

Botconf 2024 - 11th Edition

Nice, Côte d'Azur, France, 23rd (Workshops) and 24th to 26th (Main conference) April 2024

The Botnet & Malware Ecosystems Fighting Conference

DESKTOP-Group – The Saga continues

BOTCONF 2024 – LIGHTNING TALK

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

- Tom Ueltschi
- Swiss Post CERT / SOC / CSIRT since 2007 (*soon 17 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**)
- 2023 - **LT**: **DESKTOP-Group** or OPERA1ER
- 2024 - **CFP** rejected 😞 → **Lightning talk** again 😊

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»)
- 2023 – Key figure of **DESKTOP-Group** **arrested** in **INTERPOL** «Operation Nervone»

Suspected key figure of notorious cybercrime group arrested in joint operation

5 July 2023

5 July 2023

Home > News and Events > News > 2023 > Suspected key figure of notorious cybercrime group arrested in joint operation

Operation Nervone has dealt a significant blow to the OPERA1ER group.

ABIDJAN, Côte d'Ivoire – Over the last four years, a highly-organized criminal organization has targeted financial institutions and mobile banking services with malware, phishing campaigns and large-scale Business Email Compromise (BEC) scams.

Known as OPERA1ER, with aliases such as NX\$MS, **DESKTOP Group** and Common Raven, the group is believed to have stolen an estimated USD 11 million - potentially as much as 30 million - in more than 30 attacks across 15 countries in Africa, Asia and Latin America.

A detailed overview of [OPERA1ER's methods](#) was published by Group-IB and Orange S.A. in November 2022. Following extensive cooperation, INTERPOL, AFRIPOL, Group-IB and Côte d'Ivoire's Direction de l'Information et des Traces Technologiques (DITT) are announcing the arrest of a suspected senior member of the group, dealing a significant blow to their criminal activities.

— How it happened

The group's illicit e-mail campaigns were first detected by Group-IB in 2018, when they recognized spear phishing operations responsible for spreading malware such as remote access tools.

Under the auspices of Operation Nervone, INTERPOL's Cybercrime Directorate, Group-IB, and third-party stakeholder Orange exchanged intelligence which helped track the group's behaviours and identify a probable location for their activities.

Additional information was provided by the United States Secret Service's Criminal Investigative Division and Booz Allen Hamilton DarkLabs cybersecurity researchers, confirming a number of leads.

In early June, authorities in Côte d'Ivoire were able to arrest a key suspect linked to attacks against financial institutions across Africa.

ABIDJAN, Côte d'Ivoire
services with

Known as OP
11 million - po

A detailed overview
INTERPOL, A
suspected ser

According to the INTERPOL's 2022 African Cyberthreat Assessment Report, cybercrime is a growing threat in the West Africa region, with victims located worldwide. Operation NERVONE underscores INTERPOL's commitment to proactively combat the threat of cybercrime in the region.

Operation Nervone was backed by two key INTERPOL initiatives: the African Joint Operation against Cybercrime and the INTERPOL Support Programme for the African Union in relation to AFRIPOL, funded by the United Kingdom's Foreign, Commonwealth & Development Office and Germany's Federal Foreign Office, respectively.

The following is just some short analysis, why I assess that DESKTOP-group is again and still active after the arrest of a key figure from their group via INTERPOL Operation Nervone.

So far, at least the following 3 DDNS domains have been re-used in attacks that were previously used by DESKTOP-group since 2020.

