10 Things That Make a Hacker's Life Easy

David Anderson

CliftonLarsonAllen

CLAconnect.com

Intro/Summary

I am going to share with you:

1. whoami
2. “10 things” that make it easy for hackers
3. Popular Phishing Attacks
4. Key defensive strategies to mitigate risks

whoami

David Anderson

- Farm kid turned hacker
- Working in IT/IT Security for 8 years
- Yes, I am older than 18

10 Things That Make It Easy…

Same issues, over and over…

1. Email Filtering

- Attackers abuse default mail configurations
  - Spoof internal email addresses
  - Send malicious attachments
  - Reply-To address different than source address

1. Poor Email Filtering

- Email was created in 1982
- Was not designed with security
- Two main components relevant to spoofing emails
  - SMTP Envelope
  - SMTP Letter (Message)

1. Email Filtering

1. Email – Defensive Strategy

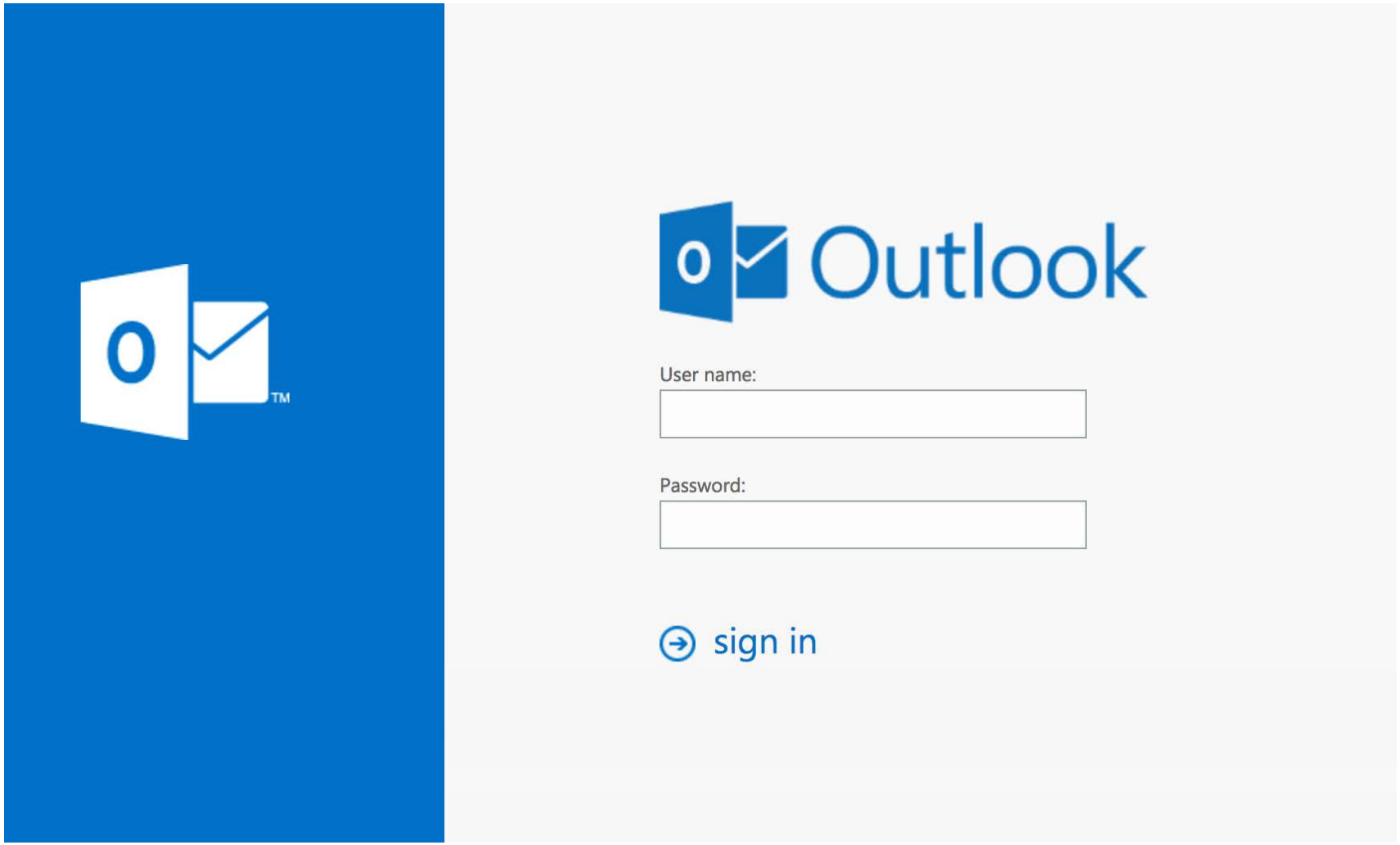
- Harden spam filter
  - Block emails that impersonate employees
  - Block all attachments that are not authorized by management
  - Add a warning to emails that originate from the Internet

