

**CENTRE FOR DEVELOPMENT OF ADVANCED
COMPUTING (C-DAC), THIRUVANANTHAPURAM,
KERALA**

A PROJECT REPORT ON

“Phishing Email Analysis”

SUBMITTED TOWARDS THE



PG-DCSF AUG 2024

BY

Group Number – 07

**Mohd Hamza Kazi
Swayam Gundawar
Aditi Dixit
Roshan Mungane
Shelly Pant**

**PRN: 240860940022
PRN: 240860940049
PRN: 240860940016
PRN: 240860940038
PRN: 240860940043**

Under The Guidance Of

Mr .Sreedeeep A L

CONTENTS

- 1. Abstract**
- 2. Introduction**
 - 2.1 Overview of Phishing Attacks
 - 2.2 Importance of Email Header Analysis
 - 2.3 Role of Social Engineering in Phishing
 - 2.4 Impact of Malicious Attachments
- 3. System Requirements**
 - 3.1 Hardware Requirements
 - 3.2 Software Requirements
- 4. Cyber Forensics Procedure: Phishing Email Analysis**
 - 4.1 Investigation Process
 - 4.2 Email Header Analysis
 - 4.3 Social Engineering Techniques Used
 - 4.4 Malicious Attachment Analysis
- 5. Conclusion**
- 6. Screenshots and References**
 - 6.1 Email Header Analysis Screenshots
 - 6.2 Social Engineering Techniques Screenshots
 - 6.3 Malicious Attachment Analysis Screenshots
 - 6.4 Malware Execution and Network Traffic Screenshots
 - 6.5 Additional File Hash Analysis

Abstract

Phishing is a deceptive cyber-attack technique that exploits human psychology to trick individuals into revealing sensitive information, such as login credentials, financial data, or personal details. Cyber criminals often use phishing emails that appear to come from trusted sources, manipulating recipients into clicking malicious links or downloading harmful attachments. This report focuses on the detailed analysis of phishing emails, particularly examining email headers, identifying social engineering tactics, and investigating attached malicious files.

Email header analysis plays a crucial role in phishing investigations, as it provides insight into the email's origin, mail server, sender authentication, and potential spoofing techniques. Through email header forensics, key indicators such as the return path, mail relay servers, and client IP addresses can be examined to verify the legitimacy of the email sender. In this analysis, we identify an email that claims to be from a well-known brand but is, in reality, a phishing attempt. By scrutinizing the header information, we detect inconsistencies in sender domains, mail server usage, and IP address reputation, confirming the fraudulent nature of the email.

Furthermore, this report explores the social engineering tactics used by attackers to manipulate victims into engaging with the phishing email. Common techniques include urgency-based messages (e.g., "Offer valid for the next 24 hours!"), financial incentives (e.g., "Get a 50% discount now!"), and misleading calls to action (e.g., "Download the attached file for more details"). These tactics create psychological pressure, increasing the likelihood that a recipient will fall victim to the attack.

Beyond header analysis, this investigation also involves inspecting the malicious attachment contained in the phishing email. The email in question includes a .zip file that, when extracted, reveals a macro-enabled Excel file (.xlsm). This attachment exploits a known vulnerability, CVE-2017-11882, which allows attackers to execute arbitrary code on the victim's machine. Further network traffic analysis reveals that upon execution, the malicious file attempts to establish contact with external domains, subsequently downloading additional payloads that could compromise system security.

The findings of this report emphasize the significance of email security awareness, email filtering solutions, and proactive threat detection measures. By identifying the key indicators of phishing and understanding the methodologies employed by attackers, individuals and organizations can better protect themselves against such threats. This research highlights the importance of technical analysis and security tools, such as sandbox environments and malware detection platforms, in mitigating phishing risks. Ultimately, the goal of this study is to enhance cybersecurity defenses by educating users on the detection and prevention of phishing-based attacks.

