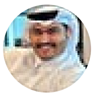
Practical Malware Analysis — Chapter 3 — Lab03–2— Solution



Kamran Saifullah · Follow

4 min read · Aug 29, 2019

Listen Share

Let’s move onto solving the 2nd Lab of Chapter 3. This time we are provided with the DLL file and we have to analyze it.

Starting with the basic static analysis using strings.

```
!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
.reloc
GetModuleFileNameA
Sleep
TerminateThread
WaitForSingleObject
GetSystemTime
CreateThread
GetProcAddress
LoadLibraryA
GetLongPathNameA
GetTempPathA
ReadFile
CloseHandle
CreateProcessA
```

> *GetStartupInfoA*
>
> *CreatePipe*
>
> *GetCurrentDirectoryA*
>
> *GetLastError*
>
> *lstrlenA*
>
> *SetLastError*
>
> *OutputDebugStringA*
>
> *KERNEL32.dll*
>
> *RegisterServiceCtrlHandlerA*
>
> *RegSetValueExA*
>
> *RegCreateKeyA*
>
> *CloseServiceHandle*
>
> *CreateServiceA*
>
> *OpenSCManagerA*
>
> *RegCloseKey*
>
> *RegQueryValueExA*
>
> *RegOpenKeyExA*
>
> *DeleteService*
>
> *OpenServiceA*
>
> *SetServiceStatus*
>
> *ADVAPI32.dll*
>
> *WSASocketA*
>
> *WS2_32.dll*
>
> *InternetReadFile*
>
> *HttpQueryInfoA*
>
> *HttpSendRequestA*
>
> *HttpOpenRequestA*
>
> *InternetConnectA*
>
> *InternetOpenA*
>
> *InternetCloseHandle*
>
> *WININET.dll*
>
> *memset*
>
> *wcstombs*
>
> *strncpy*
>
> *strcat*
>
> *strcpy*
>
> *atoi*

> fclose
>
> fflush
>
> ??3@YAXPAX@Z
>
> fwrite
>
> fopen
>
> strrchr
>
> ??2@YAPAXI@Z
>
> atol
>
> sscanf
>
> strlen
>
> strncat
>
> strstr
>
> _itoa
>
> strchr
>
> __CxxFrameHandler
>
> _EH_prolog
>
> _CxxThrowException
>
> _except_handler3
>
> MSVCRT.dll
>
> ??1type_info@@UAE@XZ
>
> free
>
> _initterm
>
> malloc
>
> _adjust_fdiv
>
> _strnicmp
>
> _chdir
>
> _stricmp
>
> Lab03–02.dll
>
> Install
>
> ServiceMain
>
> UninstallService
>
> installA
>
> uninstallA
>
> Y29ubmVjdA==
>
> practicalmalwareanalysis.com
>
> serve.html
>
> dW5zdXBwb3J0

```
c2xlZXA=
Y21k
cXVpdA==
*/*
Windows XP 6.11
CreateProcessA
kernel32.dll
.exe
GET
HTTP/1.1
%s %s
1234567890123456
quit
exit
getfile
cmd.exe /c
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
— !>
<! —
.PAX
.PAD
DependOnService
RpcSs
ServiceDll
GetModuleFileName() get dll path
Parameters
Type
Start
ObjectName
LocalSystem
ErrorControl
DisplayName
Description
Depends INA+, Collects and stores network configuration and location information, and notifies applications when this information changes.
ImagePath
%SystemRoot%\System32\svchost.exe -k
```

> *SYSTEM\CurrentControlSet\Services\*
>
> *CreateService(%s) error %d*
>
> *Intranet Network Awareness (INA+)*
>
> *%SystemRoot%\System32\svchost.exe -k netsvcs*
>
> *OpenSCManager()*
>
> *You specify service name not in Svchost//netsvcs, must be one of following:*
>
> *RegQueryValueEx(Svchost\netsvcs)*
>
> *netsvcs*
>
> *RegOpenKeyEx(%s) KEY_QUERY_VALUE success.*
>
> *RegOpenKeyEx(%s) KEY_QUERY_VALUE error .*
>
> *SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost*
>
> *IPRIP*
>
> *uninstall success*
>
> *OpenService(%s) error 2*
>
> *OpenService(%s) error 1*
>
> *uninstall is starting*
>
> *.?AVtype_info@@*

