

A decorative shield with a sword and a red banner. The shield is silver with gold rivets and a gold border. A sword with a brown hilt is positioned vertically in front of the shield. A red banner with gold lettering is draped across the shield.

THE LEGEND OF

# Windows Registry Forensics

A LINK TO THE PAST

Jason Killam

@killamjr

# Intro

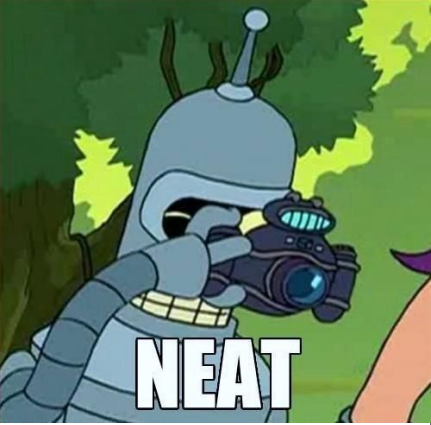
- Work at Jack Henry and Associates for three years in Digital Forensics and Incident Response (DFIR)
  - Mostly performing forensics on live machines
- SANS GCFA, GCFE
- Nine Years in the Marines as a Data Network Specialist.
- Currently an Air Force Reservist working as a Cyber Warfare Specialist
- IT Support for my parents

# What is the Registry?

- The windows registry is basically the location where settings for programs are stored for windows.
- Older versions of windows prior to 3.1 used individual .ini files for each program
- Data is stored in folder like structures called keys
- Keys contain entries for data, such as startup settings and recently opened files and folders.
- Root Keys: contain data for the machine.
  - HKLM – local machine data
  - HKU – user data
  - HKCU – data for the current user



# Registry



Registry Editor

File Edit View Favorites Help

Computer\HKEY\_CURRENT\_USER\Environment

	Name	Type	Data
Computer	(Default)	REG_SZ	(value not set)
HKEY_CLASSES_ROOT	OneDrive	REG_SZ	C:\Users\jkillam\OneDrive
HKEY_CURRENT_USER	Path	REG_EXPAND_SZ	C:\Users\jkillam\AppData\Local\Programs\Python\Python...
AppEvents	TEMP	REG_EXPAND_SZ	%USERPROFILE%\AppData\Local\Temp
Console	TMP	REG_EXPAND_SZ	%USERPROFILE%\AppData\Local\Temp
Control Panel			
Druva			
Environment			
EUDC			
InstTransferWC			
Keyboard Layout			
Network			
Printers			
Software			
System			
CurrentControlSet			
GameConfigStore			
Uninstall			
Volatile Environment			
HKEY_LOCAL_MACHINE			
BCD00000000			
HARDWARE			
SAM			
SECURITY			
SOFTWARE			
SYSTEM			
WindowsAppLockerCache			
HKEY_USERS			
HKEY_CURRENT_CONFIG			



# File Locations

- NTUSER.dat – contains user specific data
  - C:\Users\{UserName}\NTUSER.DAT
  - NTUSER.dat.LOG files contain transactional data not yet written

```
C:\Users\jkillam>dir ntuser* /a
Volume in drive C is Default
Volume Serial Number is 4AB3-44E5

Directory of C:\Users\jkillam

05/01/2018  04:04 PM                12,058,624 NTUSER.DAT
04/17/2018  02:22 PM                 3,072,000 ntuser.dat.LOG1
04/17/2018  02:22 PM                 3,170,304 ntuser.dat.LOG2
04/20/2018  04:23 PM                 65,536 NTUSER.DAT{9c915c
04/20/2018  04:23 PM                524,288 NTUSER.DAT{9c915c
04/17/2018  02:22 PM                524,288 NTUSER.DAT{9c915c
04/17/2018  02:48 PM                  20 ntuser.ini
05/01/2018  09:38 AM                 53,022 ntuser.pol
               8 File(s)      19,468,082 bytes
               0 Dir(s)  58,368,913,408 bytes free
```

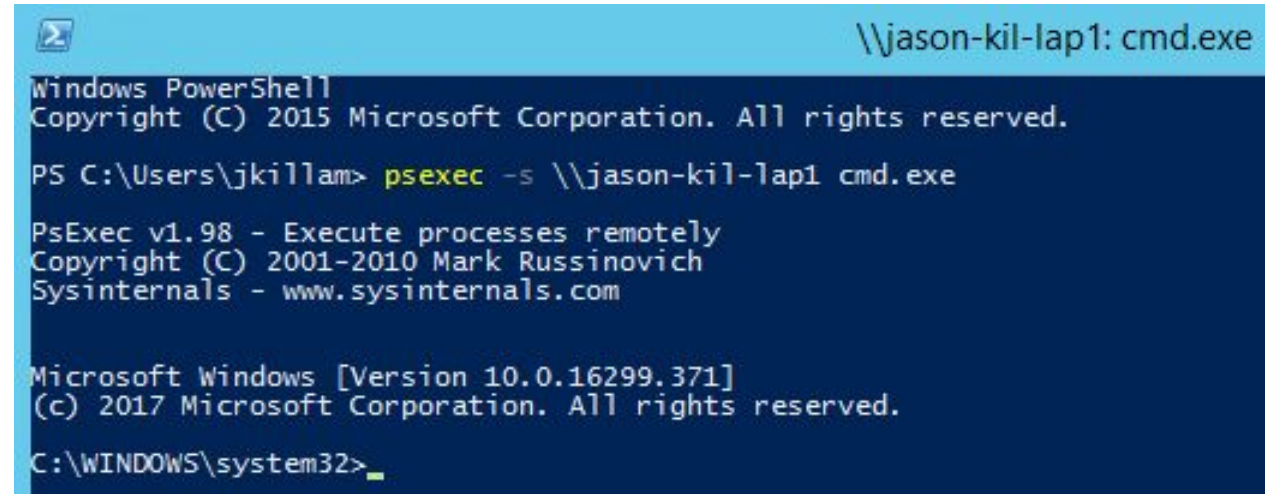
- SOFTWARE, SAM, SECURITY, SYSTEM – contains the HKLM subkey data
  - C:\Windows\System32\config
  - RegBack Contains backed up settings

```
Directory of c:\windows\system32\config

04/26/2018  07:15 AM      <DIR>      .
04/26/2018  07:15 AM      <DIR>      ..
04/20/2018  10:43 PM           524,288 BBI
04/17/2018  05:14 PM      <DIR>      bbimigrate
04/17/2018  05:19 PM           28,672 BCD-Template
04/26/2018  07:15 AM       40,108,032 COMPONENTS
04/20/2018  10:43 PM       4,456,448 DEFAULT
04/25/2018  10:01 AM       8,388,608 DRIVERS
04/20/2018  10:46 PM       131,072 ELAM
09/29/2017  08:46 AM      <DIR>      Journal
04/26/2018  02:09 PM           1,336 netlogon.ftl
09/29/2017  08:46 AM      <DIR>      RegBack
04/17/2018  05:14 PM           40,960 SAM
04/20/2018  10:43 PM           81,920 SECURITY
04/20/2018  10:43 PM       155,713,536 SOFTWARE
04/20/2018  10:43 PM       28,311,552 SYSTEM
09/29/2017  08:46 AM      <DIR>      systemprofile
04/20/2018  10:41 PM      <DIR>      TxR
04/17/2018  05:08 PM           8,192 userdiff
09/29/2017  08:44 AM           4,096 VSMIDK
               13 File(s)     237,798,712 bytes
               7 Dir(s)  35,835,891,712 bytes free
```

