\\192.168.1.99\classes

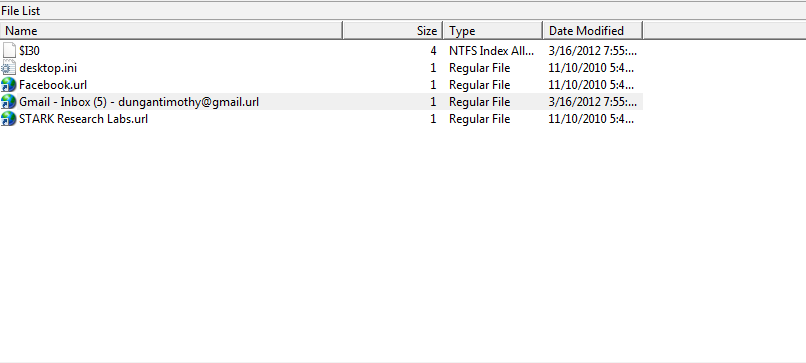
Document as you go in respective sections

Tentative version (with live updates) of the report can be viewed here: (preview doesn’t display properly so download it) <https://www.dropbox.com/s/zomk4dsh80hb5ml/130502%20Final%20Quest%20Report.docx>

I’ll (Conner) be keeping an eye on this .gdoc and update the report as more is added/changed. If you want me to invite you to a Dropbox share with the report send me your email (contact me via Canvas or other means) and I can invite you. Thanks.

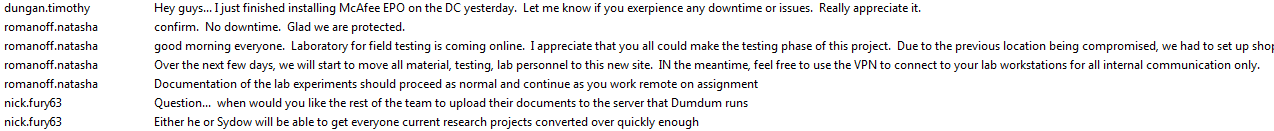
## 

## Timeline for Tdungan’s machine



Looking at Tdungans Favorites I found his Gmail dungantimothy@gmail.com.

Alex Cannell 4/27

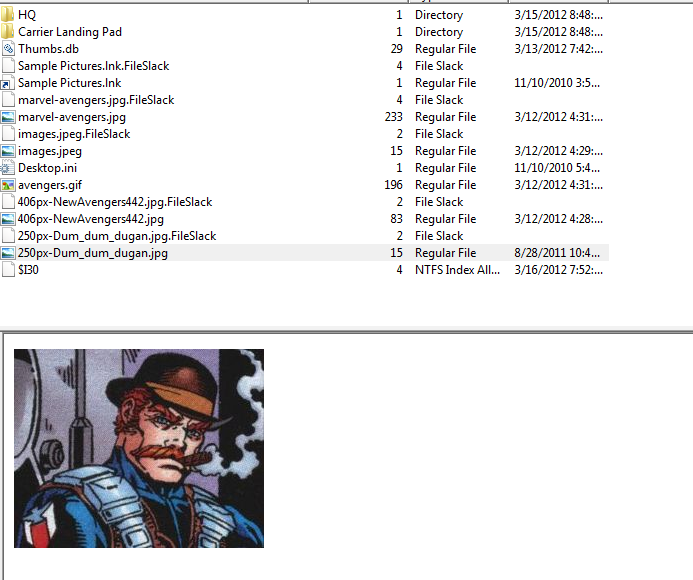


It looks like Tim Duncan(Skype ID = dungan.timothy) installed McAfee on DC(Im assuming DC is a server) on 09/17/2011 at 10:34:32 AMand he was relaying this information to Natasha Romanoff (Skype ID = romanoff.natasha)who promptly responded with a confirmation of no downtime on the DC.

Several Months later on 03/05/2012 at 7:50:17 AM Natasha Romanoff informed everyone, “good morning everyone. Laboratory for field testing is coming online. I appreciate that you all could make the testing phase of this project. Due to the previous location being compromised, we had to set up shop within stark-research-labs. As our backup laboratory, all future testing will be accomplished here. Over the next few days, we will start to move all material, testing, lab personnel to this new site. IN the meantime, feel free to use the VPN to connect to your lab workstations for all internal communication only. Documentation of the lab experiments should proceed as normal and continue as you work remote on assignment...”

Right after Nick Fury (Skype ID = nick.fury63) asked when they could upload their documentation to the Dumdum server. He continues with his confidence that the reasearch project could be converted over quickly enough.

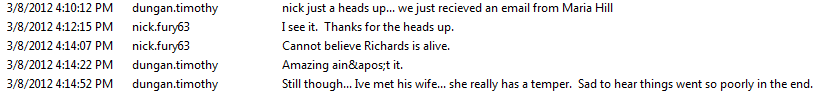
Alex Cannell 4/27



Found out who DumDum is from Nick Fury’s skype, “Right after Nick Fury (Skype ID = nick.fury63) asked when they could upload their documentation to the Dumdum server. He continues with his confidence that the research project could be converted over quickly enough.” It is actually Tim Dungan.

I also found some pictures of HQ and of their Landing Pad in Tim Dungans files. (and a whole lot of pictures of the avengers.

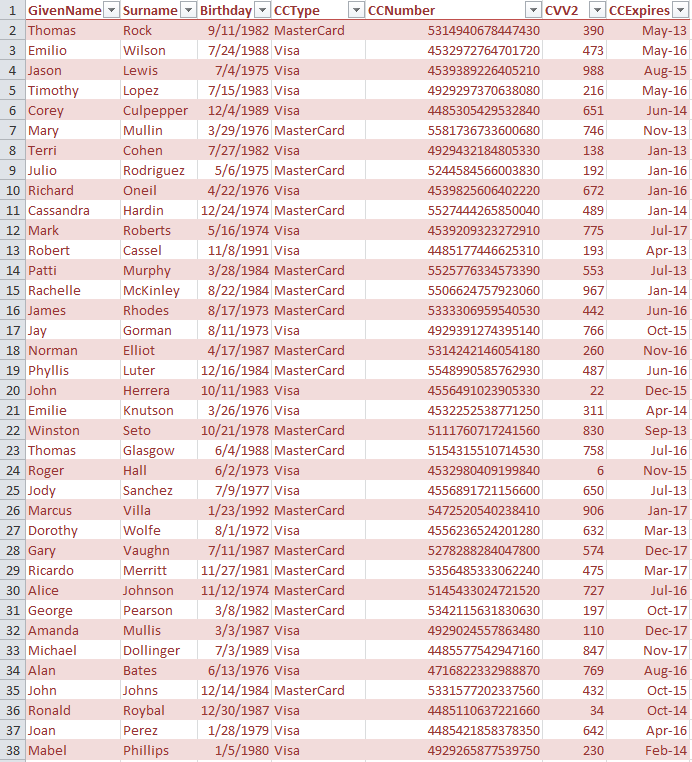
Alex Cannell 4/30



Tim Dungan informed Nick Fury about Maria Hills email.

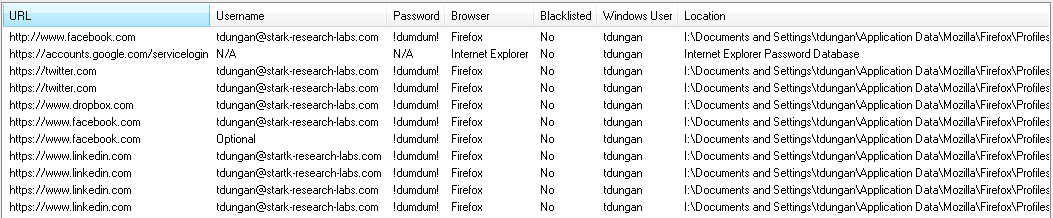
They continue talking about someone called Richards who is still alive and his wife. Time replied with, “Amazing ain&apos;t it.” dont know what “ain&apos;t” means. I assume that they are talking about Richard Fisk (antihero) and his wife Vanessa.