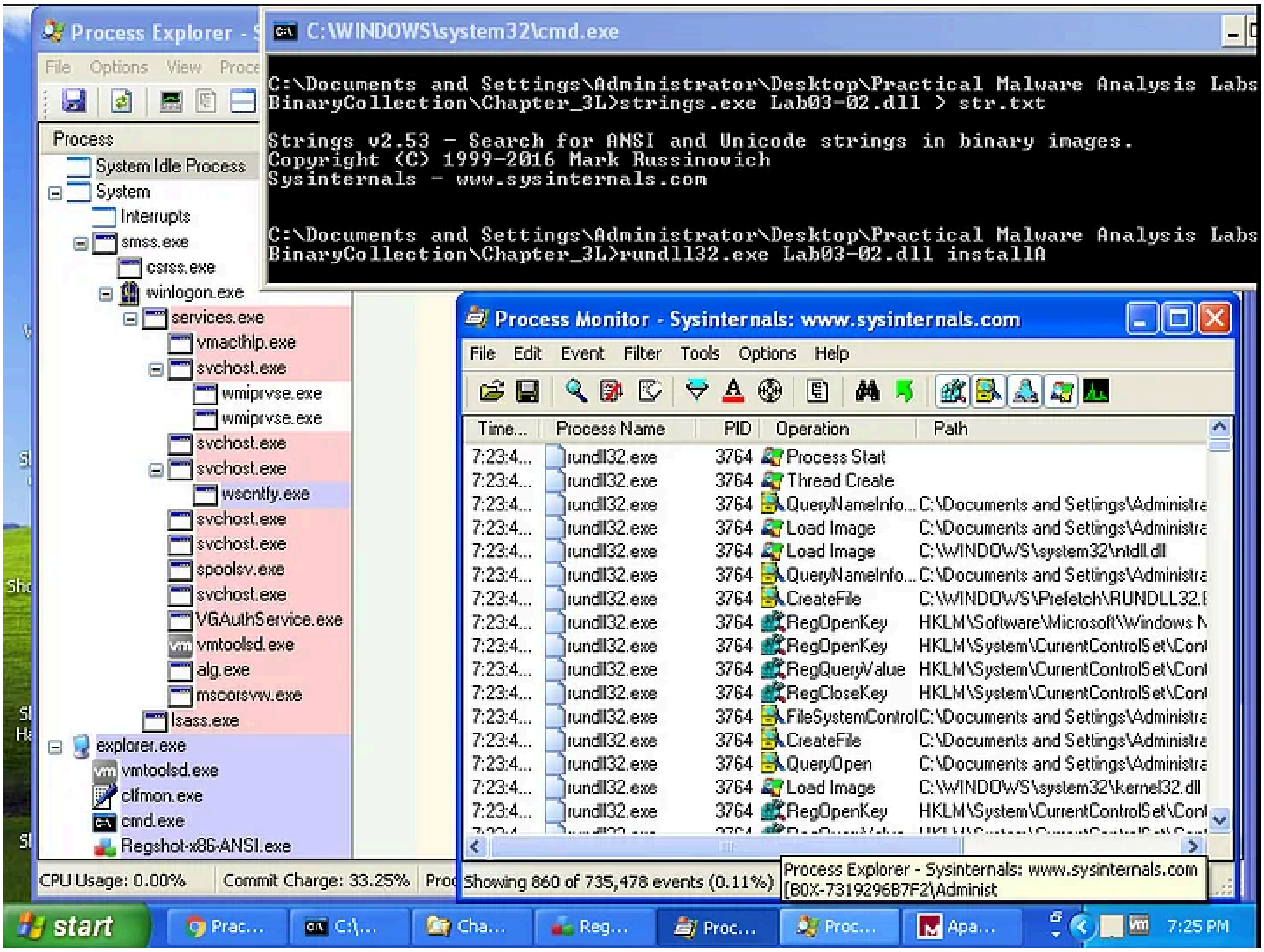
There are lots of strings but the strings we need to focus are

> *practicalmalwareanalysis.com*
>
> *RegSetValueExA*
>
> *RegCreateKeyA*
>
> *CloseServiceHandle*
>
> *CreateServiceA*
>
> *RegCloseKey*
>
> *RegQueryValueExA*
>
> *RegOpenKeyExA*
>
> *DeleteService*
>
> *OpenServiceA*
>
> *SetServiceStatus*
>
> *InternetReadFile*
>
> *HttpQueryInfoA*
>
> *HttpSendRequestA*
>
> *HttpOpenRequestA*
>
> *InternetConnectA*
>
> *InternetOpenA*

> *InternetCloseHandle*
> *SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost*
> *IPRIP*
>
> *installA*
> *uninstallA*

Now we are moving onward for dynamic analysis. Fire up regshot and take the shot 1. Fire up ApateDNS, ProcMon, Process Explorer after that.

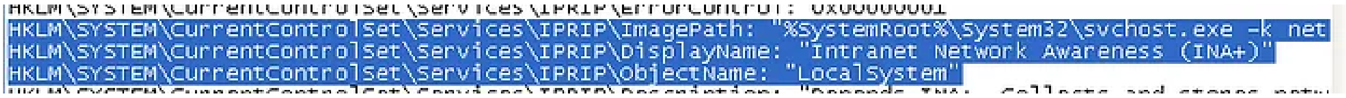
In order to run this DLL file we need to use the rundll32.exe from the system32 in C: drive. We have noticed that this DLL tries to install something via function installA so,



```
C:\Documents and Settings\Administrator\Desktop\Practical Malware Analysis Labs
BinaryCollection\Chapter_3L>strings.exe Lab03-02.dll > str.txt

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Documents and Settings\Administrator\Desktop\Practical Malware Analysis Labs
BinaryCollection\Chapter_3L>rundll32.exe Lab03-02.dll installA
```

