

TryHackMe Phishing Email Analysis Report

Greenholt PLC Case

Prepared by: Mubeen Khan

1. Scenario Summary

A Sales Executive at **Greenholt PLC** received an unexpected email from an individual claiming to be a customer. The email raised several suspicions:

- It began with a generic greeting ("Good day"), which the customer typically does not use.
- It referenced an unanticipated payment and included an attachment that the executive never requested.

Recognizing these inconsistencies, the executive reported the email to the **Security Operations Center (SOC)** for investigation. The objective of this analysis is to determine whether the email is legitimate or a phishing attempt.

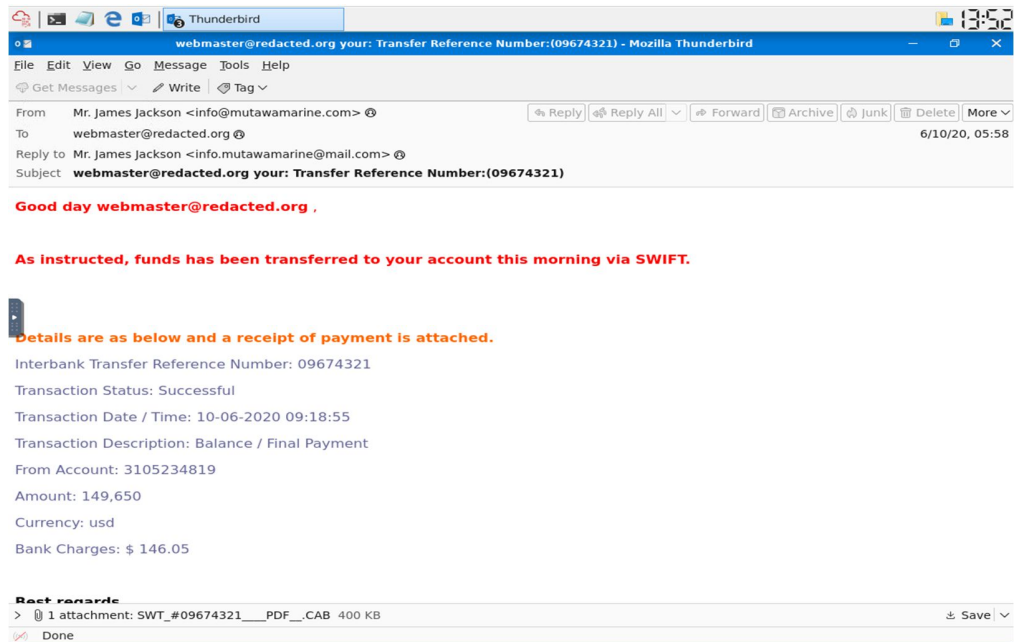
2. Investigation Tasks & Methodology

Objective: Verify email legitimacy using:

- Header Analysis (Thunderbird)
- Sender Authentication (MXToolbox SPF/DMARC checks, WhoisLookup)
- Attachment Forensics (VirusTotal, SHA256 hashing)

3. Key Findings

Overall Email:



A. Email Header Analysis:

Tool Used: Thunderbird (View > Message Source)

Fields Analyzed:

Field	Value / Observation	Risk Level
From	Mr. James Jackson <info@mutwamarine.com>	Suspicious – Possibly spoofed
Reply-To	info.mutwamarine@mail.com	Mismatch – Different from sender
To	<webmaster@redacted.org>	-
Subject	webmaster@redacted.org your Transfer Reference Number: 09674321	Included suspicious transfer ID
Return-Path	<x.x.x.x> (spoofed or redacted)	Potential Spoof
Authentication Results	SPF = fail, DMARC = unknown	Failed Authentication
Received-SPF	domain of mutwamarine.com does not designate x.x.x.x as permitted sender	SPF Fail
Originating IP	192.119.71.157 (Hostwinds LLC)	Unrelated IP
Message-ID	<BDAAEAAAF316B7461BD7C@mutwamarine.com>	-
Attachment	SWIT_#09674321__PDF__CAB	Disguised File