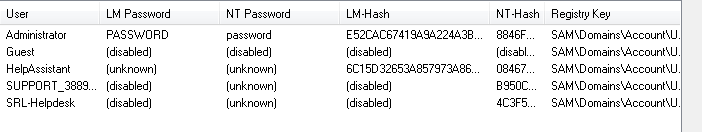
Alex Cannell 4/27



I found 251 Credit card numbers, names, birthdays, Card Types, CVV2 Numbers, and Card Expiration dates. which was modified last on 4/3/2012, in location /tdungan/Documents and Settings/MyDocuments/Backstoped Accounts -RDcosts Alloy Research/.

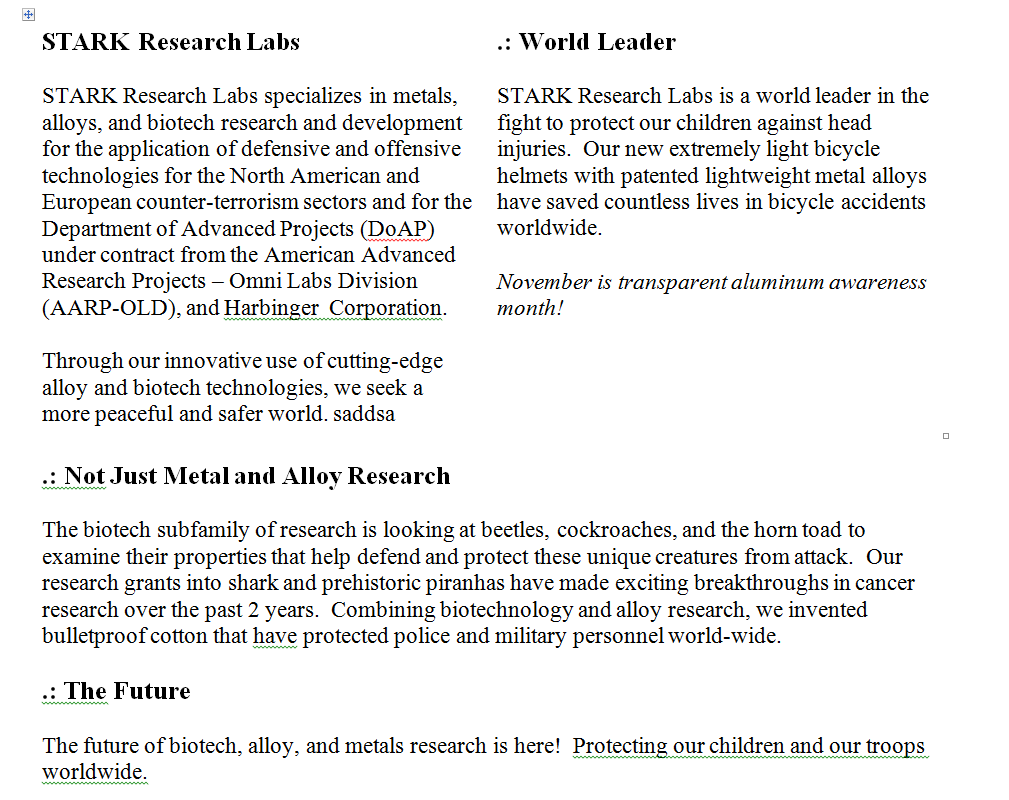
Alex Cannell 4/30





I found his social media passwords, and his administrator password(which is very secure). I used OSforensics to retrieve this information.

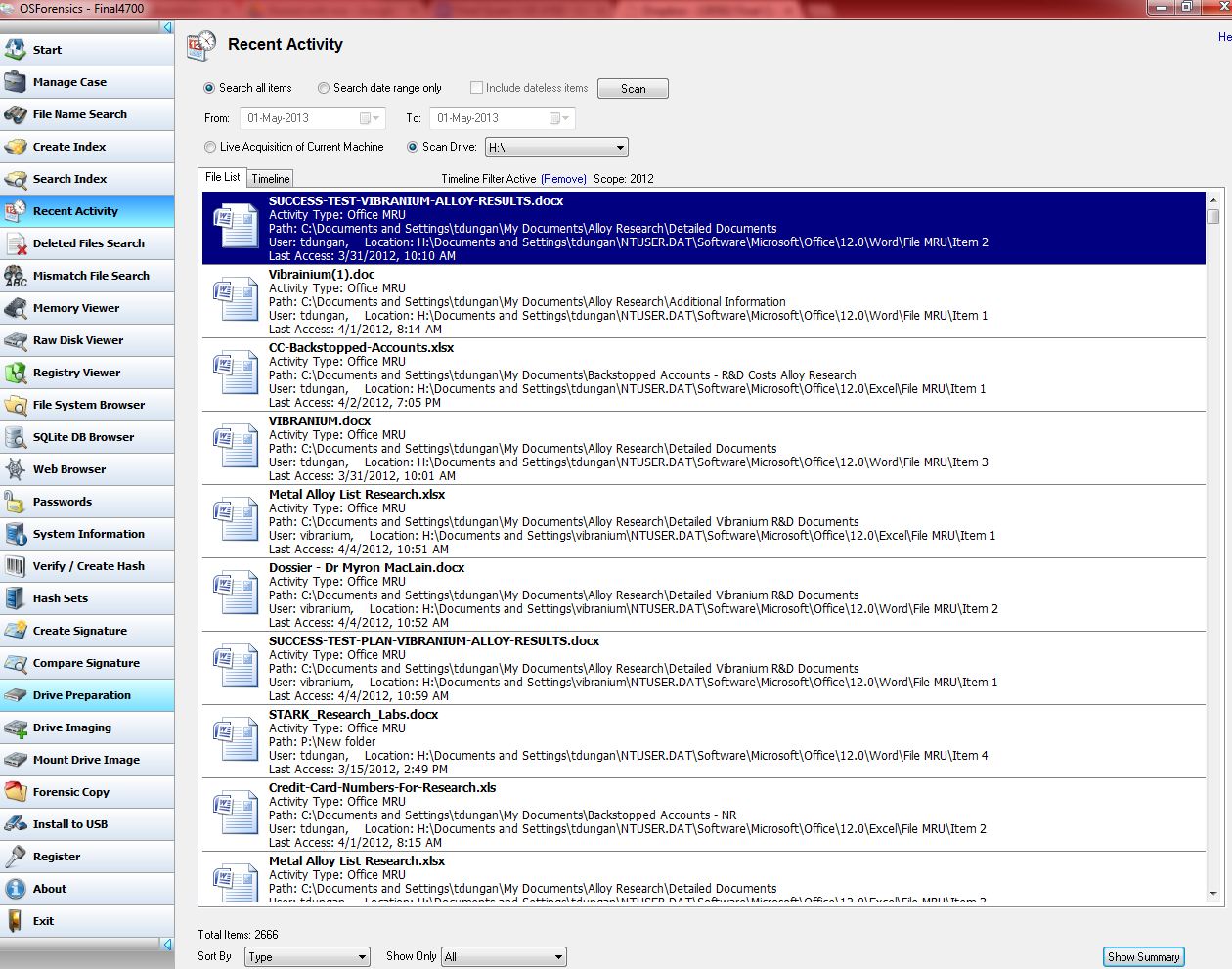
Alex Cannell and Ethan Kleinman 5/1



This was the last final that inputed into dropbox, the files name is STARK Research Labs.dox. I found this by going to \Dropbox\.dropbox.cashe.