# PSEXEC vs PowerShell Remoting

- The easiest way to gather information from a live host is with a remote shell
- PSEXEC/cmd can be preferable if you are used to using regular command prompt
- PowerShell remote shell sessions are usually considered a little bit better since tools like mimikatz can be used to extract creds



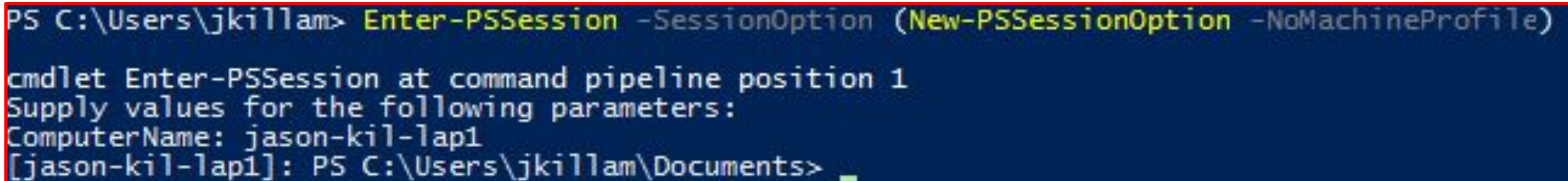
```
\\jason-kil-lap1: cmd.exe
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\jkillam> psexec -s \\jason-kil-lap1 cmd.exe

PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Version 10.0.16299.371]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>
```



```
PS C:\Users\jkillam> Enter-PSSession -SessionOption (New-PSSessionOption -NoMachineProfile)

cmdlet Enter-PSSession at command pipeline position 1
Supply values for the following parameters:
ComputerName: jason-kil-lap1
[jason-kil-lap1]: PS C:\Users\jkillam\Documents>
```



# regedit and reg query

- Reg query with /f lets you search for keywords
- Connect to remote computers with File>Connect Network Registry and give it the target computer name or IP
- Opening HKU>Security Identifier (SID) is the same thing as HKCU

```
PS C:\> reg query "hkcu\software\microsoft\office\16.0\Word\Reading Locations" /f "Open Cmd" /s

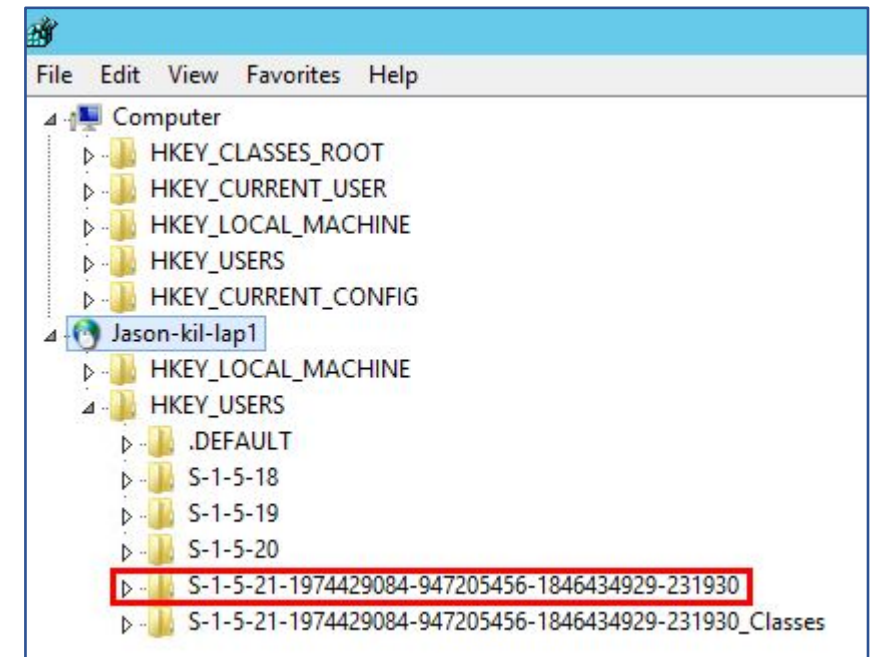
HKEY_CURRENT_USER\software\microsoft\office\16.0\Word\Reading Locations\Document 17
    File Path    REG_SZ        C:\Users\jkillam\Desktop\Tools\Test Docs\Macro - Open Cmd.docm

HKEY_CURRENT_USER\software\microsoft\office\16.0\Word\Reading Locations\Document 30
    File Path    REG_SZ        C:\Users\jkillam\Desktop\Tools\Test Docs\password Macro - Open Cmd.docm

End of search: 2 match(es) found.
PS C:\> reg query "hkcu\software\microsoft\office\16.0\Word\Reading Locations\Document 17"

HKEY_CURRENT_USER\software\microsoft\office\16.0\Word\Reading Locations\Document 17
    File Path    REG_SZ        C:\Users\jkillam\Desktop\Tools\Test Docs\Macro - Open Cmd.docm
    Datetime     REG_SZ        2018-04-25T13:41
    Position     REG_SZ        0 0

PS C:\>
```



