

The GreenHolt Phishing Email

Scenario

A Sales Executive at Greenholt PLC received an email that he didn't expect to receive from a customer. He claims that the customer never uses generic greetings such as "Good day" and didn't expect any money to be transferred to his account. The email also contains an attachment that he never requested. He forwarded the email to the SOC (Security Operations Center) department for further investigation.

Investigate the email sample to determine if it is legitimate.

Investigation.



Email Header


Headers	Received lines	X-headers	Security	Attachments	Message URLs
From	info@mutawamarine.com				
Display name	Mr. James Jackson				
To	webmaster@redacted.org				
CC	None				
Timestamp	03:58 pm, Jun 10th 2020				
Reply-To	info.mutawamarine@mail.com				
Return-Path	info@mutawamarine.com				
Originating IP	192.119.71.157 (Hop 1)				
rDNS	client-192-119-71-157.hostwinddns.com				

Figure 1: Investigation of the Headers of Phishing Email.

The sender's email address and the "Reply-To" email address do not match, which indicates a phishing email.

The legitimated email should or must have the matching email addresses from these aspects.

 Headers Received lines X-headers  Security Attachments Message URLs

Hop 1 Timestamp Wed, 10 Jun 2020 01:02:04 -0400 

Received from hwsrv-737338.hostwinddns.com (192.119.71.157)

Received by sub.redacted.com

More ▼ Show raw ▼

Hop 2 Timestamp Wed, 10 Jun 2020 05:58:54 +0000

Received from sub.redacted.com (10.197.41.148)

Received by mta4212.mail.bf1.yahoo.com

More ▼ Show raw ▼

Hop 3 Timestamp Wed, 10 Jun 2020 05:58:55 +0000

Received from x.x.x.x

Received by atlas125.free.mail.bf1.yahoo.com

More ▼ Show raw ▼

Recipient mailbox Timestamp 09 Jun 2020 22:58:27 -0700

Figure 2: Investigation of Received Lines from the Email Header.

The Original IP address is 192.[.]119[.]71[.]157, which is used for further researching the owner of this IP address.

[Home](#) > [Whois Lookup](#) > 192.119.71.157

IP Information for 192.119.71.157

— Quick Stats



IP Location	 United States Dallas Hostwinds Llc.
ASN	 AS54290 HOSTWINDS, US (registered Dec 05, 2011)
Resolve Host	client-192-119-71-157.hostwinddns.com
Whois Server	whois.arin.net
IP Address	192.119.71.157

Figure 3: Researching the owner of this IP address or the Originating sender.

The Originating sender was recorded as Hotswinds LLC, while the company's name of the sender is SEC Marine Services. This indicates that the attacker used a different IP address to masquerade as SEC Marine for their attack.





 Headers		Received lines	X-headers	 Security	Attachments	Message URLs
SPF		...				
Result	 FAIL					
Originating IP	192.119.71.157 (Hop 1) ▼					
rDNS	client-192-119-71-157.hostwindsdns.com					
Return-Path domain	mutawamarine.com					
SPF record	v=spf1 include:spf.protection.outlook.com -all					
DKIM		...				
Result	None					
Verification(s)	0 Signatures					
Selector	None					
Signing domain	None					
Algorithm	None					
Verification	None					
DMARC		...				
Result	 FAIL					
From domain	mutawamarine.com					
DMARC record	v=DMARC1; p=quarantine; fo=1					

Figure 4: Investigation of authenticity and legitimacy of the email header.

According to Figure 4, both SPF and DMARC have the "Fail" status, demonstrating that this Originating IP is not the legitimate origin for this email, and the authenticity of this email can not be relied on.

Email Body.

Good day webmaster@redacted.org ,

As instructed, funds has been transferred to your account this morning via SWIFT.

Details are as below and a receipt of payment is attached.

Interbank Transfer Reference Number: 09674321

Transaction Status: Successful

Transaction Date / Time: 10-06-2020 09:18:55

Transaction Description: Balance / Final Payment

From Account: 3105234819

Amount: 149,650

Currency: usd

Bank Charges: \$ 146.05

Best regards,

Mr. James Jackson

Accounts Payable

SEC MARINE SERVICES PTE LTD

Figure 5: Investigation of the Email body.

