
- 2017 - LT: **Sysmon** FTW! 😊
- 2018 - Hunting and detecting APTs using **Sysmon** and PowerShell logging
- 2019 - **DESKTOP-Group** - Tracking a Persistent Threat Group (using Email Headers)
- 2022 - LT: Advanced Persistent Speaker 😊 (**DESKTOP-Group**)

Who is "DESKTOP-Group"?

This is just a preliminary post about my research of a threat actor (TA) or group (TG) that we have named "DESKTOP-Group". Other companies (Orange-CERT, Group-IB, SWIFT) have other names for this TA, but they are not yet publicly known or linked yet. *(I will update this post, as soon as more becomes public)*

We started tracking this TA's activity in early 2018, while analyzing the first malware laden attack mails during February 2018. For the next three years, we saw and analyzed 170 distinct attack mails (campaigns) from this TA, but during 2021 it became harder to link malware mails back to them with high confidence.

The first public presentation "*DESKTOP-Group – Tracking a Persistent Threat Group (using Email Headers)*" was at BotConf 2019. Slides (PDF) are available from my [Github repo](#).

In 2020, I also presented about this TA at ReversingLabs [#Reversing2020](#) online conference. A [video](#) (starts around 14:30m) and PDF slides are also available.

In 2019, I started sharing on Twitter about this TA, later starting to use the hashtag [#DESKTOPgroup](#).

- 2018 – started tracking **DESKTOP-Group** @ SwissPost **(over 5 years ago!)**
- 2019 – first talk @ BotConf
- 2020 – second talk @ Reversing2020 (online)
- 2021 – Group-IB & Orange-CERT wrote Threat Report (yet unpublished)
- 2022 – SWIFT adds «**DESKTOP-Group**» alias to a TA they track & publish
- **Nov 2022 – Group-IB published OPERA1ER Threat Report («Playing God without permission»)**

Who is "DESKTOP-Group"?

Update 2022-11-06: A few days ago Group-IB released the report "OPERA1ER - Playing God without permission" (blog, [report PDF](#), webinar), linking different aliases to "DESKTOP-Group":


- Group-IB: OPERA1ER
- Orange-CERT-CC: NXSMS
- SWIFT: Common Raven
- Mandiant: UNC4044 (*not in the report*)



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

POSTED: 5 JAN, 2023 | 11 MIN READ | THREAT INTELLIGENCE

 SUBSCRIBE

FOLLOW  

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

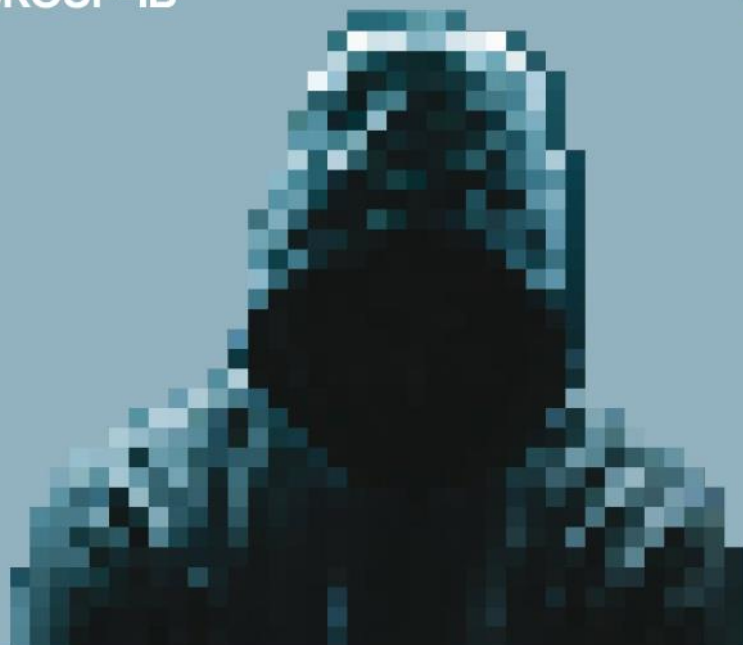
Continuation of previously documented activity leverages new TTPs.

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.