Alex Cannell and Ethan Kleinman 5/2

Using the software OSforensics I compiled a timeline that includes all recently accessed documents, I also added some of the websites that caught my attention.



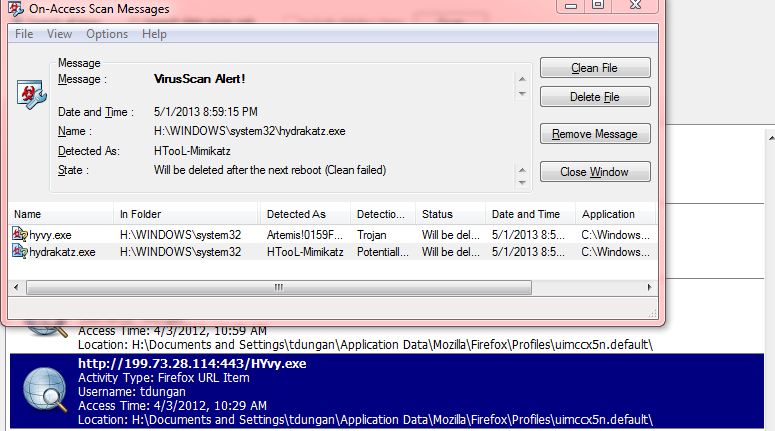
Here is the link to the document timeline ->

<https://docs.google.com/spreadsheet/ccc?key=0AkgCktRI38R4dFpqTlBCZ09OWVZOMTRpb0RpdWoxMmc&usp=sharing>

The document timeline wont export in excel with file names so here it is in text format that includes the filenames -> <https://docs.google.com/file/d/0B0gCktRI38R4Y1N5UmQxU0RjdjQ/edit?usp=sharing>

The two timelines correspond directly

I also found FireFox history with the file “HYvy.exe” being downloaded from “<http://199.73.28.114:443/HYvy.exe>”

This file was downloaded to the system32 folder and is detected as a Trojan 

Here is a link to the entire timeline in csv format ->

<https://docs.google.com/file/d/0B0gCktRI38R4WE51djhiel8zUmM/edit?usp=sharing>

Ethan Kleinman 5/1

## Determine if research was successful Found by Jessica Turek 4/24



## Found by Jessica Turek 4/24

Going off of Jessica’s post, I searched files that were edited on 31 March. Here is what I found

C:\Documents and Settings\tdungan\My Documents\Alloy Research\Detailed Vibranium R&D Documents\SUCCESS-TEST-PLAN-VIBRANIUM-ALLOY-RESULTS.docx

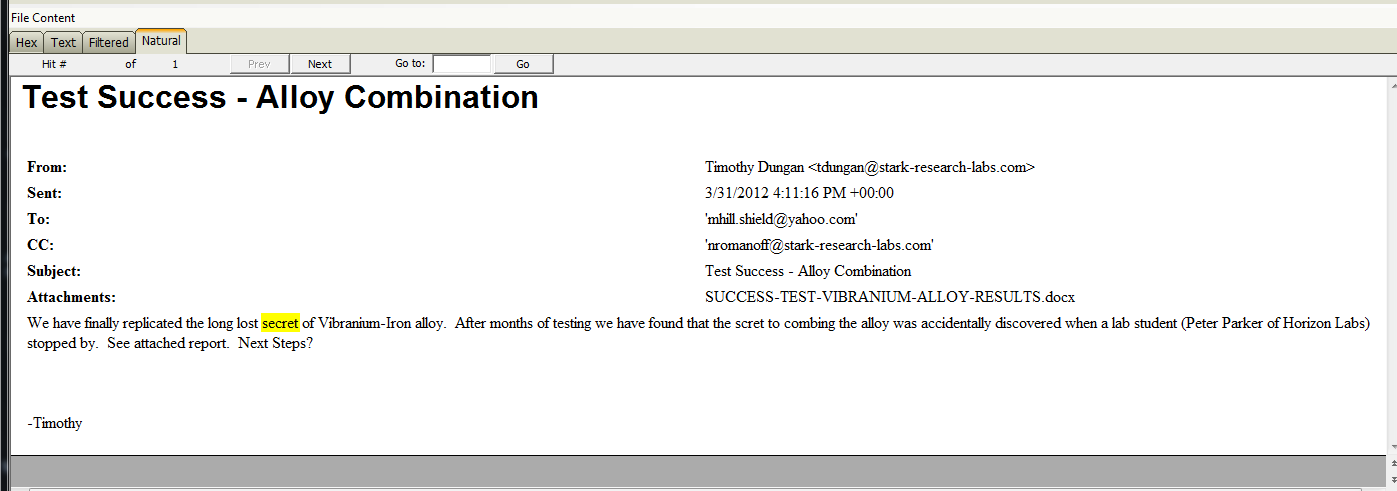
The first part of the document reads

“**Test Report – SUCCESS**

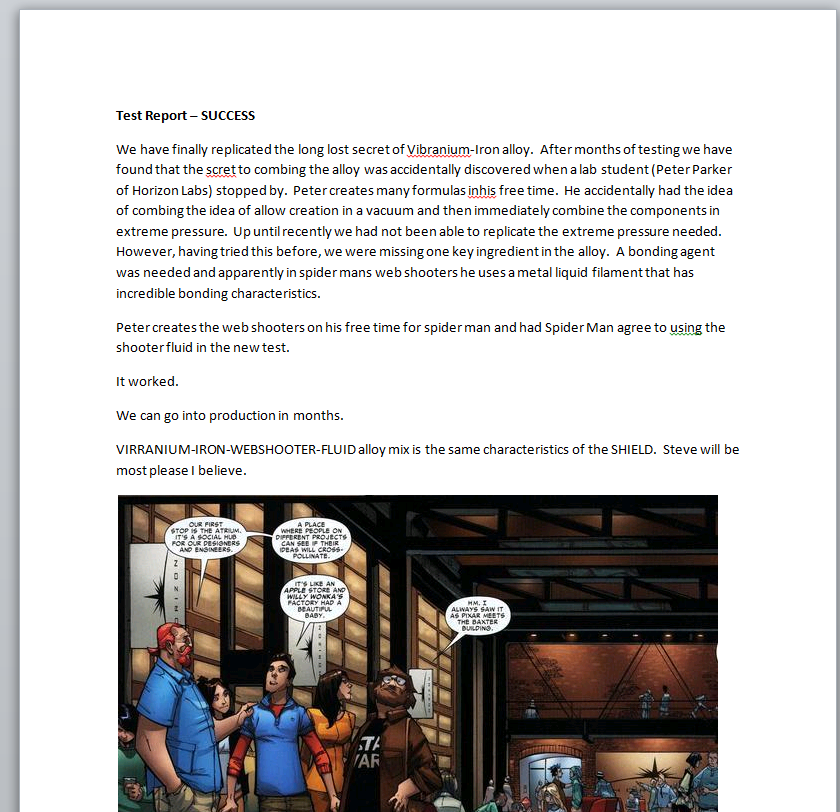
We have finally replicated the long lost secret of Vibranium-Iron alloy. After months of testing we have found that the scret to combing the alloy was accidentally discovered when a lab student (Peter Parker of Horizon Labs) stopped by.”

**Found by McKay Thompson 4/24**

The following is the actual email from Timothy Dungan to mhill.shield@yahoo.com reporting that the vibranium alloy project was a success. The test report was attached to this email.