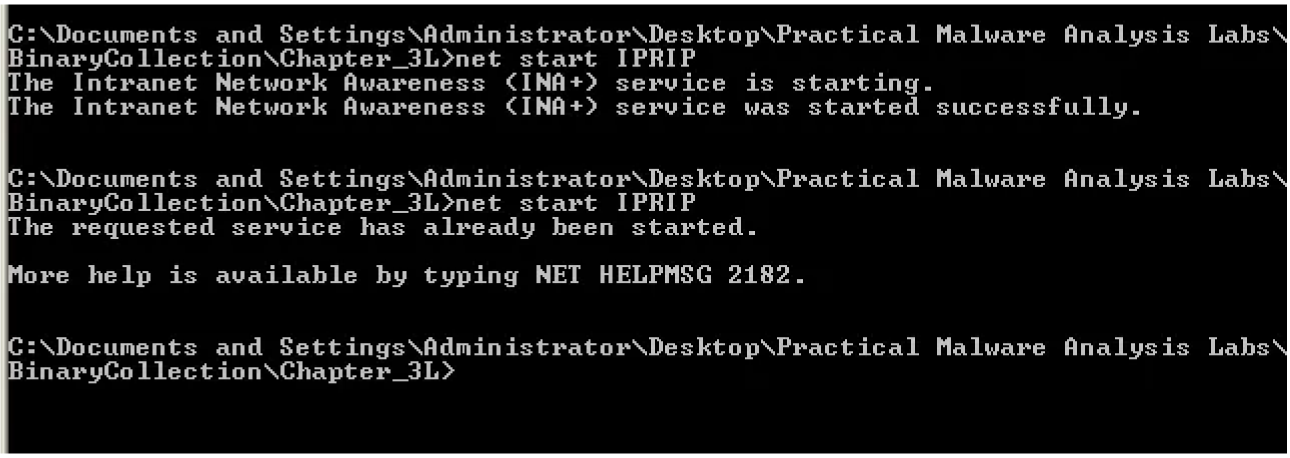
```
Time...   Process Name   PID   Operation          Path
7:23:4... rundll32.exe   3764  Process Start
7:23:4... rundll32.exe   3764  Thread Create
7:23:4... rundll32.exe   3764  QueryNameInfo...   C:\Documents and Settings\Administra
7:23:4... rundll32.exe   3764  Load Image         C:\Documents and Settings\Administra
7:23:4... rundll32.exe   3764  Load Image         C:\WINDOWS\system32\ntdll.dll
7:23:4... rundll32.exe   3764  QueryNameInfo...   C:\Documents and Settings\Administra
7:23:4... rundll32.exe   3764  CreateFile         C:\WINDOWS\Prefetch\RUNDLL32.E
7:23:4... rundll32.exe   3764  RegOpenKey         HKLM\Software\Microsoft\Windows N
7:23:4... rundll32.exe   3764  RegOpenKey         HKLM\System\CurrentControlSet\Cont
7:23:4... rundll32.exe   3764  RegQueryValue      HKLM\System\CurrentControlSet\Cont
7:23:4... rundll32.exe   3764  RegCloseKey        HKLM\System\CurrentControlSet\Cont
7:23:4... rundll32.exe   3764  FileSystemControl  C:\Documents and Settings\Administra
7:23:4... rundll32.exe   3764  CreateFile         C:\Documents and Settings\Administra
7:23:4... rundll32.exe   3764  QueryOpen          C:\Documents and Settings\Administra
7:23:4... rundll32.exe   3764  Load Image         C:\WINDOWS\system32\kernel32.dll
7:23:4... rundll32.exe   3764  RegOpenKey         HKLM\System\CurrentControlSet\Cont

Showing 860 of 735,478 events (0.11%)
```

We can clearly see that we are able to run the DLL file. Now take the second shot and compare.



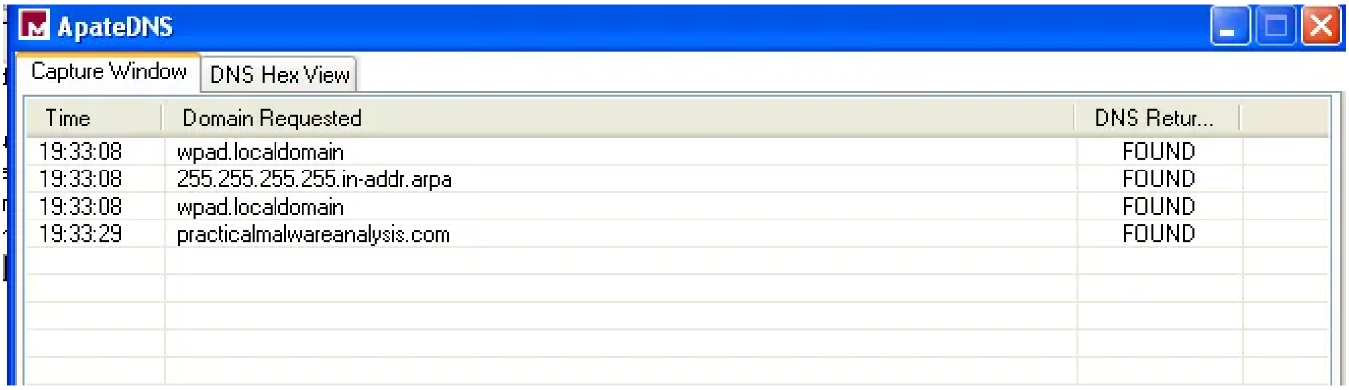
```
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ErrorControl: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ImagePath: "%SystemRoot%\System32\svchost.exe -k net
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\DisplayName: "Intranet Network Awareness (INA+)"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ObjectName: "LocalSystem"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Description: "Depends INA+. Collects and stores netw
```

We can see here that a service IPRIP is being created for communication. The



```
C:\Documents and Settings\Administrator\Desktop\Practical Malware Analysis Labs\
BinaryCollection\Chapter_3L>net start IPRIP
The Intranet Network Awareness (INA+) service is starting.
The Intranet Network Awareness (INA+) service was started successfully.


C:\Documents and Settings\Administrator\Desktop\Practical Malware Analysis Labs\
BinaryCollection\Chapter_3L>net start IPRIP
The requested service has already been started.

More help is available by typing NET HELPMSG 2182.


C:\Documents and Settings\Administrator\Desktop\Practical Malware Analysis Labs\
BinaryCollection\Chapter_3L>
```

Once we are done with it. We can clearly see that the practicalmalwareanalysis.com is being requested.



Time	Domain Requested	DNS Retur...
19:33:08	wpad.localdomain	FOUND
19:33:08	255.255.255.255.in-addr.arpa	FOUND
19:33:08	wpad.localdomain	FOUND
19:33:29	practicalmalwareanalysis.com	FOUND

That was all for this. Its time to answer the questions.