Email headers with anomalies highlighted

webmaster@redacted.org your: Transfer Reference Number:(09674321)

Subject: webmaster@redacted.org your: Transfer Reference Number:(09674321)
From: "Mr. James Jackson" <info@mutawamarine.com>
Date: 6/10/20, 05:58
To: webmaster@redacted.org
X-Atlas-Received: from 10.201.192.162 by atlas125.free.mail.bf1.yahoo.com with http; Wed, 10 Jun 2020 05:58:55 +0000
Return-Path: <info@mutawamarine.com>
Received: from x.x.x.x (EHLO sub.redacted.com) by atlas125.free.mail.bf1.yahoo.com with SMTPs; Wed, 10 Jun 2020 05:58:55 +0000
X-Originating-IP: [x.x.x.x]
Received-SPF: fail (domain of mutawamarine.com does not designate x.x.x.x as permitted sender)
Authentication-Results: atlas125.free.mail.bf1.yahoo.com; spf=fail smtp.mailfrom=mutawamarine.com; dmarc=unknown
X-Apparently-To: redacted@yahoo.com; Wed, 10 Jun 2020 05:58:55 +0000
X-YMailISG: CA2XOWoWLDuMav_xVT1F_0kXM35Y6SWpmp6zsE6LeQRxxw4YjzuEZUWxEjzHhUGbKbpzCq7GFztolFD6qKMKWunxnYA6aofb6xusgm_FJx591PPWdY5Nhw7H.Pwb9o9VnzHnbgKs3KzMM9IO7Un5j5y6rUw.dSshjuvjlRgxZYshquA.RCedSbTIMlpyxBT4LoSfMkWr0E4FgJ5W3I9zg8wk33szWpGqFHAyID0v.GOU7dBUrvMp8asqQiPa4KYC7v0oQTvmUEDtENPAImCnfcaipo gei5zs471gDrr3jWxiUMUTyChHRw9nCcZLepgGA2jt_MdbCZ7qgFqWMvvo1l nIXkl35mwKec90ZCIPj6tCHAQyFkE.030_0VmK_brmLt5oqQIGBYmyCV2i CwhdwdTwYkUldgler50ESBs5mHXsqNvtmpQoRjMPdqSXi87yvSIFaiF5rQ8 OTEw0w1CkWz4gxhNU4FH4lub03b9TLvUoX9KLEF3Del5yPTF8xxY7NY_kzA aCwKTjp4FaeT2Mk1Pq5P48DF.dB6hdMTmCoowu5wouW2M9Yp4euqKNzGrclcf 2KcRMROFFvcKDwX5aHw4tMhKvXSH0KIWMVfpXPaMmt2c0ckVpwZMyql8w8W PiponB1e66yilqNuV.v64i52HFn0jNwcuuohMo7MA7DmMP.OtkdwLiUqLS 68AfikwF35ppf_pTqtP6NPf2wuAsJlaT7_QQ.4x3khgYrC4jTmXjVBWDVRV wT0AdI0716U8Tvp.0AKvevKfMzfZoT0TsGLuQU.w8uZhv_6mwKB4sW7Pbhbr B1RjAdC0va2CjICbAC1Qnapm5eg5iExqkboy8iOUfzOqkD1a1_tn5nv1xDb bCqerO7cnAjpN1amfUvC8gjd345qb6k9i7h7a8TFsv_67Nkrok_M4_MRZcf .iuxPcffe2r1oca5FWQg6yof0WQta51sbWQidg7B_4XR2_6cbg8Ui39t2vZY bgWISOhtB1urpr.b1SANr7fvE2Zzvzj4_4PbBtBDevFUB7PjQ0GiAe_Nx_YpW8pLoFasyi1k4T9f5e5ryqAu.HT0legVimVa4xwuzjbNvaE7Tsm4m3vepb zGZ118WuDLQ-
X-Originating-IP: [x.x.x.x]
Received: from 10.197.41.148 (EHLO sub.redacted.com) (x.x.x.x) by mta4212.mail.bf1.yahoo.com with SMTP; Wed, 10 Jun 2020 05:58:54 +0000
Received: from hwsrv-737338.hostwindsdns.com ([192.119.71.157])51810 helo=mutawamarine.com) by sub.redacted.com with esmtp (Exim 4.80) (envelope-from <info@mutawamarine.com>) id 1jissD-0004g5-Ts for webmaster@redacted.org; Wed, 10 Jun 2020 01:02:04 -0400
Reply-To: "Mr. James Jackson" <info.mutawamarine@mail.com>
Message-ID: <20200609225823.DFAEAAF31A6B7414@mutawamarine.com>
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="-----_NextPart_000_0012_BDB07B06.81B59493"
X-Spam-Status: No, score=-0.5
X-Spam-Score: -4
X-Spam-Bar: /