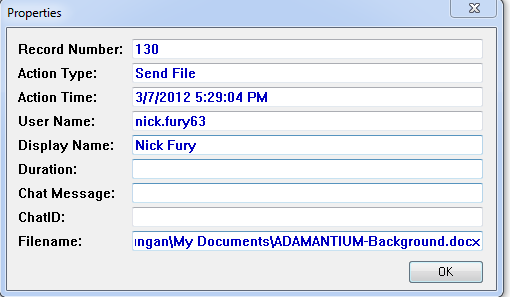


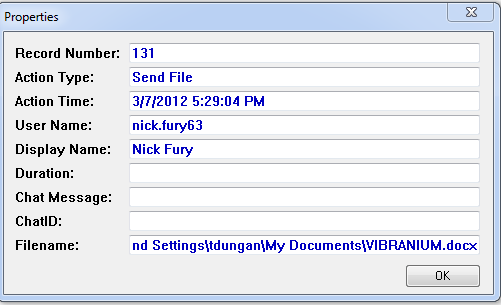
**( Dakota Gray)**



I extracted the test successful document from the image to get a better look at how the research was successful. (Dakota Gray)

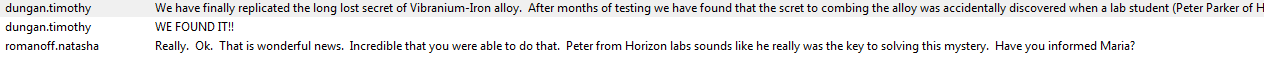






Looking at the Skype Chat logs,Tim Dungan Sent two documents to Nick Fury through Skype. The Files are ADAMANTIUM\_Background.docx and VIBRANIUM.docx.

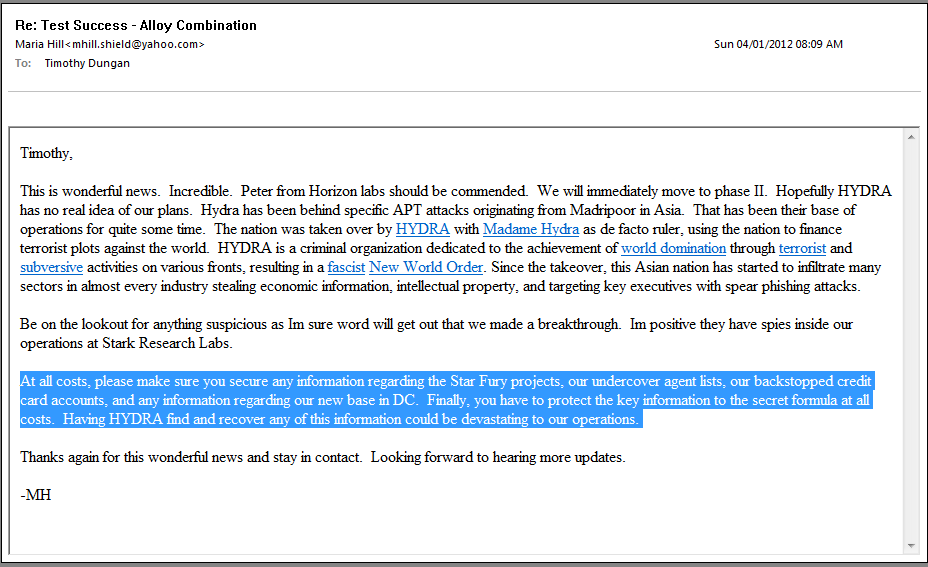
Alex Cannell 4/27



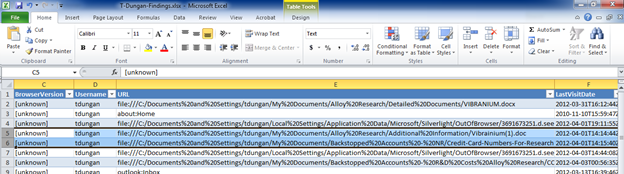
On 03/31/2012 at 10:08:05 AM on Skype Tim Duncan informs everyone that they had found the Vibranium-Iron Alloy, which was discovered by Peter Parker at Horizon Labs.

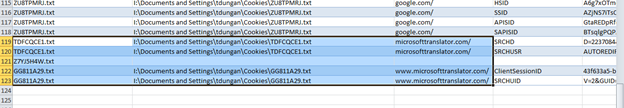
Alex Cannell 4/27

## Determine if anything was taken

The following e-mail was found in the ost file for the vibranium user account on tdungan’s c drive:

In this e-mail there are five things mentioned that needed to be secure “at all costs.” These are the Star Fury projects, undercover agent lists, backstopped credit card accounts, information regarding the new base in DC, and key information about the “secret formula.” If there were any files that may have been taken, it would likely be anything with the aforementioned information in it.

Looking through the tdungan’s web history from Web Historian, I found that these files were visited april 1, 2012:  
  
  
  
I also found these in tdungan’s Cookie History



## I don’t know if they are really significant, but if Hydra wanted information, they might want to first translate it to German.