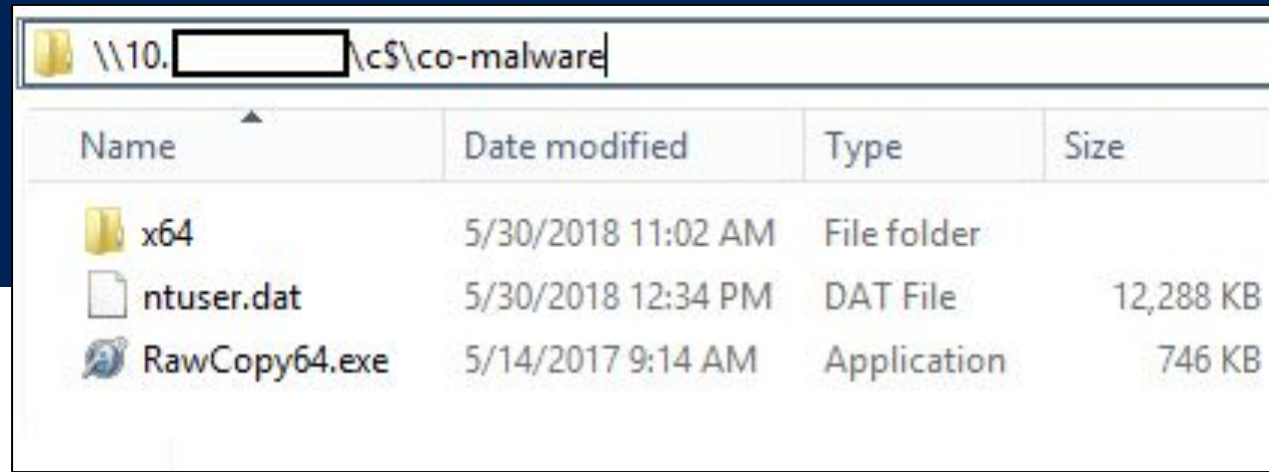
# Collecting Files From Live Hosts

- Since these files will always be in use on an active host you won't be able to copy/paste.
- RawCopy gets around this and can be run from the command line
- Raw copy must be run locally, once its run it can be transferred easily over the network across a file share

```
PS C:\co-malware> .\RawCopy64.exe /FileNamePath:c:\users\jkillam\ntuser.dat /OutputPath:c:\co-malware
RawCopy v1.0.0.18

Writing: ntuser.dat

Job took 2.9 seconds
PS C:\co-malware>
```

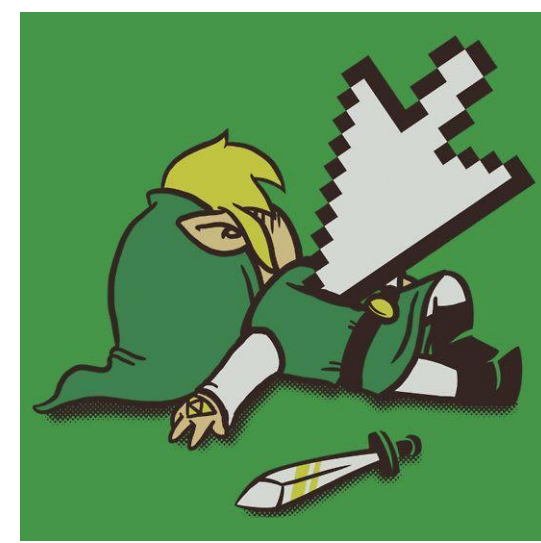


Name	Date modified	Type	Size
x64	5/30/2018 11:02 AM	File folder	
ntuser.dat	5/30/2018 12:34 PM	DAT File	12,288 KB
RawCopy64.exe	5/14/2017 9:14 AM	Application	746 KB

<https://github.com/jschicht/RawCopy>



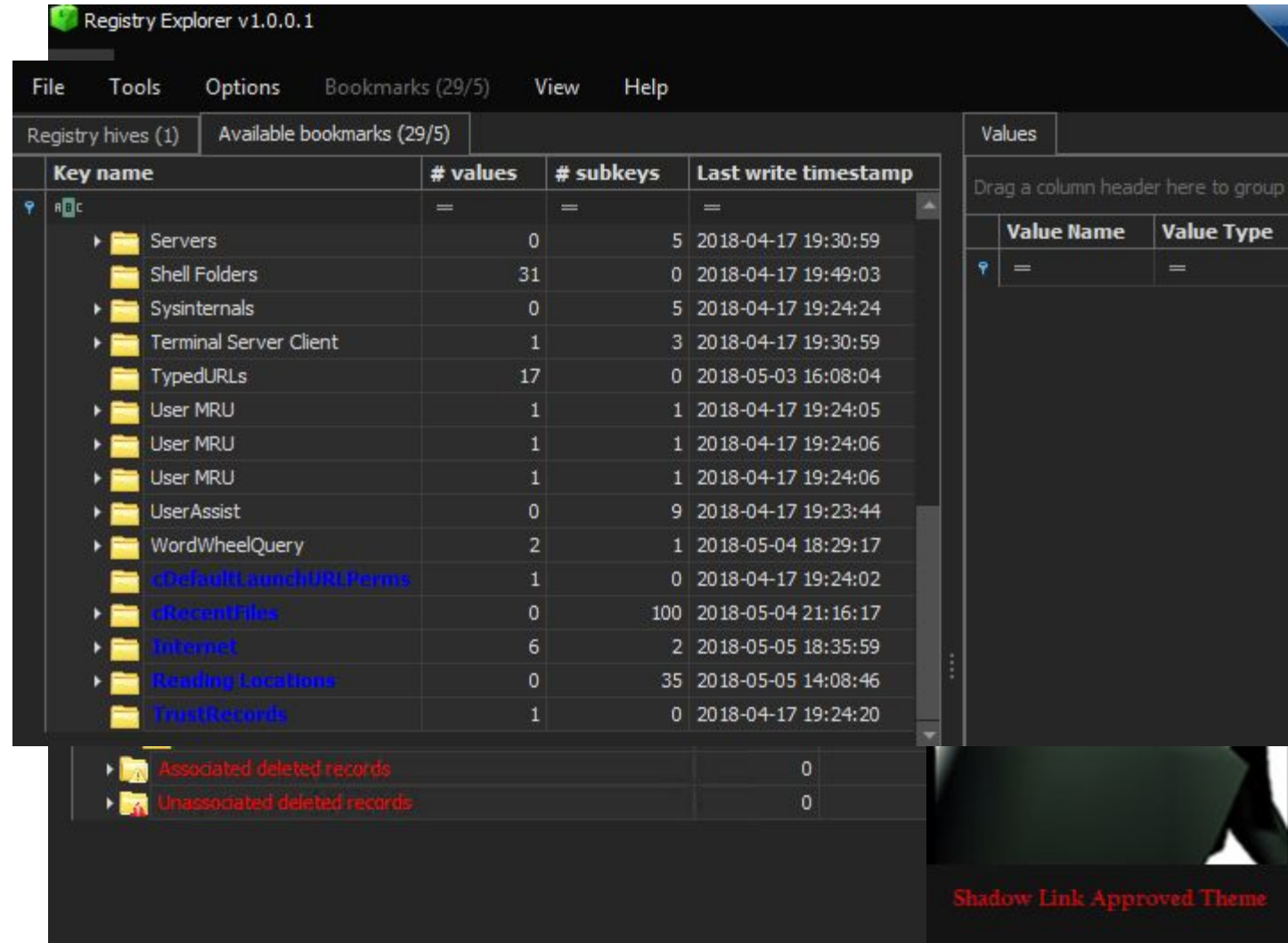
# Tools to View Registry Files



- Tools for live machines:
  - **Regedit** – Great for visually viewing keys and data
  - **Reg** – works from command line remote sessions, much faster at queries.
  - **Get-RegistryKeyLastWriteTime** – Powershell script, retrieves a timestamp from a specific machine key
    - Search “Boe Prox” Registry timestamp
- Tools for offline machines/exported files
  - **Registry Explorer** – Import registry files and dynamically search
  - **RegRipper** – Collects different keys of interest, useful for when you don’t know what you’re looking for
  - Many Others