2. Introduction

Phishing attacks have emerged as one of the most prevalent cybersecurity threats, targeting individuals, businesses, and government institutions worldwide. These attacks use deceptive techniques to trick recipients into revealing sensitive data, such as usernames, passwords, financial information, and even confidential business data. A significant portion of cyber incidents can be attributed to phishing emails, which often serve as the initial vector for more advanced attacks like ransomware, credential theft, and financial fraud.

Phishing emails often impersonate legitimate organizations by forging sender details and using professional branding, making it difficult for users to distinguish between genuine and malicious emails. Attackers take advantage of well-known domains and email servers to bypass security filters. By analyzing email headers, we can identify inconsistencies in sender authentication, such as discrepancies in return paths, mismatched mail servers, and suspicious originating IP addresses.

Another crucial aspect of phishing attacks is the delivery of malicious attachments or links leading to compromised websites. In this case, the phishing email analyzed in this report contains an attachment—a compressed .zip file—that, when extracted, reveals a macro-enabled Excel file (.xlsm). This file exploits the CVE-2017-11882 vulnerability, allowing attackers to execute arbitrary code on the victim's system. Further network analysis shows that the file contacts known malicious domains, downloading additional malware payloads to compromise the system.

2.1 Overview of Phishing Attacks

Phishing attacks deceive victims by impersonating trusted entities to steal sensitive data. These attacks use fraudulent emails with malicious links or attachments, often employing spoofing and social engineering to appear legitimate. Recognizing phishing tactics is essential for cybersecurity defense.

2.2 Importance of Email Header Analysis

Email headers provide crucial metadata, such as return paths, mail servers, and IP addresses, to verify an email's authenticity. Discrepancies in these details can reveal spoofing attempts. Authentication checks like SPF, DKIM, and DMARC help detect fraudulent emails before they cause harm.

2.3 Role of Social Engineering in Phishing

Social engineering manipulates victims using urgency, financial incentives, and misleading calls to action. Tactics like “Limited time offer!” or “Verify your account now” pressure recipients into engaging with phishing emails, increasing the likelihood of a successful attack.

2.4 Impact of Malicious Attachments

Phishing emails often contain malicious attachments that exploit system vulnerabilities. In this case, a .xlsm file used CVE-2017-11882 to execute code and download malware. Sandboxing and endpoint security tools help mitigate such threats.

3 System Requirements

Phishing email analysis requires specific hardware and software tools to safely investigate, analyze, and mitigate threats without risking system compromise. Below are the necessary hardware and software requirements for conducting this analysis effectively.

3.1 Hardware Requirements

To conduct a comprehensive phishing email analysis, the following hardware specifications are recommended:

- **Processor:** Intel Core i5 (10th Gen or higher) or AMD Ryzen 5 (or higher)
- **RAM:** Minimum 8GB (16GB recommended for handling virtual machines and network analysis tools)
- **Storage:** At least 250GB SSD (for faster data processing and storage of forensic evidence)
- **Internet Connection:** Required for researching domain reputations, IP addresses, and interacting with security tools
- **Dedicated Virtual Machine (VM) Environment:** A separate, isolated environment to execute and analyze potentially malicious files safely

3.2 Software Requirements

Analyzing phishing emails requires a combination of forensic tools, network analyzers, and security platforms. Below are the essential software components:

Email Analysis Tools:

- **Mozilla Thunderbird / Outlook / Gmail Web Interface:** For viewing and extracting email headers
- **Notepad / Sublime Text / VS Code:** To open and analyze email header files in plaintext format
- **MXToolbox / Email Header Analyzer:** Online tools for checking email server authenticity and identifying spoofed senders

Security and Malware Analysis Tools:

- **VirusTotal / Hybrid Analysis / Any.Run:** Platforms for scanning suspicious files and URLs for known threats
- **Wireshark:** A network protocol analyzer to inspect traffic generated by suspicious attachments
- **Burp Suite:** For capturing and analyzing HTTP requests from phishing emails and their attachments
- **CyberChef:** A tool for decoding and analyzing obfuscated email content