## 

5/1 I (Jessica Turek) opened romanoff’s supertimeline and did a search for “Undercover”. I copied the row for all of the entries I found into a separate excel worksheet so I could see just them. I tried to grab the most important columns to insert here:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Undercover Agent-List |  |  |  |  |
| 4/1/2012 | 10:17:20 | ..C. | NTFS $MFT | /Users/nromanoff/Documents/Undercover Agent-List-Classified |
| 4/1/2012 | 10:19:08 | ...B | NTFS $MFT | /Users/nromanoff/AppData/Roaming/Microsoft/Windows/Libraries/Undercover Agent List.library-ms |
| 4/1/2012 | 10:19:32 | MA.. | NTFS $MFT | /Users/nromanoff/AppData/Roaming/Microsoft/Windows/Libraries/Undercover Agent List.library-ms |
| 4/4/2012 | 11:21:06 | ..C. | NTFS $MFT | /Users/nromanoff/Documents/Undercover Agent-List-Classified/Agents-List-CLASSIFIED-TOP-SECRET.zip |
| 4/4/2012 | 11:21:06 | ..C. | NTFS $MFT | /Users/nromanoff/AppData/Roaming/Microsoft/Windows/Libraries/Undercover Agent List.library-ms |
| 4/4/2012 | 11:42:56 | MAC. | NTFS $MFT | /Users/nromanoff/Documents/Undercover Agent-List-Classified/Agents-List-CLASSIFIED-TOP-SECRET |
| 4/4/2012 | 11:42:56 | M... | Shortcut LNK | C:/Users/nromanoff/Documents/Undercover Agent-List-Classified/Agents-List-CLASSIFIED-TOP-SECRET |
|  |  |  |  |  |
|  |  |  |  |  |
| US |  |  |  |  |
| 4/4/2012 | 7:42:58 | M... | Internet Explorer | visited file:///C:/Users/nromanoff/Documents/Undercover%20Agent-List-Classified/Agents-List-CLASSIFIED-TOP-SECRET/**Undercover-Agents-List-For-United-States.xlsx** |
| 4/4/2012 | 11:21:06 | ..C. | NTFS $MFT | /Users/nromanoff/Documents/Undercover Agent-List-Classified/Agents-List-CLASSIFIED-TOP-SECRET/**Undercover-Agents-List-For-United-States.xlsx** |
| 4/4/2012 | 11:21:06 | ..C. | NTFS $MFT | /Users/nromanoff/AppData/Roaming/Microsoft/Office/Recent/**Undercover-Agents-List-For-United-States.LNK** |
| 4/4/2012 | 11:21:06 | ..C. | NTFS $MFT | /Users/nromanoff/AppData/Roaming/Microsoft/Windows/Recent/**Undercover-Agents-List-For-United-States.lnk** |
| 4/4/2012 | 11:42:57 | MACB | NTFS $MFT | /Users/vibranium/AppData/Roaming/Microsoft/Office/Recent/**Undercover-Agents-List-For-United-States.LNK** |
| 4/4/2012 | 11:42:58 | MACB | NTFS $MFT | /Users/vibranium/AppData/Roaming/Microsoft/Windows/Recent/**Undercover-Agents-List-For-United-States.lnk** |
| 4/4/2012 | 11:42:58 | MACB | RecentDocs key | Recently opened file of extension: .xlsx - value: **Undercover-Agents-List-For-United-States.xlsx** |
| 4/4/2012 | 15:42:58 | .ACB | Internet Explorer | visited file:///C:/Users/nromanoff/Documents/Undercover%20Agent-List-Classified/Agents-List-CLASSIFIED-TOP-SECRET/**Undercover-Agents-List-For-United-States.xlsx** |
|  |  |  |  |  |
|  |  |  |  |  |
| UK |  |  |  |  |
| 4/4/2012 | 7:43:17 | M... | Internet Explorer | visited file:///C:/Users/nromanoff/Documents/Undercover%20Agent-List-Classified/Agents-List-CLASSIFIED-TOP-SECRET/Undercover-Agents-List-For-United-Kingdom.xls |
| 4/4/2012 | 11:21:06 | ..C. | NTFS $MFT | /Users/nromanoff/AppData/Roaming/Microsoft/Office/Recent/Undercover-Agents-List-For-United-Kingdom.LNK |
| 4/4/2012 | 11:21:06 | ..C. | NTFS $MFT | /Users/nromanoff/AppData/Roaming/Microsoft/Windows/Recent/Undercover-Agents-List-For-United-Kingdom.lnk |
| 4/4/2012 | 11:43:15 | ..C. | NTFS $MFT | /Users/nromanoff/Documents/Undercover Agent-List-Classified/Agents-List-CLASSIFIED-TOP-SECRET/Undercover-Agents-List-For-United-Kingdom.xls |
| 4/4/2012 | 11:43:16 | ...B | NTFS $MFT | /Users/vibranium/AppData/Roaming/Microsoft/Office/Recent/Undercover-Agents-List-For-United-Kingdom.LNK |
| 4/4/2012 | 11:43:17 | MAC. | NTFS $MFT | /Users/vibranium/AppData/Roaming/Microsoft/Office/Recent/Undercover-Agents-List-For-United-Kingdom.LNK |
| 4/4/2012 | 11:43:17 | MACB | NTFS $MFT | /Users/vibranium/AppData/Roaming/Microsoft/Windows/Recent/Undercover-Agents-List-For-United-Kingdom.lnk |
| 4/4/2012 | 11:43:17 | MACB | RecentDocs key | Recently opened file of extension: .xls - value: Undercover-Agents-List-For-United-Kingdom.xls |
| 4/4/2012 | 15:43:17 | .ACB | Internet Explorer | visited file:///C:/Users/nromanoff/Documents/Undercover%20Agent-List-Classified/Agents-List-CLASSIFIED-TOP-SECRET/Undercover-Agents-List-For-United-Kingdom.xls |
|  |  |  |  |  |
| Australia |  |  |  |  |
| 4/4/2012 | 11:21:06 | ..C. | NTFS $MFT | /Users/nromanoff/AppData/Roaming/Microsoft/Office/Recent/Undercover-Agents-List-For-Australia.LNK |
| 4/4/2012 | 11:21:06 | ..C. | NTFS $MFT | /Users/nromanoff/Documents/Undercover Agent-List-Classified/Agents-List-CLASSIFIED-TOP-SECRET/Undercover-Agents-List-For-Australia.xls |
| 4/4/2012 | 11:21:06 | ..C. | NTFS $MFT | /Users/nromanoff/AppData/Roaming/Microsoft/Windows/Recent/Undercover-Agents-List-For-Australia.lnk |
|  |  |  |  |  |
|  |  |  |  |  |
| Spain |  |  |  |  |
| 4/4/2012 | 11:21:06 | ..C. | NTFS $MFT | /Users/nromanoff/Documents/Undercover Agent-List-Classified/Agents-List-CLASSIFIED-TOP-SECRET/Undercover-Agents-List-For-Spain.xlsx |

## I would appreciate assistance going through these MAC times and file names to see if any of these files have been copied or moved. Thanks!

## 

## 

## 

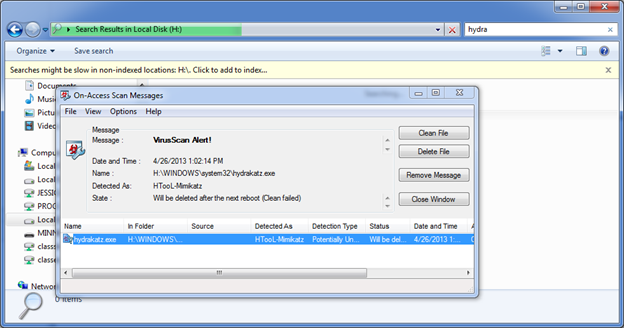
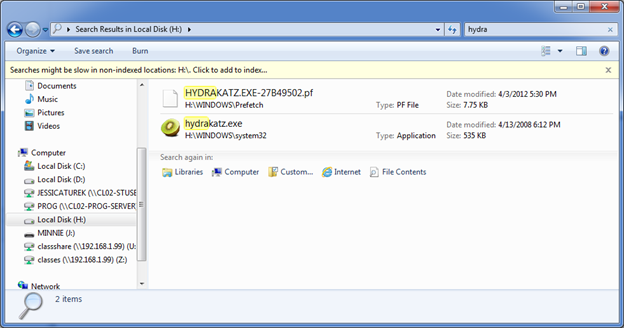
## 

## 

## Bonus information

Who compromised us? Hydra

How did they breach the network?

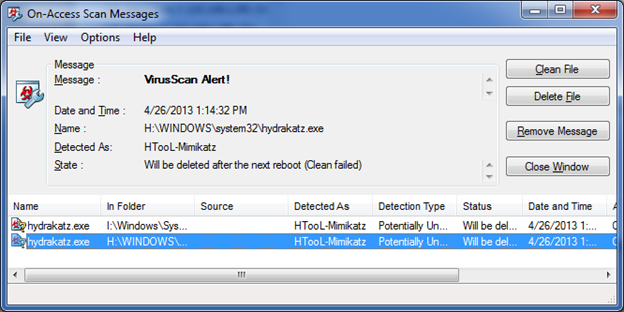
What malware was used?  
  
I (Jessica Turek) mounted Dungan’s c drive to Local Disk H, opened Windows Explorer and searched for “hydra” on Dungan’s machine, since they are enemies of Captain America. They might know his shield is made of vibranium and want that technology for themselves. As I was doing so, this alert (shown above) popped up. When the search finished it found these two files:

As shown on Wikipedia, “Katz is a common German surname”:

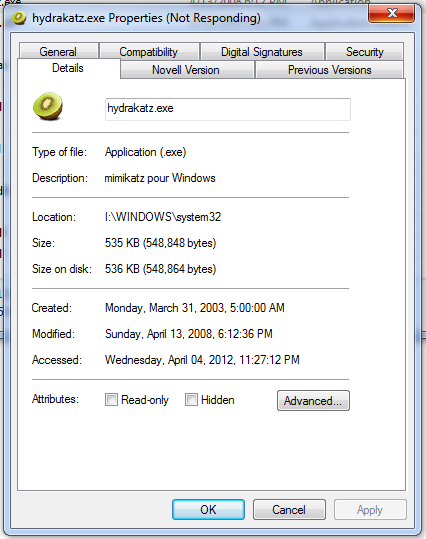


The fact that the name of the file is “hydrakatz” hydra being the name of the German based enemy and katz being a common German surname, this could be from hydra.

