Latest Techniques in Hacking the Human

Jake Williams
Rendition Infosec
www.rsec.us
@MalwareJake

RENDITION INFOSEC
Cybersecurity by any legal means

$whoami

- Founder and President of Rendition Infosec
- IANS Faculty
- Rally Security Co-Host
- SANS Senior Instructor and Course Author
- Former NSA hacker, Master CNE operator, recipient of the DoD Exception Civilian Service Medal
- **Dislikes:** those who call themselves “thought leaders,” “crypto bros,” and anyone who **needlessly adds blockchain** to a software solution

Agenda

- Phishing pretexts that are working consistently
- Exploiting third party trust relationships
- Using OWA access to gain code execution
- Review your mailbox rules
- Exfiltrating data (and delivering exploit docs) via cloud services

Phishing pretexts that are working consistently

Educate your users or they’ll absolutely fall for these…

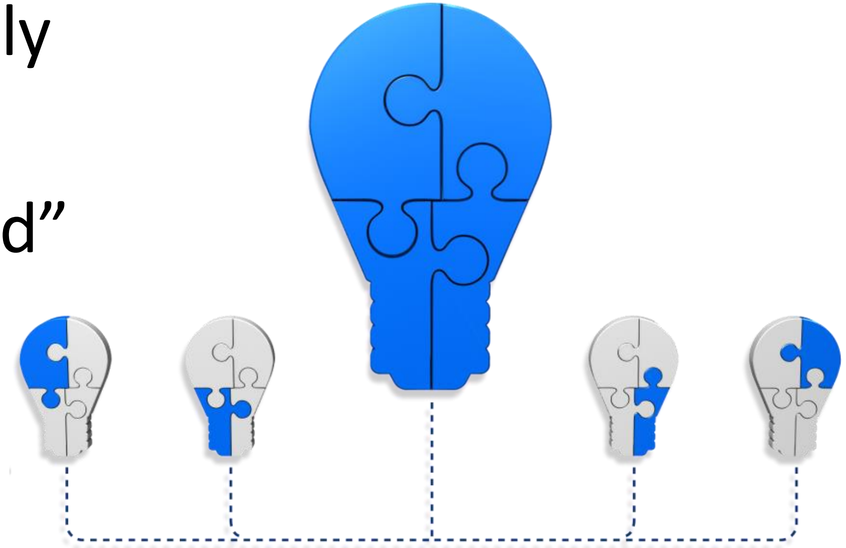
Phishing Pretext #1 – Company downsizing

- This pretext is amazing because it's the sort of thing that people feel like they ***need*** to read, even when they admit it looks suspicious
  - This is a high risk for the attacker – it's almost certainly going to be reported

- If you see this pretext used, anticipate attackers are doing a smash and grab or need something right meow!
- **Takeaway:** Focus education/testing of this pretext on users likely to have time sensitive data

Phishing Pretext #2 – M&A Information

- Have you ever been involved in an M&A?
  - We do lots of M&A work and users are regularly left in the dark
  - Attackers are happy to “fill the information void”

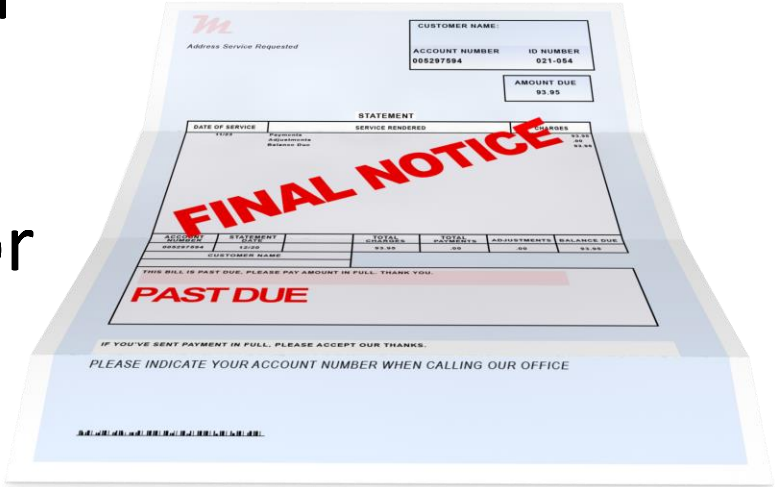


- **Takeaways:**
  - Ensure that users know the authorized channels for information
  - Educate users that attackers will attempt to trick them by supplying additional M&A data

