



CASE #1: Suspicious Employee

Group 6:
Edward, Emily, Musfirah, Haziq



Context Recap

Mark is under the suspicion from the company as he was seen working on **unusual hours** and browsing **random websites** recently. A day before he left, **John** reported a **missing USB storage drive** and was suspicious of Mark. HR decided to initiate an investigation and we got **Mark's registry hives and other files from Marks computer.**



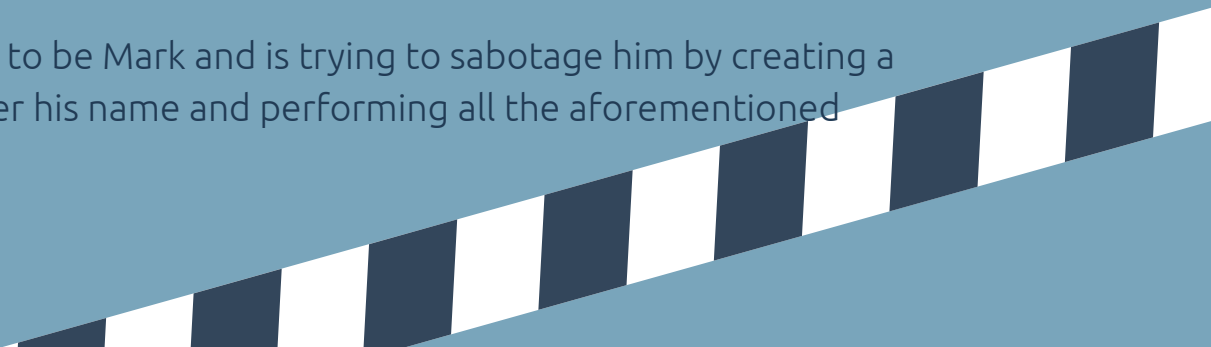


Our hypothesis:

Hypothesis 1 (Suspicious)

- He accessed confidential document from an internal FTP server, accessed a thumb drive and created an Admin account on his laptop at an unusual hour.

Hypothesis 2 (Not suspicious)

- Someone is pretending to be Mark and is trying to sabotage him by creating a computer account under his name and performing all the aforementioned suspicious actions.
- 

Mark's Computer System Information

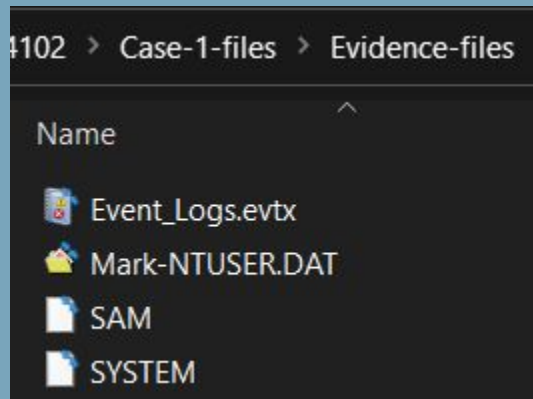
Field	Values
Computer Name	WIN-8NQK06IH20A
Processor's architecture	AMD64
Computer Time Zone	Eastern Standard Time
Computer's DHCP-based IP address	192.168.67.145
Network Mask	255.255.255.0



Our team will be using the **EST time** for this investigation.

Evidence Analyzed

4 evidence files from Mark's computer, consisting of registry hives and event logs.



Evidence No.	Evidence Name	Hash Values (MD5)	Size
00	Event_Logs.evtx	14ac1ef1a31aa42cf5fd3a4eac942f90	1092 KiB
01	Mark-NTUSER.DAT	1a5a665b3f3cfb6dc150b26b87c1f17b	512 KiB
02	SAM	297d8a862ad079f7c5da48f96a71151d	32 KiB
03	SYSTEM	e64992f9baaca0a728050677bac38ca4	9272 KiB

Tools used

Registry Analysis

Multiple tools used to ensure consistency:



Registry Editor

Version 21H2 (OS Build 22000.1455)

RegRipper
Ver 3.0



Windows Registry Recovery
www.YasDL.com

WRR64
Ver 3.1.1.0

Event Log Analysis




Event Viewer
Ver 1.0

Evidences found - website visited

“**Mark** was seen working on unusual hours and browsing **random websites** recently”

File analyzed:

 Mark-NTUSER.DAT

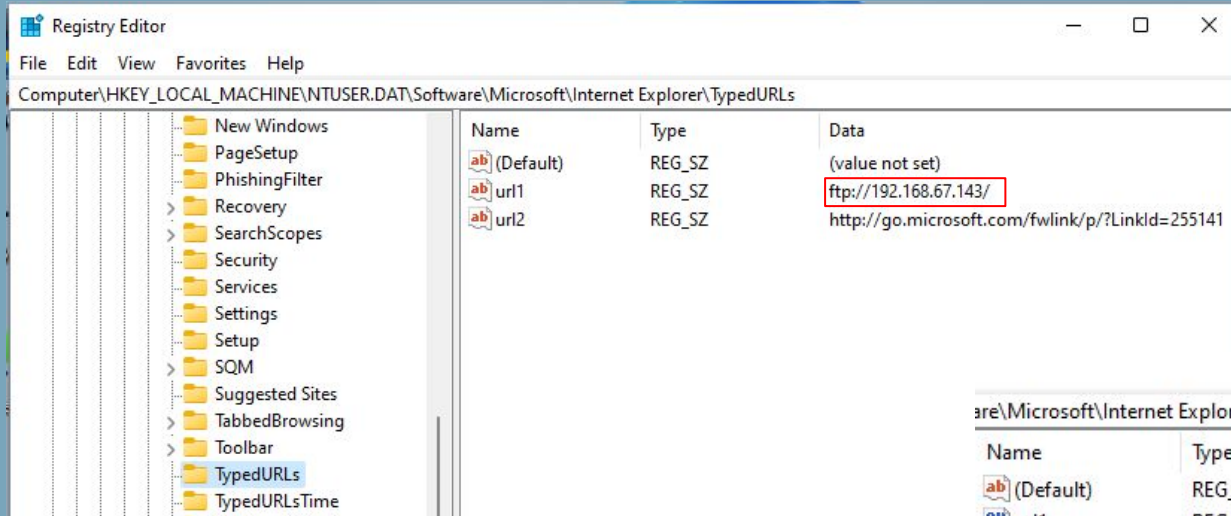
Registry location:

- 1) Finding out recent URLs:
NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs
- 2) Finding out recent URLs time:
NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLsTime

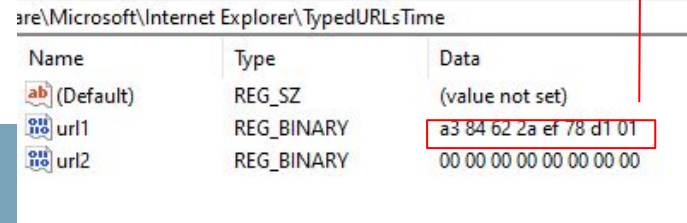
Evidences found - website visited

“**Mark** was seen working on unusual hours and browsing **random websites** recently”

A notable **FTP server** was accessed by Mark:



Tue 7 March 2016 11:01:17pm



Evidences found - website visited

“**Mark** was seen working on unusual hours and browsing **random websites** recently”

Same finding using RegRipper:

```
Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths has no values.
```

```
-----  
typedurls v.20200526
```

```
(NTUSER.DAT) Returns contents of user's TypedURLs key.
```

```
TypedURLs
```

```
Software\Microsoft\Internet Explorer\TypedURLs
```

```
LastWrite Time 2016-03-08 04:01:17Z
```

```
url1 -> ftp://192.168.67.143/
```

```
url2 -> http://go.microsoft.com/fwlink/p/?LinkId=255141
```

```
-----  
typedurlstime v.20200526
```

```
(NTUSER.DAT) Returns contents of user's TypedURLsTime key.
```

```
TypedURLsTime
```

```
Software\Microsoft\Internet Explorer\TypedURLsTime
```

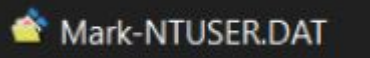
```
LastWrite Time 2016-03-08 04:01:17Z
```

```
url1 -> 2016-03-08 04:01:17Z (ftp://192.168.67.143/)
```

```
url2 -> 0  
-----
```

