REPORT

ACME Test Industries

Email Security & Phishing Assessment Report

August 2, 2021

ACCELERATING DIGITAL TRANSFORMATION

U.S. HEADQUARTERS
3 SEAVIEW BOULEVARD
PORT WASHINGTON, NY
11050

AGILANT
SOLUTIONS INC

1 DOCUMENT CONTROL

APPROVAL

The signatures below certify that this document has been reviewed and accepted and demonstrates that the signatories are aware of all the requirements contained herein and are committed to ensuring their provision.

	Name	Position
Prepared by	Steven Forti	Chief Information Security Officer
Prepared by	Vincent Gulino	Senior Security Architect
Reviewed by	Harry Taluja	Chief Technology Officer
Reviewed by	Katie Riley	Director, Business Development & Marketing

AMENDMENT RECORD

This document is reviewed to ensure its continuing relevance to the systems and process that it describes. A record of contextual additions or omissions is given below:

Page No.	Context	Revision	Date

COMPANY PROPRIETARY INFORMATION

The electronic version of this document is the latest revision. It is the responsibility of the individual to ensure that any paper material is the current revision. The printed version of this manual is uncontrolled, except when provided with a document reference number and revision in the field below:

Document Ref. _____ Rev _____

Uncontrolled Copy [•] Controlled Copy [ ] Date _____

2 EXECUTIVE SUMMARY

ACME Test Industries (herein "ACME ") engaged Agilant Solutions, Inc. (herein "Agilant") to conduct a comprehensive vulnerability assessment, testing a variety of internal and external systems. This portion of the assessment included testing email communication mechanisms and evaluating user community awareness of phishing.

Phishing scams are a likely attack vector for threat actors across the globe. Realistically, attack vectors center around two types of attacks when it comes to email:

1. To "phish" unsuspecting users for their usernames and passwords. This attack leverages the inherent trust users have in their IT department and/or websites and landing pages they believe they've visited previously.

2. Mechanisms of trust that either convince a user to visit a page that contains malicious code embedded within the site -or- attach malicious links/files to emails and embed active content within the email itself.

Our assessment evaluated these attack vectors and employed tactics to overcome the defenses employed by the ACME .

Overall, the real-time defense to malware, executable content, known phishing sites and other forms of email-based attacks provided by Microsoft are configured correctly and working effectively to combat known and unknown threats.

However, to strengthen the defense strategy, additional resources should be applied to user awareness / training efforts and be supplemented by a real-time monitoring service.

In the following sections, we outline the testing performed, the rationale behind each, the effectiveness of the control, an overall assessment of risk based on the activities performed, and suggested actions which are recommended moving forward.

3 SCOPE

ACME engaged Agilant to conduct a comprehensive email security and phishing assessment consisting of several tests as outlined below. To perform the phishing portion of the exercise, Agilant was provided with a list of 300 mailboxes which we then divided into three (3) groups. To perform the malware portion of the review effectively, Agilant was granted one (1) mailbox within the O365 tenant so that we could direct a variety of neutralized malware samples, controlled hyperlinks, and executable content to the inbox.

The goal was to determine if the emails containing "threats" would be stopped at the gateway level in order to protect the organization from the hands of the weakest link, the user.

The tasks conducted were as follows:

- **Test one**: Perform several batches of phishing tests in groups of 100 users with impersonated landing pages as a trusted sender
- **Test two:** Perform a single phishing tests with a group of 100 users with impersonated landing pages as an untrusted sender
- **Test three:** Send 100 emails to a predesignated account containing links to recently discovered malware/phishing sites.
- **Test four:** Attempt to circumvent site blacklists with base vulnerability for of several of the sites which were blocked
- **Test five:** Send several emails to a predesignated account containing RTLO formatted executables
- **Test six:** Send 20 emails to a predesignated account containing all known windows executable file types, i.e.: .cmd. .exe,ps1,vbs
- **Test seven:** Send 5 emails attempting to obfuscate the executable file extension i.e.: double dot extensions, compression, file extension re-name
- **Test eight:** Send 5 emails with known viruses as attachments.
- **Test nine:** Send 1 email with HTML JS Redirect Attachment
- **Test ten:** send 1 email with PDF attachment with malicious text link
- **Test eleven:** send 1 email with embedded Macro containing PowerShell commands
- **Test twelve** Test Email Hygiene bypass
- **Test thirteen:** Send email with spoofed source address

4 EMAIL CONTENT THREAT ANALYSIS

Overall, the configuration settings implemented by the IT staff on the O365 tenant are considered effective at blocking a wide variety of known and unknown threats, file types and viruses. Emails arriving from outside the organization are clearly marked as external and provide staff advice within the notice regarding opening attachments and clicking on links.