RENDITION INFOSEC
Cybersecurity by any legal means

Phishing Pretext #3 – Overdue invoice

- The “overdue invoice” trick works because it invokes a sense of urgency that may limit out of band validation
- Teach users to ***ALWAYS*** perform out of band validation before engaging with a new vendor or changing payment information for an existing vendor
  - Use existing contact information, not what is provided by the (potential) attacker
- **Takeaway:** Focus education on accounts payable, executives, and anyone with direct purchasing authority



Address Service Requested

CUSTOMER NAME:

ACCOUNT NUMBER 005297594 ID NUMBER 021-054

AMOUNT DUE 93.95

STATEMENT

DATE OF SERVICE	SERVICE RENDERED	CHARGES
11/22	Payments Adjustments Balance Due	93.95 .00 93.95

FINAL NOTICE

ACCOUNT NUMBER	STATEMENT DATE		TOTAL CHARGES	TOTAL PAYMENTS	ADJUSTMENTS	BALANCE DUE
005297594	12/20		93.95	.00	.00	93.95

CUSTOMER NAME

THIS BILL IS PAST DUE. PLEASE PAY AMOUNT IN FULL. THANK YOU.

PAST DUE

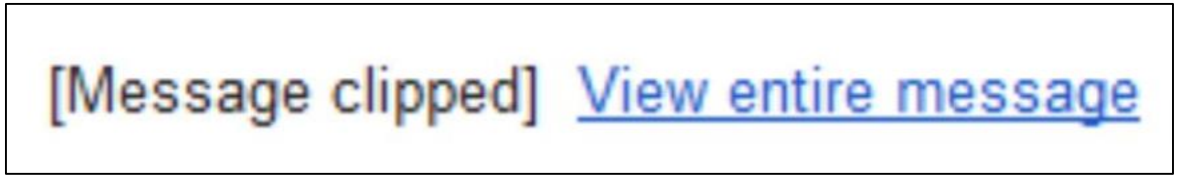
IF YOU'VE SENT PAYMENT IN FULL, PLEASE ACCEPT OUR THANKS.

PLEASE INDICATE YOUR ACCOUNT NUMBER WHEN CALLING OUR OFFICE

RENDITION INFOSEC
Cybersecurity by any legal means

Phishing Pretext #4 – "Message Clipped"

- The attacker sends a message that appears partially clipped
- This is especially effective if your organization uses webmail or supports synchronization with mobile devices



[Message clipped] View entire message

- **Takeaway:** Educate your users on this technique – it works consistently

Phishing Pretext #5 – You won an award!

- We’ve been consistently use this in assessments after observing an attacker’s success
- Usually a spear phish, victims are told that they’ve been selected to receive an award, but must first be vetted by a committee
- This works well because it capitalizes on pride and desire for recognition
- **Takeaway:** This approach is best communicated by demonstration – seeing is believing

Phishing Pretext #6 – Selected to keynote!

- This is a variation of the "award" technique
  - It capitalizes on the victim's pride

- This has been used by Russians to target senior NATO commanders, often by selecting them to attend conferences that don't really exist

- **Takeaway:** Educate users that offers to keynote a conference aren't always benign and that cursory web searches don't legitimize the invitation

Phishing Pretext #7 – BoF / Club

- In this scenario, the attacker sends out an invitation to join an org sponsored club / Birds of a Feather / etc.
  - This relies on our desire to be "in" the group

- This technique works reliably to obtain credentials when shared cloud spreadsheets are used to "sign up" or "express interest"
- **Takeaway:** Educate users that org sponsored social events will never use Google Sheets or other shared cloud documents (then ***actually*** stick to this policy)

Exploiting third party trust relationships

Our trust will be our downfall…

We want to trust

- Third party trust is a significant contribution to many successful phishing attacks we see today

- Largely due to successful security awareness programs, attackers often need better and better pretexts

- Exploiting vendor and contractor trust relationships is increasingly becoming a way to compromise networks

Trust scenario #1 – Service technician

- Company X operates a chain of surgical centers and biopsy laboratories that use highly specialized equipment
  - The equipment is leased to the organization and serviced by the manufacturer
- After one of our monthly "the sky is falling" cybersecurity events, an attacker emails saying they are handling the overflow for the patching work
  - Company PoC opens a LogMeIn remote control binary and it's all over from there…