# Registry Explorer

- Created by Eric Zimmerman
- Makes searching registry files super easy, very customizable
- Make sure to collect LOG files to update the transactional data
- Can search using simple strings, Regex, a time window and much more.
- Search results can be dynamically sorted and organized



<https://ericzimmerman.github.io/>

# Registry Explorer Queries

Find

OptionsHelp

Standard

Search for  
[0-9]{2,3}\.[0-9]{2,3}\.[0-9]{2,3}\.[0-9]{2,3}\.w2\.pdf

History

Search in

☒ Key name☒ Value name☒ Value data☒ Value slack

Search type

☐ Simple☒ Regular expression

☐ Literal

Last write timestamp

Earliest (UTC)  
2018-04-16 02:00:00

Latest (UTC)  
2018-05-25 21:00:00

☐ Before☒ Between☐ After

Search

Minimum value size

Minimum size (bytes)  
512

Search

Base64 in values

Minimum length  
50

Search

NOTE: Unassociated deleted records are not searched in this version

Results (Double click a row in the Results grid to select the search hit in the main window)

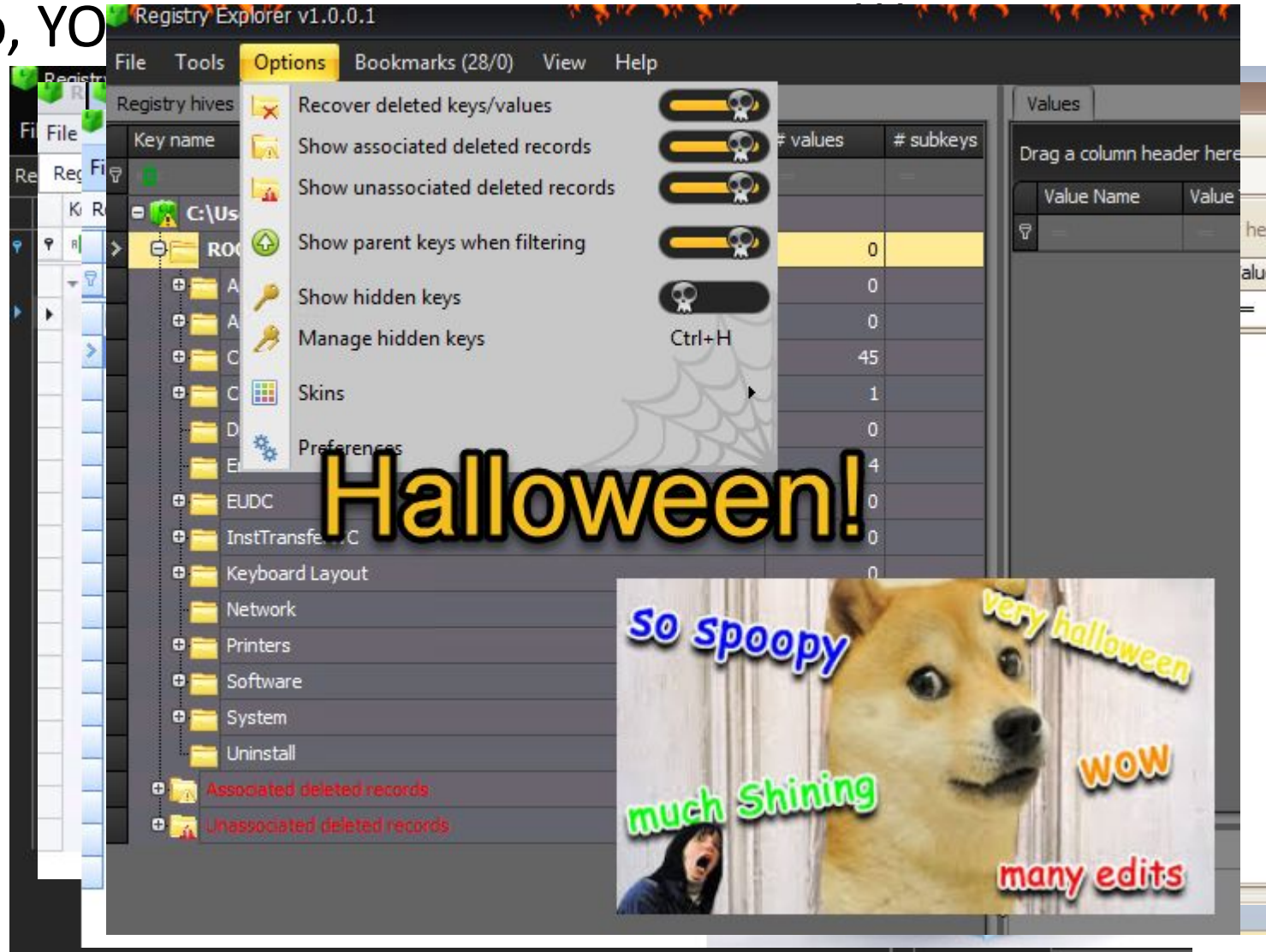
Hit Text

Hive Name	Hit Location	Last Write Time	Key Path	Value Name	Value Data
REG	REG	=	REG	REG	REG
Hit Text: w2\.pdf (Count: 2)					
NTUSER_Updated.dat	Value data	2018-05-04 21:16:17	Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c38	tFileName	w2.pdf
NTUSER_Updated.dat	Value data	2018-05-04 21:16:17	Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c38	tDIText	/C:/Users/jkillam/Downloads/w2.pdf
Hit Text: [0-9]{2,3}\.[0-9]{2,3}\.[0-9]{2,3}\.[0-9]{2,3} (Count: 16)					
NTUSER_Updated.dat	Value data	2018-04-17 19:24:24	Software\SimonTatham\PuTTY\Sessions\Default%20Settings	HostName	172.27.11.248
NTUSER_Updated.dat	Value data	2018-05-05 13:48:35	Software\RegisteredApplications	AppX83g3wajb0za3ry5gr1bem9kgh7wx0dee	Software\Classes\Local Settings\...
NTUSER_Updated.dat	Value data	2018-05-05 14:09:08	Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU	y	\\192.168.100.110\homes\jason\1
NTUSER_Updated.dat	Value data	2018-05-05 03:19:18	Software\Microsoft\Internet Explorer\GPU	AdapterInfo	vendorId="0x8086",deviceID="0...
NTUSER_Updated.dat	Value data	2018-04-17 19:24:03	Software\McAfee\SystemCore\VSCore\Alert Client	IP	172.27.226.81
NTUSER_Updated.dat	Value data	2018-05-05 18:12:08	Software\LogMeInInc\GoToMeeting	EGWAddress	216.115.208.230
NTUSER_Updated.dat	Value data	2018-04-20 13:12:03	Software\Citrix\GoToMeeting	EGWAddress	216.115.208.230
NTUSER_Updated.dat	Value name	2018-05-04 19:19:24	Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	_Common_JHAVPN_na_res - Go to 216.116....	46-00-00-00-50-01-00-00-01-00-...
NTUSER_Updated.dat	Value name	2018-04-17 19:30:59	Software\Microsoft\Terminal Server Client\LocalDevices	172.17.41.44	69