<< > 1 of 3 >>

1 of 3

5/14/25, 13:54

WHOIS Lookup

Tool: <https://whois.domaintools.com>

Method: Entered IP 192.119.71.157

Result: IP belongs to Hostwinds LLC, which is unrelated to Greenholt PLC.

Whois IP 192.119.71.157

Updated 2 days ago

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:192.119.64.0 - 192.119.127.255
CIDR:192.119.64.0/18
NetName:HOSTWINDS-18-2
NetHandle:NET-192-119-64-0-1
Parent:NET192 (NET-192-0-0-0-0)
NetType:Direct Allocation
OriginAS:AS54290
Organization:Hostwinds LLC. (HL-29)
RegDate:2012-11-12
Updated:2021-09-23
Comment:<https://www.hostwinds.com>
Comment:Abuse Contact: abuse@hostwinds.com
Ref:<https://rdap.arin.net/registry/ip/192.119.64.0>

OrgName:Hostwinds LLC.
OrgId:HL-29
Address:12101 Tukwila International Blvd, 3rd Floor, Suite 320
City:Seattle
StateProv:WA
PostalCode:98168
Country:US
RegDate:2011-11-30
Updated:2024-11-25
Comment:<https://www.hostwinds.com>

B. Sender Authentication

SPF Record:

v=spf1 include:spf.protection.outlook.com -all

SUPER TOOL

SuperTool

Mail LookupBacklinksDMARC DiagnosticsEmail HealthDNS LookupAnalytics Headers

SuperTool Base

SPF Record Lookup

spf.mutawamrine.com

Find ProblemsSolve Email Delivery Problems

spf

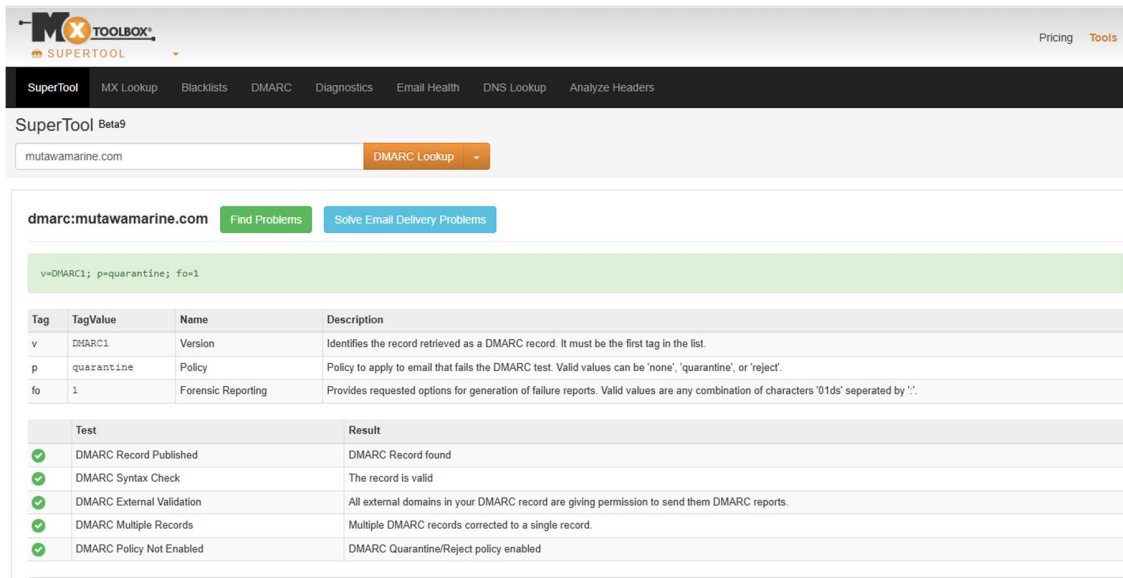
v=spf1 include:spf.protection.outlook.com -all