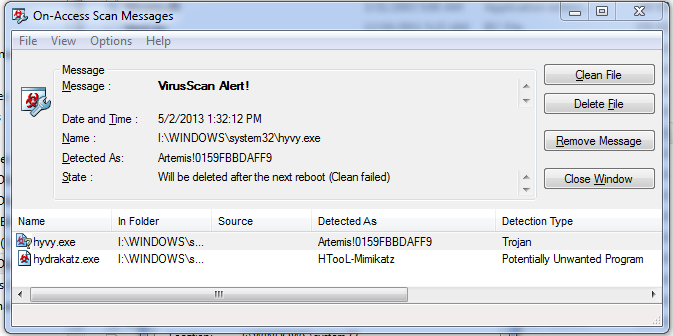
  
Also from Wikipedia, we know that Prefetch means to pre-load machine code from memory.  
  
I used FTK imager to mount Romanoff’s c drive to Local Disk I, and did a File Explorer search for hydra. Again I got the same virus alert:



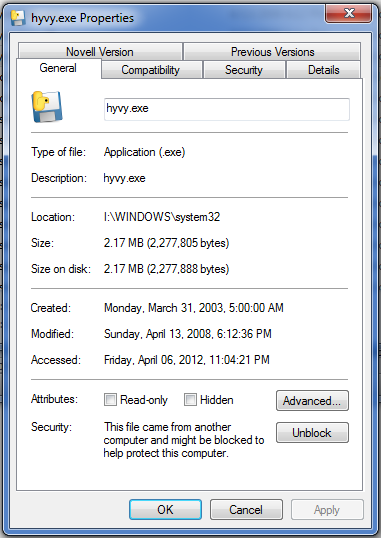
It appears that this virus was accessed on April 4th, 2012 at 11:27 PM

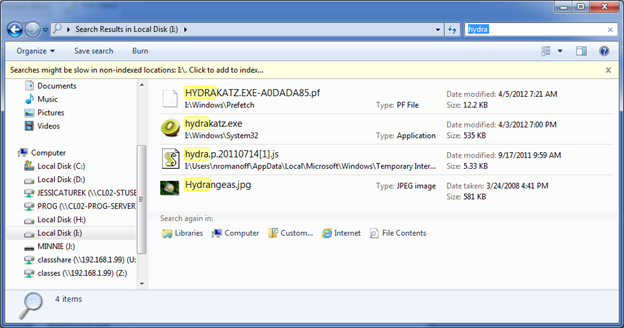


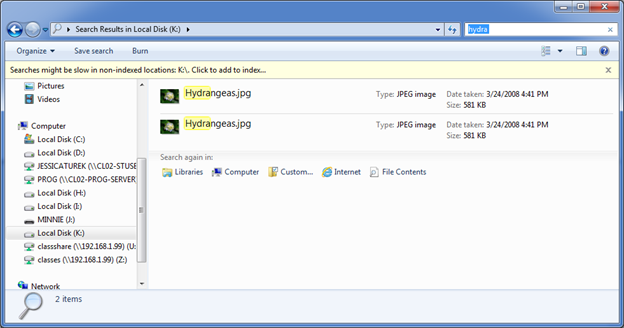
Another virus was found:



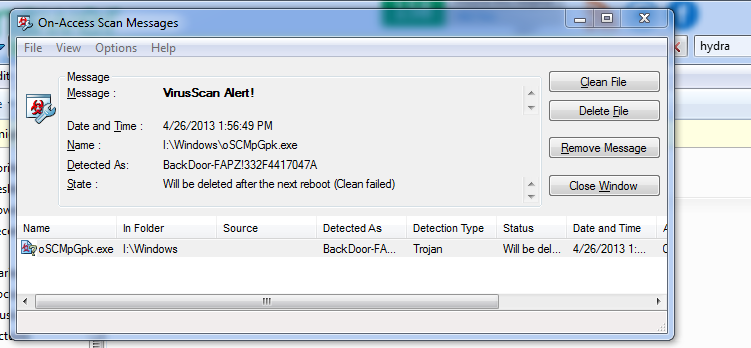
This is a Trojan, and was accessed on April 6th 2012:

  
A few more files were found this time:

  
I used FTK imager to mount Fury’s c drive to Local Disk K and performed the same search. He had two copies of the Hydrangeas picture that was on Romanoff’s machine, but it was not infected with the virus. Romanoff’s machine is the only one with a javascript file called “hydra,” so my guess is that hers is the machine that was infected.

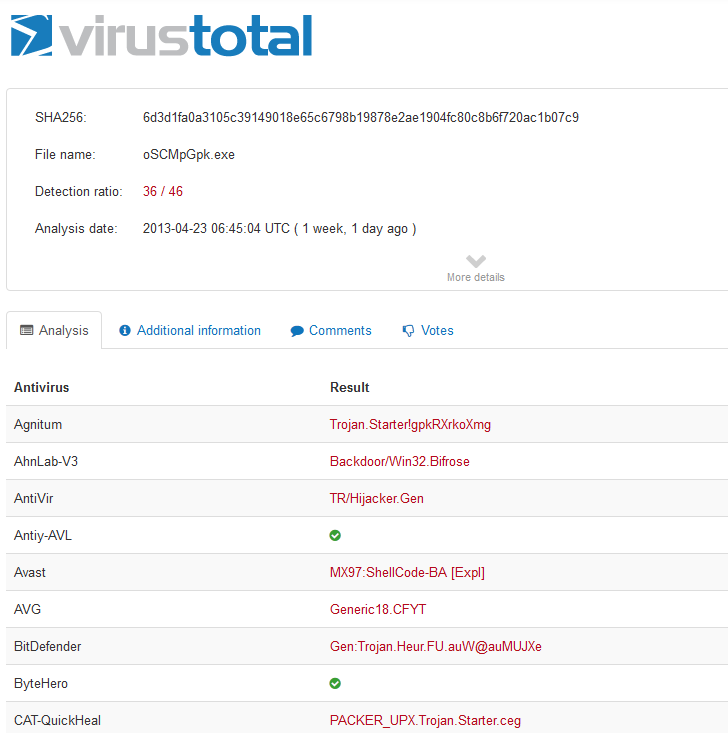


I (David Barlow) mounted Romanoff’s c drive and did a search on file names and content and it immediately found the following virus/malware:



Mark and Stephanie uploaded this file to VirusTotal.com and ran an analysis on oSCMpGpk.exe. 36 of 46 anti-virus programs recognized the file as a virus. The report can be found at this URL:

<https://www.virustotal.com/en/file/6d3d1fa0a3105c39149018e65c6798b19878e2ae1904fc80c8b6f720ac1b07c9/analysis/>



Microsoft recognizes this virus as Trojan:Win32/Swrort.A. On <http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Trojan%3AWin32%2FSwrort.A>, an analysis by Elda Dimakiling reports:

Trojan:Win32/Swrort.A is a detection for files that try to connect to a remote server. Once connected, an attacker can perform malicious routines such as downloading other files.

Trojan:Win32/Swrort.A may arrive in the system as a downloaded file from a malicious site or may be used as payloads of exploit files.

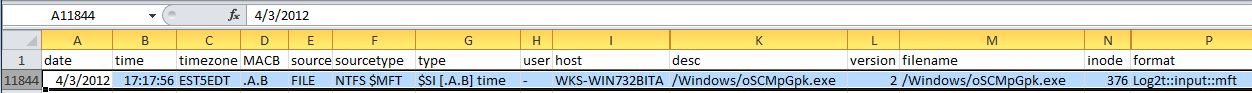
Once executed, Trojan:Win32/Swrort.A may connect to a remote server using different port numbers. Once connected, an attacker can perform malicious routines such as downloading other malware and executing them.

In the wild, Trojan:Win32/Swrort.A is known to connect to the following servers:

* 202.54.98.156 via TCP port 4444
* 10.10.10.31 via TCP port 443
* 188.50.82.246 via TCP port 1234

Searching for these ports may help us determine access times. After searching the win7-32-nromanoff\_supertimeline.csv file for the 3 aforementioned IP addresses, no hits were found.