Trust scenario #2 – Infrastructure Shakeup

- Changing out infrastructure (e.g. moving to cloud email, changing cloud email providers, etc.) is always an opportunity for attackers to capitalize on
- This is particularly true when contractors are brought in to help with the migration – new people, new technology, and many emails from outside the organization
- Attackers can often tell you're moving just by performing OSINT

RENDITION INFOSEC
Cybersecurity by any legal means

Review your mailbox rules

Mailbox rules your #1 IOC for BEC

Attackers regularly modify inbox rules

- In email compromises we work today, attackers are modifying mailbox rules
- Sample use cases:
  - Duplicating copies of all emails received to the attacker – it's a gift that keeps on giving even after passwords are changed
  - Doing the same with sent mail
  - Deleting or archiving email from those who question the legitimacy of a request - e.g. "did you REALLY want me to wire money to the deposed Prince of Nigeria?!"

Mailbox rules are hard to audit

- Because mailbox rules are used for many non-obvious (but totally legitimate) purposes, they are VERY difficult for IT security to audit
- Is there a legitimate business reason why emails from one sender are being forwarded to someone outside the organization? Maybe…
- **Security awareness takeaway:** educate users that new and modified inbox rules are an IOC. Then train them on the steps to audit their own rules

RENDITION INFOSEC
Cybersecurity by any legal means

Don’t worry, the sessions were disabled!

Um, keep worrying…

Just what does “invalidating” mean anyway?

- During an email compromise, it’s standard fare for responders to force the reset of the user’s password and disable all existing sessions
  - This is sometimes called “invalidating access tokens”

- Since computers work at the speed of light, it would be reasonable to assert that login sessions are immediately nuked
  - In O365 that’s not the case though – they may live on for more than an hour, depending on circumstances

What can we do about it?

- Unfortunately, there’s little that can be done to fix this, it’s just part of how Office365 works on the back-end

- Security awareness professionals, we should absolutely tell our users that we can’t simply “lock the attacker out” if their account is compromised
  - Let them know that the pain could potentially continue for a period of time you don’t control
  - Remove the thought that “IT can just reset my password”

Code execution through OWA

But… it’s just email access, right?

OWA Access – now what?

- Once an attacker has access to an Outlook Web Access account, they can turn this into code execution
  - Some organizations allow synchronization of mail via IMAP without MFA, even when MFA is required for OWA

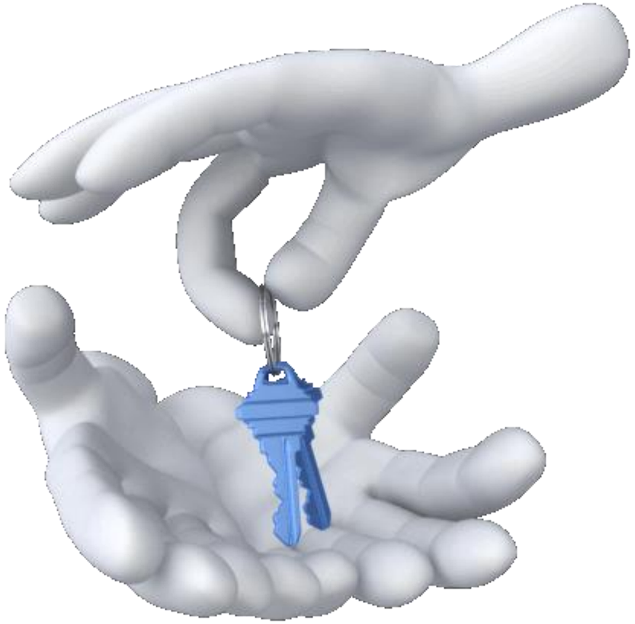
- With access to Outlook, attackers can import a new email rule (remember those email rules?)
  - Rules can be created to run a command when the email is received
  - It turns out that command can be run from a WebDAV share…

Attack Walkthrough

- Attacker compromises the web based email environment
- The attacker uses that access to connect to Outlook
- New inbox rules are created to run a command on receipt of a specific subject line
  - – Outlook won't allow a rule to be input if the command runs from a remote share
  - – Unfortunately checking is performed at rule insertion time, **NOT** at rule execution time