Prefix	Type	Value	Prefix Desc	Description
v	spf1			The SPF record version
include		spf.protection.outlook.com	Pass	The specified domain is searched for an 'allow'.
-all			Fail	Always fails here. It goes at the end of your record.

Text	Result
SPF Record Published	SPF Record found
SPF Record Degraded	No deprecated records found
SPF Multiple Records	Less than ten records found
SPF Contains characters after ALL	No terms after 'ALL'.
SPF Syntax Check	The record is valid
SPF Included Lookups	Number of included lookups is OK
SPF Recursive Loop	No Recursive Loops on Includes
SPF Duplicate Includes	No Duplicate Includes Found
SPF Typo PTR Check	No typo PTR found
SPF Void Lookups	Number of void lookups is OK
SPF MX Resource Records	Number of MX Resource Records is OK
SPF Record Null Value	No Null DNS Lookups found

DMARC Policy:

v=DMARC1; p=quarantine; fo=1



The screenshot shows the MXToolbox DMARC Lookup tool interface. The domain 'mutawamarine.com' is entered, and the DMARC record is displayed as 'v=DMARC1; p=quarantine; fo=1'. Below this, a table lists the tags and their descriptions. A second table shows the results of various DMARC tests, all of which passed except for the 'DMARC Policy Not Enabled' test, which indicates that the quarantine/reject policy is enabled.

Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	quarantine	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.
fo	1	Forensic Reporting	Provides requested options for generation of failure reports. Valid values are any combination of characters '01ds' separated by ','.

	Test	Result
✓	DMARC Record Published	DMARC Record found
✓	DMARC Syntax Check	The record is valid
✓	DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.
✓	DMARC Multiple Records	Multiple DMARC records corrected to a single record.
✓	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy enabled

Conclusion: SPF and DMARC records exist but don't protect against spoofing from unknown domain.

C. Attachment Analysis

File Name: SWT_#09674321__PDF_.CAB

Actual Type: RAR

SHA256 Hash:

2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f

VirusTotal: 49/63 security vendors flagged this file as malicious

Tool: **Ubuntu Terminal**

Method: SHA256 hash of file using command:

```
ubuntu@ip-10-10-197-89: ~/Desktop
File Edit View Search Terminal Help
ubuntu@ip-10-10-197-89:~$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
ubuntu@ip-10-10-197-89:~$ cd Desktop
ubuntu@ip-10-10-197-89:~/Desktop$ ls
SWT_#09674321 PDF .CAB Tools challenge.eml
ubuntu@ip-10-10-197-89:~/Desktop$ S WT_#09674321__PDF_.CAB
S: command not found
ubuntu@ip-10-10-197-89:~/Desktop$ sha256sum SWT_#09674321__PDF_.CAB
2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f  SWT_#09674321__
PDF_.CAB
ubuntu@ip-10-10-197-89:~/Desktop$
```