Evidences found - files accessed

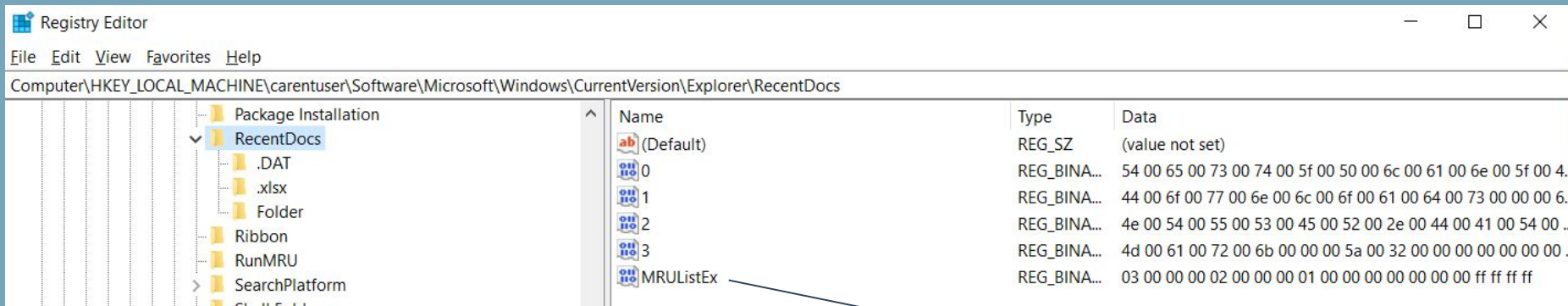
File analyzed:



Registry location:

- 1) Finding out recently accessed documents
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion
\Explorer\RecentDocs
- 2) NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion
\Applets\Wordpad\Recent File List

Evidences found - files accessed



MRU	Docs name
0	Test_Plan_Confidential.xlsx
1	Downloads (folder)
2	NTUSER.DAT
3	Mark (folder)

Accessed at
7/3/2016, 11:03PM,
after FTP server
access (11:01PM)
previously.

Checking MRUListEx (Most Recently
Used list), he accessed the docs in the
following order:

Mark folder → Downloads folder →
Test_Plan_Confidential.xlsx



Evidences found - files accessed

Mark folder → Downloads folder → Test_Plan_Confidential.xlsx

What does the order of the docs tell us?

- Mark possibly **downloaded** the suspicious file **Test_Plan_Confidential.xlsx** (from FTP server).
- Whenever we download a file, the file is default saved under:
C:\Users\<Name>\Downloads\<downloaded file>


So:

Mark\Downloads\Test_Plan_Confidential.xlsx

Evidences found - applications accessed

Can use **UserAssist** registry keys to track GUI-based programs launched from desktop.

File analyzed:

 Mark-NTUSER.DAT

Registry location:

1) Finding GUI opened

NTUser.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count

Evidences found - applications accessed

Found 3 UserAssist keys with values inside it's Count keys:

The screenshot shows the Windows Registry Editor with the path `MACHINE\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count` selected. The left pane shows a tree view with several UserAssist keys, including `{BCB48336-4DDD-48FF-BB0B-D3190DACB3}`, `{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}`, and `{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}`. The right pane shows a list of registry values:

Name	Type	Data
(Default)	REG_SZ	(value not set)
{1NP14R77-02R7-4R5Q-0744-2RO1NR519807}\...	REG_BINA...	00 00 00 00 00 00 00 00 04 00 00 00 2d 6b 00 00 00 00 80 bf ..
{1NP14R77-02R7-4R5Q-0744-2RO1NR519807}\...	REG_BINA...	00 00 00 00 01 00 00 00 01 00 00 00 f8 2a 00 00 00 00 80 bf 0.
{6Q809377-6NS0-4440-8957-N3773S02200R}\v...	REG_BINA...	00 00 00 00 02 00 00 00 01 00 00 00 6f 17 00 00 00 00 80 bf 0.
HRZR_PGYFRFFVBA	REG_BINA...	00 00 00 00 08 00 00 00 21 00 00 00 76 91 0f 00 03 00 00 00 0.
HRZR_PGYPHNPbhag;pgbe	REG_BINA...	ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 bf 00 ..
jvaqbjf.vzzrefvirpbagebycnary_pj5a1u2gklrjl!zvp...	REG_BINA...	00 00 00 00 01 00 00 00 01 00 00 00 53 35 01 00 00 00 80 bf ...
Zvpebfbsg.Jvaqbjf.Furry.EhaQvnybt	REG_BINA...	00 00 00 00 00 00 00 00 00 00 00 00 70 0a 00 00 00 00 80 bf ...
Zvpebfbsg.Jvaqbjf.PbagebyCnary	REG_BINA...	00 00 00 00 00 00 00 00 02 00 00 00 83 19 00 00 00 00 80 bf ...
Zvpebfbsg.Jvaqbjf.Qrfxgbc	REG_BINA...	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 80 bf ...
Zvpebfbsg.Jvaqbjf.Rkcybere	REG_BINA...	00 00 00 00 00 00 00 00 10 00 00 00 d6 54 0a 00 00 00 80 bf ...
Zvpebfbsg.VagreargRkcybere.Qrsnhyg	REG_BINA...	00 00 00 00 03 00 00 00 08 00 00 00 c6 35 03 00 00 00 80 bf 0.

