

Lab 1.6 User Activity Profiling via NTUSER.DAT

Teoría y Práctica



Analizando la actividad de archivos de los usuarios: **NTUSER.DAT**

Win7 Search History



Localización

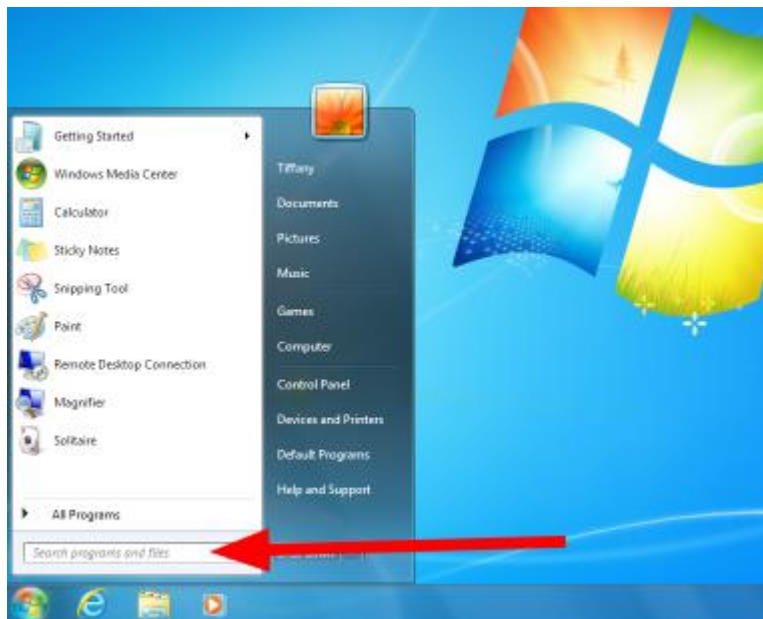
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

Aunque Windows Vista no tiene ningún valor de búsqueda registrado en el registro, Windows 7 y Windows 8/10 sí lo hacen.

La clave del registro llamada "**WordWheelQuery**" se ha encontrado a partir de Windows 7 en adelante. **WordWheelQuery** registrará las búsquedas históricas de programas y archivos en la máquina.

La consulta de búsqueda puede introducirse en el menú Inicio o en la barra de búsqueda de la vista de carpetas del Explorador en el lado derecho de cualquier ventana de vista de carpeta del Explorador.

Ser capaz de saber exactamente cuándo un usuario específico buscó un artefacto es extremadamente útil para una investigación. Para Windows 7, además de la barra de búsqueda del Explorador, cualquier búsqueda escrita en el "**Menú de Inicio de Windows**" también se registraría en la clave del registro WordWheelQuery.



Win8/10 Search History



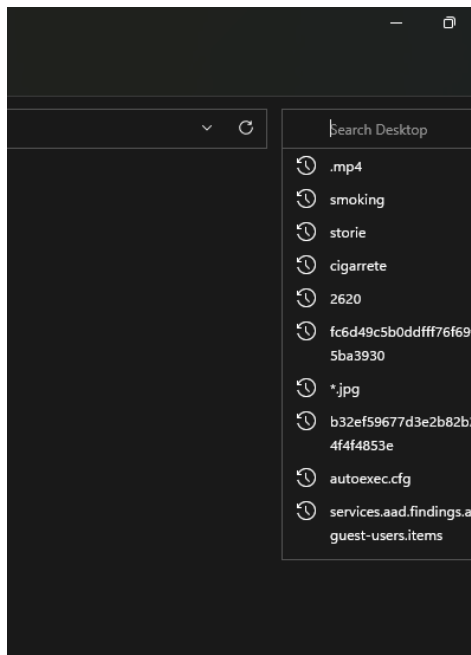
Localización:

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

En Windows 10, WordWheelQuery sigue existiendo, pero está limitado a las búsquedas realizadas a través de la barra de búsqueda del Explorador.

Estas búsquedas recientes se pueden ver (y borrar) seleccionando la pestaña Herramientas de búsqueda en la parte superior de la ventana del Explorador y seleccionando Búsquedas recientes.

Estas búsquedas se registran en orden temporal en la ubicación del registro de Windows 8 WordWheelQuery.



Typed Paths



Localización

`NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths`

Este es un ejemplo de dónde puedes encontrar las "Rutas Escritas/TypePaths" en sistemas Windows 7:

`NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths`

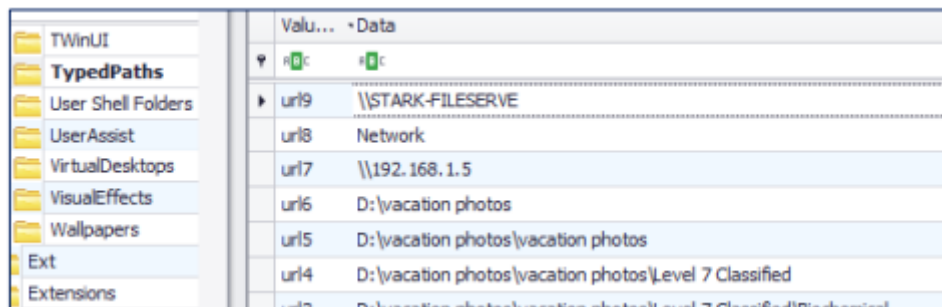
Esta clave mostrará cuándo has escrito manualmente una ruta en el menú Inicio o en la barra de exploración.

Esta clave sería útil en una situación en la que estás tratando de demostrar que el usuario tenía conocimiento específico de una ubicación. Mostrar que el usuario realmente tuvo que escribir o copiar

y pegar la ubicación en el Explorador mostraría conocimiento directo de la ubicación.

Es claro que esta no sería una ubicación accidental a la que el Explorador accedió por sí mismo. Esta clave se ordena automáticamente por más reciente (**con el puesto #1 siendo el más reciente**).