Lab 3–2

Analyze the malware found in the file Lab03–02.dll using basic dynamic analysis tools.

Questions

1. **How can you get this malware to install itself?**

We can get this malware installed using the rundll32.exe and by knowing the first argument to install i.e installA in this case.

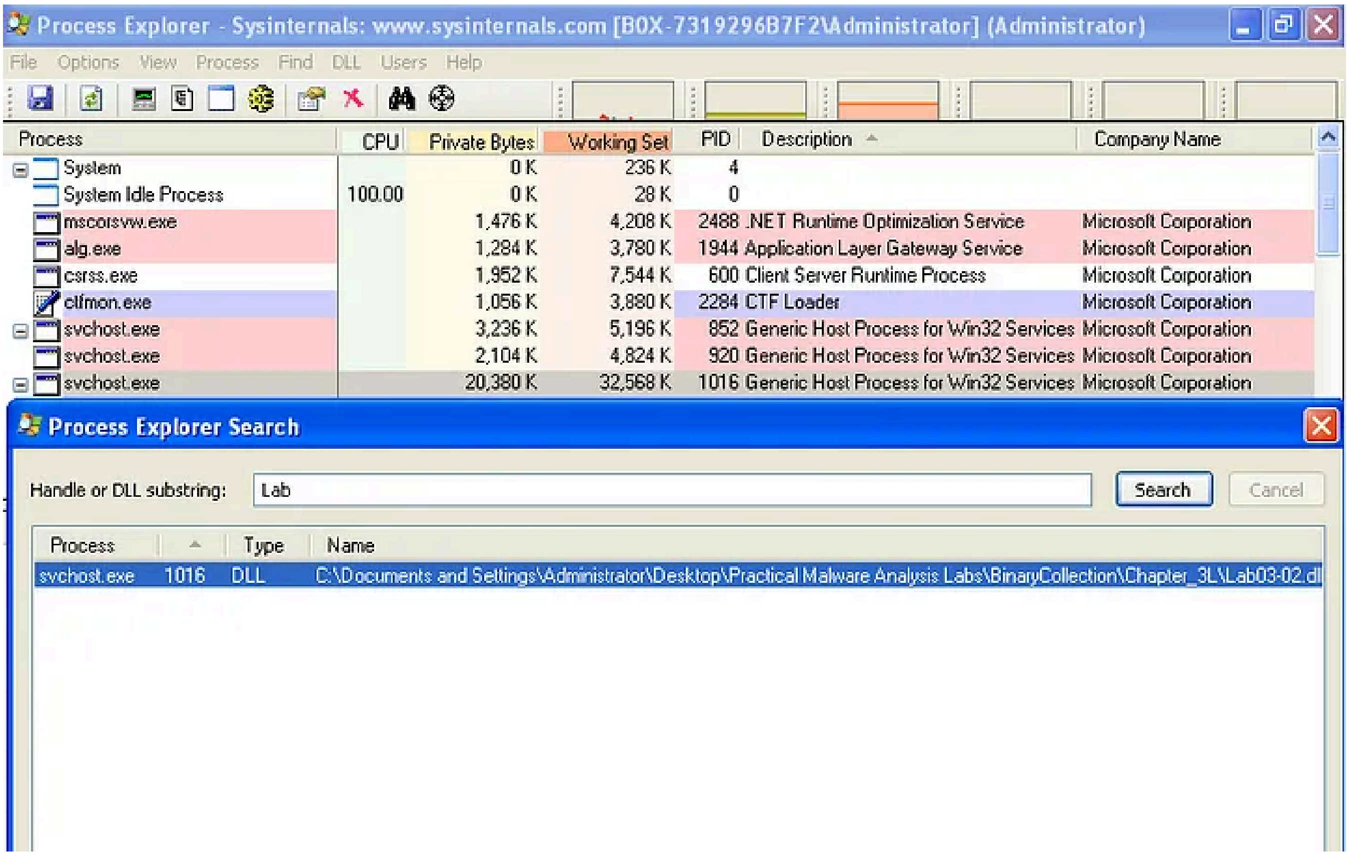
2. How would you get this malware to run after installation?

Once we are done with installing the malware we can see a new service named IPRIP registry added. We can run it by using the network command in windows.

> *net start IPRIP*

3. How can you find the process under which this malware is running?

In Process Explorer we can click in Find and the provide the name of the DLL and so we get the details under which the malware is running.



Process Explorer - Sysinternals: www.sysinternals.com [BOX-7319296B7F2\Administrator] (Administrator)

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System		0 K	236 K	4		
System Idle Process	100.00	0 K	28 K	0		
mscorsvw.exe		1,476 K	4,208 K	2488	.NET Runtime Optimization Service	Microsoft Corporation
alg.exe		1,284 K	3,780 K	1944	Application Layer Gateway Service	Microsoft Corporation
csrss.exe		1,952 K	7,544 K	600	Client Server Runtime Process	Microsoft Corporation
ctfmon.exe		1,056 K	3,880 K	2284	CTF Loader	Microsoft Corporation
svchost.exe		3,236 K	5,196 K	852	Generic Host Process for Win32 Services	Microsoft Corporation
svchost.exe		2,104 K	4,824 K	920	Generic Host Process for Win32 Services	Microsoft Corporation
svchost.exe		20,380 K	32,568 K	1016	Generic Host Process for Win32 Services	Microsoft Corporation

Process Explorer Search

Handle or DLL substring: Lab

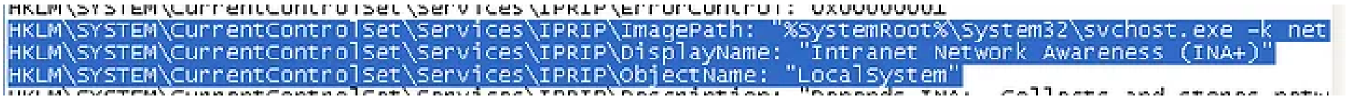
Process	Type	Name
svchost.exe 1016	DLL	C:\Documents and Settings\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_3L\Lab03-02.dl

4. Which filters could you set in order to use procmon to glean information?

We can use the pid in this case “1016” to filter everything.