We then turned to the win7-32-nromanoff\_supertimeline.csv file and searched for “oSCMpGPK.exe” and found only one hit on line 11844 on 4/3/2012 at 17:17:56



I searched for this string in T-Dungan-Findings.xlsx and found nothing.

Copied into file at 5/1/2013 22:07 - Mark Broadhead

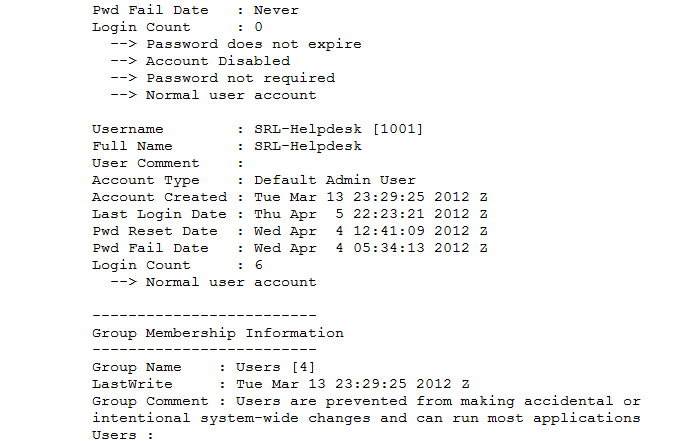
All signs currently point to Hydra as being the foe. I am currently investigating how they breached the network. I will look for irregularities in event logs, user accounts specifically trying to find when the breach occurred in order to find the methods.

First I decided to look at the 2008R2 box and looked through the event logs. I filtered the logs looking for only Critical and Warning entries. In the application logs, an error started on 3/28/2012 at 1:39:34 PM. From SceCli, event id 1202, an error 0x532: No mapping between account names and security IDs was done. Error 0x533 occurs when a user account in one or more GPOs could not be resolved to a SID. This error is possibly caused by a mistyped or deleted user account referenced in either the User Rights or Restricted Groups branch of a GPO.

I checked the win2008R2\_SAM\_rip.txt and don’t see any users created after Dec 5th 2009, when the default Guest and Admin accounts were created. I found nothing out of the ordinary.

NFURY ANALYSIS

On the win7-64\_SAM\_rip.txt an account was created on Tue Mar 13 at 23:29:25 2012, (the night after the discovery was announced on twitter.) called SRL-Helpdesk. This account was used 6 times and was last used on Thu Apr 5th at 22:23:21 2012 Also, the times of access, being so late at night, are very suspicious.



In the win7-64\_SOFTWARE\_rip.txt file, I searched for “Mar “ to see all activity in March of 2012. These caught my attention.

Image File Execution Options is a method used to ensure malicious code executes at start-up. (according to<http://blogs.mcafee.com/mcafee-labs/image-file-execution-options>)

Image File Execution Options

Microsoft\Windows NT\CurrentVersion\Image File Execution Options

LastWrite Time Tue Mar 13 20:16:54 2012 (UTC)

Microsoft\Windows\CurrentVersion\Shell Extensions\Approved

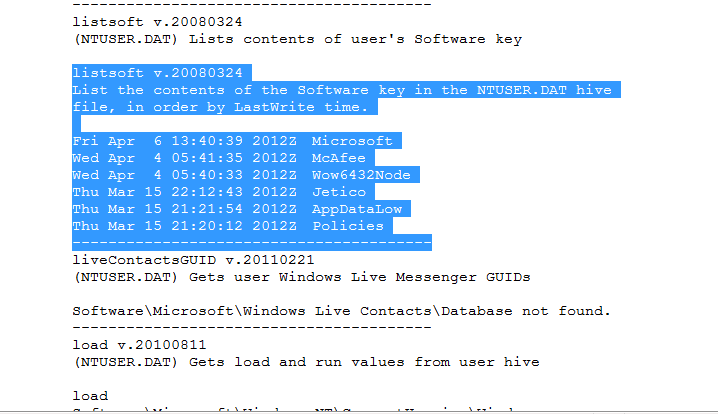
LastWrite Time Thu Mar 15 22:11:55 2012 (UTC)

SPP\_Clients

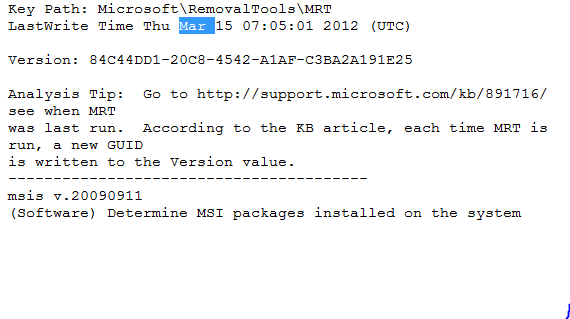
Microsoft\WINDOWS NT\CURRENTVERSION\SPP\Clients

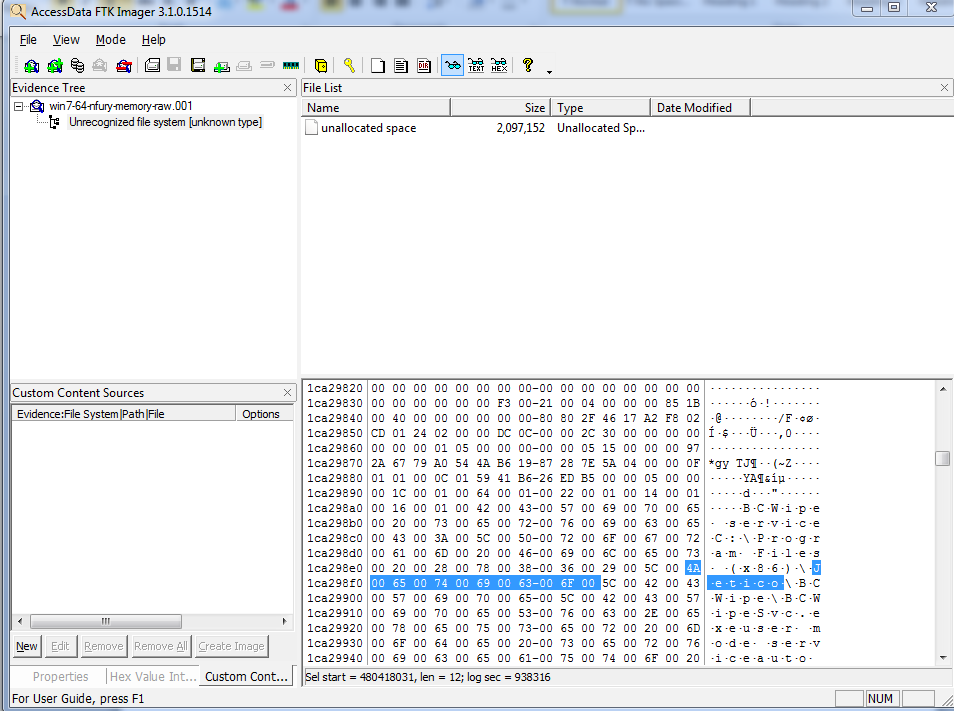
LastWrite Time Thu Mar 15 22:19:14 2012 (UTC)

{09F7EDC5-294E-4180-AF6A-FB0E6A0E9513} = \\?\Volume{d38a501b-ecfc-11df-a2d7-806e6f6e6963}\:(C%3A)

Looking through the win7-64\_SRL-Helpdesk\_NTUSER\_rip.txt, I found something interesting. 

A google search of jetico revealed the software to be used for securely removing data from hard drives.