2020-10-01_23	bestsuccess.ddns[.]net	79[.]134.225.95	AveMaria / WarZone RAT
2020-10-10_137	bestsuccess.ddns[.]net	185[.]174.40.142	AveMaria / WarZone RAT
2020-10-29_123	bestsuccess.ddns[.]net	153[.]92.126.202	AveMaria / WarZone RAT
2020-12-02_27	bestsuccess.ddns[.]net	80[.]85.159.33	AveMaria / WarZone RAT
2021-10-19_67	bestsuccess.ddns[.]net	185[.]118.167.229	AveMaria / WarZone RAT
2021-11-18_49	bestsuccess.ddns[.]net	185[.]118.167.229	AveMaria / WarZone RAT
2022-07-30_717	bestsuccess.ddns[.]net	80[.]85.153.132	Remcos RAT
2022-08-15_133	bestsuccess.ddns[.]net	80[.]85.153.132	Remcos RAT
2022-11-16_106	bestsuccess.ddns[.]net	197[.]210.54.233	AveMaria / WarZone RAT
2022-11-24_61	nightmare4666.ddns[.]net	91[.]192.100.57	AveMaria / WarZone RAT
2022-11-29_21	nightmare4666.ddns[.]net	64[.]188.23.167	AveMaria / WarZone RAT
2023-04-14_20	nightmare4666.ddns[.]net	45[.]88.67.63	AveMaria / WarZone RAT
2023-05-02_9	nightmare4666.ddns[.]net	45[.]88.67.63	AveMaria / WarZone RAT
2023-05-04_8	doneipacino.ddns[.]net	212[.]193.30.230	AveMaria / WarZone RAT
2023-05-14_611	nightmare4666.ddns[.]net	212[.]193.30.230	AveMaria / WarZone RAT
2023-05-16_40	nightmare4666.ddns[.]net	212[.]193.30.230	AveMaria / WarZone RAT

** 2023-06-?? INTERPOL Operation Nervone arrest in early June **

* .ddns.net domains (VT: 1st seen)

- bestsuccess (2020-09-10)
- nightmare** (2022-11-21)
- doneipacino (2023-04-03)

AveMaria / WarZone RAT

Remcos RAT

Operation Nervone has dealt a significant blow to the OPERA1ER group.

THE END ?? 😊

The following is just some short analysis, why I assess that DESKTOP key figure from their group via INTERPOL Operation Nervone.

So far, at least the following 3 DDNS domains have been re-used in the group since 2020.

2020-10-01_23	bestsuccess.ddns[.]net	79[.]134
2020-10-10_137	bestsuccess.ddns[.]net	185[.]17
2020-10-29_123	bestsuccess.ddns[.]net	153[.]92
2020-12-02_27	bestsuccess.ddns[.]net	80[.]85

bestsuccess	2023-10-08
nightmare**	2023-08-29
donelpacino	2023-10-20

2023-05-02_9	nightmare4666.ddns[.]net	45[.]88
2023-05-04_8	donelpacino.ddns[.]net	212[.]19
2023-05-14_611	nightmare4666.ddns[.]net	212[.]19
2023-05-16_40	nightmare4666.ddns[.]net	212[.]19

