

Phishing Email Investigation Methodology

1. Tools & Setup

- **Notepad++**
 - Open the email header in Notepad++.
 - For better formatting and readability:
 - Go to **Languages → YAML** → headers and fields will be highlighted.
 - This makes it easier to analyze fields during phishing investigations.
- **OSINT Tools**
 - VirusTotal
 - DomainTools
 - WHOIS lookups
 - Other open-source intelligence platforms

2. Methodology: “What to Look For”

When investigating phishing emails, focus on these **key fields**:

- **From:** Sender's display name and email address
- **To:** Recipient (sometimes “undisclosed-recipients”)
- **Subject:** Subject line of the email
- **Message-ID:** Unique identifier; the domain shows the mail service used
- **Date:** Timestamp of when the email was sent
- **Received:** Mail servers that processed the message (infrastructure clues)
- **Authentication-Results:** SPF, DKIM, DMARC results
- **Return-Path:** Often used to spot spoofing attempts

| **Note:** With more investigations, you'll refine and build your own methodology.

3. Step-by-Step Analysis (Case Example)

Header Analysis

- **From:** ERIKA JOHANNA LOPEZ <erikajohana.lopez@uptc.edu.co>

```
From: ERIKA JOHANNA LOPEZ VALIENTE <erikajohana.lopez@uptc.edu.co>
Date: Thu, 9 Dec 2022 09:58:26 +0100
Message-ID: <CABWu4iua5_uex6=G8pi_OJz1tBLJiNakMK-1=7128orpzxbKxw@mail.gmail.com>
Subject: COMMERCIAL PURCHASE RECEIPT ONLINE 27 NOV
To: undisclosed-recipients;
X-TM-Authentication-Results: spf=pass (sender IP address: 209.85.221.65)
```

- **To:** undisclosed-recipients (recipient hidden)
- **Subject:** COMMERCIAL PURCHASE RECEIPT ONLINE 27 NOV
- **Message-ID:** Ends with @mail.gmail.com → indicates Gmail delivery system
- **Date:** Thu, 9 Dec 2022 09:58:26 +0100

Received Field

- First receiving mail server domain: @fsfb.org.co
- OSINT can be used here to learn about attacker infrastructure.

Authentication-Results

- SPF → **Fail**
- DKIM → **Fail**
- DMARC → **Fail**
- Suggests spoofing or poor configuration.

```
Authentication-Results: spf=softfail (sender IP is 18.208.22.104)
smtp.mailfrom=uptc.edu.co; dkim=fail (no key for signature)
header.d=uptc.edu.co; dmarc=none action=none
header.from=uptc.edu.co; compauth=softpass reason=201
```

Return-Path

- `erikajohana.lopez@uptc.edu.co` (slightly different domain than From)
- Common tactic in phishing → mismatched Return-Path vs From.

4. Body Analysis

- Text: "COMMERCIAL PURCHASE RECEIPT" with reference to **625,000 pesos**.
- Hyperlink present:

```
http://107.175.247.199/loader/install.exe
```

- → Suspicious file download (likely malware).

5. Next Steps (OSINT & Threat Hunting)

- **Check the domain & IP** on **VirusTotal**
- Look for related phishing/malware campaigns
- Verify sender domains with WHOIS/DomainTools
- Map infrastructure (IP, domain, hosting provider)
- Document findings for reporting and defense

Using **VirusTotal** to scan the **domain** from the **Received** field, we can see that this domain was created **26 years ago**. While an **old domain** is generally less suspicious than a newly registered one, it does not automatically mean the email is legitimate, because attackers can compromise older domains for phishing campaigns. If the domain were **newly created**, it would be a strong indicator of potential phishing, prompting a deeper investigation. Additional checks are necessary to confirm the email's legitimacy.

0

/ 95

Community Score

At least 10 detected files embedding this domain

Reanalyze Similar More

fsfb.org.co

Registrar

.CO Internet S.A.S.

Creation Date

26 years ago

Last Analysis Date

17 days ago

top-1M

DETECTION

DETAILS

RELATIONS

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean

Further analysis of the **Authentication-Results** shows that the sender's **IP address** is **18.208.22.104**. VirusTotal indicates that this IP belongs to **Amazon AWS**, which is commonly used for hosting and email delivery. While the IP itself is not inherently malicious, attackers sometimes abuse cloud services like AWS to send phishing emails. Therefore, we should **not block the IP outright**, as it could disrupt legitimate traffic. Instead, this information serves as a **pivot point for investigation**, helping analysts identify potential abuse without affecting overall availability.