5. What are the malware’s host-based indicators?

The malware installs a service called IPRIP, displays name of Intranet Network Awareness (INA+) along with the description “Depends INA+, Collects and stores network configuration and location information , and notifies applications when this information changes.”



```
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ErrorControl: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ImagePath: "%SystemRoot%\System32\svchost.exe -k net
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\DisplayName: "Intranet Network Awareness (INA+)"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ObjectName: "LocalSystem"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Description: "Depends INA+. Collects and stores netw
```

It writes to HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters\ServiceDll: %CurrentDirectory%\Lab03–02.dll in the registry for persistence.

6. Are there any useful network-based signatures for this malware?

It tries to connect to “practicalmalwareanalysis.com”.

Cybersecurity

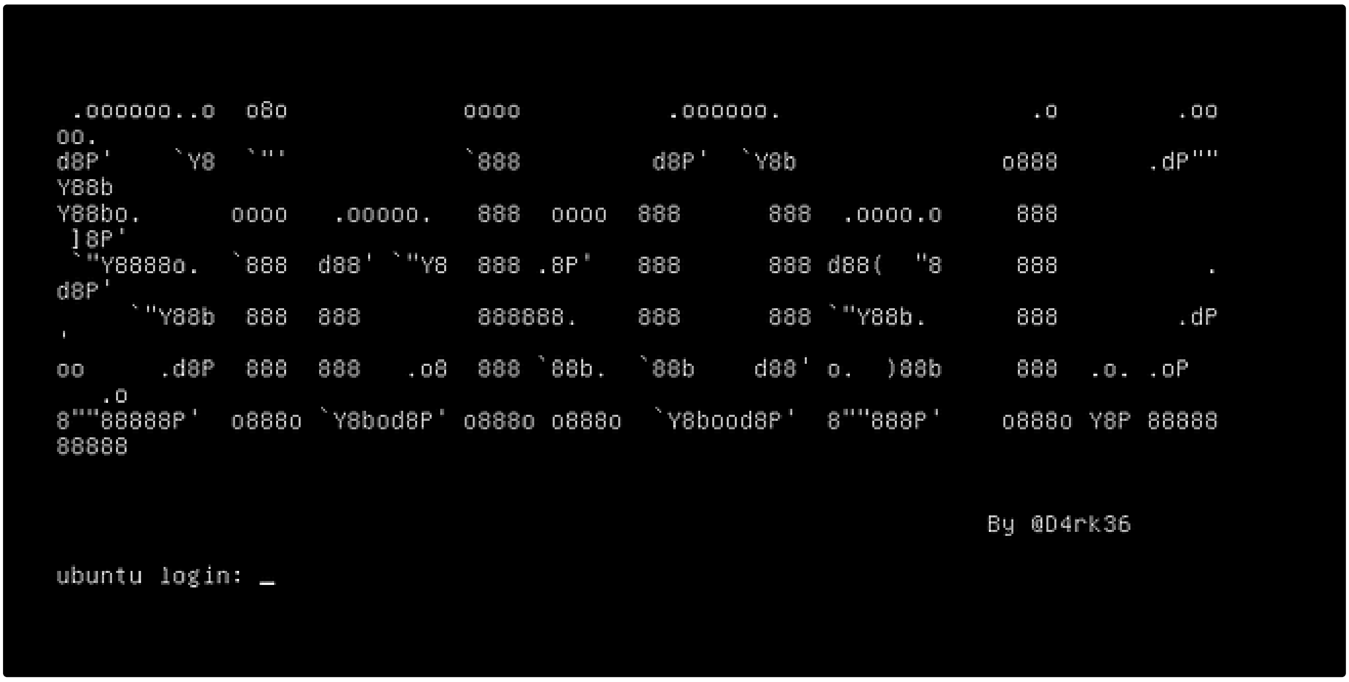
Follow

Written by Kamran Saifullah

378 Followers

Malware/RE/Firmware Analysis, App Sec/Off Sec, VAPT, Phishing Simulations/SE | Risk Management, IS Governance, Audits, ISO 27001 LI

More from Kamran Saifullah



```
 .oooooo..o  o8o            oooo          .oooooo.                 .o        .oo
oo.
d8P'    `Y8  `"'            `888         d8P'  `Y8b              o888      .dP""
Y88b
Y88bo.      oooo   .ooooo.   888  oooo  888      888  .oooo.o     888
 ]8P'
 `"Y8888o.  `888  d88' `"Y8  888 .8P'   888      888 d88(  "8     888          .
d8P'
     `"Y88b  888  888        888888.    888      888 `"Y88b.      888        .dP
'
oo     .d8P  888  888   .o8  888 `88b.  `88b    d88' o.  )88b     888  .o. .oP
   .o
8""88888P'  o888o `Y8bod8P' o888o o888o  `Y8bood8P'  8""888P'    o888o Y8P 88888
88888


                                                              By @D4rk36

ubuntu login: _
```