** 2023-06-?? INTER

LuminosityLink RAT
STRRAT (Java)
AsyncRAT

NOT
THE END ☹️

** 2023-06-?? INTERPOL Operation Nervone arrest in early June **

2023-07-26_14	donelpacino.ddns[.]net	79[.]110.49.161	Luminosity Link RAT
261b9cccbf347d864e683502e8679a4a	Order_23040.jar		
2023-07-26_26	donelpacino.ddns[.]net	79[.]110.49.161	Luminosity Link RAT
fcf09ec5a1f5629f31b7f74bddb5777a	july_order_23040.jar		
2023-08-08_14	donelpacino.ddns[.]net	2[.]59.254.111	STRRAT
30bb7390115b12a186b7669772988121	NETBANCO TRANSFER 3307281 EUR .jar		
mx1_116459271.eml			
2023-08-29_2	bestsuccess.ddns[.]net	197[.]210.84.253	STRRAT
2023-08-29_2	bestsuccess.ddns[.]net	80[.]85.153.248	STRRAT
2023-08-29_2	nightmare4666.ddns[.]net	80[.]85.153.248	STRRAT
1dc60148b29a6ac0e46ac10306b3b3db	BVNGEN61523 dt.24-7-23.jar		
mx1_118281019.eml			
2023-09-17_21	donelpacino.ddns[.]net	2[.]59.254.111	AsyncRAT
a4b2e852228b19f3db8c4bb7a40c3e5f	Notification of transfer made - Santander142023.rar		
460c5e2904724e5babe7c3f7eaaaf8de9	Notification of transfer made - Santander142023.exe		
mx1_120007793.eml			
2023-10-08_31	bestsuccess.ddns[.]net	95[.]214.27.6	AsyncRAT
19285861e301c85129ec1b5de17e0107	PW-23-003 TIEM2 Stainless Steel Tank (WWTP.tar		
34f632802a37841968d962af8fbb570b	PW-23-003 TIEM2 Stainless Steel Tank (WWTP.exe		
mx1_122331231.eml			
2023-10-20_608	donelpacino.ddns[.]net	95[.]214.27.6	AsyncRAT
81bac3d7181cra51c5196b665a121d73	DRAWINGS SPECS PRODUCTIONOCT19.tar.gz		
0a6b309ba8626654ad7c3a86eb12dd81	DRAWINGS SPECS PRODUCTIONOCT19.tar		
7f1d46d49965b7730f2eaccce9137992	DRAWINGS SPECS PRODUCTIONOCT19.exe		
mx1_123323013.eml			
2023-10-31_25	AgentTesla	"https://discord.com/api/webhooks/1150692736119361588/Rwbv7P9AYcg9eoTRXZ59ctAZJYpuoJGk2ChE0KxT-blNwa8HnnpS9UeliszrhNNN3Hpmp"	
1641104425ae2ee456edf0c3a17e9972	Notificacao de transferencia.zip		
bc6233fbc2fd08acef75d9f90cb54efc	Notificacao de transferencia.exe		
mx1_124304837.eml			



DESKTOP-Group research - correlation event (work in progress...)

Related Events [Show \(354 more\)](#)

Event ID	205312
UUID	d779bc29-0c4b-4a0f-8886-b486e7c6d668
Creator org	SwissPost
Protected Event (experimental)	Event is in unprotected mode.
Tags	DESKTOP-group tip:green
Date	2023-12-22
Threat Level	Medium
Analysis	Ongoing
Distribution	All communities
Published	Yes 2024-04-19 16:42:48
#Attributes	1216 (0 Objects)
First recorded change	2023-12-22 09:34:00
Last change	2024-04-19 16:42:11
Modification map	
Sightings	0 (0)
Correlation	Enabled (disable)

- Daily Incremental ThreatFox Import - 2024-04-20 (1)
- MalwareBazaar malware samples for 2024-04-19 (2)
- Remcos host indicators [2024-04-18] (1)
- MalwareBazaar malware samples for 2024-04-18 (1)
- Daily Incremental ThreatFox Import - 2024-04-17 (1)
- Remcos host indicators [2024-04-17] (1)
- MalwareBazaar malware samples for 2024-04-17 (1)
- [Malware/STRRAT] detectado desde comerciale@paltachnology.chile (1)
- Daily Incremental ThreatFox Import - 2024-04-15 (1)
- MalwareBazaar malware samples for 2024-04-08 (1)

Distribution All communities

#Attributes 1216 (0 Objects)

UUID: d779bc29-0c4b-4a0f-8886-b486e7c6d668



TomU | I'm still here... til the end 🇺🇸 🇨🇦

@c_APT_ure

I guess it's official now. Will be presenting my (still ongoing research) about "DESKTOP-group" at @Botconf

Thu 12/5 @ 9am seems like a tough spot 😞

botconf.eu/botconf-2019/s...

Still looking for collaboration on research
groups.google.com/d/forum/deskto...

If interested please apply

#BotConf

Thursday 05th December 2019

08:30 09:00

Welcome and registration

09:00 09:30

"DESKTOP-Group" – Tracking a Persistent Threat Group (using Email Headers)

Tom Ueltschi 🇺🇸

At BotConf 2019, I presented a lightning talk "Creating your own CTI in 5 minutes". This presentation is building on that capability to do semi-automated malware analysis based on a commercial sandbox solution. I will discuss a malware campaign analysis from a persistent threat actor (or group) over the past 18 months and still ongoing. The attacks are linked by email headers, targeting, and malware C&C infrastructure...

5:54 PM · Oct 1, 2019

https://twitter.com/c_APT_ure/status/1179062052150743040

Thanks for accepting my LT!!

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