Upon checking the key timings, these GUI programs were accessed on around the same day the suspicious file `Test_plan_confidential.xlsx` was accessed.

The screenshot shows a Notepad window displaying the following information:

```
File Edit Format View Help
Key Name: HKEY_LOCAL_MACHINE\carentuser\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
Class Name: <NO CLASS>
Last Write Time: 08/03/2016 - 11:27 AM
Value 0
Name: Version
Type: REG_DWORD
Data: 0x5
```

Evidences found - applications accessed

These are ROT13 encoded names:

```
HRZR_PGYPHNPbhag:pgbe
HRZR_PGYFRFFVBA
frg_2747713814_ra-hf
Zvpebfbsg.VagreargRkcybere.Qrsnhyg
\Jvaqbjf AG\Npprffbevr\JBEQCNQ.RKR
Zvpebfbsg.Jvaqbjf.Qrfgbc
\pzq.rkr
jvaqbjf.vzzrefvirpbagebycnary_pj5a1u2gklrjllzvpebfbsg.jvaqbjf.vzzrefvirpbagebycnary
Zvpebfbsg.Jvaqbjf.Rkcybere
\BcraJvgu.rkr
Zvpebfbsg.Jvaqbjf.PbagebyCnary
Zvpebfbsg.Jvaqbjf.Furyy.EhaQvnybt
\GnfxOne\Vagrearg Rkcybere.yax
\Qrfgbc.yax
```

Therefore, applications Mark may have opened are:

- Internet Explorer (for FTP)
- Wordpad
- CMD (nothing notable found)

Output

```
UEME_CTLCUACount:ctor
UEME_CTLSESSION
set_2747713814_en-us
Microsoft.InternetExplorer.Default
\Windows NT\Accessories\WORDPAD.EXE
Microsoft.Windows.Desktop
\cmd.exe
windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel
Microsoft.Windows.Explorer
\OpenWith.exe
Microsoft.Windows.ControlPanel
Microsoft.Windows.Shell.RunDialog
\TaskBar\Internet Explorer.lnk
\Desktop.lnk
```

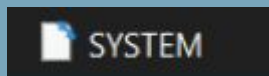
time: 1ms
length: 398
lines: 14

save con

Evidences found - USB access

“A day before he left, John reported a missing USB storage drive and was suspicious of Mark.”

File analyzed:



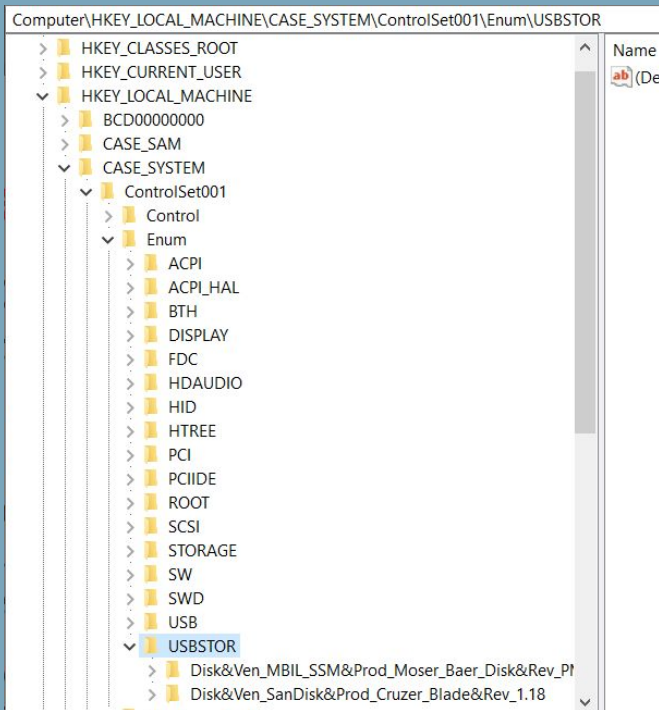
Registry location:

- 1) Finding out USB plugged into computer before:
SYSTEM\ControlSet001\EnumUSBSTOR



Evidences found - USB access

“A day before he left, John reported a **missing USB storage drive** and was suspicious of Mark.”

