In the wild....

Official malware report

TrojanDropper.Win32-Rovnix.I

Procedure Summary	
Procedure:	Malware reverse engineering (dynamic malware analysis)
Author:	*Rick Flores*
In the wild:	*https://twitter.com/nanotechz9l*
Effective Date:	07/28/2013
Greetz to my peeps:	@iqlusion, @JC_SoCal, @kongo_86, @isomorphix, @yourmom
Source File Location:	-TBD

Revision Summary				
Rev	**Description of changes**	**Changes by:**	**Review / Approval by:**	**Date**
1.0	Rough DRAFT	*Flores, Rick*	*N/A*	07/28/2013

Report Details			
Infected user	**Computer Name**	**Malware Analyst**	**Date**
INTERWEBZ	DEN-0425V_F.anon.local	*Flores, Rick*	07/28/2013

Table of Contents

1. SCOPE

1.1 I created this malware report in an effort to track write effective snort sigs, categorize, contain, understand root cause and infection vector of said malware sample, user account/s, networked equipment and or computer/s.

2. INVESTIGATION GOALS

2.1 Determine extent of infection, uncover actual business risk, data exposure, network weakness, and figure out infection vector and propogation methods.

2.2 More importantly this report should uncover host based indicators that can be uploaded and used to detect infection, and include network signatures used to alert/prevent potential infection (*Snort, DNS sinkhole*… etc).

3. MALWARE SAMPLE/S ANALYZED

3.1 TrojanDropper.Win32/Rovnix.I variant

Filename : ronvix.exe | *exe.ex*

MD5 : 605daaa9662b82c0d5982ad3a742d2e7 ronvix.exe

SHA1 : a9fd55b88636f0a66748c205b0a3918aec6a1a20 ronvix.exe

SHA256 : 9eb49c945a102c8f7ec9cc6f44502e167913ddd2c4a5f42fbb7a4009e1c9cf75 ronvix.exe

SSDEEP : ssdeep,1.1--blocksize:hash:hash,filename

6144:FP5fPcb7bfEO2FJQ0NZzeVMzxXb6OTHhUF0qcJCqE21fD3tC5E9QsOwUQ:HcbcFLHKVMzxXBTHKF0pcOzU/w3,"/malware/ronvix.exe"

3.2 Location C:\Documents and Settings**anonymousvictim**\Local Settings\Temp\ronvix.exe

3.3 Moving forward, and for brevity I will be referring to "ronvix.exe" simply as the malware sample. When you read `malware sample` or simply 'sample' in the remainder of this report, safely assume I am referring to ronvix.exe which is the malicious sample used as the basis of this malware report.

3.4 Malware Sample properties. Note the Usb HDD temperature monitoring information recorded, and Original File Name below : "usbhdd.exe"

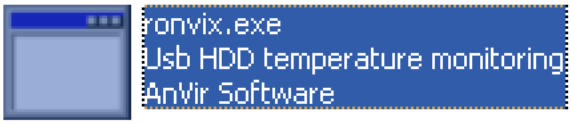


Figure 1: Filename and description.

4.0 Windows executable resource attributes.

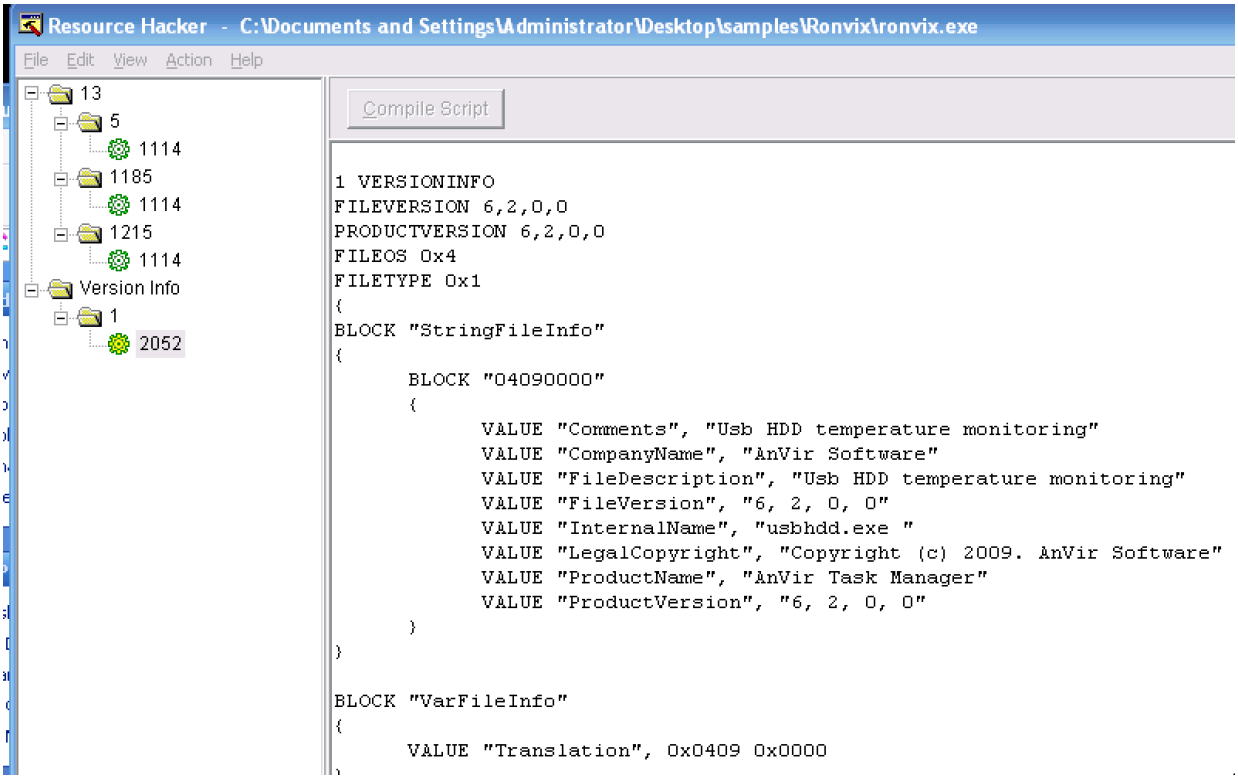


Figure 2: Resource information on executable.