With respect to the tests listed above, Test 3 through Test 12 were rated with perfect scores – not a single malicious link, email with active content, executable file type or malware sample made it through the filter.

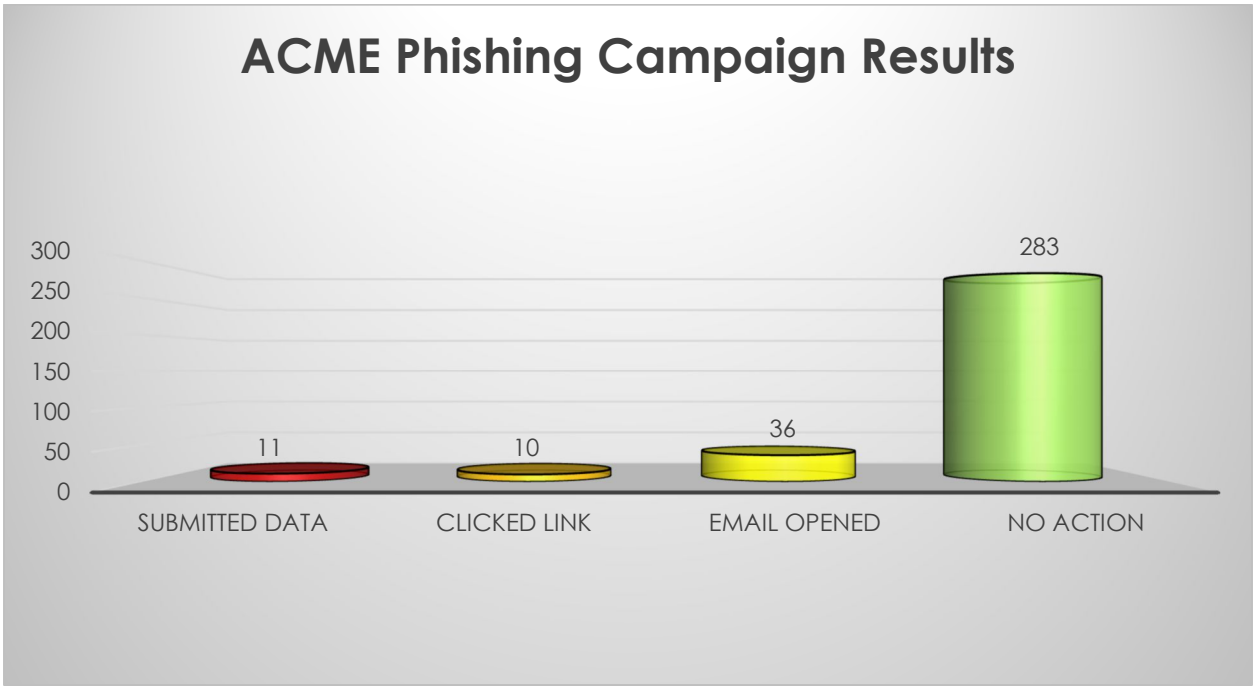
Vulnerability Test	Penetration Rate	Control Effectiveness
Send 100 emails to a predesignated account containing links to recently discovered malware/phishing sites.	0	High
Attempt to circumvent site blacklists with base vulnerability for of several of the sites which were blocked	0	High
Send several emails to a predesignated account containing RTLO formatted executables	0	High
Send 20 emails to a predesignated account containing all known windows executable file types i.e. : .cmd. .exe,ps1,vbs	0	High
Send 5 emails attempting to obfuscate the executable file extension i.e.: double dot extensions, compression, file extension re-name	0	High
Send 5 emails with known viruses as attachments	0	High
Send 1 email with HTML JS Redirect Attachment	0	High
send 1 email with PDF attachment with malicious text link	0	High
send 1 email with embedded Macro containing PowerShell commands	0	High
Send email with spoofed source address	0	High
Test email hygiene bypass routines	0	High

5 PHISHING THREAT ANALYSIS

While the majority of the targeted users avoided the phishing emails, a substantial amount opened the emails, leaving the organization vulnerable to executed code from embedded active content. This demonstrates the value in maintaining the controls listed in the previous section.