Virtualization and Sandbox Environments:

- **VMware Workstation / VirtualBox:** To create an isolated testing environment for analyzing malicious attachments
- **Windows Sandbox:** A lightweight virtual environment for safe execution of potentially harmful files
- **Cuckoo Sandbox:** An automated malware analysis system to examine file behavior in a controlled environment

Additional Security Measures:

- **FireEye / Palo Alto WildFire / CrowdStrike Falcon:** Advanced threat intelligence solutions for identifying sophisticated phishing campaigns
- **OSINT Framework:** Open-source intelligence tools for gathering information on suspicious domains, IPs, and phishing actors

Having the right hardware and software setup ensures that phishing email analysis can be conducted in a safe, controlled, and effective manner. By leveraging these tools, cybersecurity professionals can dissect phishing attempts, extract meaningful forensic evidence, and develop countermeasures to prevent future attacks.

4. Cyber Forensics Procedure: Phishing Email Analysis Overview

This report documents the forensic analysis of a suspected phishing email claiming to offer an “Exclusive Nike Offer.” The objective is to identify indicators of compromise, social engineering techniques, and potential malicious payloads. The findings confirm that this email is indeed a phishing attempt.

4 Investigation Process

4.1 Email Header Analysis

1. The phishing email was opened in **Notepad** to analyze the raw email headers.
2. As seen in **1.png**, the recipient of the email is hamzz2002i@gmail.com.
3. The sender domain appears to be google.com, and the mail server used is mx.google.com.
4. The Return-Path in the email header shows nikestorenew221@gmail.com, which is suspicious because it does not belong to a legitimate Nike SMTP address.
5. The client IP address (209.85.220.41) was extracted from the headers.
6. By cross-referencing **2.png** and **3.png**, we verified that this IP belongs to Google's infrastructure.

```
Delivered-To: hamzz2002i@gmail.com
Received: by 2002:a17:906:2c55:b0:ab6:efaa:2c8a with SMTP id f21csp129545ejh;
Mon, 10 Feb 2025 22:15:11 -0800 (PST)
X-Received: by 2002:a17:90b:4a4c:b0:2ee:d024:e4e2 with SMTP id 98e67ed59e1d1-2fa23f55e19mr25704349a91.7.1739254511206;
Mon, 10 Feb 2025 22:15:11 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1739254511; cv=none;
d=google.com; s=arc-20240605;
b=LzqM1y0ndPlptBPx8wUoCu1x85774o10E7Q3RyuksnDvH8YYSwb9nXJ20AKafxw0
hdyVjhaos7m1SrV08BYz+1CDunq5Wk+b4+SmUUVrhdQfCh79buireVZHwutCFmrO0/
sm4rm3oa70iY02HDKp2DvJ9M3eEsrf4eX29KsvyD882JII2kYHOGq+nOuZbR3IA8qJafM
fm17u8F5awwyNVv1dquJFNDZ7rw/0471CfbYH75qa/HUWf11cUfKuxtsGT03bGM4kds
eHQ1w09ppYAGT54aIZU0mR0FOEL5FV1s3YmW5vP/2qxlLu0V13dTIue5Sohm818Lhp
D3lw==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605;
h=to:subject:message-id:date:from:mime-version:dkim-signature;
bh=kj0nvJDsXkzyQINzrEH0Z5daN+df1scdk7TgEYZ8DKU=;
fh=w/UjClzr+R600UQfj0YotduUdFnlK9mag1J7s4=;
b-Dypmkt6zFrGj0xhJpL9HmMcudQ9B/LC3UE/fzY7Eg+y+iz4jBdiQ/8ma6IorUt
SVgrctLVK3tHhfbtkCSMhp7+ys0ggt37Q360KY8I7hC613tFvziPo5W0/L/r6aR8
jP80gsehtnHef+XBLA16EsyPoAF9VJNjreVZi6jyJUC+D49YK4X9lQWRF0czS3a3pb3
szVdvVvC8RwAnqsG4SXJNPkxb05d5q3XRC0n9CQ500wF05CvY19NjQxCLDB24LwFQZ
Bq4U3PE/nxwnK9kVwQ0w6w1XLCQihJnuclHrjv9vct3UqvH9nKSDt8fclLwCRGZfQq
S0IA==;
d=google.com
ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@gmail.com header.s=20230601 header.b="Nh3b0ZF/";
spf=pass (google.com: domain of nikestorenew221@gmail.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=nikestorenew221@gmail.com;
dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com;
Return-Path: nikestorenew221@gmail.com
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
by mx.google.com with SMTPS id 98e67ed59e1d1-2fa1e59eeSes0r7355741a91.0.2025.02.10.22.15.11
for <hamzz2002i@gmail.com>
(Google Transport Security);
Mon, 10 Feb 2025 22:15:11 -0800 (PST)
Received-SPF: pass (google.com: domain of nikestorenew221@gmail.com designates 209.85.220.41 as permitted sender) client-ip=209.85.220.41;
Authentication-Results: mx.google.com;
dkim=pass header.i=@gmail.com header.s=20230601 header.b="Nh3b0ZF/";
spf=pass (google.com: domain of nikestorenew221@gmail.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=nikestorenew221@gmail.com;
dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com;
d=google.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=gmail.com; s=20230601; t=1739254510; x=1739859310; dara=google.com;
```