En otras palabras, no hay una clave MRU, pero las rutas parecen mantenerse en orden, **comenzando con el valor url1 siendo el último añadido y url2 siendo el siguiente en orden**. Los valores no se escriben en la clave hasta que se cierra la ventana del Explorador. Por lo tanto, el tiempo de escritura de la clave reflejará cuándo se cerró la ventana del Explorador, no cuándo se escribió la ruta.



Valu... *Data	
url9	\\STARK-FILESERVE
url8	Network
url7	\\192.168.1.5
url6	D:\vacation photos
url5	D:\vacation photos\vacation photos
url4	D:\vacation photos\vacation photos\Level 7 Classified
url3	D:\vacation photos\vacation photos\Level 7 Classified\Biological

RecentDocs via Registry Explorer



File Opening/ Creation

Localizacion

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Los documentos más recientes utilizados en sistemas Windows XP a Windows 10 pueden examinarse fácilmente al observar la clave **RecentDocs**. Esta clave y las subclaves debajo de ella son extremadamente valiosas cuando se busca actividad relacionada con un archivo específico.

Cuando examinamos los valores en bruto de esta clave, estos valores son difíciles de leer. Sin embargo, Registry Explorer puede analizar el contenido de estas claves para que puedan ser fácilmente visualizadas.

Los valores, cuando se muestran a través de un visor, se mostrarán en orden de MRUList. La MRUList muestra el archivo más reciente abierto primero. El archivo que se abrió más atrás en el tiempo se enumerará al final.

# values	Last write time...	Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On
1	2016-10-14 18:0...						
1	2017-01-17 14:4...						
151	2017-01-24 03:1...	.com/	0	support.lenovo.com/	https-support.lenovo.com-.lnk	0	2016-12-29 05:4
2	2017-01-17 22:0...	.png	0	Unbenannt.png	Unbenannt.png.lnk	0	2016-12-29 16:4
2	2017-01-10 00:2...	.1	3	For500_Ex2.1	For500_Ex2.1.lnk	0	2016-12-29 17:3
5	2016-10-17 16:1...	.dotm	0	Normal.dotm	Normal.dotm.lnk	0	2016-12-30 17:2
5	2016-12-29 17:3...	.txt	16	tzworks_log.txt	tzworks_log.txt.lnk	0	2017-01-04 16:1
0	2016-10-10 07:4...	.vmx	4	Windows SIFT Workstation.vmx	Windows SIFT Workstation.vmx.lnk	0	2017-01-09 17:4
0	2016-10-10 07:4...	.csv	7	userassist.csv	userassist.csv.lnk	0	2017-01-09 19:1
2	2016-10-10 07:4...	.JPG	0	DSC01952.JPG	DSC01952.JPG.lnk	0	2017-01-09 23:1
1	2016-10-10 07:4...		0	0004148team-TOM/10/30	20d-COM/TT/11AA&merran-14840	0	2017-01-10 00:2
2	2016-10-10 07:4...						

Este es un ejemplo de la misma información del registro de RecentDocs, pero vista a través de Registry Explorer, lo que es mucho más fácil de interpretar por varias razones:

1. La MRUList se utiliza para crear el orden real en el que se abren los archivos.
2. Puedes ver todos los archivos en una sola lista en lugar de tener que analizar manualmente cada entrada individual.

Microsoft Office File MRU
Cada version de Office se puede encontrar en el registro, unos ejemplos:
<ol style="list-style-type: none"> 1. 15.0 = Office 2013 2. 11.0 = Office 2003 3. 14.0 = Office 2010 4. 10.0 = Office XP 5. 12.0 = Office 2007
NTUSER.DAT\Software\Microsoft\Office\VERSION
Microsoft 365 Versions 16.0 = Office 2016/2019/M365
NTUSER.DAT\Software\Microsoft\Office\VERSION\ \User MRU\LiveID_####\File MRU
NTUSER.DAT\Software\Microsoft\Office\VERSION\ \User MRU\ADAL_####\File MRU

No solo el sistema operativo llevará un registro de los últimos documentos guardados en la clave RecentDocs del usuario, sino que Microsoft Office también mantiene su propio conjunto de datos aún más completo.

Cada versión de Office mantendrá una lista de archivos abiertos dentro de aplicaciones específicas de Office. La ubicación de estos datos está en una clave llamada File MRU. Esta clave enumerará muchos de los documentos, Excel y presentaciones de PowerPoint más recientes que el usuario ha abierto.

Esta lista puede ser bastante extensa e incluso retroceder más en el tiempo que la clave RecentDocs del sistema.

Los datos se almacenan en claves nombradas con los números de versión de Office conocidos. **Una pregunta que a menudo surge es ¿por qué la numeración se detuvo en 16.0?**

Resulta que Microsoft 365 y Office 2016/2019 están contruidos sobre la misma base de código y se diferencian mediante marcas y licencias.

En las instancias de Microsoft 365, la clave del registro para cada aplicación de Office está vinculada directamente a la cuenta de Microsoft del usuario. Si la cuenta es una Cuenta de Microsoft personal, los datos estarán ubicados bajo la clave \User MRU\LiveID_####\File MRU. Si la cuenta es parte de Azure Active Directory (cuentas organizativas o laborales), estará bajo ADAL (Active Directory Authentication Library).

Explorer Common Dialog Box.



