

Oh-My-Phish!!

...

Leveraging Office365 & Azure for Phishing

DISCLAIMER

The opinions expressed in this presentation and in any corresponding comments are the personal opinions of the original authors, not those of CVS Health and Digit Labs.

Introduction to the Presenters

Samuel Ferguson

- IT Leadership Development Professional
- Red/Purple team specialist
- Volunteer at Digital Overdose

Shahrukh Iqbal Mirza

- Hacker / Red Teamer / Security Analyst
- Republic of Hackers Staff Member
- Hacking Is NOT A Crime Advocate
- CTF Player (HTB and THM)

Introducing Phishing

- Social Engineering Attack
- Used to steal sensitive data or install malicious tools.
- Objectives of Phishing during Red Team Assessments:
 - Credential Harvesting
 - Payload Delivery

Challenges in Phishing

- Email Security Gateways (Attachment/link analysis)
- Flagging as Spam
- User security awareness training

Phishing SaaS

- Building “proper” infra isn’t always necessary
 - Short engagements, “one off” tests
- Microsoft provides a couple solutions
 - Outlook
 - MS365 for Small Business

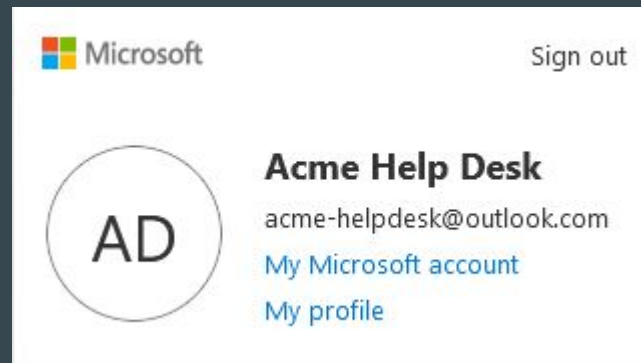
Microsoft Outlook

- The free email platform you know and love
- MS product, so compatible with Exchange
 - Provides some platform-specific phishing opportunities
- Downsides
 - Can get blocked by MS for spam
 - Trained users will likely spot out questionable



Outlook Social Engineering Techniques

- Name and Email
 - Email can't include "security"
- Signature



Acme Help Desk
123 Main Street
City, ST 01234
123-456-7890|

Microsoft 365 for Small Business





- SaaS solution for small business users
- Free one month trial!
 - After that anywhere from \$5 - \$20 USD/user
- Access to Office Suite



Microsoft 365

MS365 for Small Business Social Eng Techniques

- All techniques from Outlook
- Domain name
- Multiple users
- Customized SharePoint site

Name ↑		Username for sign-in	
	Acme Help Desk	⋮	HelpDesk@acrne.onmicrosoft.com
	Jeff Jones	⋮	jeff.jones@acrne.onmicrosoft.com
	Sarah Davidson	 ⋮	sarah.davidson@acrne.onmicrosoft.com

Secure Email Gateways

- SEGs are the frontline defence against malicious messages
- Provide detections on both URLs and attachments
 - Even URLs that download or redirect to download can be inspected
- Examples
 - Forcepoint
 - Proofpoint
 - Mimecast
 - FireEye MX
 - O365 Defender Safe Links

Outlook Bypass - OneDrive

- Legitimate URL for file location (OneDrive)
 - Can be rewritten by SEG
- Appears similar to standard attachment



Acme Help Desk <acme-helpdesk@outlook.com>

Wed 10/27/2021 10:24 PM

To:



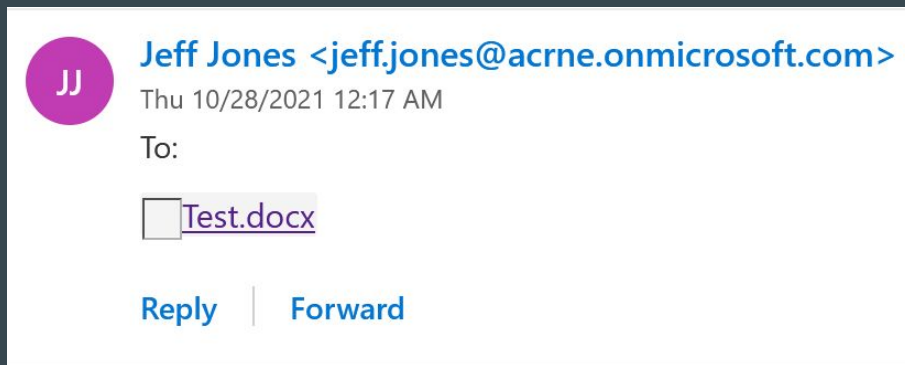
FergusonResume-CURRE...

nam12.safelinks.protection...



MS365 - SharePoint

- Shareable link embedded in email
- Legitimate domain (SharePoint)
- Can be
- Nice little icon
 - Not shown if URL is rewritten by SEG



More Generic Bypasses

- As mentioned before, SEGs inspect files
 - Even downloaded from links and redirects to downloads
- SEGs may not be able to get passed interaction
 - CAPTCHA
 - OTP
 - Etc.
- This provides us with path to bypass

Example: Firebase + Azure Blob Storage

- Google Firebase allows for easy deployment of reCAPTCHA
- Azure Blob Storage serves direct downloads from legit URL
- Steps
 - Create Firebase app
 - Generate reCAPTCHA keys for app
 - Add necessary keys and logic to Firebase
 - Create Azure blob storage with public read access
 - Add redirect to Azure blob storage URL
 - ??????
 - Profit

Azure Information Protection

- Uses Rights Management Service to encrypt emails and attachments
- Restrict the email and attachments to specific targets
- Set an expiry time for emails/attachments
- Easy setup if you already use Azure



Why use AIP to bypass Email Security Gateways

Because



But



Why use AIP to bypass Email Security Gateways

- Advantages of using AIP to bypass SEGs:
 - Tracking of sent emails - see when email was viewed/opened
 - Email encryption
 - Payload encryption
 - Access revocation
 - Supports a variety of file formats (yes, not just MS Office file formats)
 - All the file formats except for those of MS Office files, get a little 'p' added in the extension
- Limitation
 - AIP GUI Client is required to view encrypted files, other than Office files

Example: Using AIP for Payload Delivery

- Create sensitivity labels in MS admin centre
- Prepare a maldoc and apply the label to protect it
- Alternatively, encrypt the maldoc using the AIP Client
 - Custom permissions can also be set
- Prepare a phishing email and apply the label to protect the email as well
- Happy phishing!! :)

Thanks for Listening! Questions?

- **Connect with Shah!**

- Twitter: @shahrukhiqbal24
- LinkedIn: /in/shahrukhiqbal24

- **Connect with Sam!**

- Twitter: @AffineSecurity
- LinkedIn: /in/AffineSecurity