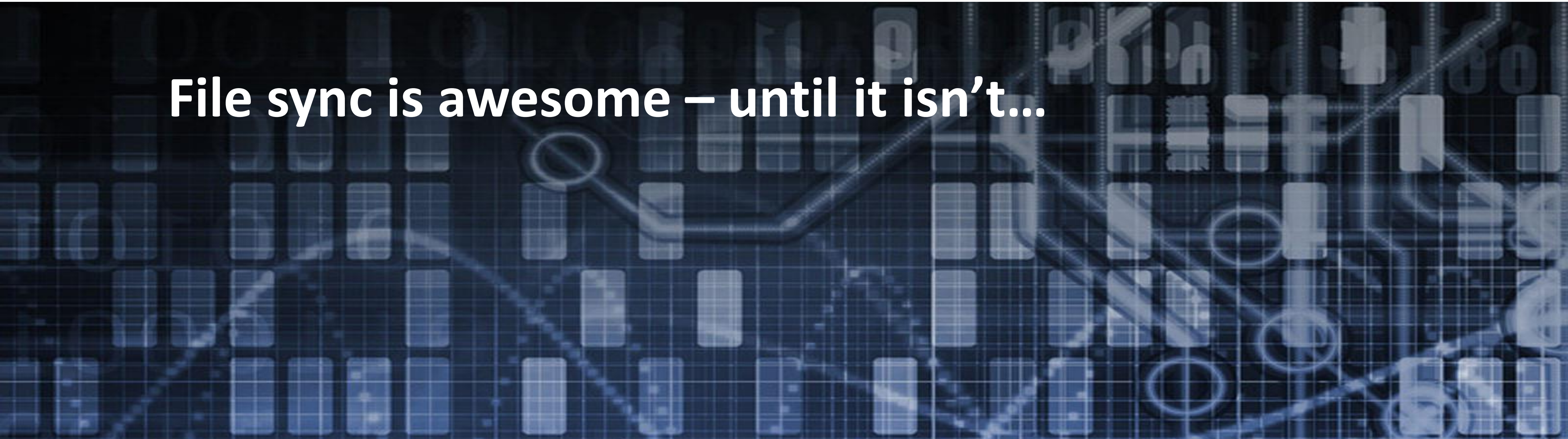
Attack Walkthrough (2)

- Attackers use special tools to create custom rules, which synchronize with Outlook
- When a user opens their Outlook, the rule fires inside the target network
- The attacker gains code execution inside the domain and pilfers from there



- **Security awareness takeaway:** Educate users that an email compromise can lead to full domain takeover

Exfiltrating data via cloud sharing



File sync is awesome – until it isn’t…

Cloud Data Sharing

- Cloud synchronization is a security cancer
  - Sure users love it, but the data being synchronized is difficult to inspect (rather intentionally we suspect)

- Attackers use data synchronization tools to bypass DLP and other network security controls
  - Applications are digitally signed
  - Most DLP can't inspect their traffic
  - The traffic looks "normal" from the NSM perspective

Cloud Data Sharing - OneDrive

- Windows 10 includes OneDrive by default when you use a Microsoft Online login
  - Most organizations don’t use OneDrive extensively
  - But many/most organizations allow (e.g. don’t disallow) BYOD

- OneDrive is not usually the choice of attackers
  - Due to its ubiquity, more endpoint security solutions monitor it
  - But in networks with very tight whitelisting controls, it is usually still allowed since it is signed by Microsoft

Bonus - Skype

- Do you use Skype as part of your internal communications workflow?
  - Attackers (and insiders) can use Skype to exfiltrate data
  - Very few endpoint products detect file sharing through Skype (and other platforms)

- Attackers may also use unsolicited Skype messages to get malicious files into the network
  - While Microsoft performs some antivirus checking of files, it appears to be signature based – files are not detonated in a sandbox

Cloud Data Sharing – Case Study

- An attacker compromised user credentials through social engineering and used this to access a virtual desktop environment remotely (VDI)
- The VDI allowed only applications that were digitally signed by a trusted certificate but also had decent EPP software installed
- Attackers used a portable copy of “Yandex Disk” and exfiltrated **hundreds of gigabytes** of data from the public file share before the attack was discovered

RENDITION INFOSEC
Cybersecurity by any legal means

Questions?

[redacted]