4. MALWARE VARIANT HISTORY, TIMELINE, AND SPECIAL FEATURES

4.1 The fact that this sample introduces a private TCP/IP stack that works in both kernel/user land makes it a sample we should keep tabs on.

4.2 Microsoft discovered a sample utilizing private TCP/IP stacks first in Dec 9 2012. The backdoor implemented at the NDIS (Network Driver Interface Specification) level. It does this in an effort to conceal its networking communications via stealth.

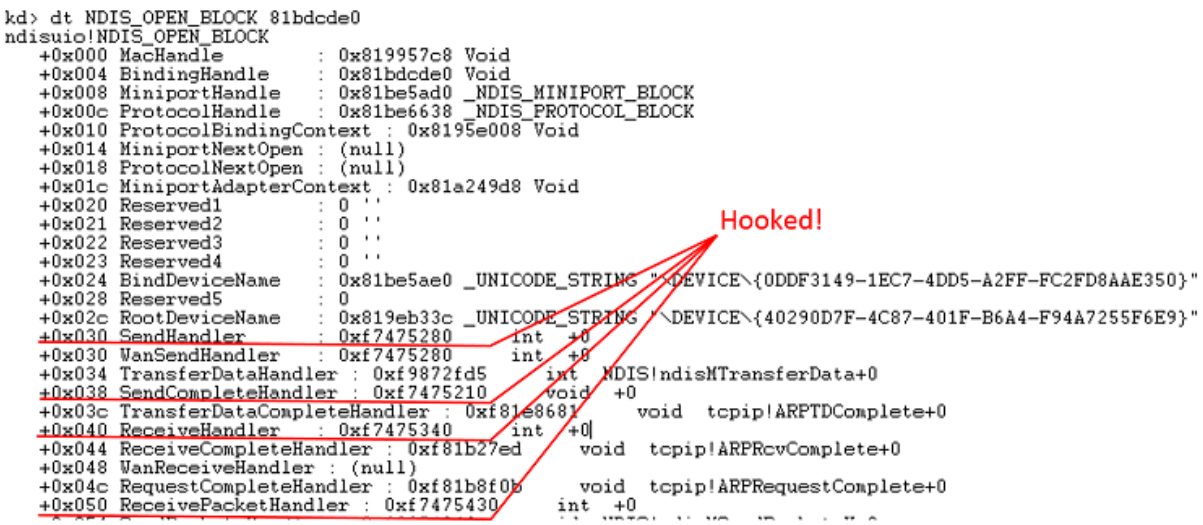


Figure 3: Hooked functions in NDIS_OPEN_BLOCK.

5. GENERAL FUNCTION AND FUNCTIONALITY OF THE MALWARE

5.1 The main function of this malware is to download additional malware from the **youtubeflashserver.com** website. However since the website has been taken down, knowing exactly what is downloaded is uncertain at this time because both ways of the conversation (client/server) could not be viewed within the packet capture.

6. BEHAVIORAL PATTERNS OF THE MALWARE AND LOCAL SYSTEM INTERACTION

6.1 As soon as I executed the sample it immediately deleted itself, and it triggered a system reboot upon successful malware installation.

6.2 Deleted files can be seen below. It looks like it deleted the system security log file.

Description	Name
Deleted File	C:\WINDOWS\system32\config\systemprofile\Local Settings\Temp\Perflib_Perfdata_7a8.dat
Deleted File	C:\WINDOWS\system32\CatRoot2\tmp.edb
Deleted File	C:\WINDOWS\security\logs\scecomp.log
Deleted File	C:\Documents and Settings\Administrator\Local Settings\Temp\Perflib_Perfdata_5ec.dat

Description	Name
Deleted File	C:\WINDOWS\System32\config\systemprofile\Local Settings\Temp\Perflib_Perfdata_7a8.dat
Deleted File	C:\WINDOWS\System32\CatRoot2\tmp.edb

Figure 4: Deleted files.

7. FILES AND REGISTRY KEYS CREATED, MODIFIED AND ACCESSED

7.1 The dropped files/folders can be seen below.

Description	Name
New Folder	C:\Documents and Settings\All Users\Application Data\Adobe\Reader
New Folder	C:\Documents and Settings\All Users\Application Data\Adobe\Reader\9.5
New Folder	C:\Documents and Settings\All Users\Application Data\Adobe\Reader\9.5\ARM
New Folder	C:\Documents and Settings\Administrator\Application Data\Adobe\Acrobat\9.0\JavaScripts
New File	C:\WINDOWS\system32\spool\drivers\w32x86\PS5UI.DLL
New File	C:\WINDOWS\system32\config\systemprofile\Local Settings\Temp\Perflib_Perfdata_6ec.dat
New File	C:\WINDOWS\SoftwareDistribution\DataStore\Logs\tmp.edb
New File	C:\WINDOWS\security\logs\scecomp.old
New File	C:\WINDOWS\Prefetch\ATTRIB.EXE-39EAFB02.pf
New File	C:\Documents and Settings\Administrator\Local Settings\Temp\ArmUI.ini
New File	C:\Documents and Settings\Administrator\Local Settings\Temp\Perflib_Perfdata_4fc.dat
New File	C:\Documents and Settings\Administrator\Local Settings\Temp\wireshark_pcapng_7C85AFC4-4BA5-4A17-8D03-9418EA6E04E6_20130731144831_a01140
New File	C:\Documents and Settings\Administrator\Desktop\samples\Ronvix\26432281.bat
New File	C:\Documents and Settings\Administrator\Application Data\Adobe\Acrobat\9.0\JavaScripts\glob.js
New File	C:\Documents and Settings\Administrator\Application Data\Adobe\Acrobat\9.0\JavaScripts\glob.settings.js
New File	C:\Documents and Settings\Administrator\Application Data\Adobe\Acrobat\9.0\TMDocs.sav
New File	C:\Documents and Settings\Administrator\Application Data\Adobe\Acrobat\9.0\TMGrpPrm.sav

Figure 4: Dropped files, and folders.