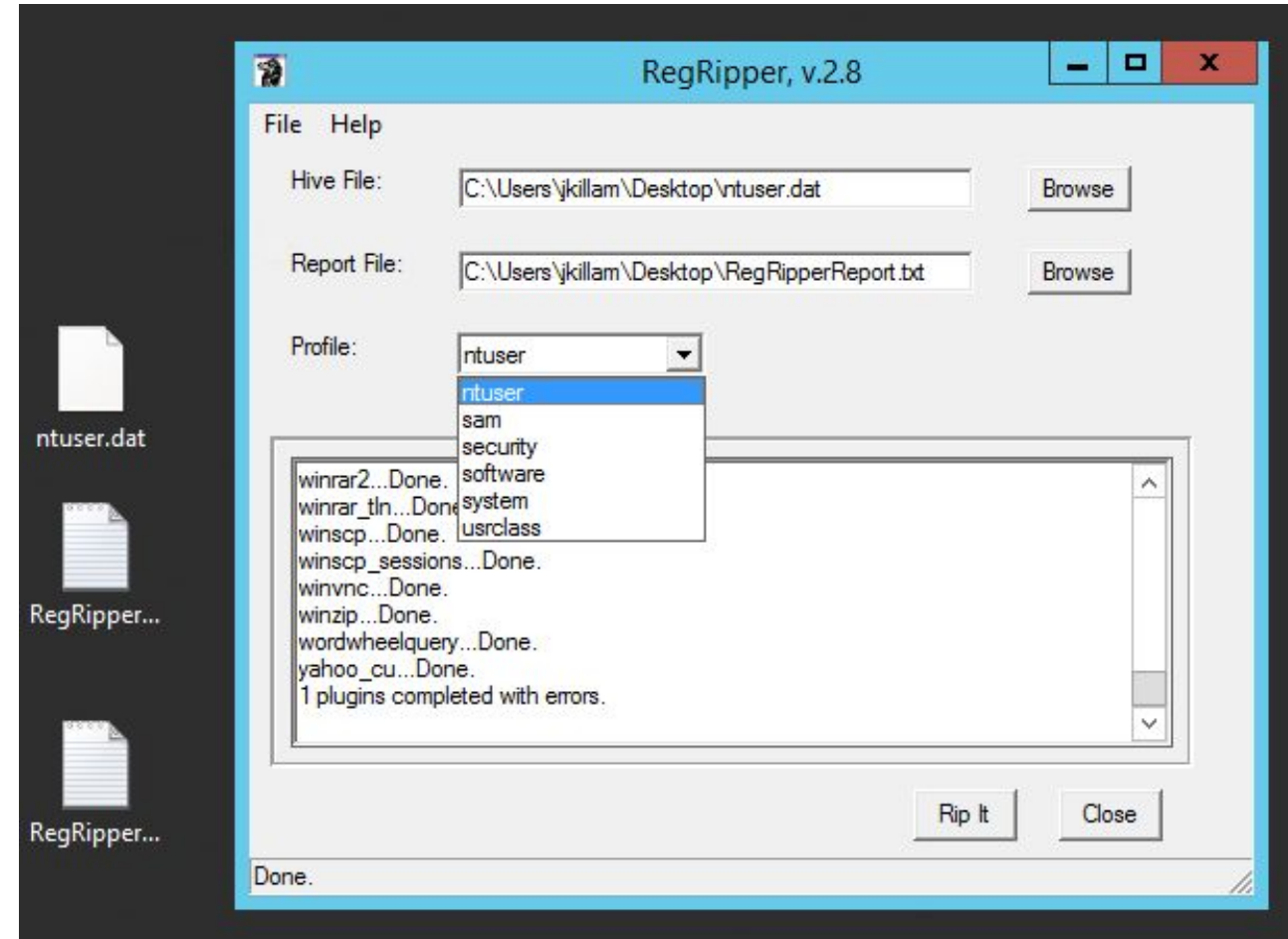
# Registry Explorer (cont.)

- Also, YO



# RegRipper

- Created by Harlan Carvey
- Creates a text report of a registry file
- Great tool for when you want to pull out the “Greatest Hits” or common registry information that might be of interest.
- Helpful for when you need a starting point.



<https://github.com/keydet89/RegRipper2.8>

# Some Examples We'll Go Over

- PDF Phishing
- Word Macros
- URLs clicked from Office



# Reg Keys of Interest for PDFs

- Lots of phishing links are delivered by single link pdfs
- When a link is clicked Adobe Reader, the domain is added to a “Trusted Hosts” lists which is great for proving a user clicked on a link to a phishing domain
  - `HKCU\SOFTWARE\Adobe\Acrobat Reader\DC\TrustManager\cDefaultLaunchPerms`
- cRecentFiles Reg key prove that a user opened the pdf
  - `HCKU\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles`
- Each subkey contains an entry for a file opened and a timestamp

# Opened PDFs

- Key contains subkeys with entries for each file
- Contains the file location, timestamp
- Each key entry always contains a system timestamp as well

Values

Drag a column header here to group by that column

	Val...	Val...	Data	Value Slack
📌	ABC	ABC	ABC	ABC
	aFS	Re...	DOS	80-68-0B-00
	tDI...	Re...	/C/Users/jkillam/Downloads/w2.pdf	
	tFil...	Re...	w2.pdf	0B-00-48-5F-0B-00
	tFil...	Re...	local	
	sFil...	Re...	5B-5D-00	
	sDI	Re...	2F-43-2F-55-73-65-72-73-2F-6A-6B-69-6C-6C-61...	74-75
▶	sDate	Re...	44-3A-32-30-31-38-30-33-31-36-30-37-30-35-31...	65-78-74-00
	uFil...	Re...	126820	
	uPa...	Re...	4	

....