Localizaciones:

OpenSaveMRU [**File Opening/Creation**]:

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU

LastVisitedMRU [**ProgramExecution**]

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU

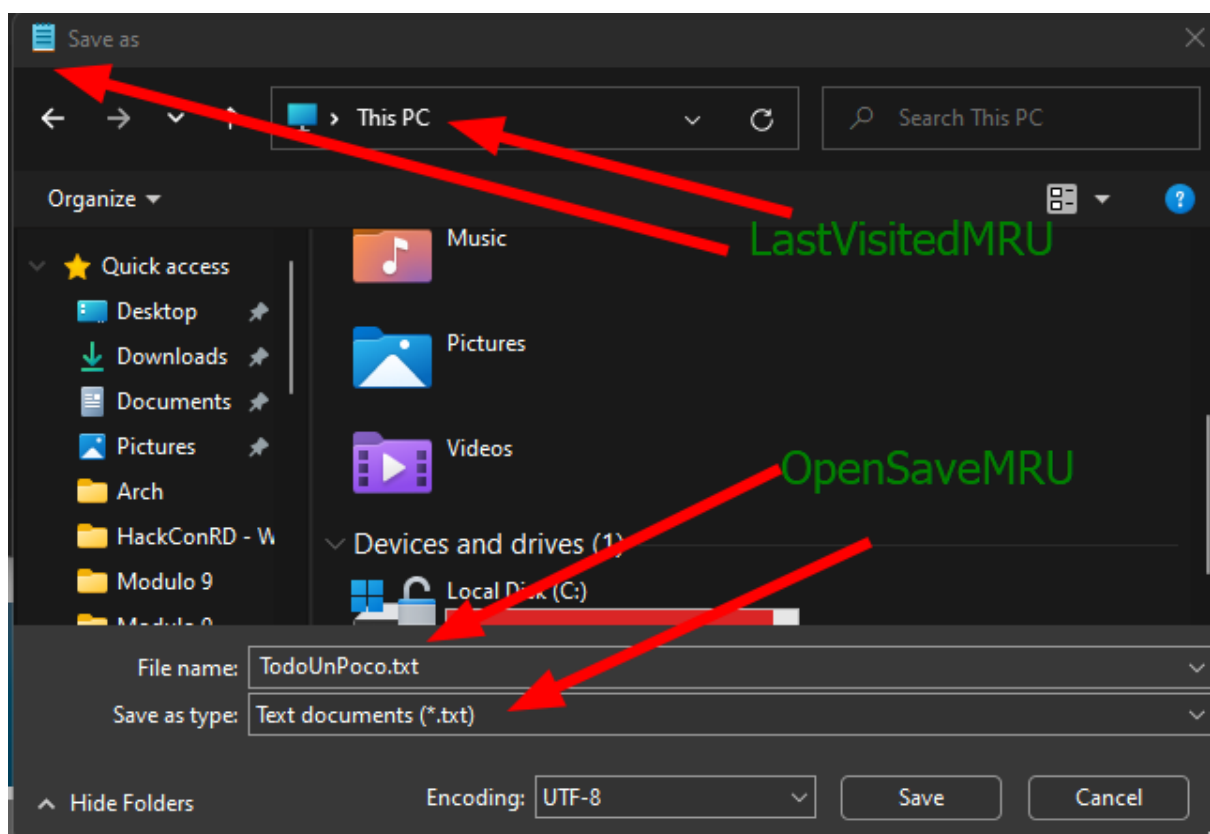
LastVisitedMRU
<ul style="list-style-type: none">• Last path of file opened• Executable used
OpenSaveMRU
<ul style="list-style-type: none">• Save or open dialog box• Last files opened by a specific extension

Windows tiene algunos cuadros de diálogo básicos que todos los programas utilizan rutinariamente. ¿Alguna vez has notado que cuando "guardas o abres un archivo", podríamos recordar la ubicación

donde guardaste o abriste un archivo anteriormente? ¿Has notado que cuando guardas o abres un archivo, hay un cuadro de diálogo desplegable que recuerda tus ubicaciones o archivos abiertos previamente?

Como ejemplo, veamos las claves del **registro OpenSaveMRU y LastVisitedMRU**. Ambas han sido documentadas durante años y son citadas con frecuencia en exámenes.

Hay dos situaciones específicas rastreadas dentro de Microsoft Windows: **LastVisitedMRU y OpenSaveMRU**. OpenSaveMRU y LastVisitedMRU cambiaron significativamente en Windows 8. Hasta que exista una mejor capacidad, **YARU** es una de las mejores opciones para examinar el contenido del hexadecimal dentro de estas claves y valores.



Lab 1.6

NTUSER.DAT Analysis



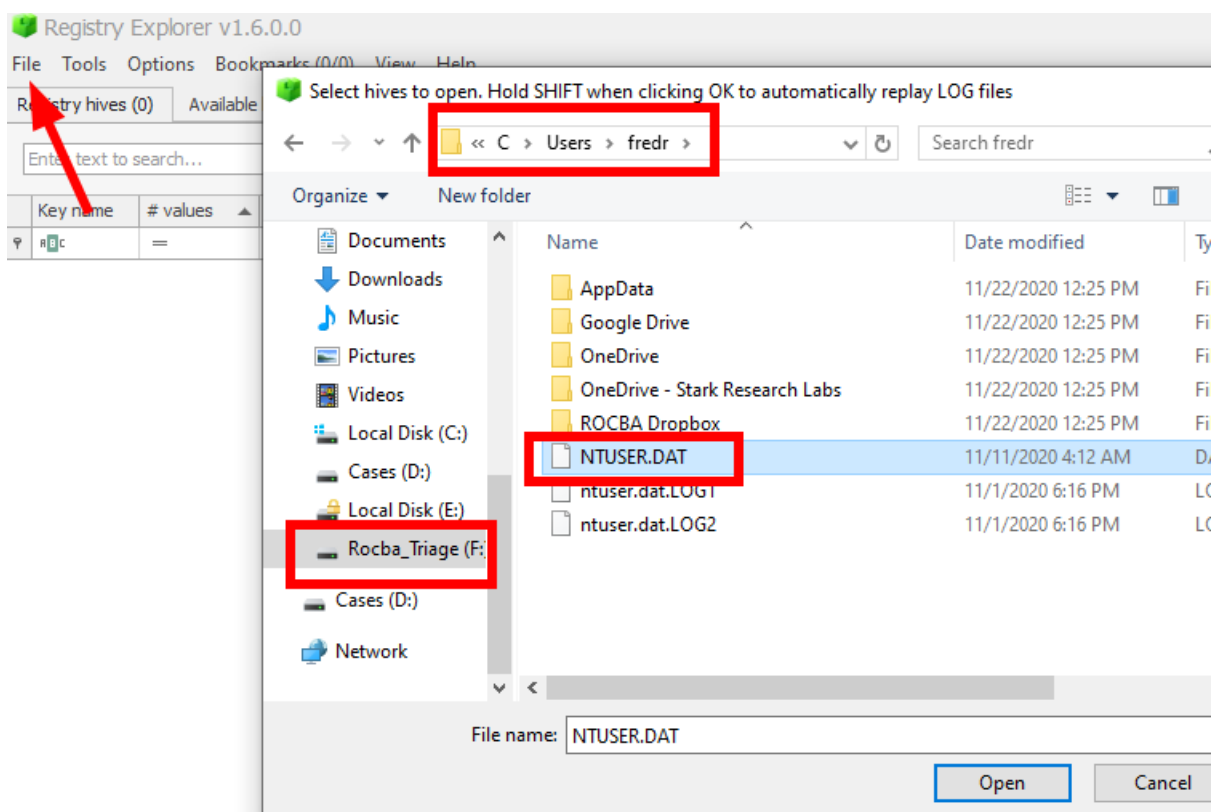
Objetivos:

El archivo hive NTUSER.DAT está lleno de artefactos extremadamente interesantes y rastreables, y **cada usuario en el sistema tiene uno**. Es importante destacar que esto significa que podemos diferenciar actividades entre cada una de las cuentas de usuario en Windows. Un análisis adecuado del hive NTUSER.DAT de cada usuario permitirá a un investigador identificar la ejecución de programas, la apertura de archivos, la apertura de carpetas y mucho más.

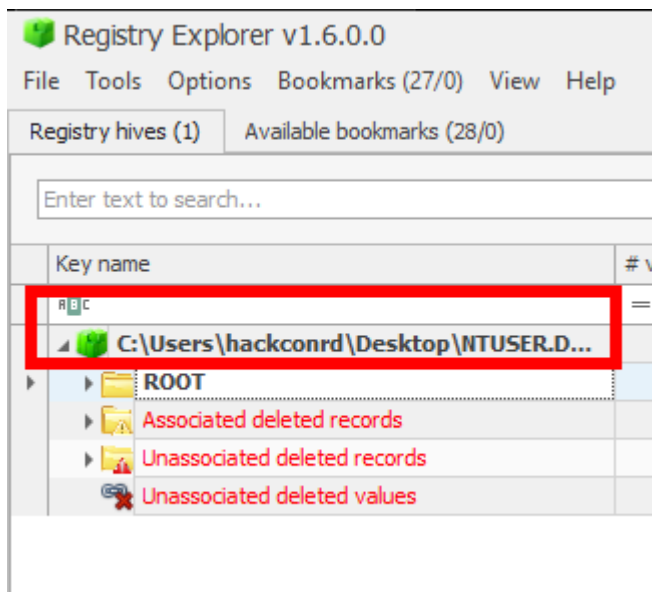
NTUSER.DAT puede contener una gran cantidad de información importante.

- Encuentra artefactos asociados con la Evidencia de Apertura de Archivos y Carpetas, como las claves RecentDocs, OpenSaveMru y ComDlg32.
- Aprende a identificar términos de búsqueda y rutas de archivos que el usuario escribió en el sistema a través de las claves TypedPaths y WordWheelQuery.
- Perfil de actividad de la cuenta e identifica comportamientos del usuario.

Con la evidencia montada (Triage evidence) tal cual en los otros ejercicios, procedemos a abrir el Registry Explorer y cargar el hive NTUSER.DAT : C\Users\fredr\NTUSER.DAT



Si hay Dirty Hive, procederemos a seguir los pasos para obtener un clean hive, quedaría así :



WordWheelQuery Key:

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

Revisa las búsquedas escritas por la cuenta de Fred Rocba. **¿Qué términos de búsqueda podrían ser relevantes en una investigación de robo de datos?**

No hay respuestas correctas o incorrectas para esta pregunta. Sin embargo, los elementos más recientes en la lista (ordenados por posición en la lista MRU) parecen ser particularmente relevantes. Alguien estaba buscando archivos PST de Outlook, incluido un PST específico llamado **backup.pst**. Se realizó una búsqueda de **sdelete**, el nombre de una herramienta muy común de destrucción/borrado de datos. Las búsquedas sobre **Bitlocker** indican que puede haber cifrado presente en el sistema. Y los otros términos podrían volverse más relevantes a medida que aprendamos más sobre lo que sucedió en este sistema.

Registry hives (1) Available bookmarks (28/0)				Values WordWheelQuery	
Enter text to search... Find				Drag a column header here to group by that column	
Key name	# values	# subkeys	La	Search Term	Mrv Position
SearchPlatform	0	1		backup.pst	0
StartupApproved	0	2		backup	1
Streams	0	1		*.pst	2
TWinUI	0	1		sdelete	3
UserAssist	0	9		bitlocker recovery key	4
VisualEffects	0	19		bitlocker	5
AutoplayHandlers	1	5		cobra	6
BitBucket	1	1		crimson	7
DiskSpaceChecking	1	0		airwolf	8
ExtractionWizard	1	0		kitt	9
FeatureUsage	1	5		starfury	10
OperationStatusManager	1	0			
Package Installation	1	0			
Shutdown	1	0			
StuckRects3	1	0			
VirtualDesktops	1	0			
CabinetState	2	0			
LogonStats	2	0			
StartPage	2	0			
TabletMode	2	0			
Accent	3	0			
Ribbon	3	0			
TypedPaths	3	0			
Taskband	5	1			
Wallpapers	7	1			
WordWheelQuery	12	0			
User Shell Folders	22	0			
Advanced	28	1			

¿Qué término de búsqueda tiene asociada una marca de tiempo?
¿A qué hora se ejecutó esa búsqueda?