Threat Hunter Team
Symantec



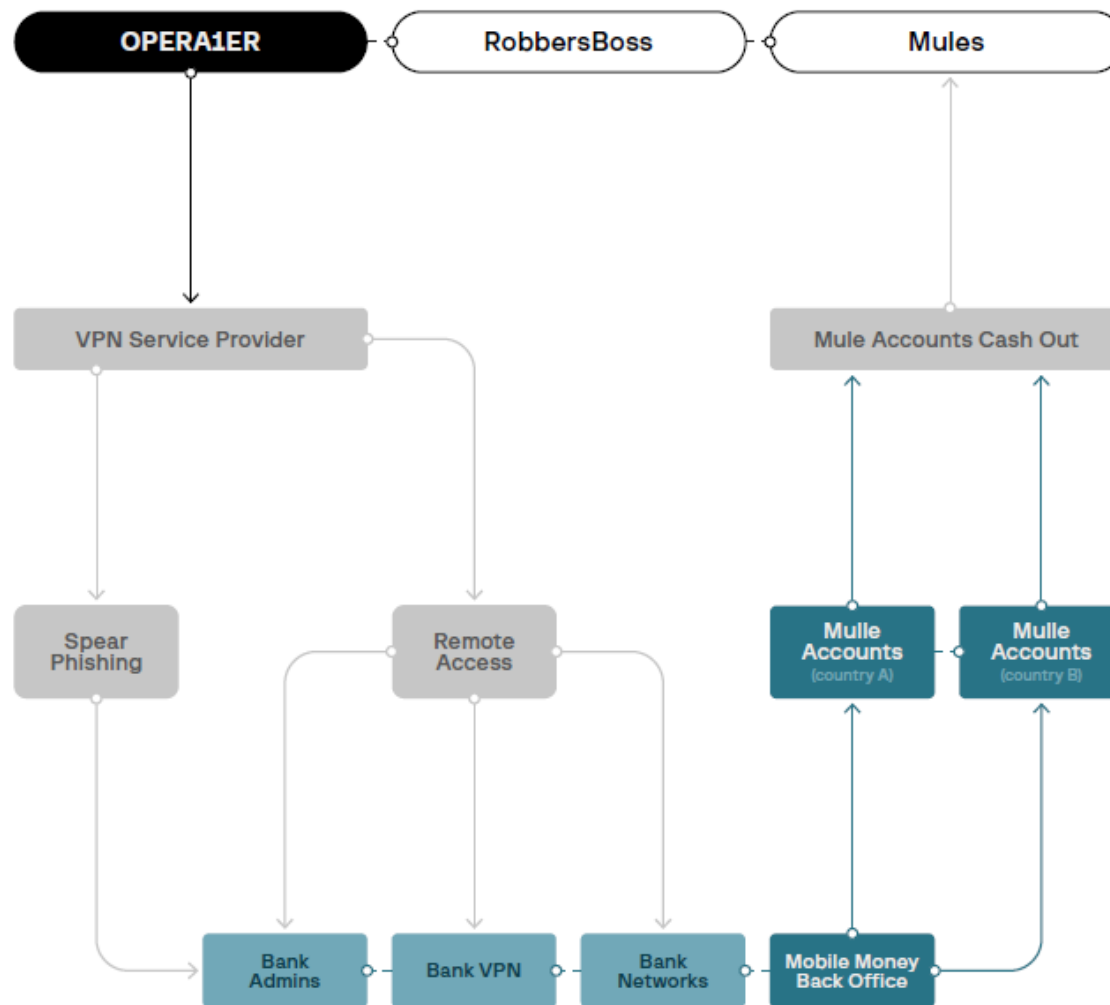
THREAT REPORT

OPERA1ER

Playing god without permission

KEY FINDINGS

Synopsis



GROUP-IB



THREAT REPORT

OPERA1ER

Playing god without permission

Highlights

30+ attacks attributed to OPERA1ER

\$30 million in estimated damages

15 countries where OPERA1ER struck

5 years of operation

Key findings

Name	OPERA1ER (aka DESKTOP-GROUP, Common Raven, NXSMS)
Motivation	Financial, exfiltration of documentation for further use in spear phishing
Targeted systems	Payment gateways, SWIFT messaging interface (presumably Alliance Access)
Activity	<ul style="list-style-type: none">• 2016 — present• The oldest domain registered to the group, helpdesk-security[.]org, was created in 2016.
Number of attacks	More than 30 successful attacks could have been carried out since 2019
Geography of attacks	Ivory Coast, Mali, Burkina Faso, Cameroon, Bangladesh, Gabon, Niger, Nigeria, Paraguay, Senegal, Sierra Leone, Uganda, Togo, Argentina.

GROUP-IB



THREAT REPORT

OPERA1ER

Playing god without permission

Highlights

30+ attacks attributed to OPERA1ER

\$30 million in estimated damages

15 countries where OPERA1ER struck

5 years of operation

Key findings

Name OPERA1ER (aka DESKTOP-GROUP, Common Raven, NXSMS)

Motivation Financial, exfiltration of documentation for further use in spear phishing

Victims Financial service, banks, mobile banking service, and telecom companies

Damages due to theft

- Confirmed: \$11 million since 2019.
- Approximate amount of theft is believed to be more than \$30 million.

Language

- Primary: French
- Their English is quite poor and so is their Russian.

Initial vector

- Spear phishing.
- Target list is created very precisely to attack a specific team in a targeted organization.

Time spent from initial access to impact From 3 to 12 months from initial intrusion to withdraw money from ATMs.

Take aways (or recipe “how I did it” 😊)

(e.g. for private company SOC / CERT / CTI teams & others)

- Block all malicious email attachments (as much as you can)
- Analyze malware samples from quarantined emails
- Track malware families and C2 infrastructure, correlate & cluster
- **Look at email headers for correlation as well**
- Share and collaborate with others (create own research group)
- **Find and name your own threat groups that matter most to you 😊**

Thanks for accepting my LT!!

- Twitter: @c_APT_ure
- Blog: <http://c-apt-ure.blogspot.com/>