0

/ 95

Community Score

10+ detected files embedding this IP address

Reanalyze Similar More

18.208.22.104 (18.208.0.0/13)

US

Last Analysis Date

16 hours ago

AS 14618 (AMAZON-AES)

DETECTION

DETAILS

RELATIONS

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Lastly, we can analyze the **link in the body of the email** using **VirusTotal**. It is often helpful to first examine the **IP address** associated with the link before pasting the full URL. From the IP check, we can see that **9 out of 95 vendors** reported it as **malicious malware**, which already raises a red flag about the link's safety.

If you click on relations, you will get more information on the IP. There you will see the files communicating with that IP address under communicaing file whicgh resulted in 6 binaries.

9

/ 95

Community Score

-59

9/95 security vendors flagged this IP address as malicious

107.175.247.199 (107.175.240.0/21)

AS 36352 (AS-COLOCROSSING)

US

Last Analysis Date

1 day ago

DETECTION

DETAILS

RELATIONS

COMMUNITY 7

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis ⓘ

Do you want to automate checks?

alphaMountain.ai ⓘ	Malicious ⓘ	BitDefender ⓘ	Malware ⓘ
CyRadar ⓘ	Malicious ⓘ	Emsisoft ⓘ	Malware ⓘ
G-Data ⓘ	Malware ⓘ	Lionic ⓘ	Malicious ⓘ
SOCRadar ⓘ	Malware ⓘ	VIPRE ⓘ	Malware ⓘ
Webroot ⓘ	Malicious ⓘ	ESET ⓘ	Suspicious ⓘ

Checking the Details, you will see more information on that. Looking at Abuse.ch, it is quite interesting , more informations can be gotten from taht . click on teh URI of the Abuse.ch to get further analysis on taht .

Google results ⓘ

Ongeveer 7 resultaten (0.08 seconden)

Sorteren op: Relevance ▾

MalwareBazaar Database - Abuse.ch

bazaar.abuse.ch

25 okt 2022 107.175.247.199, 49704, 49707, 49708 AS-COLOCROSSINGUS United States C:\Users\user\AppData\...\Kjcrksvp.exe, PE32 dropped C:\Users ...

Cyber Defenders: PhishStrike Lab Write-up | by Justin Mangaoang

medium.com

7 nov 2024 ... Answer: **107.175.247.199**. 4. Determining which malware exploits system resources to mine cryptocurrencies helps prioritize threat response ...

URLhaus | bitrat - Abuse.ch

urlhaus.abuse.ch

Malware URLs ; 2022-11-05 20:53:05, http://141.98.6.69/bit.exe, Offline, bitrat - exe - benkow_ ; 2022-10-22 12:39:04, http://**107.175.247.199**/loader/install.exe ...

IP address information (107.175.0.0 - IP/Domain Lookup)

en.ntunhs.net

... **107.175.247.199** 107.175.247.200 107.175.247.201 107.175.247.202 107.175.247.203 107.175.247.204 107.175.247.205 107.175.247.206 107 175 247 207 107 175

Next, by pasting the **complete URL** `http://107.175.247.199/loader/install.exe` into VirusTotal, we find that **13 out of 98 vendors** flagged it as **malicious malware**. This confirms that the link is indeed dangerous and likely part of a phishing or

malware campaign, reinforcing the need for caution and further investigation before interacting with any content from this email.

13

/ 98

Community Score

-3

13/98 security vendors flagged this URL as malicious

Reanalyze Search More

http://107.175.247.199/loader/install.exe

107.175.247.199

ip

Last Analysis Date

1 day ago

DETECTION

DETAILS

COMMUNITY 7

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

alphaMountain.ai	Malicious	BitDefender	Malware
CyRadar	Malicious	Emsisoft	Malware
ESET	Malware	Fortinet	Malware
G-Data	Malware	Kaspersky	Malware
Lionic	Malicious	SOCradar	Malware

When analyzing the file in **VirusTotal**, clicking on the **Community** and **Details** sections provides additional insights. Under the **Details** tab, the **Google Results** indicate that the file is classified as **malware**. By following the link to **Abuse.ch**, we can confirm that this malware is tagged as **AsyncRAT** and **RAT**. Further research shows that **AsyncRAT** is a **Remote Access Trojan (RAT)** commonly used in cyberattacks to gain unauthorized control of compromised systems.