- Aunque WordWheelQuery no mantiene marcas de tiempo para sus valores, sí tiene una marca de tiempo, que es la última vez que se escribió la clave en sí misma. Dado que la clave contiene una lista de uso más reciente (MRU), sabemos que la búsqueda más reciente realizada está presente en la posición MRU 0. Por lo tanto, esa búsqueda se realizó en el momento en que se escribió por última vez WordWheelQuery.
- Se buscó backup.pst el 2020-11-14 a las 14:04:07 UTC.

File Tools Options Bookmarks (27/0) View Help				
Registry hives (1)		Available bookmarks (28/0)		
Enter text to search...		Find		
	# values	# subkeys	Last write timestamp	
Wallpapers	7	1	2020-11-02 14:33:45	
WordWheelQuery	12	0	2020-11-14 14:04:07	
User Shell Folders	22	0	2020-11-02 13:01:46	
Advanced	28	1	2020-11-14 04:59:26	
Shell Folders	31	0	2020-11-02 13:01:47	
RecentDocs	129	21	2020-11-16 02:32:19	
ContentDeliveryManager	18	6	2020-11-06 04:40:11	
ApplicationAssociationToasts	385	0	2020-11-14 03:58:02	
	0	3	2020-11-01 22:18:32	
etPC	0	2	2020-11-01 22:16:40	
ogon	0	1	2020-11-02 13:02:13	
ows Error Reporting	1	1	2020-11-14 04:38:19	
	11	0	2020-11-02 14:22:45	
s Defender Security Center	0	1	2020-11-01 22:17:05	
s NT	0	1	2020-11-01 22:16:40	
s Search	0	2	2020-11-02 14:21:01	
s Security Health	0	1	2020-11-01 22:17:05	

Values WordWheelQuery	
Drag a column header here to group by that column	
Search Term	
backup.pst	0 V
backup	1 V
*.pst	2 V
sdelete	3 V
bitlocker recovery key	4 V
bitlocker	5 V
cobra	6 V
crimson	7 V
airwolf	8 V
kitt	9 V
starfury	10 V

TypedPaths Key:

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths

TypedPaths identifica las ubicaciones escritas por el usuario en la barra de direcciones del Explorador de archivos de Windows. Sin embargo, parece que esta función fue utilizada solo de manera esporádica en este sistema.

¿Qué tienen en común todas las entradas?

Toda contienen **“My Drive”**

Value Name	Value Type	Data
url1	RegSz	G:\My Drive\STARK-RESEARCH-LABS FOLDER\SRL-Projects - Gunstar
url2	RegSz	G:\My Drive\STARK-RESEARCH-LABS FOLDER
url3	RegSz	G:\My Drive

¿Cuál es la entrada más reciente de TypedPaths? ¿A qué hora fue utilizada?

TypedPaths no mantiene una lista MRU, pero sí mantiene sus entradas en orden por nombre de valor. En esta clave, url1 es el elemento más reciente.

G:\Mi unidad\CARPETA DE STARK RESEARCH LABS\Proyectos SRL - Gunstar fue utilizada por última vez como TypedPath el **2020-11-14 a las 04:43:37 UTC**.

Registry hives (1) Available bookmarks (28/0)			
Enter text to search... Find			
	# values	# subkeys	Last write timestamp
ExtractionWizard	1	0	2020-11-14 13:41:19
FeatureUsage	1	5	2020-11-01 22:18:32
OperationStatusManager	1	0	2020-11-14 14:00:21
Package Installation	1	0	2020-11-14 03:52:10
Shutdown	1	0	2020-11-11 08:13:46
StuckRects3	1	0	2020-11-10 12:00:22
VirtualDesktops	1	0	2020-11-11 08:13:47
CabinetState	2	0	2020-11-01 22:18:32
LogonStats	2	0	2020-11-02 13:01:43
StartPage	2	0	2020-11-01 22:18:32
TabletMode	2	0	2020-11-02 14:26:58
Accent	3	0	2020-11-02 14:22:45
Ribbon	3	0	2020-11-10 12:00:22
TypedPaths	3	0	2020-11-14 04:43:37
Taskband	5	1	2020-11-03 02:05:16
Wallpapers	7	1	2020-11-02 14:22:45
WordWheelQuery	12	0	2020-11-14 14:04:07
User Shell Folders	22	0	2020-11-02 13:01:46

Values		
Drag a column header here to group by that column		
Value Name	Value Type	Data
url1	RegSz	G:\My Drive\STARK-RESEARCH-LABS FOLDER
url2	RegSz	G:\My Drive\STARK-RESEARCH-LABS FOLDER
url3	RegSz	G:\My Drive

RecentDocs

Key:

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Los registros de tiempo en la clave RecentDocs se identifican mediante listas MRU y las horas de escritura de las claves del registro.

Debemos recordar que cada clave tiene una marca de tiempo, por lo tanto, cada una de las subclaves de RecentDocs mantiene el tiempo del último archivo de ese tipo que se abrió. Estos registros de tiempo adicionales se recopilan en la columna Última apertura de la extensión en el complemento de documentos recientes de Registry Explorer. Al revisar esta columna, puedes establecer los límites temporales dentro de los cuales múltiples archivos debieron haber sido abiertos.

Revisa la columna Última Apertura de la Extensión e identifica el nombre de archivo relacionado con la marca de tiempo más temprana registrada el 2020-11-14.

Uno de los conceptos más importantes con RecentDocs es entender cómo utilizar las marcas de tiempo disponibles.