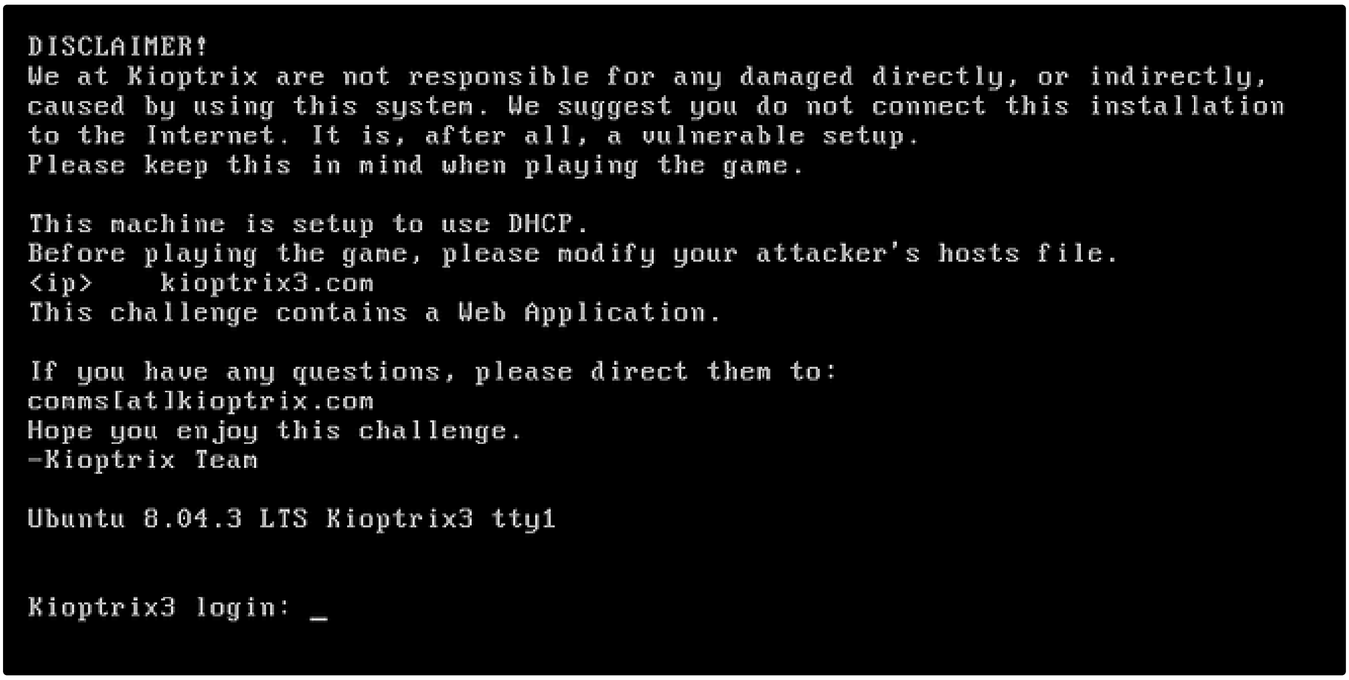
Kamran Saifullah

SickOS 1.2 WalkThrough

Hi,

5 min read · Apr 14, 2018

10



```
DISCLAIMER!
We at Kioptrix are not responsible for any damaged directly, or indirectly,
caused by using this system. We suggest you do not connect this installation
to the Internet. It is, after all, a vulnerable setup.
Please keep this in mind when playing the game.

This machine is setup to use DHCP.
Before playing the game, please modify your attacker's hosts file.
<ip>    kioptrix3.com
This challenge contains a Web Application.

If you have any questions, please direct them to:
comms[at]kioptrix.com
Hope you enjoy this challenge.
-Kioptrix Team

Ubuntu 8.04.3 LTS Kioptrix3 tty1


Kioptrix3 login: _
```

Kamran Saifullah

WalkThrough! Kioptrix — 3 By VulnHub

Hi,

8 min read · Mar 13, 2018

24

52

Written by: Jeremy Hui

Keith is watching chickens cross a road in his grandfather's farm. He once heard from his grandfather that there was something significant about this behavior, but he can't figure out why. Help Keith discover what the chickens are doing from this seemingly simple behavior.