7.2 The malware sample made 176 critical changes to the registry.

Name	Critical	Warning	Info	Ignored	Tested	Snapshot
HKLM\	176	84	258	2537	7/31/2013 2:49:18 PM	7/31/2013 2:45:38 PM

Figure 6: Critical registry changes.

7.3 The sample deleted the following registry keys from the registry.

Description	Name
Deleted Key	HKLM\SYSTEM\CurrentControlSet\Services\USBSTOR\Enum
Deleted Key	HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_Lexar&Prod_USB_Flash_Drive&Rev_1100\RLCT0OOV1CRYHPN8O5AC&0\Control
Deleted Key	HKLM\SYSTEM\CurrentControlSet\Enum\USB\Vid_05dc&Pid_a788\RLCT0OOV1CRYHPN8O5AC\Control
Deleted Key	HKLM\SYSTEM\CurrentControlSet\Enum\STORAGE\RemovableMedia\8&272f5bd7&0&RM\Control
Deleted Key	HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MSISERVER\0000\Control
Deleted Key	HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_CRYPTSVC\0000\Control
Deleted Key	HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{a5dcbf10-6530-11d2-901f-00c04fb951ed}\##?#USB#Vid_05dc&Pid_a788#RLCT0O
Deleted Key	HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{a5dcbf10-6530-11d2-901f-00c04fb951ed}\##?#USB#Vid_05dc&Pid_a788#RLCT0O
Deleted Key	HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#STORAGE#RemovableMedia#8&27
Deleted Key	HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#STORAGE#RemovableMedia#8&27
Deleted Key	HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f5630a-b6bf-11d0-94f2-00a0c91efb8b}\##?#STORAGE#RemovableMedia#8&27
Deleted Key	HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f5630a-b6bf-11d0-94f2-00a0c91efb8b}\##?#STORAGE#RemovableMedia#8&27
Deleted Key	HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#USBSTOR#Disk&Ven_Lexar&Prod_L
Deleted Key	HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#USBSTOR#Disk&Ven_Lexar&Prod_L
Deleted Key	HKLM\SYSTEM\ControlSet001\Services\USBSTOR\Enum
Deleted Key	HKLM\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_Lexar&Prod_USB_Flash_Drive&Rev_1100\RLCT0OOV1CRYHPN8O5AC&0\Control
Deleted Key	HKLM\SYSTEM\ControlSet001\Enum\USB\Vid_05dc&Pid_a788\RLCT0OOV1CRYHPN8O5AC\Control
Deleted Key	HKLM\SYSTEM\ControlSet001\Enum\STORAGE\RemovableMedia\8&272f5bd7&0&RM\Control
Deleted Key	HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MSISERVER\0000\Control
Deleted Key	HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_CRYPTSVC\0000\Control

Figure 7: Deleted registry keys.