Vibrainium(1).doc fue abierto por última vez por el usuario el 2020-11-14 a las 03:59:19 UTC. La clave RecentDocs mantiene el orden de los elementos abiertos a través de su clave MRU. Vibrainium(1).doc ocupa la posición 51 en MRU. Esto significa que los 50 elementos por encima de él en la lista fueron todos abiertos DESPUÉS de él. Por lo tanto, esto nos indica que al menos 51 archivos y carpetas fueron abiertos por la cuenta fredr en este sistema el 2020-11-14 a las 03:59:19 UTC o después. Esa es información muy útil.

Drag a column header here to group by that column						
	Extension	Valu...	Target Name	Lnk Name	Mru ...	Opened On
♀	h[...]	h[...]	h[...]	h[...]	=	=
	RecentDocs	109	Airwolf II.jpg	Airwolf II.lnk	39	
	RecentDocs	86	Files from SRL system	Files from SRL system.lnk	40	
	RecentDocs	0	D:\	SRL IRT (D).lnk	41	
	RecentDocs	79	VC Files	VC Files.lnk	42	
	RecentDocs	78	TIVO Research.docx	TIVO Research.lnk	43	
	RecentDocs	57	starfury	starfury (2).lnk	44	
	RecentDocs	15	StarFury.zip	StarFury.lnk	45	
	RecentDocs	107	Screenshots	Screenshots.lnk	46	
	RecentDocs	46	Screenshot (1).png	Screenshot (1).lnk	47	
	RecentDocs	106	Pictures	Pictures.lnk	48	
	RecentDocs	105	10l_brianlaiphotography-north cotepoint.jpg	10l_brianlaiphotography-north cotepoint.lnk	49	
	RecentDocs	54	Research	Research.lnk	50	
	RecentDocs	30	Vibrainium(1).doc	Vibrainium(1).lnk	51	2020-11-14 03:59:19
	RecentDocs	104	France DGSE Intel Analysis Adamantium .pptx	France DGSE Intel Analysis Adamantium .lnk	52	
	RecentDocs	18	Vibrainium - SRL.docx	Vibrainium - SRL.lnk	53	
	RecentDocs	102	Research to Weaponize the	Research to Weaponize the	54	
Total rows: 235						

El Sr. Rocba se fue de vacaciones el 10 de noviembre de 2020. De los registros de tiempo disponibles en la columna Última Apertura de la Extensión, **¿cuál es el último elemento abierto en ese día?**

La clave de recuperación de BitLocker 1694D560-A615-4ABB-B721-E7C3E884F8BD.TXT fue abierta por última vez por el usuario el 10 de noviembre de 2020 a las 14:23:01 UTC. Pudieron haberse abierto otros archivos en ese mismo día después de este, pero desafortunadamente RecentDocs no mantiene registros de tiempo para cada entrada y esta es una de las pocas veces disponibles para la actividad el 10 de noviembre de 2020.

RecentDocs	37	ms-gamingoverlay-///	ms-gamingoverlay-///.lnk	75	
RecentDocs	19	kgldcheck/	ms-gamingoverlay-kgldcheck-.lnk	76	
RecentDocs	33	Key	Key.lnk	77	
RecentDocs	25	BitLocker Recovery Key 1694D560-A615-4ABB-B721-E7C3E884F8BD.TXT	BitLocker Recovery Key 1694D560-A615-4ABB-B721-E7C3E884F8BD.lnk	78	2020-11-10 14:23:01
RecentDocs	91	Google Drive File Stream (G:)	Google Drive File Stream (G:).lnk	79	
RecentDocs	89	::{D9EF8727-CAC2-4E60-809E-86F80A666C91}	BitLocker Drive Encryption.lnk	80	
Total rows: 235					
					Export

Registry Explorer tiene varias características muy útiles para lidiar con grandes fuentes de datos. Una característica es la capacidad de filtrar en cualquier columna. Encuentra la columna Nombre de Destino en Documentos Recientes y escribe bitlocker en la fila blanca inmediatamente debajo del encabezado de la columna. Esto debería mostrar solo las filas que contienen el término que escribiste.

¿Cuántas claves BitLocker diferentes se abrieron con esta

cuenta? ¿Por qué no tenemos marcas de tiempo disponibles para cada una de estas?

Target Name
BitLocker

Hubo un total de tres archivos de Clave de Recuperación de Bitlocker diferentes abiertos por este usuario:

- BitLocker Recovery Key 1694D560-A615-4ABB-B721-E7C3E884F8BD.TXT
- BitLocker Recovery Key C42458BB-09FE-4232-9086-BA9B3C642E83.TXT
- BitLocker Recovery Key 26F77152-999C-45E8-8BD4-C83FAC7BB72D.TXT

Esto indica al menos tres volúmenes cifrados que podrían estar en uso (o el mismo volumen pasando por múltiples ciclos de encriptación/desencryptación).

Observa que nuestro filtro muestra dos de cada nombre de archivo. Esto se debe a que los datos provienen tanto de la clave "rollup" de RecentDocs como de la subclave .TXT. Recuerda que cada clave solo tiene una marca de tiempo, y esa hora está asociada con el elemento MRU "0" en esa lista. Por lo tanto, solo uno de los archivos clave recibe una marca de tiempo de la subclave .TXT y ninguno de ellos recibe una marca de tiempo de la clave RecentDocs (ya que ninguno es la entrada MRU 0 dentro de la lista de RecentDocs).