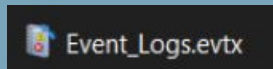


USB Device	Last Write Time
SanDisk Cruzer Blade USB Device	7/3/2016 - 11:10 PM EST
MBIL SSM Moser Baer Disk USB Device	7/3/2016 - 11:57 PM EST



Relation between USB & sensitive file access time

Last write time of Test_Plan_Confidential.xlsx is at **7/3/2016 - 11:03 PM**. USB write time is updated whenever data are written or removed from the device. Both USB devices are plugged and written after this timing, hence, **both USB devices are suspicious** as files could have been written to it.



Event Log Analysis

We look at notable important findings from the event logs

Event 4720, Microsoft Windows security auditing.

General Details

A user account was created.

Subject:

Security ID:	SYSTEM
Account Name:	WIN-8NQK06IH20A\$
Account Domain:	WORKGROUP
Logon ID:	0x3E7

New Account:

Security ID:	S-1-5-21-4115010050-4293081376-766057376-1001
Account Name:	Mark
Account Domain:	WIN-8NQK06IH20A

Attributes:

SAM Account Name:	Mark
Display Name:	<value not set>
User Principal Name:	-
Home Directory:	<value not set>

Log Name: Security

Source: Microsoft Windows security

Event ID: 4720

Level: Information

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

Logged: 07-Mar-2016 8:59:30 PM

Task Category: User Account Management

Keywords: Audit Success

Computer: WIN-8NQK06IH20A

At **8:59:30 PM on 7 March 2016**, an account called “Mark” was created.

The other subsequent logs shows changes to this new user account (e.g. changes to User Access Control)

Event Log Analysis

Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

Security ID:	SYSTEM
Account Name:	WIN-8NQQ06IH20AS
Account Domain:	WORKGROUP
Logon ID:	0x3E7

Logon Type: 2

Impersonation Level: Impersonation

New Logon:

Security ID:	S-1-5-21-4115010050-4293081376-766057376-1001
Account Name:	Mark
Account Domain:	WIN-8NQQ06IH20A
Logon ID:	0xCC278
Logon GUID:	{00000000-0000-0000-0000-000000000000}

Log Name: Security

Source: Microsoft Windows security Logged: 07-Mar-2016 10:27:34 PM

Event ID: 4624 Task Category: Logon

Level: Information Keywords: Audit Success

User: N/A Computer: WIN-8NQQ06IH20A

OpCode: Info

More Information: [Event Log Online Help](#)

At **10:27:34 PM on 7 March 2016**, someone logged into Mark's account.

Event Log Analysis

Event 4720, Microsoft Windows security auditing.

General Details

A user account was created.

Subject:

Security ID:	S-1-5-21-4115010050-4293081376-766057376-1001
Account Name:	Mark
Account Domain:	WIN-8NQQ06IH20A
Logon ID:	0xCC254

New Account:

Security ID:	S-1-5-21-4115010050-4293081376-766057376-1002
Account Name:	Admin
Account Domain:	WIN-8NQQ06IH20A

Attributes:

SAM Account Name:	Admin
Display Name:	<value not set>
User Principal Name:	-
Home Directory:	<value not set>
Home Drive:	<value not set>
Script Path:	<value not set>

Log Name: Security

Source: Microsoft Windows security

Event ID: 4720

Level: Information

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

Logged: 07-Mar-2016 11:40:14 PM

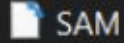
Task Category: User Account Management

Keywords: Audit Success

Computer: WIN-8NQQ06IH20A

At **11:40:14 PM on 7 March 2016**, Mark created an account called "Admin".

This is a suspicious time as this is the time after Mark has accessed the sensitive file (accessed Test_Plan_Confidential at 11:03PM on same day).



Event Log Analysis

MiTeC Windows Registry Recovery x64 - [SAM]

File Options Explore Windows Help

Free to use for private, educational and non-commercial purposes

SAM

NAVIGATOR

- File Information
- Security Records
- SAM**
- Windows Installation
- Hardware
- Startup Applications

General Groups and Users

Users

- Administrator
- Guest
- Mark
- Admin**
- Built-In Users

Groups

- WinRMRemoteWMIUsers_

Property	Value
SID	S-1-5-21-4115010050-4293081376-766057376-1002
Full name	Admin
Last logon	08/03/2016 4:41:12 AM
Last password set	08/03/2016 4:40:14 AM
Account expiration	30/12/1899 2:48:05 AM

If we check the SAM registry hive with WRR, we see that “Admin” is part of the computer users in Mark’s computer.

Event Log Analysis

Event 4738, Microsoft Windows security auditing.

General Details

A user account was changed.