The company's name is usually used as the domain name or subdomain name. This means the company's name should be Mutawamarine, or the email address should be info.secmarineserivces.com.

However, the company's name and email address cannot meet this requirement, so it is considered one of the Indicators of Malicious.




 Headers	Received lines	X-headers	 Security	Attachments	Message URLs
 1 ...					
File name	SWT_#09674321____PDF___.CAB				
File type	RAR				
File size	400.26 KB				
VirusTotal	Configure				
File hashes					
MD5	f4dd3456cdb1976a145c1179a4d461ec				
SHA-1	5a2bb8188377c15c036843b4a6ab9b0c0f2c1607				
SHA-256	2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f				

Figure 6: Investigation of the Attachment of Phishing Email.

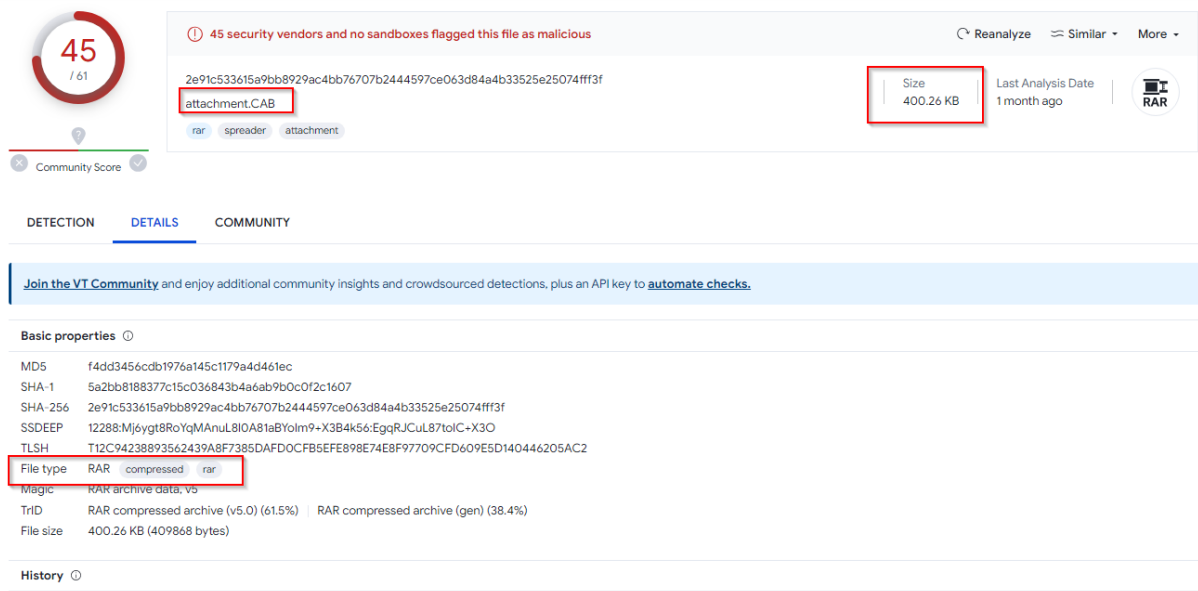


Figure 7: Investigation of attachment file via Virustotal tool.

The file extension is CAB, but the natural extension of this file is RAR. In addition, this file has been recorded as a malicious file from 45 security vendors classified as a trojan.

Summary.

Tools are used for the investigation.

- phishtool.com
- virustotal.com.
- <https://whois.domaintools.com/>

Procedure of adversary.

- The adversary uses 192[.]119[.]71[.]157 from Hotswinds LLC for the attack.
- The adversary tries masquerading as SEC Marine Services PTE LTD and Mutawamarine to gain the victim's trust.
- The attachment file is the trojan, obfuscated as a different file extension, RAR.

Prevention.

- The IP address must be listed within the Firewalls and IPS for blocking.