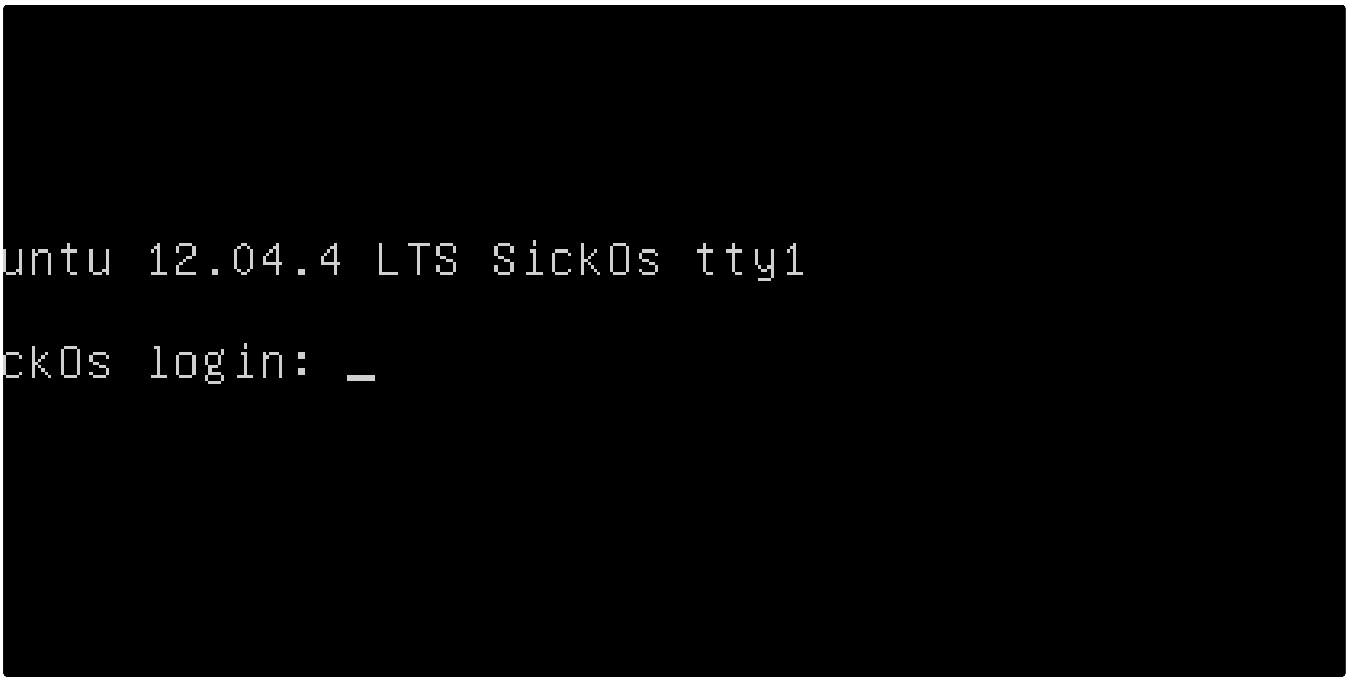
Kamran Saifullah

HSCTF 6—Forensics Challenges—Solutions

After publishing the solutions of the web challenges now it's time to move on with forensics challenges and this is all about how i solved...