Google results

Ongeveer 7 resultaten (0.08 seconden)

Sorteren op: Relevance

MalwareBazaar Database - Abuse.ch

bazaar.abuse.ch

25 okt 2022 107.175.247.199, 49704, 49707, 49708 AS-COLOCROSSINGUS United States C:\Users\user\AppData\...\Kjcrksvp.exe, PE32 dropped C:\Users\ ...

Cyber Defenders: PhishStrike Lab Write-up | by Justin Mangaoang

medium.com

7 nov 2024 ... Answer: **107.175.247.199**. 4. Determining which malware exploits system resources to mine cryptocurrencies helps prioritize threat response ...

URLhaus | bitrat - Abuse.ch

urlhaus.abuse.ch

Malware URLs ; 2022-11-05 20:53:05, http://141.98.6.69/bit.exe, Offline, bitrat - - exe - benkow_ ; 2022-10-22 12:39:04, http://**107.175.247.199**/loader/install.exe ...

IP address information (107.175.0.0 - IP/Domain Lookup)

en.ntunhs.net

... **107.175.247.199** 107.175.247.200 107.175.247.201 107.175.247.202 107.175.247.203 107.175.247.204 107.175.247.205 107.175.247.206 107.175.247.207 107.175 ...

MALWAREbazaar

from ABUSE^{ch} | SPAMHAUS

🔍 Browse

📁 Upload

🔔 Hunting Alerts

📄 Access Data

🔗 FAQ


🏠 About


👤 Login

MalwareBazaar Database

You are currently viewing the MalwareBazaar entry for **SHA256 5ca468704e7ccb8e1b37c0f7595c54df4e2f4035345b6e442e8bd4e11c58f791**. While MalwareBazaar tries to identify whether the sample provided is malicious or not, there is no guarantee that a sample in MalwareBazaar is malicious.

Database Entry


AsyncRAT


Vendor detections: **11**

Intelligence **11**

IOCs


YARA **2**

File information

Comments

Actions

SHA256 hash:

 5ca468704e7ccb8e1b37c0f7595c54df4e2f4035345b6e442e8bd4e11c58f791

If we take the **file hash** and paste it into VirusTotal, we see that **53 out of 72 vendors** have flagged it as a **Trojan**. Additional open-source searches confirm that **AsyncRAT** is indeed a **remote access tool** used by attackers for persistent access, surveillance, and data exfiltration.

53 / 72

Community Score

🔔 53/72 security vendors flagged this file as malicious

🔄 Reanalyze


🔍 Similar

⋮ More

5ca468704e7ccb8e1b37c0f7595c54df4e2f4035345b6e442e8bd4e11c58f791

Size
193.00 KB

Last Analysis Date
1 month ago



install.exe

peexe

runtime-modules

shellcode

malware

direct-cpu-clock-access

detect-debug-environment

checks-network-adapters

assembly

spreader

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY **8**

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label **trojan.msil/scarsi**

Threat categories

trojan

downloader

Family labels

msil

scarsi

fdnj

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	🔔 Trojan.Win.Injection.C5286536	Alibaba	🔔 Trojan:MSIL/Scarsi.9840cdec
AliCloud	🔔 Trojan[downloader]:MSIL/Scarsi.gyf	ALYac	🔔 IL:Trojan.MSIL.Zilla.23569
Arcabit	🔔 IL:Trojan.MSIL.Zilla.D5C11	Arctic Wolf	🔔 Unsafe
Avast	🔔 Win32:MalwareX-gen [Drp]	AVG	🔔 Win32:MalwareX-gen [Drp]

Looking at the **Community section** in VirusTotal, we can also see various comments and shared reports from other analysts. In particular, highlighting the **HTML analysis report** gives us a deeper look into the malware's behavior. For instance, under the **Process Tree**, we find suspicious command-line activity. Decoding the embedded **Base64 command** using **CyberChef** reveals that the malware forces the system to **start, then sleep for 5 seconds**—a technique often used to evade detection.

[Products](#)
[Solutions](#)
[Platform](#)
[Services](#)
[Resources](#)
[Partners](#)
[About Us](#)

[Cyber Hub](#) / [Secure Users & Access](#) / [What is Malware?](#) / AsyncRAT Malware Explained: Remote Access Trojan Used in Cyberattacks

[Contact](#)

AsyncRAT Malware Explained: Remote Access Trojan Used in Cyberattacks

AsyncRAT is a family of malware commonly used in cyberattacks as a Remote Access Trojan (RAT), providing remote control to a victim's system. Once AsyncRAT malware infiltrates a system, attackers covertly execute commands, exfiltrate sensitive data, or monitor user activity in the background.