7.4 The malware sample created the following new registry keys, Subkeys, and values.

Description	Name	New Value
New Value	HKLM\SYSTEM\ControlSet003\Enum\USBSTOR\Disk&Ven_Lexar&Prod_USB_Flash_Drive&Rev_1100\RLCT0OOV1CRYHPN8O5AC&0\ConfigFlags	0
New Value	HKLM\SYSTEM\ControlSet003\Enum\USBSTOR\Disk&Ven_Lexar&Prod_USB_Flash_Drive&Rev_1100\RLCT0OOV1CRYHPN8O5AC&0\ParentIdPrefix	8&272f5bd7&0
New Value	HKLM\SYSTEM\ControlSet003\Enum\USBSTOR\Disk&Ven_Lexar&Prod_USB_Flash_Drive&Rev_1100\RLCT0OOV1CRYHPN8O5AC&0\Driver	{4D36E967-E325-11CE-BFC1-08002BE10318}\0001
New Value	HKLM\SYSTEM\ControlSet003\Enum\USBSTOR\Disk&Ven_Lexar&Prod_USB_Flash_Drive&Rev_1100\RLCT0OOV1CRYHPN8O5AC&0\Class	DiskDrive
New Value	HKLM\SYSTEM\ControlSet003\Enum\USBSTOR\Disk&Ven_Lexar&Prod_USB_Flash_Drive&Rev_1100\RLCT0OOV1CRYHPN8O5AC&0\Mfg	(Standard disk drives)
New Value	HKLM\SYSTEM\ControlSet003\Enum\USBSTOR\Disk&Ven_Lexar&Prod_USB_Flash_Drive&Rev_1100\RLCT0OOV1CRYHPN8O5AC&0\FriendlyName	Lexar USB Flash Drive USB Device
New Value	HKLM\SYSTEM\ControlSet003\Enum\USB\Vid_05dc&Pid_a788\RLCT0OOV1CRYHPN8O5AC\DeviceDesc	USB Mass Storage Device
New Value	HKLM\SYSTEM\ControlSet003\Enum\USB\Vid_05dc&Pid_a788\RLCT0OOV1CRYHPN8O5AC\LocationInformation	USB Flash Drive
New Value	HKLM\SYSTEM\ControlSet003\Enum\USB\Vid_05dc&Pid_a788\RLCT0OOV1CRYHPN8O5AC\Capabilities	20
New Value	HKLM\SYSTEM\ControlSet003\Enum\USB\Vid_05dc&Pid_a788\RLCT0OOV1CRYHPN8O5AC\UINumber	0
New Value	HKLM\SYSTEM\ControlSet003\Enum\USB\Vid_05dc&Pid_a788\RLCT0OOV1CRYHPN8O5AC\HardwareID	USB\Vid_05dc&Pid_a788&Rev_1100
New Value	HKLM\SYSTEM\ControlSet003\Enum\USB\Vid_05dc&Pid_a788\RLCT0OOV1CRYHPN8O5AC\CompatibleIDs	USB\Class_08&SubClass_06&Prot_50
New Value	HKLM\SYSTEM\ControlSet003\Enum\USB\Vid_05dc&Pid_a788\RLCT0OOV1CRYHPN8O5AC\ClassGUID	{36FC9E60-C465-11CF-8056-444553540000}
New Value	HKLM\SYSTEM\ControlSet003\Enum\USB\Vid_05dc&Pid_a788\RLCT0OOV1CRYHPN8O5AC\Class	USB
New Value	HKLM\SYSTEM\ControlSet003\Enum\USB\Vid_05dc&Pid_a788\RLCT0OOV1CRYHPN8O5AC\Driver	{36FC9E60-C465-11CF-8056-444553540000}\0007
New Value	HKLM\SYSTEM\ControlSet003\Enum\USB\Vid_05dc&Pid_a788\RLCT0OOV1CRYHPN8O5AC\Mfg	Compatible USB storage device
New Value	HKLM\SYSTEM\ControlSet003\Enum\USB\Vid_05dc&Pid_a788\RLCT0OOV1CRYHPN8O5AC\Service	USBSTOR
New Value	HKLM\SYSTEM\ControlSet003\Enum\USB\Vid_05dc&Pid_a788\RLCT0OOV1CRYHPN8O5AC\ConfigFlags	0
New Value	HKLM\SYSTEM\ControlSet003\Enum\USB\Vid_05dc&Pid_a788\RLCT0OOV1CRYHPN8O5AC\Device Parameters\ExtPropDescSemaphore	1
New Value	HKLM\SYSTEM\ControlSet003\Enum\USB\Vid_05dc&Pid_a788\RLCT0OOV1CRYHPN8O5AC\Device Parameters\SymbolicName	\??\USB#Vid_05dc&Pid_a788#RLCT0OOV1CRYHPN8O5AC#...
New Value	HKLM\SYSTEM\ControlSet003\Enum\STORAGE\RemovableMedia\8&272f5bd7&0&RM\Capabilities	96
New Value	HKLM\SYSTEM\ControlSet003\Enum\STORAGE\RemovableMedia\8&272f5bd7&0&RM\ConfigFlags	0
New Value	HKLM\SYSTEM\ControlSet003\Enum\STORAGE\RemovableMedia\8&272f5bd7&0&RM\HardwareID	STORAGE\Volume
New Value	HKLM\SYSTEM\ControlSet003\Enum\STORAGE\RemovableMedia\8&272f5bd7&0&RM\CompatibleIDs	STORAGE\Volume
New Value	HKLM\SYSTEM\ControlSet003\Enum\STORAGE\RemovableMedia\8&272f5bd7&0&RM\ClassGUID	{71A27CDD-812A-11D0-BEC7-08002BE2092F}
New Value	HKLM\SYSTEM\ControlSet003\Enum\STORAGE\RemovableMedia\8&272f5bd7&0&RM\Class	Volume
New Value	HKLM\SYSTEM\ControlSet003\Enum\STORAGE\RemovableMedia\8&272f5bd7&0&RM\Driver	{71A27CDD-812A-11D0-BEC7-08002BE2092F}\0001
New Value	HKLM\SYSTEM\ControlSet003\Enum\STORAGE\RemovableMedia\8&272f5bd7&0&RM\Mfg	Microsoft

Figure 8: New registry keys/values.

7.5 The malware sample modified the following services on the victim machine.

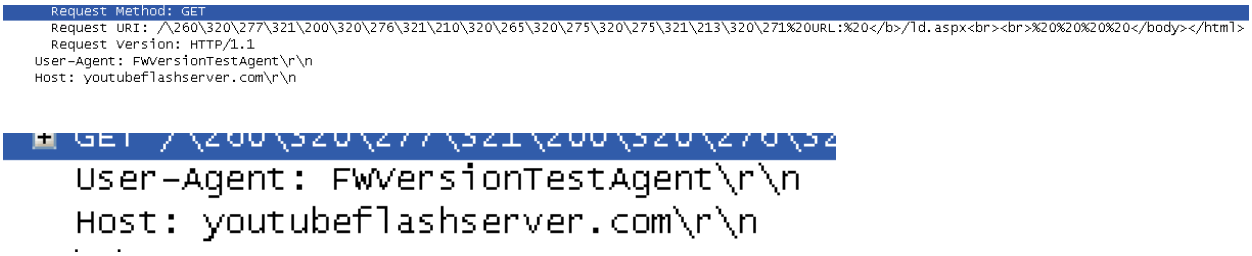
The crypto service provides three management services: Catalog Database Service, which confirms the signatures of Windows files; Protected Root Service, which adds and removes Trusted Root Certification Authority certificates from this computer; and Key Service, which helps enroll this computer for certificates. If this service is stopped, these management services will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start like Windows update, task manager errors, and other OS security features.

Description	Name	New Value	Old Value	Severity
Service State	Cryptographic Services	Stopped	Running	2
Controls Accepted	Cryptographic Services		Stop,Shutdown	3

Figure 9: Stopped the Windows cryptographic service.

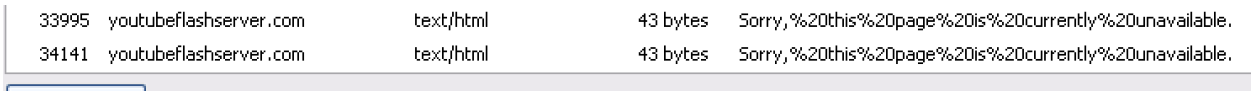
8. NETWORK BEHAVIOR (INCLUDING HOSTS, DOMAINS AND IP'S ACCESSED)

8.1 The user agent string used, and malicious beacon can be seen below.



User-Agent: **FWVersionTestAgent**

Host: **youtubeflashserver.com**



GET /Sorry,%20this%20page%20is%20currently%20unavailable. HTTP/1.1

Figure 10: User-Agent and malicious host.