1.png

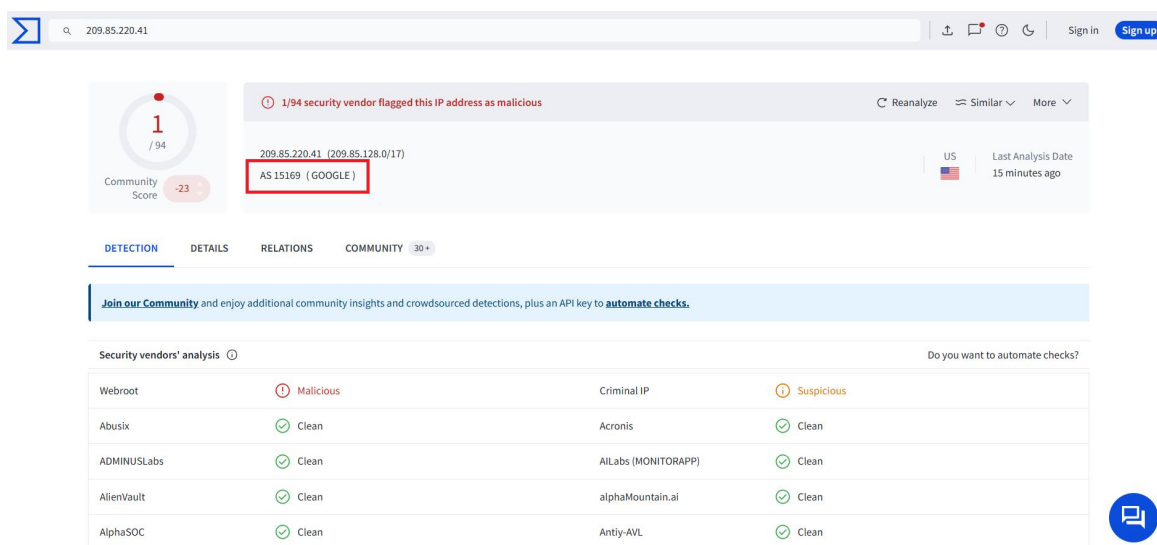
```
(letsdefend@kali)-[~]
$ whois 209.85.220.41

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#

NetRange:      209.85.128.0 - 209.85.255.255
CIDR:          209.85.128.0/17
NetName:       GOOGLE
NetHandle:     NET-209-85-128-0-1
Parent:        NET209 (NET-209-0-0-0-0)
NetType:       Direct Allocation
OriginAS:
Organization:  Google LLC (GOGL)
RegDate:      2006-01-13
Updated:       2012-02-24
Ref:           https://rdap.arin.net/registry/ip/209.85.128.0

OrgName:       Google LLC
OrgId:         GOGL
Address:       1600 Amphitheatre Parkway
City:          Mountain View
StateProv:     CA
PostalCode:    94043
Country:       US
```