Subject:

Security ID:	S-1-5-21-4115010050-4293081376-766057376-1001
Account Name:	Mark
Account Domain:	WIN-8NQK06IH20A
Logon ID:	0xCC254

Target Account:

Security ID:	S-1-5-21-4115010050-4293081376-766057376-1002
Account Name:	Admin
Account Domain:	WIN-8NQK06IH20A

Changed Attributes:

SAM Account Name:	Admin
-------------------	-------

Log Name: Security

Source: Microsoft Windows security

Event ID: 4738

Level: Information

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

Logged: 07-Mar-2016 11:40:14 PM

Task Category: User Account Management

Keywords: Audit Success

Computer: WIN-8NQK06IH20A

After which, certain changes were made to the “Admin” account such as the user access control (**0x15** → **0x210**).

This means account changed from “Account disabled, password not required” to “Account enabled, password never expires.”

Possibility:

Person who created this account would want to log into this account in the future and doesn't want anyone to log into it or change its password by setting a password that never expires.

Old UAC Value: 0x15
New UAC Value: 0x210
User Account Control:
Account Enabled
'Password Not Required' - Disabled
'Don't Expire Password' - Enabled

Event Log Analysis

Event 4732, Microsoft Windows security auditing.

General Details

A member was added to a security-enabled local group.

Subject:

Security ID: S-1-5-21-4115010050-4293081376-766057376-1001
Account Name: Mark
Account Domain: WIN-8NQK06IH20A
Logon ID: 0xCC254

Member:

Security ID: S-1-5-21-4115010050-4293081376-766057376-1002
Account Name: -

Group:

Security ID: BUILTIN\Administrators
Group Name: Administrators
Group Domain: Builtin

Additional Information:

Log Name: Security

Source: Microsoft Windows security Logged: 07-Mar-2016 11:40:26

Event ID: 4732 Task Category: Security Group Management

Level: Information Keywords: Audit Success

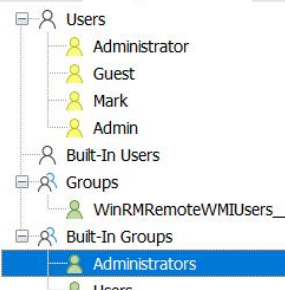
User: N/A Computer: WIN-8NQK06IH20A

OpCode: Info

More Information: [Event Log Online Help](#)

The "Admin" account has **super privileges** as it was added to the Built in Administrators group.

General Groups and Users



Property

SID S-1-5-32-544

Comment Administrators have complete and unrestricted access to the computer/domain

User count 2

Event Log Analysis

Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

Security ID: SYSTEM
Account Name: WIN-8NQK06IH20AS
Account Domain: WORKGROUP
Logon ID: 0x3E7

Logon Type: 2

Impersonation Level: Impersonation

New Logon:

Security ID: S-1-5-21-4115010050-4293081376-766057376-1002
Account Name: Admin
Account Domain: WIN-8NQK06IH20A
Logon ID: 0x1F31F0
Logon GUID: {00000000-0000-0000-0000-000000000000}

Log Name: Security

Source: Microsoft Windows security Logged: 07-Mar-2016 11:41:12 PM

Event ID: 4624 Task Category: Logon

Level: Information Keywords: Audit Success

User: N/A Computer: WIN-8NQK06IH20A

OpCode: Info

More Information: [Event Log Online Help](#)

Finally at **11:41:12 PM on 7 March 2016**, someone logged into the “Admin” account.

Possibly to test out that the account can be logged into.

Event Log Analysis

Event 4738, Microsoft Windows security auditing.

General Details

A user account was changed.

Subject:

Security ID:	SYSTEM
Account Name:	WINDOWS-MRT14B2S
Account Domain:	WORKGROUP
Logon ID:	0x3E7

Target Account:

Security ID:	S-1-5-21-4115010050-4293081376-766057376-500
Account Name:	Administrator
Account Domain:	WINDOWS-MRT14B2

Changed Attributes:

SAM Account Name:	-
Display Name:	-
User Principal Name:	-
Home Directory:	-
Home Drive:	-
Script Path:	-
Profile Path:	-
User Workstations:	-
Password Last Set:	-
Account Expires:	-
Primary Group ID:	-
AllowedToDelegateTo:	-
Old UAC Value:	0x211
New UAC Value:	0x211
User Account Control:	-
User Parameters:	-
SID History:	-

Log Name: Security

Source: Microsoft Windows security

Event ID: 4738

Level: Information

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

Logged: 07-Mar-2016 11:58:51 PM

Task Category: User Account Management

Keywords: Audit Success

Computer: windows-mrt14b2

Additionally, we noticed at a later time on the **same day at 11:58:51 PM**, the administrator account in Mark's laptop was disabled.