8.2 The malicious IP's can be seen below. Multiple IP's were witnessed being accessed in wireshark.

1. **200.86.82.126:80**
2. **46.98.198.253:80**
3. **23.72.95.75:80**
4. **109.86.58.178:80**
5. **24.101.46.15:80**

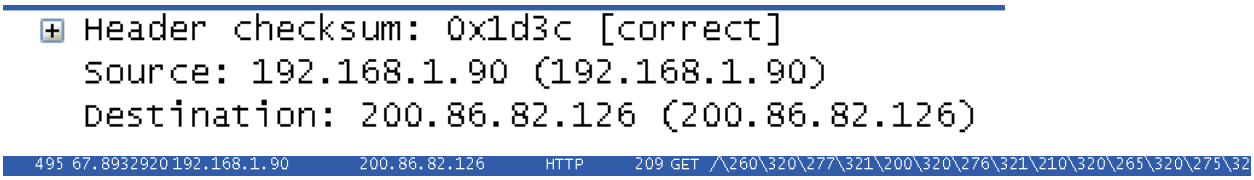


Figure 11: Malicious IP.

8.3 The malicious server details can be found below.

Bulk IP address location

Find the city, country and time zone of one or more IP addresses at a time.

IP ADDRESS	CONTINENT	FLAG	COUNTRY	REGION	CITY	TIME ZONE
200.86.82.126	South America		Chile		Santiago	EST+1

Figure 12: Malicious IP/Host.

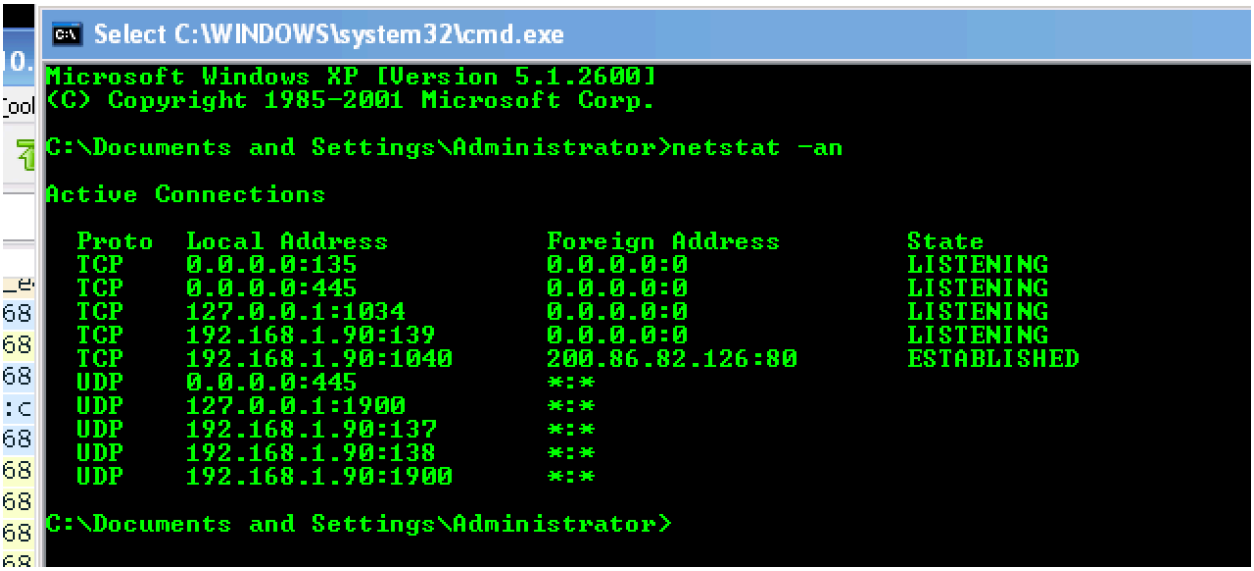


Figure 13: Malicious IP/Host.

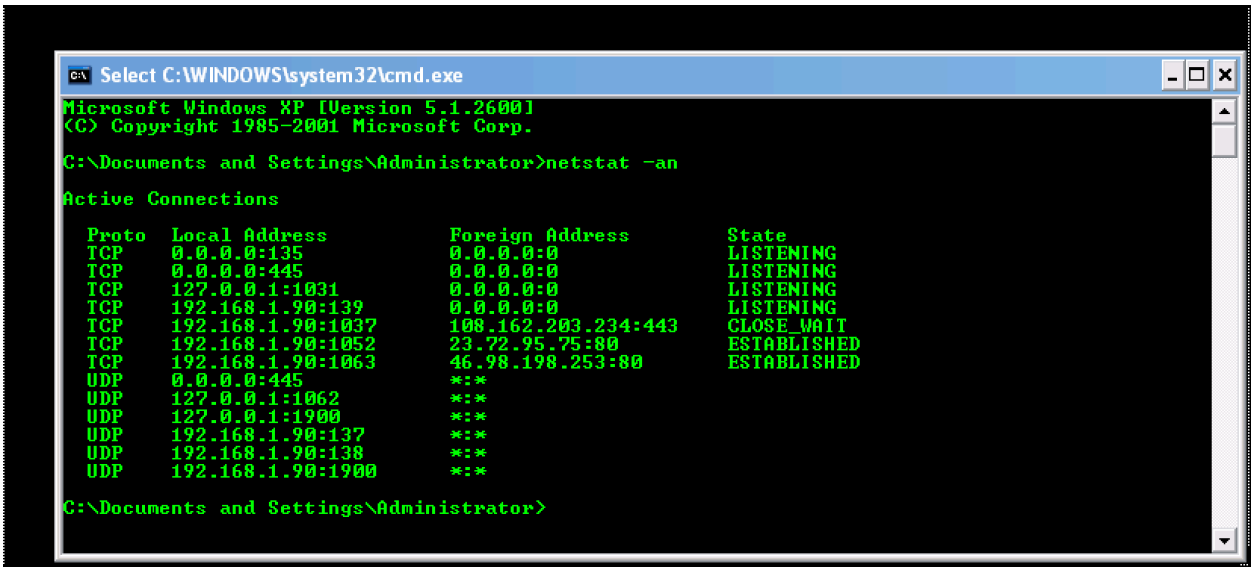


Figure 14: Malicious IP/Host.