Type viewer

Slack viewer

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000

44 3A 32 30 31 38 30 33 31 36 30 37 30 35 31 39

00000010

2D 30 35 27 30 30 27 00

D: 20180316070519

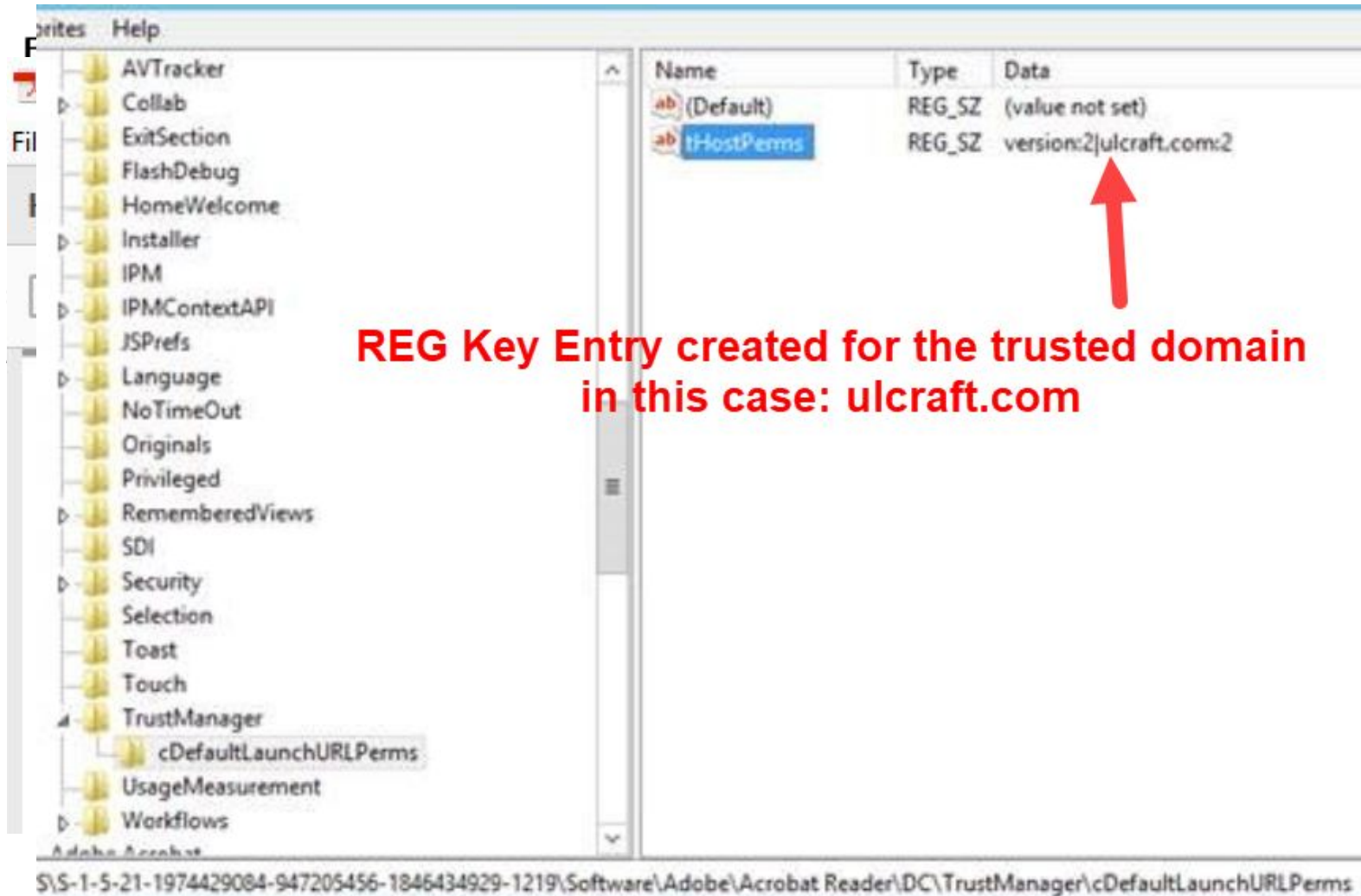
- 05' 00' .

Location:

HCKU\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles

# PDF Phishing Link

1. User Receives email from the "Help Desk"
2. User Opens PDF
3. A prompt from Adobe Reader DC prompts the user if they want to open the URL
4. Reg Key is written to recording the user "Trusted" site



*links from an unknown or suspicious origin*

ade.

Never trust

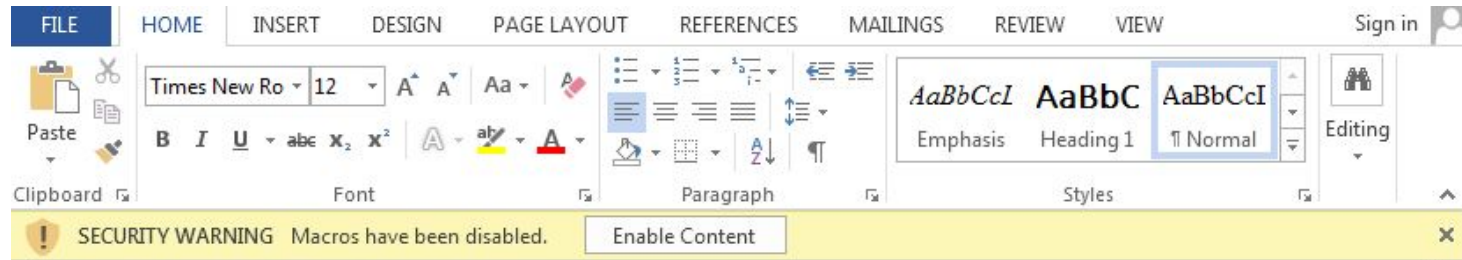


suspicious Links.



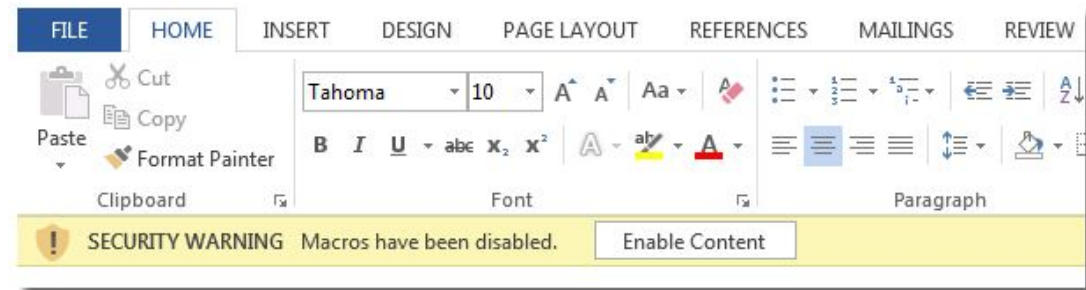
# Malicious Documents

- Most malicious documents usually rely on macros for payload execution
- Registry entries occur when:
  - Being opened
  - Using edit (non-preview mode)
  - Enabling of macros