A sophisticated strain of malware that can be customized for different campaigns, AsyncRAT poses a significant threat. By acting stealthily and not immediately revealing its presence, AsyncRAT detection often poses more challenges compared to traditional malware.

Organizations require robust security measures to protect themselves against AsyncRAT malware and similar remote access trojan threats.

Cyber Security Report

[Cyber Hub](#) / [Secure Users & Access](#) / What is Remote Access Trojan (RAT)?

[Contact](#)

What is Remote Access Trojan (RAT)?

Remote access trojans (RATs) are malware designed to allow an attacker to remotely control an infected computer. Once the RAT is running on a compromised system, the attacker can send commands to it and receive data back in response.

2022 Security Report

Demo Endpoint RAT Protection

Continuing with the HTML report, we also observe evidence of **persistence and installation behavior**. Specifically, under the **Boot Survival** section, the malware is seen creating a **registry key**, which allows it to survive system reboots and maintain long-term access.

joesecurity
 2 years ago

Joe Sandbox Analysis:

Verdict: MAL

Score: 100/100

Domains: ripleystudio

Hosts: 192.168.2.1 107.175.247.199

HTML Report: <https://www.joesandbox.com/analysis/730122/0/html>

PDF Report: <https://www.joesandbox.com/analysis/730122/0/pdf>

[Show more](#)

The **HTML report** provides additional details confirming that the file is indeed **malware**. This section of the analysis is especially valuable for understanding the malware's behavior and execution flow.

[←](#)
[→](#)
[joesandbox.com/analysis/730122/0/html](#)

[Google](#)
[Gmail](#)
[YouTube](#)
[Maps](#)
[Adobe Acrobat](#)
[ChatGPT](#)
[are being - Google...](#)
[Funcieomschrijving](#)
[Support ULB - Supp...](#)
[Management of Dat...](#)
[LANG-8-906_C.156...](#)

[☆](#)
[📁](#)
[🔍](#)

[Overview](#)
[Signatures](#)
[Process Tree](#)
[Domains / IPs](#)
[Dropped](#)
[Static](#)
[Network](#)
[Stats](#)
[Behavior](#)
[Disassembly](#)

D41tYapPDR.exe

Overview

General Information

Sample Name:	D41tYapPDR.exe
Analysis ID:	730122
MD5:	34793c6520dcf3c6...
SHA1:	200417a239bb0ac8...
SHA256:	5ca468704e7ccb8e...
Tags:	AsyncRAT exe RAT
Infos:	📁 📄 🔍 📡 📶 📶

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for submitted file
- Malicious sample detected (through com...)
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropped file
- Snort IDS alert for network traffic
- Yara detected Costura Assembly Loader
- Encrypted powershell cmdline option found
- Machine Learning detection for sample
- .NET source code contains potential unpa...
- Injects a PE file into a foreign processes
- Machine Learning detection for dropped file
- Uses 32bit PE files

Classification

Analyzing further on the HTML Report, under Process Tree, we can see the following. Copy and paste the base 64 command line on "CyberChef" to see what it does.

```
Process Tree

  • System is w10x64
  • D411YapPDr.exe (PID: 5568 cmdline: "C:\Users\user\Desktop\D411YapPDr.exe MD5: 34793C6520DCF3C6130DC031FA640C71")
    • powershell.exe (PID: 2216 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcbB0AC0AUwBsAGUAZQBwACAAALQBTAGUAYwBvAG4AZABzACAAANQAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      • conhost.exe (PID: 4692 cmdline: "C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782EBB4D7C7C3BBFB844496)
    • D411YapPDr.exe (PID: 6132 cmdline: "C:\Users\user\Desktop\D411YapPDr.exe MD5: 34793C6520DCF3C6130DC031FA640C71")
      • D411YapPDr.exe (PID: 1632 cmdline: "C:\Users\user\Desktop\D411YapPDr.exe MD5: 34793C6520DCF3C6130DC031FA640C71")
      • D411YapPDr.exe (PID: 6060 cmdline: "C:\Users\user\Desktop\D411YapPDr.exe MD5: 34793C6520DCF3C6130DC031FA640C71")
  • Kjrksvp.exe (PID: 5204 cmdline: "C:\Users\user\AppData\Roaming\Vlevqbxxsx\Kjrksvp.exe" MD5: 34793C6520DCF3C6130DC031FA640C71")
  • Kjrksvp.exe (PID: 3236 cmdline: "C:\Users\user\AppData\Roaming\Vlevqbxxsx\Kjrksvp.exe" MD5: 34793C6520DCF3C6130DC031FA640C71")
  • cleanup
```

Looking deeper into the **Process Tree** within the HTML report, we can identify a suspicious **Base64-encoded command line**. By copying and pasting this into **CyberChef** for decoding, we discover that the command instructs the system to **start and then sleep for 5 seconds**. This type of behavior is a common **evasion technique**, allowing the malware to delay execution and avoid immediate detection by security tools.