9. TIME AND LOCAL SYSTEM DEPENDANT FEATURES

9.1 This malware sample requires a valid internet connection, and execution to activate its payload.

10. METHOD AND MEANS OF COMMUNICATION

10.1 It communications, and receives the payload/instructions from the malicious servers via port TCP 80.

11. ORIGINAL INFECTION VECTOR AND PROPOGATION METHODOLOGY

11.1 The victim could have visited a normal looking site or may have been the victim of a brower exploit running an unpatched browser version. Typical drive by download is another scenario.

12. ANY INFORMATION CONCERNING DEVELOPMENT OF MALWARE (COMPILER TYPE, PACKER USED, COUNTRY OF ORIGIN, AUTHOR, NAMES/HANDLES, ETC.)

12.1 Reverse engineering using static analysis on the malware sample allows me to understand its functionality. Loading the malware sample indicated it might be packed/compressed for several reasons. The memory visualization bar within the IDA GUI was not able to find any encoded/executable data. Usually normal un-packed executables have several blue sections with readable data. Below is a comparison of a packed executable vs a non packed executable application. Also the Imports section is a good indication of a packer being used

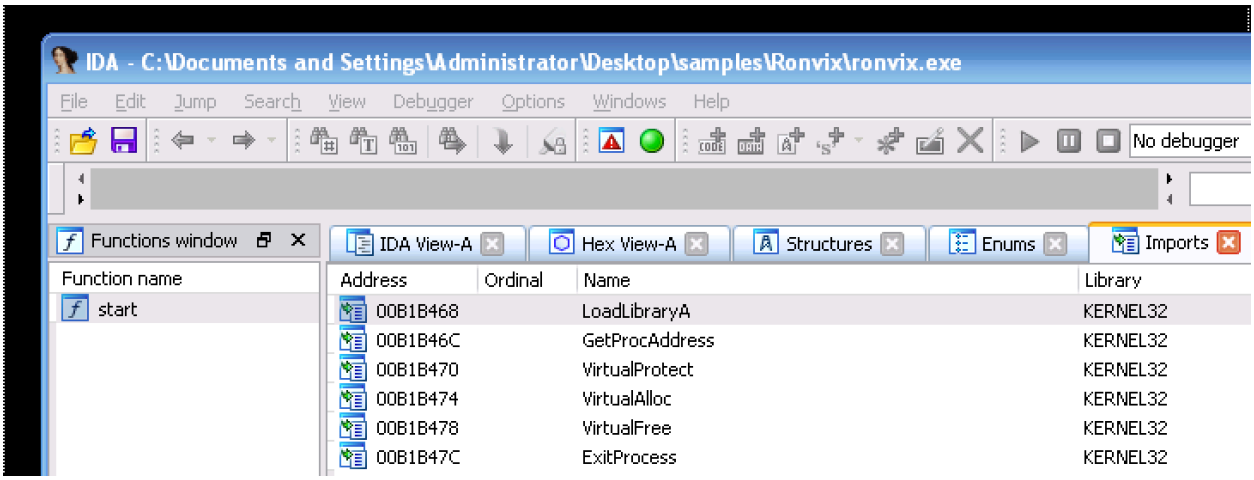
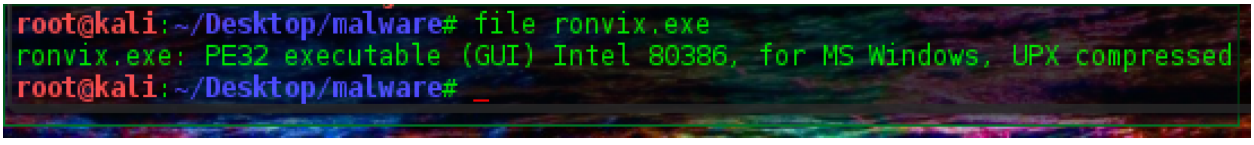


Figure 15: Packed example.

12.2 The unpacking of the malware sample can be seen below. UPX was the popular packer of choice for this sample.



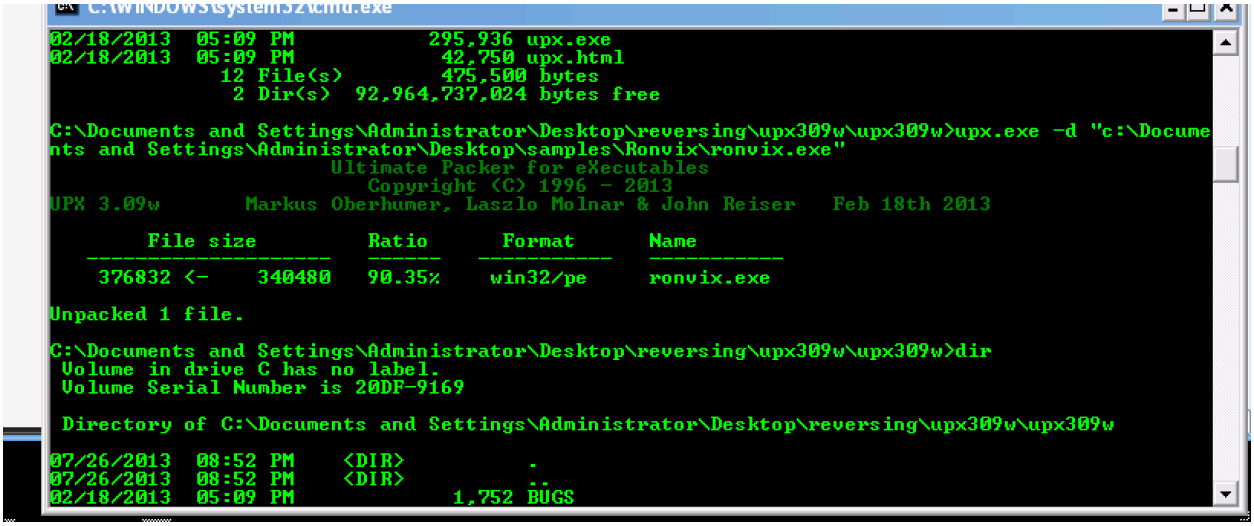


Figure 16: Unpacking the sample with UPX.