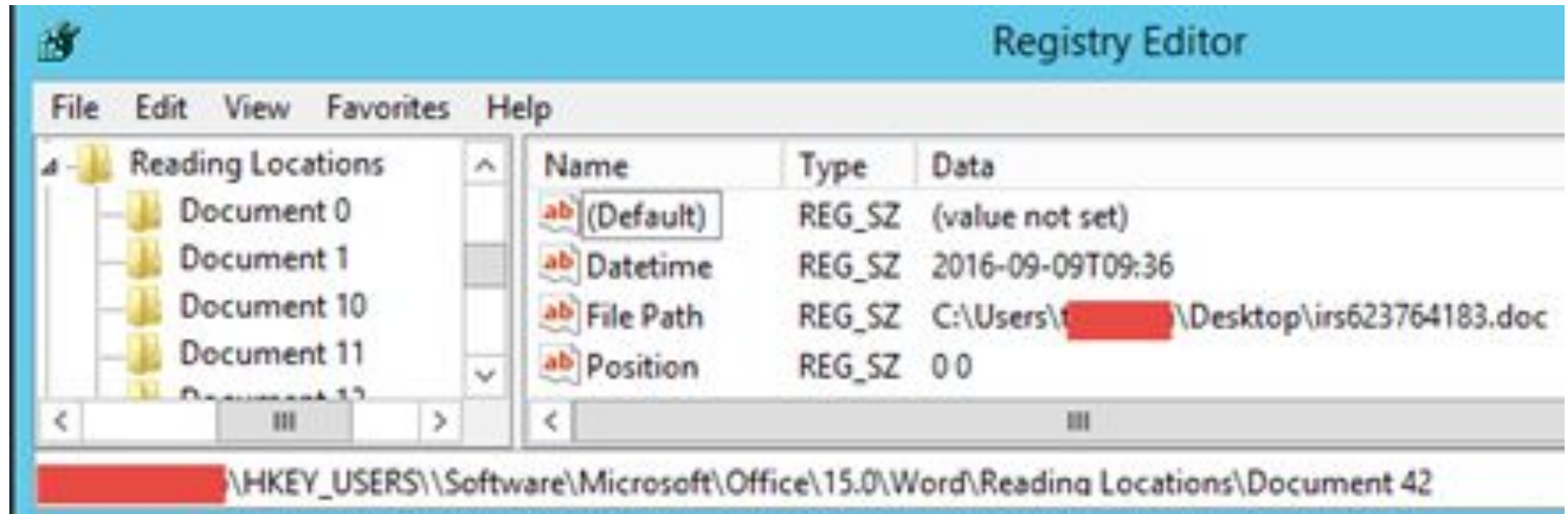
Attention! This document was created by a newer version of [Microsoft Office™](#).  
**Macros must be enabled** to display the contents of the document

To display the contents of the document click “**Enable Editing**” and “**Enable Content**” button



# Opened Documents Reg Keys

- The Reading locations section records the best.
- Recorded Data
  - File path
  - Time last opened



Location:

HKCU\Software\Microsoft\Office\15.0\Word\Reading Locations

# Enabled Macros Reg Keys

- When “Enable Content” is clicked in a document it changes the Value of a file’s data section from all zero’s to “ff ff ff 7f”
- This indicates to Office that the document is “Trusted” and to always enable the content when opened.

Name	Type	Data
ab (Default)	REG_SZ	(value not set)
%USERPROFILE%/Desktop/Example.xlsx	REG_BINARY	d7 71 16 42 1f ba d3 01 00 f8 29 17 d6 ff ff ff 80 cc 82 01 ff ff ff 7f
%USERPROFILE%/Desktop/HIBP/Pwned%20email%20accounts%20-...	REG_BINARY	44 c7 27 ac 47 cc d3 01 00 f8 29 17 d6 ff ff ff 34 65 83 01 01 00 00 00
%USERPROFILE%/Desktop/vss-supertimeline.xlsx	REG_BINARY	ad e5 49 15 f4 66 d3 01 00 90 65 b5 cd ff ff ff c6 73 80 01 ff ff ff 7f
%USERPROFILE%/Desktop/win7-nfury/NFURY-FINAL-TIMELINE.xlsx	REG_BINARY	de c3 32 68 89 68 d3 01 00 90 65 b5 cd ff ff ff 1b 7f 80 01 ff ff ff 7f
%USERPROFILE%/Desktop/WIN7-NROMANOFF-TIMELINE-FINAL.xlsx	REG_BINARY	11 2d e3 9a 62 66 d3 01 00 90 65 b5 cd ff ff ff 04 70 80 01 ff ff ff 7f
file://[REDACTED]/Network%20Security/Security%...	REG_BINARY	37 1a b4 14 d5 84 d3 01 00 90 65 b5 cd ff ff ff a6 3f 82 01 01 00 00 00

Location:

HKCU\Software\Microsoft\Office\16.0\Excel\Security\Trusted Documents\TrustRecords  
HKCU\Software\Microsoft\Office\16.0\Word\Security\Trusted Documents\TrustRecords