2. Two-Factor Authentication

- Many organizations don't implement two-factor authentication (2FA) on all external services
  - Webmail
  - VPN
  - Etc.

- 2FA
  - Something you know (i.e. username and password)
  - Something you have (i.e. hard or soft token)
  - Something you are (i.e. biometrics)

2. Two-Factor Authentication



2. 2FA – Defensive Strategy

- Implement and require 2FA on *ALL* external services that employees use
- Offer 2FA for customer services
- Implement robust logging and alerting on these services

3. Filtering on Perimeter

- Organizations need to restrict what users can access on the Internet
  - Domain whitelisting
  - Egress filtering
  - SSL/TLS inspection

3. Filtering on Perimeter

- Do staff have the ability to:
  - Use Dropbox, OneDrive, Google Drive, etc.
  - Connect to any external FTP/SFT server
  - Download programs over HTTPS

3. Perimeter Filtering – Defensive Strategy

- Block websites not needed for business
  - In Web Filter, block “Unknown” category
- Block ports not needed for business
  - Usually, only HTTP and HTTPS are needed
- Implement SSL/TLS inspection
  - Sites that you do not want to decrypt can be whitelisted

4. Giving User Admin Rights

- Users can install/uninstall software
- Malware can steal passwords from the computer
- Malware can propagate much easier

4. Admin Rights – Defensive Strategy

- Remove admin rights from all users

- Users who need admin rights
  - Provision 2nd account
  - Ensure users don't browse web or check email as an administrator

5. Administrator Hygiene

- IT Administrators don't follow best practices
  - Don't use separate user accounts
  - Browse the web and check email with admin account
  - Log into workstations with privileged account

5. Admin Hygiene – Defensive Strategy

- Create policies that govern how administrators protect their privileged user accounts
- Technically enforce these policies where practical
  - I.e. Prevent admin accounts from logging into workstations
- Audit privileged user accounts

6. IT Sharing Passwords

- It is common for IT departments to reuse passwords
  - Local administrator account on Windows systems
  - Employee's user account and administrator account
  - Service accounts

6. Sharing Passwords – Defensive Strategy

- Implement Microsoft Local Administrator Password Solutions (LAPS)
  - Randomizes the local admin password
- Enforce stronger password requirements for administrative accounts
- Look into password managers **
  - Make sure to use two-factor authentication
  - Do not use password manager from account you browse web or check email

7. Weak Passwords

- 90% of assessments we abuse weak passwords
  - Sprint2017
  - CompanyName
  - Password1234567890

- Employees aren't trained to understand good password hygiene

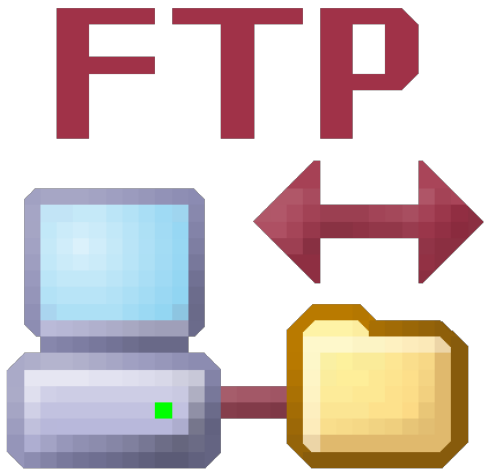
- We can crack *ANY* 8 character Windows password in ~1 day

7. Weak Passwords

- Train employees how to pick strong **passPHRASES**
  - Pick 3 random words/objects around you
  - Add some complexity
  - Understand length is more important than complexity
  - E.g. FedEx Lamp*Scissors?

8. Weak Encryption

- We see many systems configured to utilize protocols with weak encryption or no encryption at all
  - FTP
  - Telnet
  - HTTP
  - Etc.