Drag a column header here to group by that column							
Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Last Opened	
.TXT	4	BitLocker Recovery Key 1694D560-A615-4ABB-B721-E7C3E884F8BD.TXT	BitLocker Recovery Key 1694D560-A615-4ABB-B721-E7C3E884F8BD.lnk	0	2020-11-10 14:23:01		
.TXT	3	BitLocker Recovery Key C42458BB-09FE-4232-9086-BA9B3C642E83.TXT	BitLocker Recovery Key C42458BB-09FE-4232-9086-BA9B3C642E83.lnk	1			
.TXT	0	BitLocker Recovery Key 26F77152-999C-45E8-8BD4-C83FAC7BB72D.TXT	BitLocker Recovery Key 26F77152-999C-45E8-8BD4-C83FAC7BB72D.lnk	4			
RecentDocs	25	BitLocker Recovery Key 1694D560-A615-4ABB-B721-E7C3E884F8BD.TXT	BitLocker Recovery Key 1694D560-A615-4ABB-B721-E7C3E884F8BD.lnk	78			2020-11-10 14:23:01
RecentDocs	70	BitLocker Recovery Key C42458BB-09FE-4232-9086-BA9B3C642E83.TXT	BitLocker Recovery Key C42458BB-09FE-4232-9086-BA9B3C642E83.lnk	93			
RecentDocs	29	BitLocker Recovery Key 26F77152-999C-45E8-8BD4-C83FAC7BB72D.TXT	BitLocker Recovery Key 26F77152-999C-45E8-8BD4-C83FAC7BB72D.lnk	116			

Office File MRU File MRU Key:

NTUSER.DAT\SOFTWARE\Microsoft\Office\16.0\Word\User MRU\ADAL_71509F4C9F29E24E25306165B32FE79B68FD54A88446B7C792A3A9D5AB6BB5AE\File MRU

Los documentos de Microsoft Office rastreados por las claves File MRU tienen dos ventajas principales sobre la clave RecentDocs: información completa de la ruta y marcas de tiempo para cada entrada.

¿Qué letras de unidad se utilizaron para abrir documentos de Word el 14 de noviembre de 2020?

- G:
- F:

Value Name	Last Opened	Last Closed	File Name
#c	=	=	#c
FOLDERID_Desktop			C:\Users\fredr\OneDrive\Desktop\
FOLDERID_Documents			C:\Users\fredr\OneDrive\Documents\
Item 1	2020-11-14 04:29:50	2020-11-14 04:29:55	G:\My Drive\STARK-RESEARCH-LABS FOLDER\SRL-Projects - Gunstar
Item 2	2020-11-14 03:59:20	2020-11-14 03:59:24	G:\My Drive\STARK-RESEARCH-LABS FOLDER\Research\Vibrainium(1)
Item 3	2020-11-14 03:57:22	2020-11-14 03:57:46	G:\My Drive\STARK-RESEARCH-LABS FOLDER\Research to Weaponize
Item 4	2020-11-14 03:52:45	2020-11-14 03:52:51	F:\Files of interest\SRL-Projects - Megaforce\Megaforce\S
Item 5	2020-11-11 08:14:58	2020-11-11 08:12:03	E:\New Homework\Homework Grade 3.docx
Item 6	2020-11-06 22:44:40	2020-11-05 02:16:32	C:\Users\fredr\Google Drive\BetterWidgets Business Plan\BusinessPl
Item 7	2020-11-03 01:55:22	2020-11-05 02:16:32	C:\Users\fredr\Stark Research Labs\GunStar Death Blossom Data.doc

OpenSavePidlMRU

Clave OpenSavePidlMRUKey:

NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU

La mayoría de los archivos mencionados en OpenSavePidlMRU también están presentes en RecentDocs. Sin embargo, esta es una buena fuente de datos para revisar principalmente porque proporciona

información completa de la ruta, que no está disponible en RecentDocs.

Utiliza la información completa de la ruta disponible aquí para buscar archivos abiertos dentro de Google Drive. Filtra la columna Ruta Absoluta por "MyDrive". ¿Cuántas entradas hay para archivos abiertos o guardados en este conjunto de carpetas? ¿Ves cómo esta información puede ser más valiosa que simplemente los nombres que proporciona RecentDocs?

Cuatro entradas dentro de **OpenSavePidlMRU** hacen referencia a G:\Mi unidad, aunque solo dos archivos están representados debido a que los archivos están duplicados tanto en las subcarpetas * como pst\TXT (ver la columna Extensión en la salida de Registry Explorer).

Extension	Value Name	Mru P...	Absolute Path	Opened On
c	c	=	My Drive	=
TXT	3	0	My Computer\G:\My Drive\Key\BitLocker Recovery Key 1694D5007A613-4AB8-8721-E7C3E884F8BD.TXT	2020-11-10 14:23:01
pst	0	0	My Computer\G:\My Drive\TARK-RESEARCH-LABS FOLDER\Exported+PST\SQL-EMAIL-EXPORT.pst	2020-11-14 14:01:34
*	7	10	My Computer\G:\My Drive\Key\BitLocker Recovery Key 1694D5007A613-4AB8-8721-E7C3E884F8BD.TXT	
*	16	1	My Computer\G:\My Drive\TARK-RESEARCH-LABS FOLDER\Exported+PST\SQL-EMAIL-EXPORT.pst	

Elimina el filtro en la columna Absolute Path ¿Cuál es el último archivo abierto o guardado por este usuario?

My Computer\D:\ROCBA-SYSTEM\Rocba-Memory.raw

La imagen capturada por el equipo de Incident Response

ag a column header here to group by that column

Extension	Value Name	Mru P...	Absolute Path	Opened On
c	c	=	c	=
raw	0	0	My Computer\D:\ROCBA-SYSTEM\Rocba-Memory.raw	2020-11-16 02:32:19
*	17	0	My Computer\D:\ROCBA-SYSTEM\Rocba-Memory.raw	2020-11-16 02:32:19

Ahora intentemos relacionar la información de OpenSavePidlMRU con la información de la aplicación presente en la clave

LastVisitedPidlMRU (solo dos claves arriba de la que estás viendo actualmente). ¿Qué aplicación probablemente abrió o guardó el archivo My Computer\D:\ROCBA-SYSTEM\Rocba-Memory.raw?