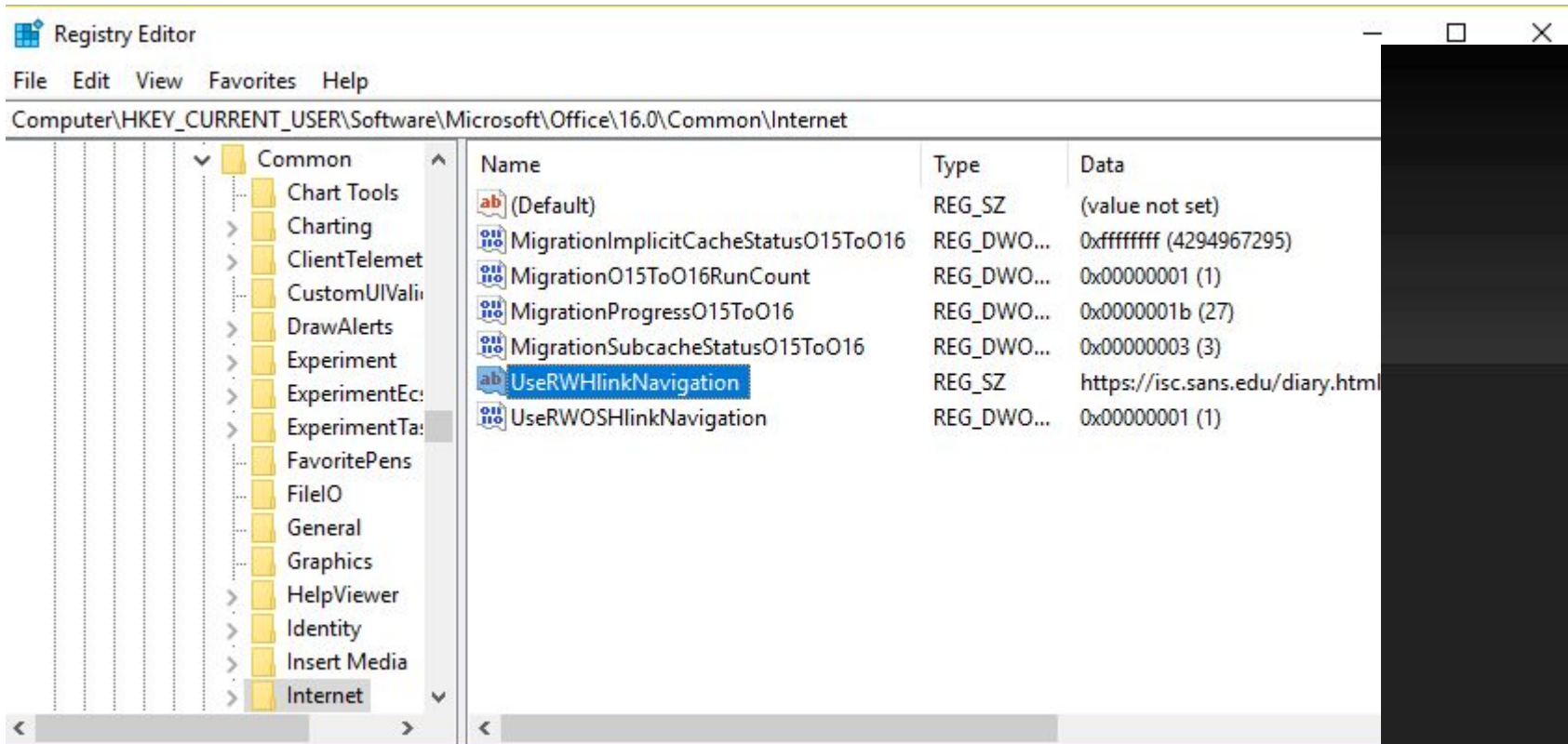
# Phishing Links

- Emails with a link to a phishing site don't leave behind as much evidence on the host compared to other events
- But MS Office records the last link clicked
- Downside - This information is very volatile since its overwritten each time a link is clicked

HKCU\Software\Microsoft\Office\16.0\Common\Internet

# Reg Keys for Clicked Links

- One of the most convenient keys for researching phishing links from emails
- Anytime an link is clicked from an Office application the full URL is recorded



Location:

[HKCU\Software\Microsoft\Office\16.0\Common\Internet](#)

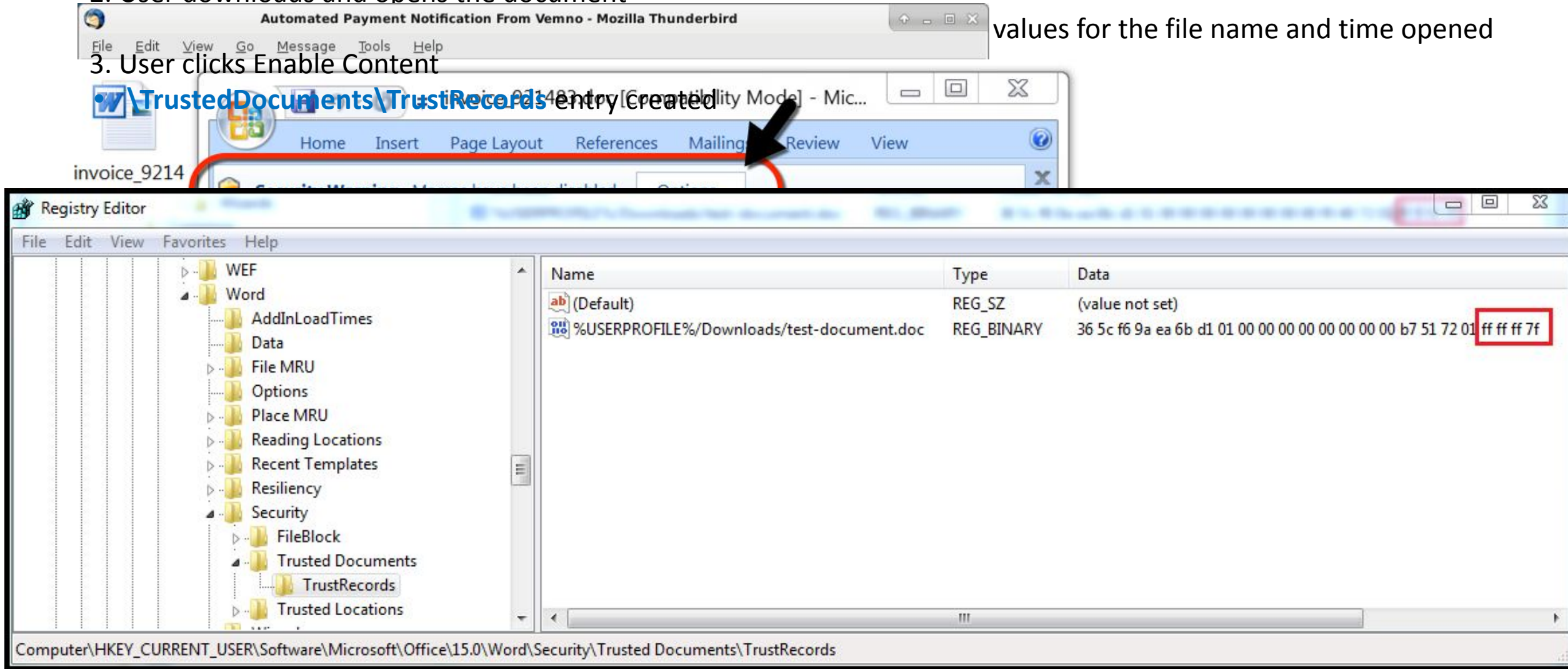
# Malicious Word Doc Timeline

1. User receives an email and clicks on the link from the email
  - `\Common\Internet UseRWHlinkNavigation` Key is written to with the URL
2. User downloads and opens the document

values for the file name and time opened

3. User clicks Enable Content

• `\TrustedDocuments\TrustRecords` entry created



# Summary

- Some key data be very volatile, so collect data as soon as possible
- Make sure you're looking in the correct Hive
  - The subkeys for some Hives can look very similar initially
- Delete any files you're creating on the host, since this might cause the user to get confused or suspicious
- PSEXEC with cmd can be easier to work with if you're used to the regular command prompt
  - Also viewing the recycle bin on works from a traditional command prompt
- PowerShell remote sessions have handier features like autocomplete
  - It's safer to use since mimikatz can't export creds
  - Commands are logged



Questions?