2.png



209.85.220.41

1 / 94
Community Score -23

1/94 security vendor flagged this IP address as malicious

209.85.220.41 (209.85.128.0/17)
AS 15169 (GOOGLE)

US Last Analysis Date 15 minutes ago

DETECTION DETAILS RELATIONS COMMUNITY 30

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

Security vendors' analysis

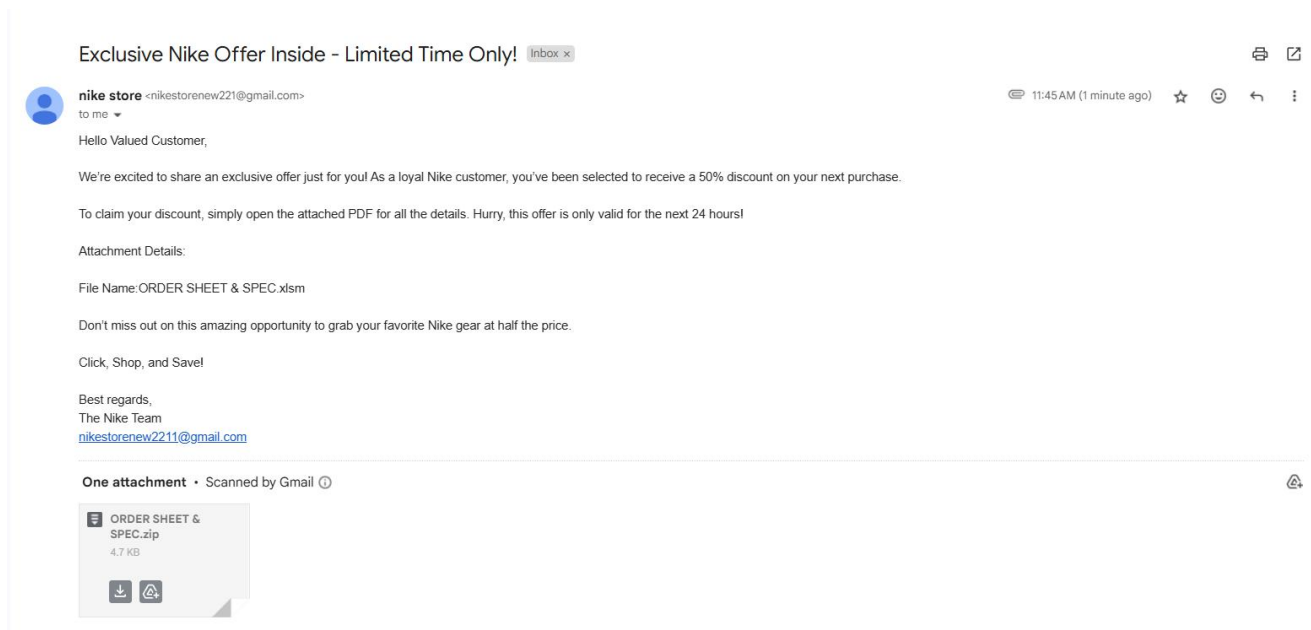
Vendor	Analysis	Vendor	Analysis
Webroot	Malicious	Criminal IP	Suspicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean
AlphaSOC	Clean	Antiy-AVL	Clean

3.png

4.2 Social Engineering Techniques Used

Attackers use various psychological tricks to manipulate victims into opening phishing emails. This email employs the following tactics:

- **Urgency:** "Only valid for the next 24 hours!" (Creates a sense of pressure to act quickly.)
- **Reward:** "50% discount on your next purchase!" (Too good to be true offer to lure victims.)
- **Call to Action:** "Simply open the attached file." (Encourages interaction with a potentially malicious attachment.)
- **Lack of Personalization:** The email does not address the recipient by name but instead uses generic terms like "Valued Customer," which is common in phishing attempts.