Such action is especially suspicious because it seems like the individual do not want anyone to be the most privileged user.

Final Timeline

7 March 2016

"Mark" account
was created.



Accessed FTP
server URL.



Access to SanDisk USB

10:27:34 PM

11:03 PM

11:40:14 PM

8:59:30 PM

11:01:17 PM

11:10 PM

"Mark" account
was logged into.

Accessed
Test_Plan_Confidential.xlsx
that is placed under:

Mark\Downloads

"Mark" account
created new
"Admin" account.

Final Timeline

Changes made to "Admin" account. The account password never expires and is enabled.

"Admin" account was logged on into.

Administrator account disabled

11:58:51 PM

11:40:26 PM

11:57 PM

11:40:14 PM

11:41:12 PM

"Admin" account added to Built in Administrator account.

Access to Moser Baer USB



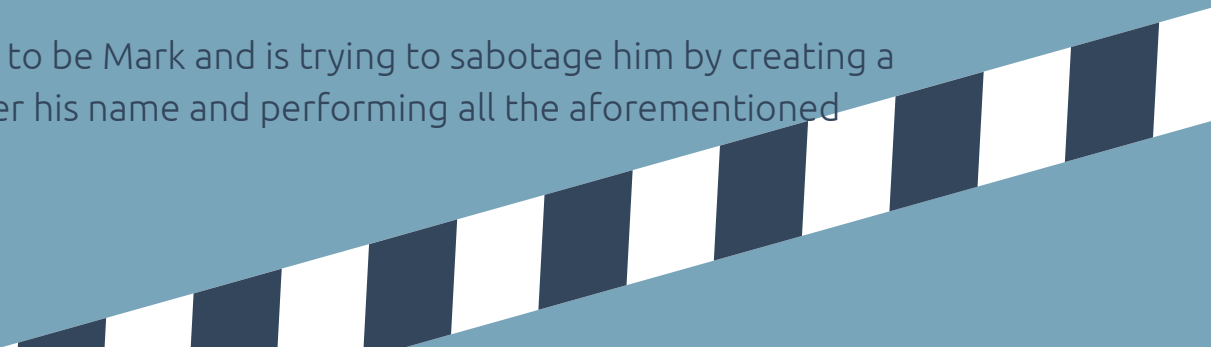


Our hypothesis:

Hypothesis 1 (Guilty) - Our main hypothesis

- He accessed confidential document from a FTP server, accessed a thumb drive and created an Admin account on his laptop at an unusual hour.

Hypothesis 2 (Not guilty)

- Someone is pretending to be Mark and is trying to sabotage him by creating a computer account under his name and performing all the aforementioned suspicious actions.
- 

Hypothesis #1: GUILTY

- 1) The timeline started with an account called “Mark” being created. We assume that the case creator has created this.
- 2) Definite evidence that he has indeed worked at **unusual hours** (e.g. after usual work hours at more than 8pm).
- 3) There is evidence that he accessed an FTP server and downloaded a file (as he accessed his Downloads folder at that day). The file downloaded and accessed has somewhat a **suspicious** name “Test_Plan_Confidential.xlsx”. Perhaps trying to steal company secrets.
- 4) He has definitely accessed and plugged in **USB drives** into his computer.

Cont'd

- 5) He has created an **"Admin"** account in his computer even though there is already an existing "administrator" account.
- He has named this account "Admin", similar to the "administrator" account. This might indicate that he is trying to make this account sound **less suspicious** to users who might takeover his computer. Users might think nothing of it.
 - The account has a password that never expires. This shows that he wants no one to access this account (by setting a password) and also wants to have **persistency** with a password that never expires.
 - The account has **super privileges** - similar to administrator.
 - The administrator account was then subsequently deactivated