5 min read · Jun 13, 2019

17



```
untu 12.04.4 LTS SickOs tty1

ckOs login: _
```

Kamran Saifullah

SickOS 1.1 Walkthrough

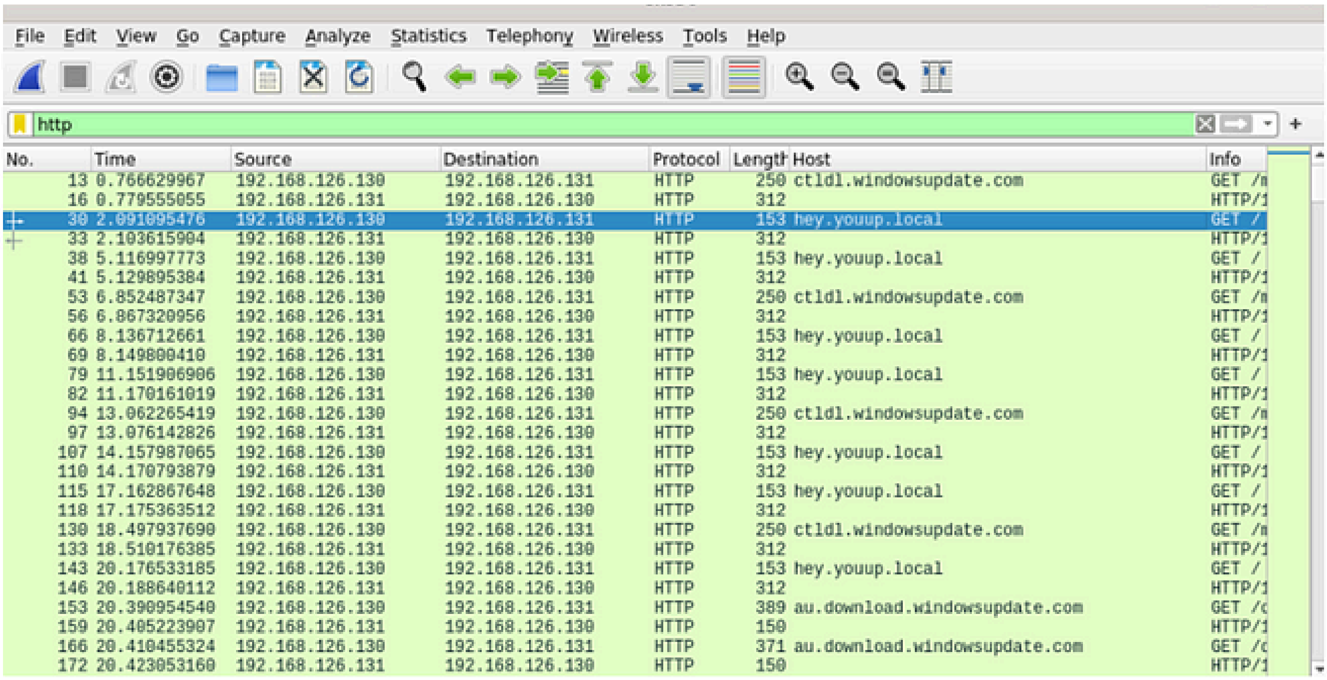
Hi,

5 min read · Apr 11, 2018

9

See all from Kamran Saifullah

Recommended from Medium



http

```
No.  Time          Source           Destination      Protocol Length Host                          Info
  13 0.766629967   192.168.126.130  192.168.126.131  HTTP     250 ctldl.windowsupdate.com          GET /n
  16 0.779555055   192.168.126.131  192.168.126.130  HTTP     312                                  HTTP/1
  30 2.091095476   192.168.126.130  192.168.126.131  HTTP     153 hey.youup.local                  GET /
  33 2.103615904   192.168.126.131  192.168.126.130  HTTP     312                                  HTTP/1
  38 5.116997773   192.168.126.130  192.168.126.131  HTTP     153 hey.youup.local                  GET /
  41 5.129895384   192.168.126.131  192.168.126.130  HTTP     312                                  HTTP/1
  53 6.852487347   192.168.126.130  192.168.126.131  HTTP     250 ctldl.windowsupdate.com          GET /n
  56 6.867320956   192.168.126.131  192.168.126.130  HTTP     312                                  HTTP/1
  66 8.136712661   192.168.126.130  192.168.126.131  HTTP     153 hey.youup.local                  GET /
  69 8.149800410   192.168.126.131  192.168.126.130  HTTP     312                                  HTTP/1
  79 11.151906906  192.168.126.130  192.168.126.131  HTTP     153 hey.youup.local                  GET /
  82 11.170161019  192.168.126.131  192.168.126.130  HTTP     312                                  HTTP/1
  94 13.062265419  192.168.126.130  192.168.126.131  HTTP     250 ctldl.windowsupdate.com          GET /n
  97 13.076142826  192.168.126.131  192.168.126.130  HTTP     312                                  HTTP/1
 107 14.157987065  192.168.126.130  192.168.126.131  HTTP     153 hey.youup.local                  GET /
 110 14.170793879  192.168.126.131  192.168.126.130  HTTP     312                                  HTTP/1
 115 17.162867648  192.168.126.130  192.168.126.131  HTTP     153 hey.youup.local                  GET /
 118 17.175363512  192.168.126.131  192.168.126.130  HTTP     312                                  HTTP/1
 130 18.497937690  192.168.126.130  192.168.126.131  HTTP     250 ctldl.windowsupdate.com          GET /n
 133 18.510176385  192.168.126.131  192.168.126.130  HTTP     312                                  HTTP/1
 143 20.176533185  192.168.126.130  192.168.126.131  HTTP     153 hey.youup.local                  GET /
 146 20.188640112  192.168.126.131  192.168.126.130  HTTP     312                                  HTTP/1
 153 20.390954540  192.168.126.130  192.168.126.131  HTTP     389 au.download.windowsupdate.com    GET /c
 159 20.405223907  192.168.126.131  192.168.126.130  HTTP     150                                  HTTP/1
 166 20.410455324  192.168.126.130  192.168.126.131  HTTP     371 au.download.windowsupdate.com    GET /c
 172 20.423053160  192.168.126.131  192.168.126.130  HTTP     150                                  HTTP/1
```

Hüseyin EKŞİ

Malware Analysis of PMAT-Bonus Unknown malware

I have analyzed the Bonus malware called unknown and would like to share my findings. If you have analyzed this piece of malware please…

3 min read · Jan 21, 2024

13

Abdelwahab Shandy

CyberDefenders :Qradar101 Blue Team Challenge

Category : Threat Hunting

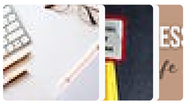
11 min read · Nov 23, 2023

4

Lists

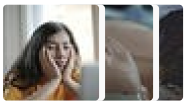
Tech & Tools

16 stories · 210 saves



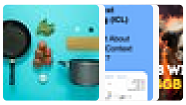
Medium's Huge List of Publications Accepting Submissions

285 stories · 2523 saves



Staff Picks

630 stories · 920 saves



Natural Language Processing

1402 stories · 901 saves

Rewa Aslekar

Malware Analysis

A Beginner’s guide to Malware Analysis

13 min read · Oct 31, 2023

16

Salim Salimov

Hunting Malware in Sysmon Log with Splunk

Hello Medium,

11 min read · Nov 28, 2023

19 1

```
 25 11:53:38 2023 as: nmap -sCVS -vvv -oA nmap/exfiltrated 192.168.216.163
63
l 61 (0.27s latency).
 for 111s
eset)
  VERSION
1 OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)

5:20:d3:63:b4:48:bb:cf (RSA)
AAABgQDH6PH1/ST7TUJ4Mp/l4c7G+TM07YbX7YIsnHzq1TRpvtiBh8MQufkL15WW9+za+h6ZraqoZ0ewwkH+0la436t9Q+2H/Nh4Cnt3OrRbpLJKg4hChjgCHd5KiLCOKHhXPs/FA3mm0
D4Mu17wB5w6yvXyj+lleKjQ6Hnje7KozW5q4U6ijd3LmvHE34Umq/qUbCUbiwY06N2MjBNQiZqWN8z48eTzGsuh6u15fGIDnCCq3sWm37Y5LIUvqAFyIEJZVsC/UyrJDPBE+YIDDNbN2Q
3SNqUq2enfPwQt399nigtUercckdyUD0oRKqVnhZCjEYfX3qOnlAqejr3ipm8nA31pp6lrKNAmQEjd5O8Jxk04OR2JBxcfVNfs=
:f0:36:ac:19:d0:0e:f3 (ECDSA)
LXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBI0EdIHR7NOReMN0G7C8zxbLgwB3ump+nb2D3Pe3tXqp/6jNJ/GbUZe4Ab44njMKHJbm/PzrtYzojMjGDu8lQCg=
:f4:80:8d:33:ce:9b:3a (ED25519)
AAAAIDCc0saExmeOXtqm5FS+D5RnDke8aJEvFq3DJIr0KZML
1 Apache httpd 2.4.41 ((Ubuntu))
tries
l/ /panel/ /tmp/

5: 09BDDB30D6AE11E854BFF82ED638542B
ect to http://exfiltrated.offsec/
1 (Ubuntu)

ST OPTIONS
/o:linux:linux_kernel

share/nmap
e report any incorrect results at https://nmap.org/submit/ .
 2023 -- 1 IP address (1 host up) scanned in 118.16 seconds
```

Ardian Danny

[OSCP Practice Series 1] Proving Grounds — Exfiltrated

Machine Type: Linux

3 min read · Dec 26, 2023

Worldsleaks

OpenWire —

CyberDefenders CTF

7 min read · Jan 25, 2024

13

See more recommendations