At the conclusion of the exam, a total of eleven (11) users submitted their network credentials to our phony landing page which, in a real-world scenario, could lead to significant compromise in the following ways:

- If the user maintains remote VPN access, the attacker could use those credentials to access to the network by identifying the VPN server with a simple IKE reconnaissance tool, downloading the publicly available client, and providing the phished credentials.
- The submit button on the landing page could contain executable content that detonates on click. This would lead to potential content downloads, script execution and other nefarious activities.
- Sensitive information in the mailbox could be read and /or downloaded by the attacker.
- The trust between the compromised user and peers could be leveraged to further infiltrate the network



Email Address		Status	Source IP	Total
				11 users submitted data.
b**st@pol		Submitted Data	145.60	
c******or		Submitted Data	145.60	
c****n2@		Submitted Data	50	
d*****jr@		Submitted Data	145.60	
j*****tt@		Submitted Data	5.195	
l****ey@		Submitted Data	50	
m****h2@		Submitted Data	145.60	
r********		Submitted Data	145.60	
s****ey@		Submitted Data	138	
s****la@p		Submitted Data	145.60	
s*****ns@		Submitted Data	06.117	
				10 users clicked the phishing link.
c***a2@p		Clicked Link	50	
e*******e		Clicked Link	55.255	
e*****jo@		Clicked Link	153	
j***re@pc		Clicked Link	218	
j***l6@pc		Clicked Link	197	
j****rd@p		Clicked Link	155	
j********	org	Clicked Link	166	
k*****ey@		Clicked Link	174	
m*****l2@		Clicked Link	235.129	
r***ce@p		Clicked Link	160	
				36 users opened the phishing email.
d******rs		Email Opened	128.73	
d******s2		Email Opened	43.139	
d******or		Email Opened	232	
d*****ns@		Email Opened	58.201	
e****er@		Email Opened	50	
e**sa@po		Email Opened	58.27	
g****ck@		Email Opened	99.157	
g*****ll@		Email Opened	19.58	
g******er		Email Opened	75.109	
g****er@		Email Opened	50	
h****es@		Email Opened	5.55	
i****on@		Email Opened	50	
j**ay@pol		Email Opened	159.63	
j****er@p		Email Opened	100.113	
j*******s		Email Opened	57.45	
k****um@		Email Opened	131.79	
l****in@p		Email Opened	145.60	
l****h3@		Email Opened	3.180	
l***th-ho*	g	Email Opened	49.70	
l*******in		Email Opened	175.195	
m**hn@p		Email Opened	75.5	
m***au@		Email Opened	19.33	
p****vo@		Email Opened	145.60	
p****ud@		Email Opened	161.120	
r***is@pc		Email Opened	2.48	
r********		Email Opened	3.233	
s***ch@p		Email Opened	160.209	
s*****er@		Email Opened	52.89	
s****in@p		Email Opened	4.119	
s******ez		Email Opened	207	
s****ge@		Email Opened	50	
s******er		Email Opened	55.119	
s*******a		Email Opened	164.138	
t****ak@p		Email Opened	32.41	
v****es@		Email Opened	5.155	
z***on@p		Email Opened	1.50	

6 RECOMMENDATIONS

1. **Configure a GeoIP-based access filters**.
   Most of the attacks we see come from areas outside of the U.S. If ACME has no need to allow for incoming connections from outside the U.S., we strongly recommend blocking that traffic.

2. **Security Awareness Training**
   Implement a service such as Knowbe4 to maintain consistent security awareness and to allow the security team to systematically remove email threats from mailboxes without interrupting users.

3. **Conditional Access**
   Implement conditional access filters in Azure AD to help mitigate the surface attack in Office 365. Note that conditional access requires the following SKU additions per protected user account; Azure AD P1, Azure AD P2 or EMM+Security.

4. **MFA**
   Implement MFA on email accounts, Office 365 Global Admin accounts, and on all forms of remote access by utilizing a service such as Duo or Okta.