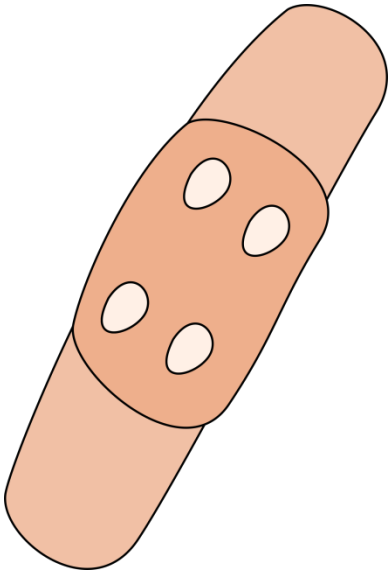
- Attackers can easily intercept sensitive information as it is transmitted

8. Weak Encryption – Defensive Strategy

- Audit network for weak encryption
  - Scan for FTP, Telnet, HTTP, etc.
  - Free tools
    - Nmap
- Turn on secure alternative
  - SFTP, SSH, HTTPS, etc.

9. Poor Patching

- Keeping everything up-to-date is difficult
  - Need to evaluate all systems for patches, not just Windows computers
  - Often find legacy systems people are too afraid to touch
  - Who is responsible for patching vendor systems on your network?



9. Poor Patching - Defensive Strategy

- Scan network for missing patches
  - Patch management solution, Nessus, Nexpose, Qualys, OpenVAS, etc.
- Document known exceptions and implement mitigating controls
  - I.e. stricter firewall rules
- Review vendor contracts
  - Ensure the vendor system will get patches installed in a timely manner

10. End Users

- Attackers spend a lot of time going after employees
  - Often they are the weakest link in the security program

- Most of the success in our assessments are the result of social engineering
  - Email phishing
  - Phone calls

10. End Users – Defensive Strategy

- Users are the first line of defense

- Train users on
  - Notifying personnel of suspicious emails/activity
  - Train users on how to identify phishing messages
  - Train users not to trust links/attachments they were not expecting