4.Png

4.3 Malicious Attachment Analysis

1. The phishing email contained a .zip file, which was downloaded in a **sandboxed environment** to prevent system compromise.
2. After extracting, the file inside was an .xlsm (macro-enabled Excel file), a common format used for malware delivery.
3. As shown in 5.png, security analysis flagged the file as **malicious**.
4. 6.png confirms that the malware exploits **CVE-2017-11882**, a vulnerability that allows attackers to execute arbitrary code on a victim's machine. According to [Microsoft's security advisory](#), this vulnerability affects Microsoft Office, allowing remote code execution via memory corruption.
5. Upon execution, as seen in 7.png, the file attempts to establish external connections to:
 - ocs[.]pki[.]goog
 - multiwaretecnologia[.]com[.]br/js/Podaliri4.exe
6. This external domain downloads **Podaliri4.exe**, a further malicious payload designed to infect the victim's system.
7. As seen in 8.png, the final malware payload is flagged as **malicious** by security tools.
8. Additional analysis of the file hash on an online malware scanning service (e.g., VirusTotal) provides further confirmation.

7bcd31bd41686c32663c7cabf42b18c50399e3b3b4533fc2ff002d9f2e058813

46

Community Score

46/64 security vendors flagged this file as malicious

Reanalyze

Similar

More

7bcd31bd41686c32663c7cabf42b18c50399e3b3b4533fc2ff002d9f2e058813

Size2.66 MB

Last Analysis Date14 hours ago

ORDER SHEET & SPEC.xlsm

xlsm

run-file

exe-pattern

auto-open

executes-dropped-file

run-dll

open-file

write-file

checks-user-input

clipboard

detect-debug-environment

macro-run-file

exploit

long-sleeps

cve-2017-11882

macros

calls-wmi

DETECTION

DETAILS

RELATIONS

ASSOCIATIONS

BEHAVIOR

COMMUNITY13

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

Code insights

This macro exhibits several behaviors commonly associated with malicious intent:

1. Obfuscation:

* The code uses heavily obfuscated variable and function names, making it difficult to understand its true purpose.

Show more

Crowdsourced AI

Hispacec flags this file as malicious

The macros extracted from the document exhibit several signs of malicious intent, as outlined below:

Show more

Popular threat labelTrojan:acao/valyria

Threat categoriestrojan dropper downloader

Family Labelsacao valyria

5.png

AhnLab-V3	OLE/Cve-2017-11882.Gen	Alibaba	Exploit:VBS/CVE-2017-11882.a04c840d
AliCloud	Exploit:Win/CVE-2017-11882.VM	ALYac	VB:Trojan.Valyria.5296
Antiy-AVL	Trojan[Downloader]/MSOffice.Agent.buv	Arcabit	Trojan.Generic.D2296136
Avast	VBA: Dropper-AN [Trj]	AVG	VBA: Dropper-AN [Trj]
Avira (no cloud)	VBS/Dldr.Agent.VPNI	Baidu	Archive.Bomb
BitDefender	Trojan.GenericKD.36266294	Bkav Pro	Darksnow.A.Macro
ClamAV	Xls.DropperValyria-10030821-0	CTX	Xlsx.trojan_generic
Cynet	Malicious (score: 99)	DrWeb	Exploit.Siggen3.15297
Elastic	Malicious (high Confidence)	Emsisoft	Trojan.GenericKD.36266294 (B)
eScan	Trojan.GenericKD.36266294	ESET-NOD32	VBS/TrojanDownloader.Agent.UMT
Fortinet	VBA/CoinMiner.ACAOItr	GData	Trojan.GenericKD.36266294
Huorong	HEUR:OMacro/Obfuscated.c	Ikarus	Trojan.JS.Runner
Kaspersky	HEUR:Trojan-Dropper.Script.Generic	Kingsoft	Script.Trojan-Dropper.Generic.a
Lionic	Trojan.MSExcel.Generic.blc	Microsoft	Exploit-O97M/CVE-2017-11882.VA
NANO-Antivirus	Trojan.Script.ExpKit.fbenub	QuickHeal	OLE.APT.42097
Rising	Trojan.Obfus/VBAI1.10468 (CLASSIC)	Sangfor Engine Zero	Exploit.Doc.CVE-2017-11882.b