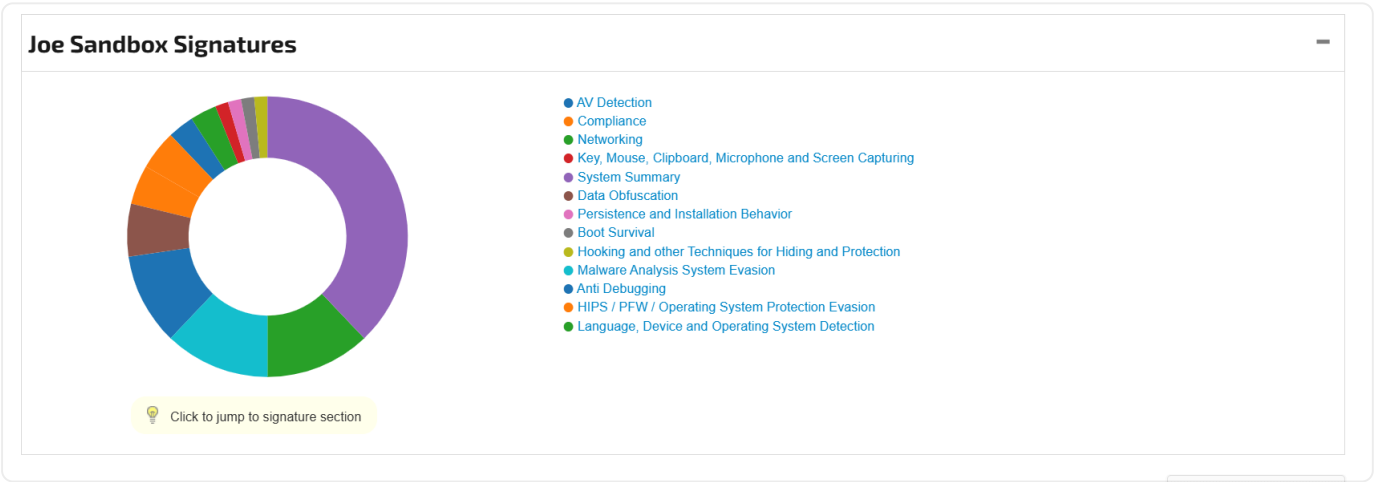
Download CyberChef
Last build: 3 years ago
Options
About / Support

Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression

Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars

Input
length: 62
lines: 1
UmB0AGEAcgB0AC0AUmBSAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAAwAA
Output
time: 0ms
length: 46
lines: 1
S.t.a.r.t.-.S.l.e.e.p.-.S.e.c.o.n.d.s.-.5.0.

Still within the HTML report, we find evidence of the malware’s **persistence and installation mechanisms**. Specifically, under the **Boot Survival** section, the report shows that the malware creates a **registry key**, which enables it to survive reboots and maintain a long-term presence on the compromised system. Following the provided link gives even more technical details about these persistence techniques.



Persistence and Installation Behavior		
Drops PE files		
Source: C:\Users\user\Desktop\ID41tYapP Dr.exe	File created: C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9QTQHWWN\server[1].exe	Jump to dropped file
Source: C:\Users\user\Desktop\ID41tYapP Dr.exe	File created: C:\Users\user\AppData\Roaming\Ilevqbxxsx\Kjcrksvp.exe	Jump to dropped file
Boot Survival		
Creates an autostart registry key		
Source: C:\Users\user\Desktop\ID41tYapP Dr.exe	Registry value created or modified: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run Kjcrksvp	Jump to behavior
Source: C:\Users\user\Desktop\ID41tYapP Dr.exe	Registry value created or modified: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run Kjcrksvp	Jump to behavior
Hooking and other Techniques for Hiding and Protection		
Disables application error messages (SetErrorMode)		
Malware Analysis System Evasion		