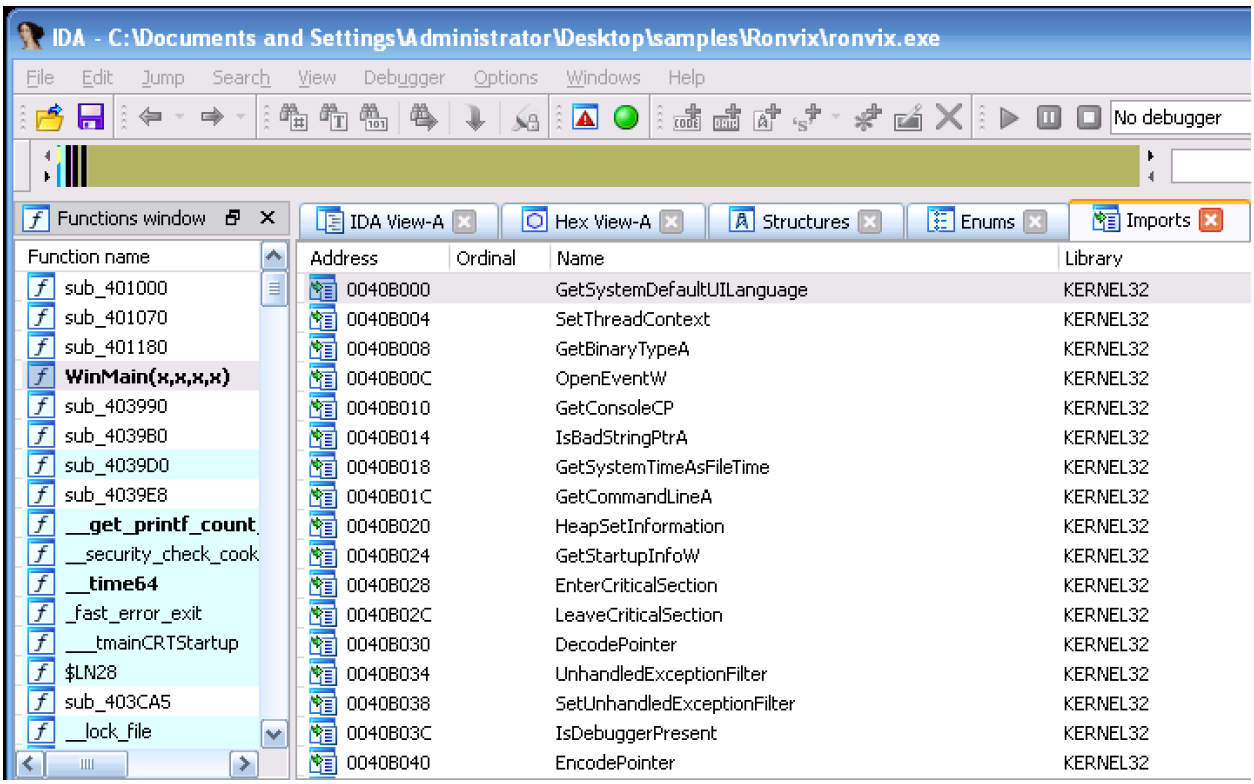
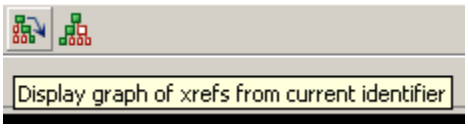


Figure 17: Unpacked example.

Note the memory visualization bar within the unpacked ronvix.exe application.

12.3 Next is a high level overview of the malware sample which involves using the start function and the “display graph of xref’s from current identifier” button. This method allows us to generate a visualization graph. The graph allows us to zoom in and inspect various portions of the program and see how much of it is actually system API calls versus custom implemented code. We can also use the graph overview to see all the function calls the application is making.