Key:

NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

- MRC.exe
- De la pregunta anterior, observa que Rocba-Memory.raw fue abierto o guardado por última vez en la ubicación D:\ROCBA-SYSTEM. Podemos usar esa información para intentar relacionar esta fuente de datos con LastVisitedPidlMRU para ver qué aplicación estuvo involucrada. En esa clave, observa que MRC.EXE abrió o guardó algo por última vez en D:\ROCBA-SYSTEM. ¡Tenemos una coincidencia! Alguna investigación mostraría que la aplicación es "Magnet RAM Capture" y probablemente guardó la imagen de memoria del sistema en el dispositivo extraíble conectado como la unidad D: (las herramientas de dumping de memoria suelen guardar archivos, no abrirlos).

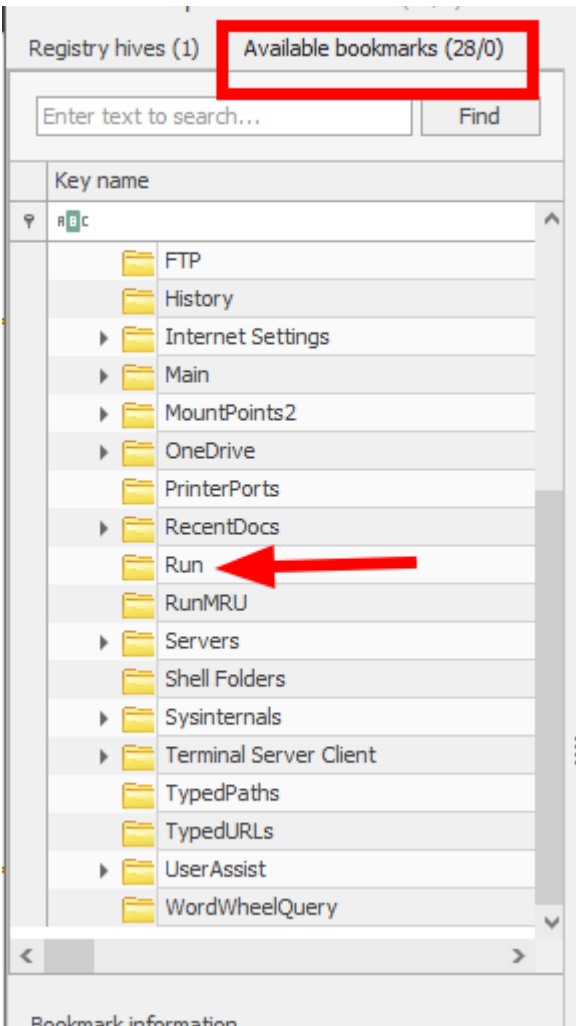
	Executable	Absolute Path	Opened On
0	MRC.exe	My Computer\D:\ROCBA-SYSTEM	2020-11-16 02:32:19
1	{FFF02A95-27D9-4DEF-B1C7-D902F44FFFA8}	My Computer\G:\My Drive\STARK-RESEARCH-LABS FOLDER\Exported-PST	
2	chrome.exe	My Computer\Downloads	
3	msedge.exe	My Computer\Downloads	

Autostart "Run" Keys

Para finalizar este ejercicio, echemos un vistazo a la infame clave "Run" del archivo NTUSER.DAT. Los elementos en esta clave se ejecutan cada vez que el usuario inicia sesión. Por esta razón, esta clave es el lugar más común para que el malware agregue una referencia a sí mismo en un intento de sobrevivir a un reinicio (comúnmente llamado un "mecanismo de persistencia"). Además de buscar malware, esta clave también indica las aplicaciones instaladas por el usuario.

Ya hemos utilizado varios "plugins" que Registry Explorer tiene incorporados para analizar ubicaciones comunes del registro. Registry Explorer mantiene estos plugins y cualquier ubicación guardada generada por el usuario en la pestaña Bookmarks dentro de la herramienta. Esta puede ser una manera fácil de "saltar" a claves de

interés y asegurarse de no olvidar claves que aún no se han revisado. Ve a la pestaña Bookmarks y haz clic en el marcador Run.



Run Key:
NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Drag a column header here to group by that column

	Value Name	Value Type	Data
🔍	NTUSER.DAT	NTUSER.DAT	NTUSER.DAT
	OneDrive	RegSz	"C:\Users\fredr\AppData\Local\Microsoft\OneDrive\One...
	com.squirrel.Teams.Teams	RegSz	C:\Users\fredr\AppData\Local\Microsoft\Teams\Update...
▶	GoogleDriveSync	RegSz	"C:\Program Files\Google\Drive\googledrivesync.exe" /aut...
	C18E42C7363A0E298C5594A2ABE53A0760B71220._service_run	RegSz	"C:\Program Files (x86)\Microsoft\Edge\Application\msed...
	GoogleDriveFS	RegSz	"C:\Program Files\Google\Drive File Stream\43.0.8.0\Goog...

Tenemos hasta ahora:

- Alguien estaba buscando archivos PST, sdelete y BitLocker utilizando la cuenta fredr.
 - backup.pst fue buscado el 14 de noviembre de 2020 a las 14:04:07 UTC.
- Múltiples fuentes de datos indican que Google Drive está presente en el sistema:
 - G:\My Drive_____ \Proyect SRL - Gunstar fue utilizado por última vez como TypedPath el 14 de noviembre de 2020 a las 04:43:37 UTC.
 - Los datos de SRL para GunStar, Vibranium, Ion Thrusters y Megaforce parecen estar presentes en este Google Drive personal.
 - La clave de ejecución NTUSER.DAT indica que tanto Google Drive personal como empresarial (Google Workspace) estaban instalados en el sistema.
- RecentDocs indica que al menos se accedieron a 50 archivos y carpetas el 14 de noviembre de 2020 a las 03:59:19 UTC o después. Esto es durante el tiempo en que el Sr. Rocba estaba de vacaciones y lejos de su sistema.
- Tres claves de recuperación de BitLocker diferentes han sido abiertas por la cuenta fredr.