Popular Phishing Attacks

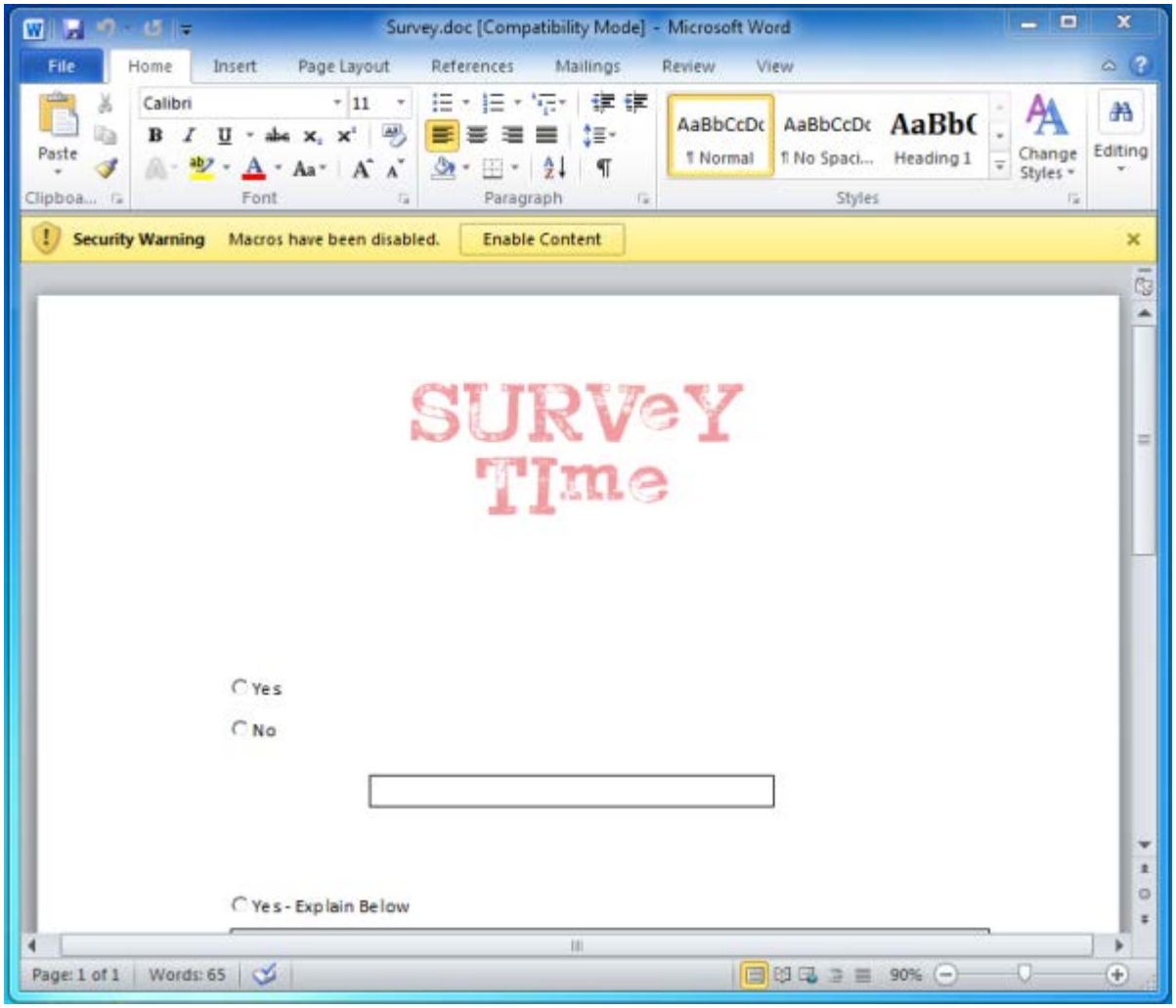
Please send me everyone's W2's

K…thx…bye…

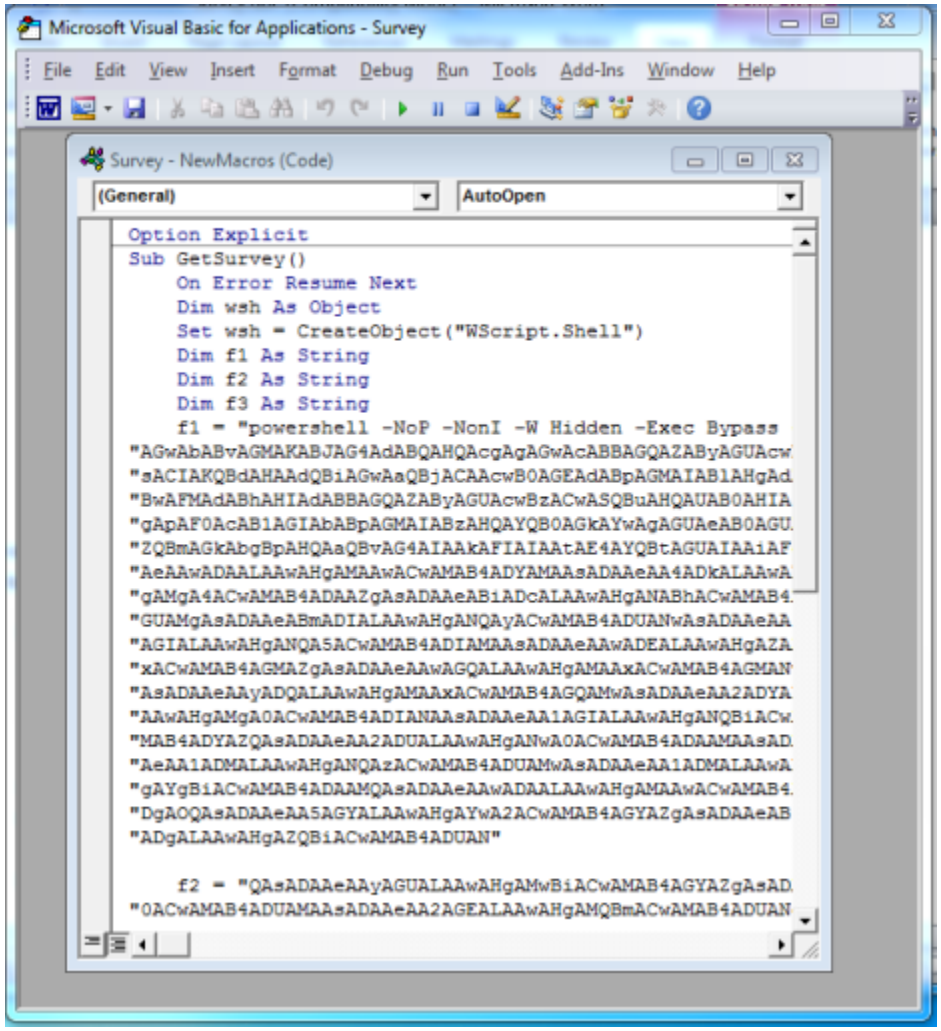
Office Macros

- Macros allow attackers to access any applications/features that are installed or available on the user's workstation
- Utilizing PowerShell, attackers can execute malicious code easily
- Common way attackers deliver ransomware