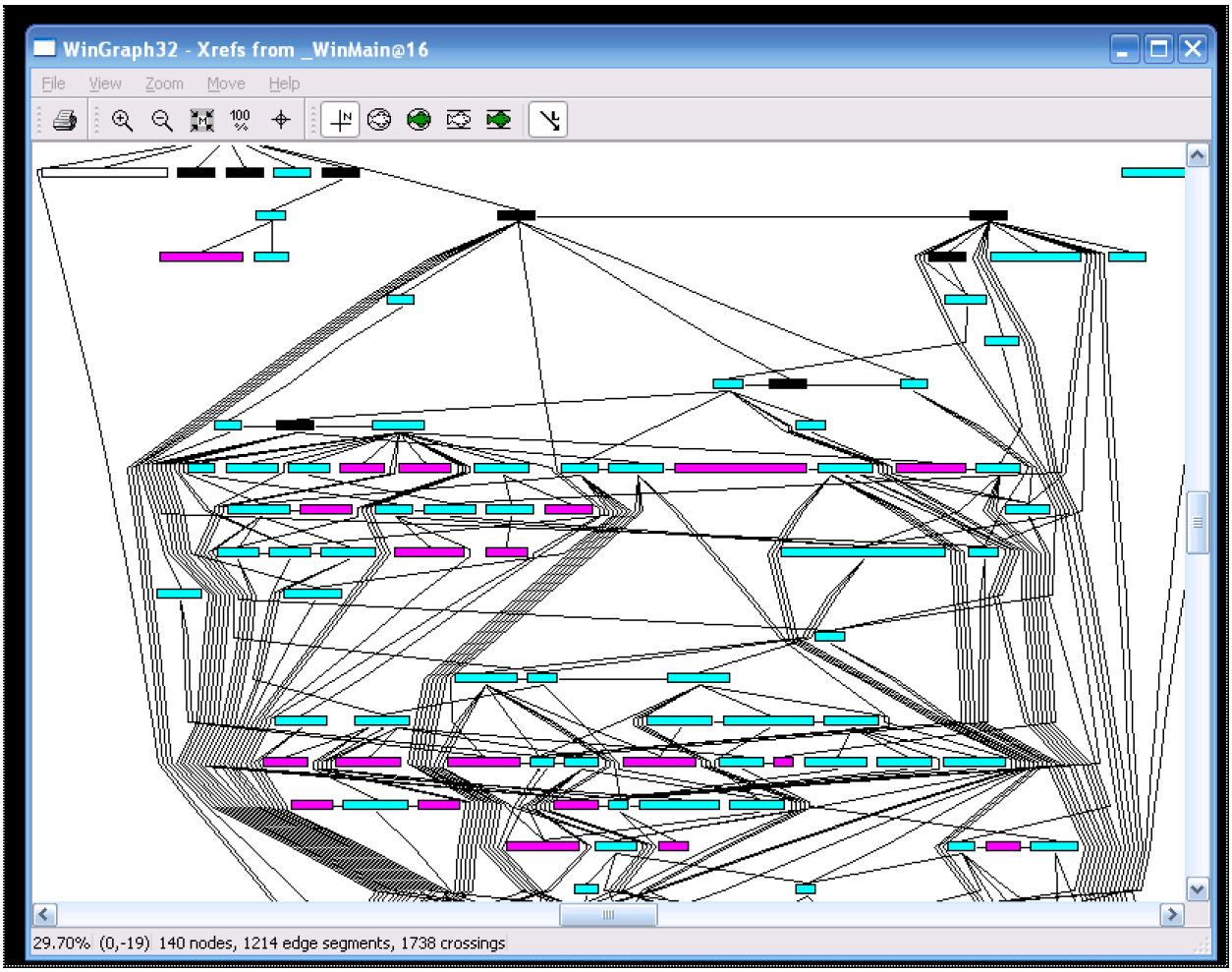


Figure 18: Xref’s from WinMain within the malware sample.

13. KEY QUESTIONS AND ANSWERS

- How did the malware infection occur?

  [Uncertian at this time]

- When did the malware infection occur?

  [Uncertian at this time]

- What vulnerabilities allowed the infection to occur?

  [Uncertian at this time]

- What is the risk of data loss?

  [Uncertian at this time because the malicious host **youtubeflashserver.com** has been taken offline]

14. CONCLUSIONS AND RECOMMENDATIONS TO PREVENT INFECTION/INCIDENT FROM RECURRING

N/A

15. FOLLOWUP ACTIONS AND LESSONS LEARNED

N/A

16. SNORT SIGNATURE TO DETETCT ROVNIX MALICIOUS TRAFFIC

16.1 Below are examples of rough snort sigs that look for specific Rovnix traffic. If the variant changes however these sigs will be useless. More time is needed to analyze the sample and create a solid sig.

16.2 alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"Rovnix malware beacon detected"; flow:to_server,established; content:"User-Agent: FWVersionTestAgent"; content: "|2f b0|"; distance: 6; within: 5; content:"GET"; http_method; content:"ld.aspx?key="; classtype:trojan-activity; rev:1;)

16.3 alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"Rovnix malware beacon detected"; flow:to_server,established; content:"User-Agent: FWVersionTestAgent"; content:"GET"; content:"youtubeflashserver.com"; nocase; classtype:trojan-activity; rev:1;)

16.4 alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"Rovnix malware User-Agent FWVersionTestAgent detected"; flow:to_server,established; content:"User-Agent: FWVersionTestAgent"; classtype:trojan-activity; rev:1;)

16.5 alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"Rovnix malicious host file download from C&C detected"; flow:to_server,established; content:"GET"; content:"youtubeflashserver.com"; nocase; classtype:trojan-activity; rev:1;)

16.6 **Optimized rule**: alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"Rovnix Trojan malicious beacon detected."; flow:to_server,established; offset: 54; depth: 102; flags: PA; content:"GET"; http_method; content:"ld.aspx?key="; content:"User-Agent|3a| FWVersionTestAgent"; nocase; content:"Host|3a| youtubeflashserver.com"; nocase; classtype:trojan-activity; rev:1; reference:url,http://blogs.technet.com/b/mmpc/archive/2013/07/25/the-evolution-of-ronvix-private-tcp-ip-stacks.aspx)

17. REFERENCES

1. Download Rovnix pcap or binary executable: Contact 0xnanoquetz9l +<@>+ gmail.com

2. Virus Total pcap analysis: Contact me<@> email above…

3. http://blogs.technet.com/b/mmpc/archive/2012/12/09/the-quot-hidden-quot-backdoor-virtool-winnt-exforel-a.aspx

4. http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=VirTool:WinNT/Exforel.A#tab=2

5. http://www.esetindia.com/company/news/?show=261653

6. http://www.welivesecurity.com/2011/08/23/hasta-la-vista-bootkit-exploiting-the-vbr/

7. http://blogs.technet.com/b/mmpc/archive/2013/07/25/the-evolution-of-ronvix-private-tcp-ip-stacks.aspx

8. http://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Trojan%3aDOS%2fRovnix.F

9. http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=TrojanDropper%3aWin32%2fRovnix.I

10. http://www.techrepublic.com/blog/10-things/10-windows-xp-services-you-should-never-disable/