The most suspicious and crucial action that shows that Mark is guilty

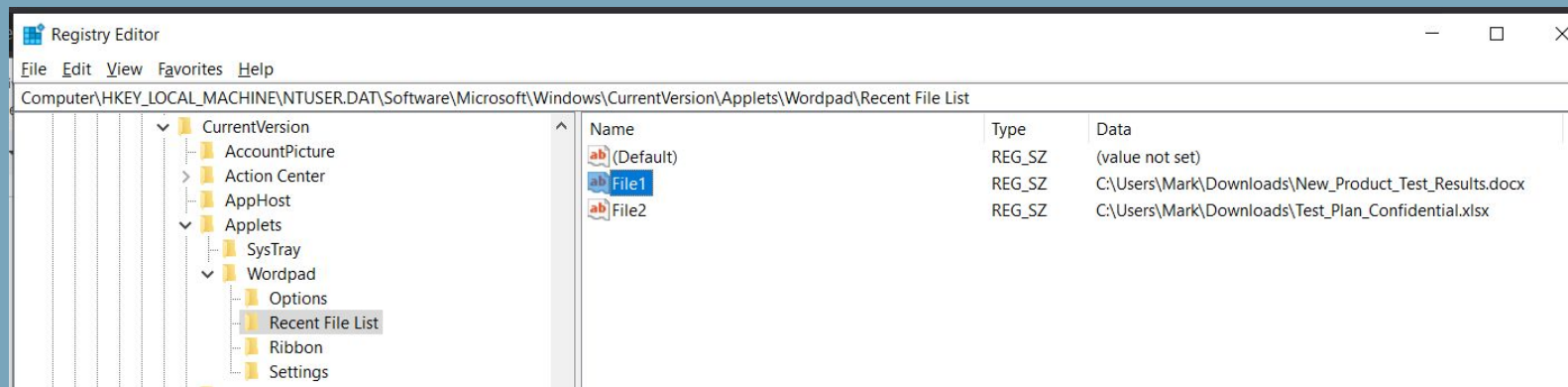
Hypothesis #2: NOT guilty

- 1) The timeline started with an account called “Mark” being created. We assume that some **rogue individual** has created this in order to sabotage Mark. If this is the case, then Mark is not guilty as someone else has pretended to be him doing the suspicious actions.
- 2) As mentioned, “Test_Plan_Confidential.xlsx” sounds like a suspicious filename. However, there is no way to conclude that it is 100% suspicious as **we are unable to check its content**. We only deem it as suspicious based on its filename. If we are able to check its content, then Mark is suspicious.
- 3) There are USB drives plugged into Mark’s computer. However, we **cannot conclude that it has been stolen** as there is no indication to show that it does.

Other Interesting Findings - files accessed

A notable finding: **Wordpad.exe** was used to open **TWO** files (a docx and xlsx file). Can find information under

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Applets\Wordpad\Recent File List



However, `New_Product_Test_Result.docx` wasn't found in RecentDocs registry key for recently accessed files even though it's under RecentFileList for Wordpad. It could have been deleted or renamed.

Other Interesting Findings - Event Logs

We found another computer "windows-mrt14b2", accessing Mark's computer (WIN-8NQG061H20A). Upon analyzing the logs, many events are network related (e.g. creating Remote Desktop Users - possibly to remote into the computer after Mark leaves.) But none of this could be confirmed if it is related to the timeline/case.

Log Name:	Security	Logged:	26-Mar-2016 10:25:33 PM
Source:	Microsoft Windows security	Task Category:	User Account Management
Event ID:	4797	Keywords:	Audit Success
Level:	Information	Computer:	WIN-8NQG061H20A
User:	N/A		
OpCode:	Info		
More Information:	Event Log Online Help		

Event 4608, Microsoft Windows security auditing.

General Details

Windows is starting up.

This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.

Log Name:	Security	Logged:	07-Mar-2016 11:58:02 PM
Source:	Microsoft Windows security	Task Category:	Security State Change
Event ID:	4608	Keywords:	Audit Success
Level:	Information	Computer:	windows-mrt14b2
User:	N/A		
OpCode:	Info		
More Information:	Event Log Online Help		

Conclusion

Mark is **suspicious**. Mainly due to the event logs (e.g. purpose of creating Admin account).

However, we **cannot guarantee** that Mark is fully suspicious with confidence as there are some uncertainty to some of the evidences found, as mentioned (USB drives and Test_Plan_Confidential file).

Unless more evidence from Mark's computer is given, we can be more certain that Mark is indeed suspicious.



Recommendations

Additional evidence/information we need to be certain that Mark is indeed guilty:

- 1) **An image of Mark's laptop.** This is to look through the file system and access the contents of "Test_Plan_Confidential.xlsx". If the contents are indeed suspicious, then Mark is suspicious as he has a suspicious file in his computer.
- 2) Inventory list of company's USB devices
- 3) John's **SYSTEM registry hive.** To compare the values of the USBSTOR plugged into Mark's system.
- 4) **More event logs.** The event log file given for this case seems limited and is for security events. More event logs that provides information about PnP (Plug and Play devices) like USB plug ins could be provided.
- 5) More comprehensive description of the case (e.g. date when Mark left the company so that we can match it with the timeline, company's SOP).
- 6) The physical USB device

Thank you!

QNA