Office Macros



Office Macros



Office Macros

- **How to protect yourself…**

- Use Group Policy to disable macros
  - Office 2016 and 2013has new Macro security features to block macros in docs that came from Internet

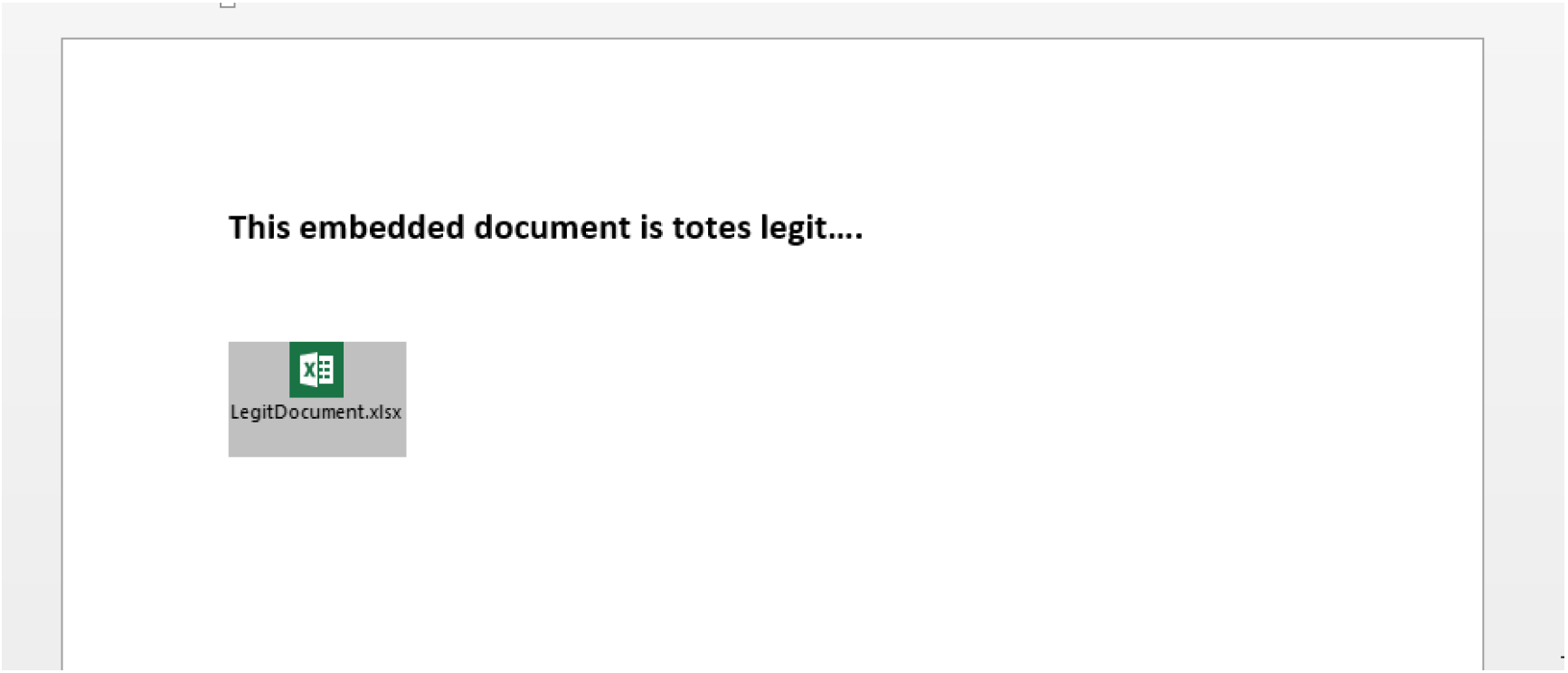
- Teach users who utilize Macros the dangers of opening unknown documents