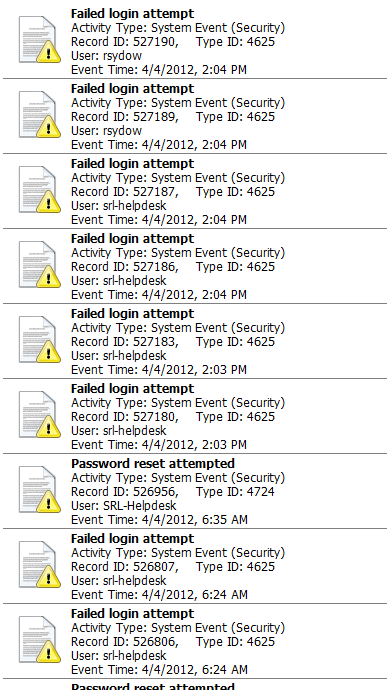
Microsoft Removal Tool has a last write time of Mar 15 07:05:01 2012

I mounted the win7-64-nfury-memory-raw.001 and searched for jetico. At memory location 1ca298f0 I found:

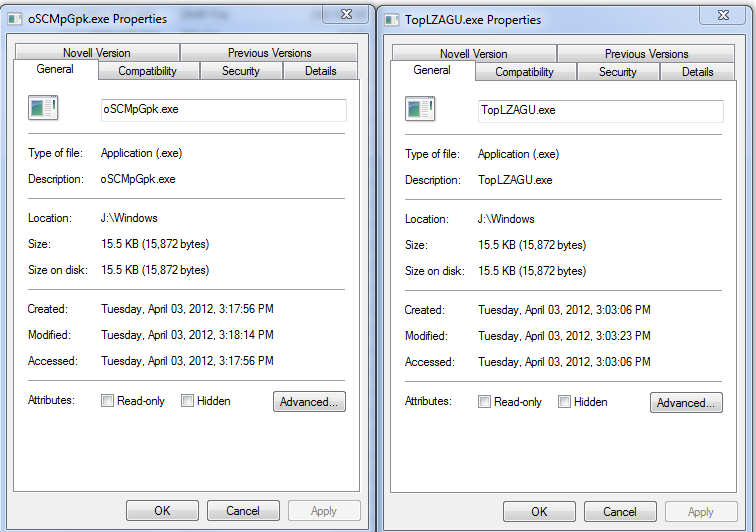
“BCWipe service C:\Program Files (x86)\Jetico\BCWipe\BCWipeSvc.exeuser mode serviceautostartLocalSystem

According to [jetico.com](http://www.jetico.com/bcwipe4_web_help/html/02_main_functions/01_main_functions.htm), The main functions and tools of the BCWipe system are Transparent Wiping, Delete with wiping, Wipe Temporary Internet files, Wipe local history, Swap file protection, File slacks wiping, Wipe of directory entries and MFT records. This shows that someone potentially mischievous software may be working on this computer, or, it may be a precaution taken by S.H.I.E.L.D. to prevent data leakage.

I (Stephanie Sharp) found a lot of unusual activity on 4/3 & 4/4 on Romanoff’s C Drive. There were over a dozen failed login attempts:



Looking more at nromanoffs drive I got another virus alert. for TopLZAGU.exe. I decided to look at the creation/access times of the programs that were flagged as a virus. I noticed that both of these files are exactly 15,872 bytes. I suspected that it was the same file with different names so I got the hashes of each of them to verify this. I expected to have the same hash value for both files, but it wasn’t meaning it is possible it is another file altogether. I tried to scan the file on VirusTotal.com but didn’t have any success.



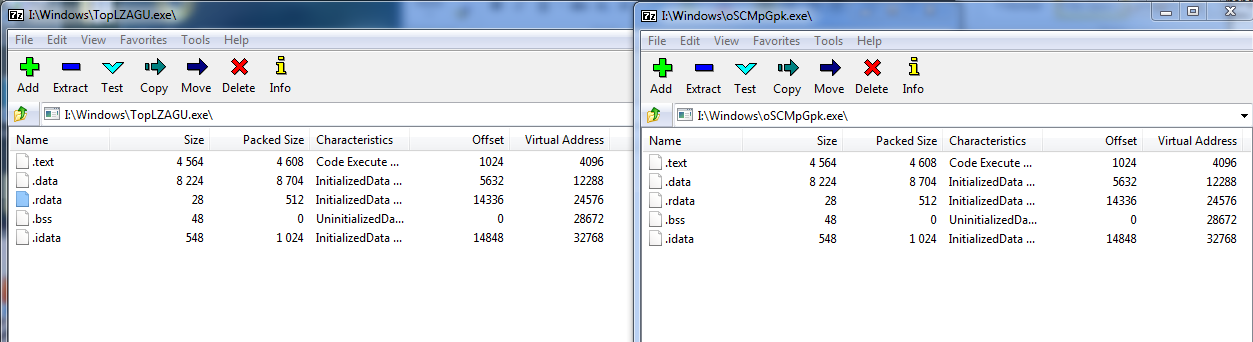
oSCMpGpk.exe hash 332f4417047a14e7379fd6ec24b302e1

TopLZAGU.exe hash 4ea46cab21a0146e5f12a8757b01694e

McKay Thompson

(Stephanie, McKay, Mark)

We found that the oSCMpGpk.exe file and the TopLZAGU.exe file are detected as different viruses however they have the exact same structure:



Were Files exfiltrated? If so, what? by Cassidy

I used web historian to look at the access of each user to sensitive files on their machine. Using this method, I should be able to view if they accessed a sensitive file from a flash drive or location other than the C: on which it resides.

TDUNGAN: has credit card files, vibranium research files, and HQ information files.



Tdungan only accessed his files from within the C drive, leaving no evidence of exfiltration. One exception is the “Stark Research Labs” document, which was put on the website and is not sensitive information. As for his knowledge of the future headquarters of SHIELD:

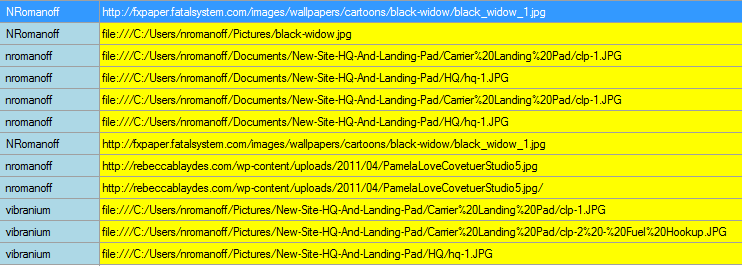


The same case applies. All sensitive material was accessed from the appropriate location.

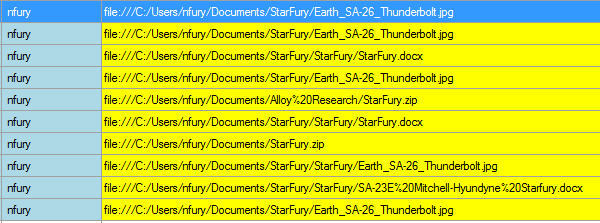
NROMANOFF: has undercover agent files, and pictures of the new HQ:



All undercover information files were accessed from an appropriate location. As were pictures of HQ:



NFURY: has information on StarFury research but only accesses it in appropriate places:



The evidence points to compromise by HYDRA, but they did not have any inside help exfiltrating files.

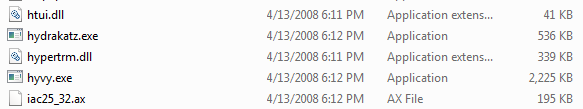
How did the malware get on the system? By Cassidy

One piece of malware connected to hydrakatz.exe, is hyvy.exe



We can see it is a trojan, and below, we see that tdungan accessed the directory that holds this trojan file.





The dates for these files do not look as if they match, but that is the modified date, which stays the same when downloaded or copied. On the properties view below, we can see thy hyvy file was accessed more recently, opening up the possibility of data exfiltration through this trojan program.