VirusTotal results

49
/ 63

Community Score

49/63 security vendors flagged this file as malicious

2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f
SWT_#09674321__PDF_.CAB

Size
400.26 KB

Last Analysis Date
13 hours ago

RAR

rar attachment spreader

DETECTION

DETAILS

RELATIONS

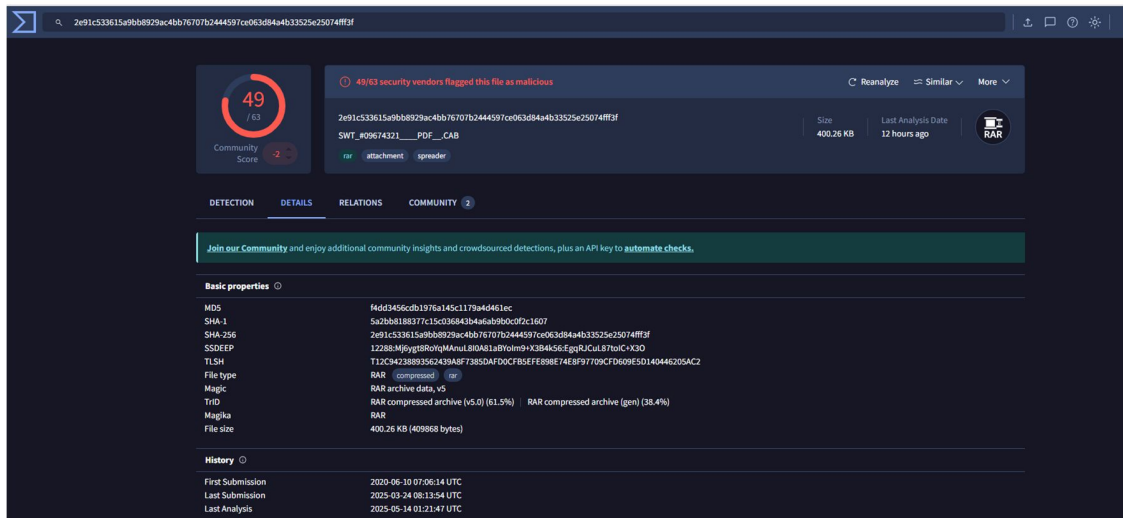
COMMUNITY 2

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

Popular threat label trojan.msl/loki Threat categories trojan ransomware Family labels msl loki agenda

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan:Win32.Kryptik.R345359	AliCloud	Trojan:MSIL/Kryptik.WGM
ALYac	Gen:Variant.Ransom.Loki.8140	Antiy-AVL	RiskWare[Obfuscator].MSIL.Reactor.a
Arcabit	Trojan.Ransom.LoKi.D1FCC	Avast	Win32:MalwareX-gen [Pws]
AVG	Win32:MalwareX-gen [Pws]	Avira (no cloud)	HEUR/AGEN.1305524
BitDefender	Gen:Variant.Ransom.Loki.8140	ClamAV	Win.Dropper.Formbook-9870653-0
CTX	Rar.trojan.msl	Cynet	Malicious (score: 99)
DeepInstinct	MALICIOUS	DrWeb	Trojan.PackedNET.331
Emsisoft	Gen:Variant.Ransom.Loki.8140 (B)	eScan	Gen:Variant.Ransom.Loki.8140



4. Conclusion & Recommendations

Verdict: Confirmed Phishing Attempt

IOCs:

- IP: 192.119.71.157
- Domain: mutawamarine.com
- Attachment Hash:
2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f

Actions Recommended:

- Block originating IP at firewall.
- Alert employees about this campaign.
- Blacklist attachment hash organization-wide.

5. Skills Demonstrated

Technical: Email forensics, malware analysis, threat intelligence.

Analytical: IOC extraction, risk prioritization.

Communication: Professional reporting for SOC teams.

6. Solution

- Conducted in-depth header analysis to identify mismatched sender information.
- Verified SPF/DMARC settings and found inconsistencies and invalid records.
- Analyzed attachment and confirmed it was an executable masquerading as a PDF.
- Used VirusTotal to identify malware type and cross-referenced with known indicators of

compromise.

- Suggested appropriate SOC response actions such as blocking IP and blacklisting file hash.

7. Final Conclusion

The investigation confirmed a well-crafted phishing attempt aimed at tricking the sales department into executing malicious software. Based on IOC validation and malware detection, immediate preventive actions have been recommended. This case highlights the importance of routine email scrutiny and rapid SOC response in mitigating phishing risks.