Office OLE

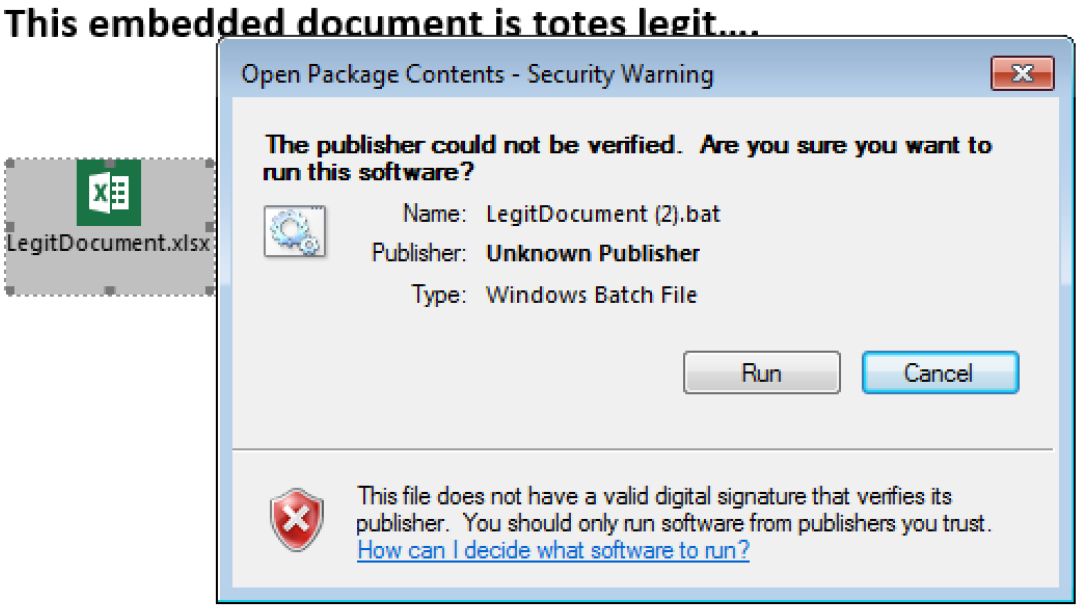
- Object Linking and Embedding
  - Can embed objects (i.e. malicious scripts) in Office documents

- Attackers change filename and icon to trick users

Office OLE

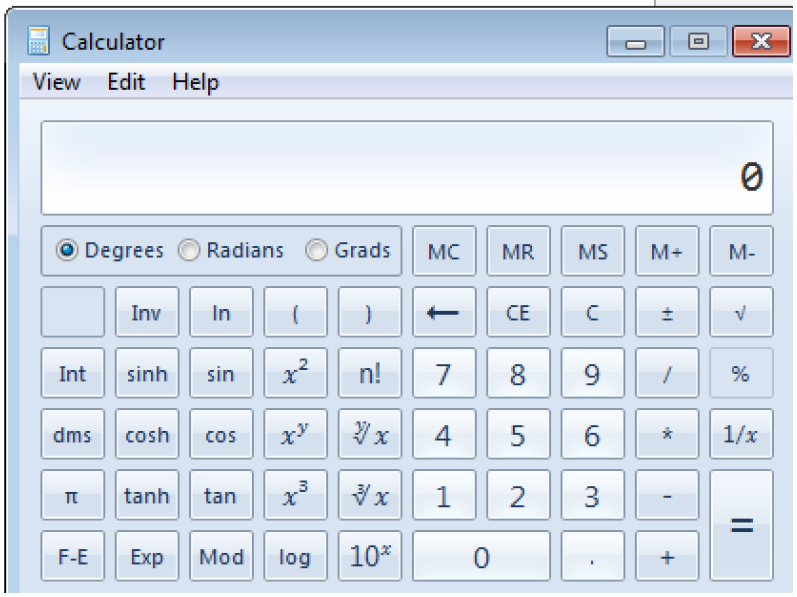


Office OLE



Office OLE

This embedded document is totes legit....



Office OLE

- How to protect yourself…
- Modify registry key:
  - *HKCU\Software\Microsoft\Office\<Office version>\<Office application>\Security\PackagerPrompt*
    - ◊ The Office version values should be:
    - ◊ 16.0 (Office 2016)
    - ◊ 15.0 (Office 2013)
    - ◊ 14.0 (Office 2010)
    - ◊ 12.0 (Office 2007)
  - 0 – No prompt from Office when user clicks, object executes
  - 1 – Prompt from Office when user clicks, object executes
  - 2 – No prompt, Object does not execute

Questions

Thank you!

David Anderson

Manager, Information Security

612-376-4699

david.anderson@claconnect.com