6.png

Contacted URLs (2)

Scanned	Detections	Status	URL
2024-12-09	0 / 96	200	http://ocsp.pki.goog
2024-12-07	10 / 96	403	/gsr2/ME4wTDBKMEgwRjAJBgUrDgMCGGUABBTgXIsxbvr2lBkPpolEVRE6gHlCnAQUm+IHV2ccHsBqBt5ZtJot39wZhi4CDQHjtJqhYqpgSVpULg=
			https://multiwaretecnologia.com.br/js/Podaliri4.exe

Contacted Domains (17)

Domain	Detections	Created	Registrar
12.179.89.13.in-addr.arpa	0 / 94	-	-
20.173.189.20.in-addr.arpa	0 / 94	-	-
202.64.54.20.in-addr.arpa	0 / 94	-	-
21.173.189.20.in-addr.arpa	0 / 94	-	-
212.143.182.52.in-addr.arpa	0 / 94	-	-
22.173.189.20.in-addr.arpa	0 / 94	-	-
29.73.42.20.in-addr.arpa	0 / 94	-	-
42.86.98.104.in-addr.arpa	1 / 94	-	-
94.16.208.104.in-addr.arpa	0 / 94	-	-
doc-05-8g-docs.googleusercontent.com	0 / 94	2008-11-17	MarkMonitor Inc.

Contacted IP addresses (17)

IP	Detections	Autonomous System	Country
172.217.17.142	0 / 94	15169	US
172.217.20.99	0 / 94	15169	US
177.53.143.89	0 / 94	53243	BR
185.157.161.61	0 / 94	42675	SE
20.190.155.130	0 / 94	8075	US

7.png

10 / 96

Community Score

10/96 security vendors flagged this URL as malicious

Reanalyze Search More

https://multiwaretecnologia.com.br/js/Podaliri4.exe

Status 403

Content type text/html; charset=iso-8859-1

Last Analysis Date 2 months ago

DETECTION

DETAILS

COMMUNITY 1

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	Phishing
CRDF	Malicious	G-Dat	Phishing
Kaspersky	Malware	Lionic	Malicious
MalwareURL	Malware	Seclookup	Malicious
Sophos	Malware	Webroot	Malicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean

8.png

5. Conclusion

Based on the above findings, this email was conclusively identified as a **phishing attempt**. The indicators of compromise include:

- **A fake sender domain and return path** that do not match legitimate Nike email addresses.
- **Psychological manipulation** using urgency, rewards, and misleading CTAs.
- **A suspicious attachment** that was flagged as malicious.
- **Exploitation of a known vulnerability (CVE-2017-11882)**.
- **Malware execution** that attempted to connect to external malicious domains.

This analysis highlights the importance of vigilance in identifying phishing attempts, as well as the need for strong security controls to mitigate such threats.

6. Screenshots and References

Below is a list of reference images used in the analysis:

- **1.png** – Email recipient information.
- **2.png & 3.png** – Confirmation that the IP address belongs to Google.
- **4.png** - showing social engineering.
- **5.png** – Malicious attachment detected.
- **6.png** – Exploitation of CVE-2017-11882.
- **7.png** – Malicious external connections observed.
- **8.png** – Final payload flagged as malware.

Additionally, a file hash analysis was conducted using [Tip.Neiki](#), further confirming that this email was part of a phishing attempt.

By following structured analysis methodologies, we can effectively identify and prevent phishing attacks, enhancing overall cybersecurity awareness and defense mechanisms.