ClubHACK Mag

1st Indian "HACKING" Magazine

Angry Malware

www.clubhack.com

Issue 20 | Sep 2011

TechGyan Rootkits are back with the boot infection | **LegalGyan** Cyber Pornography Law | **Mom's Guide** Introduction to Malware & Malware Analysis | **Matriux Vibhag** Ostinato | **ToolGyan** Tools for Reverse Engineering and Malware Analysis |

Hello Readers, How are you doing? Hope you are enjoying the magazine. This time the theme is Malwares. In this issue you will read about malwares, malwares anaylsis, various tools and techniques for analysis . You will also read about Windows Bootkits, Ostinato - a packet generator/analyzer and laws related to Pornography! Sounds interesting isn't it?

Abhijeet Patil

And well, the cover-page is even more interesting! I liked it and i am sure even you must have liked it. The "Angry Malware" poster concept is taken from our favourite game - angry birds! Thanks Pankit Thakkar for the lovely poster :)

Apart from this, This time ClubHack Mag is going to a few Hacking and Security conferences around the globe as Media Partners such as c0c0n, Securitybyte 2011, Hacktivity 2011, Cyberlympics, HITB Malaysia and Cyber Defense Summit. Detailed information of these events you'll find inside.

You can always contact us, submit your articles, give feedback to info@chmag.in

ClubHACK Mag

Issue 20, September 2011.

Team CHmag

Rohit Srivastwa
rohit@clubhack.com

Aarja Bhattacharyya
aarja@chmag.in

Abhijeet R Patil
abhijeet@chmag.in

Abhishek Nagar
abhishek@chmag.in

Pankit Thakkar
pankit@chmag.in

Varun V Hirve
varun@chmag.in

www.chmag.in
info@chmag.in

CONTENTS

Rootkits are back with the boot infection

Preface

Windows rootikits have been around since year 2005 and have become a buzzword in the security industry over recent years. While rootkits have traditionally been used by sophisticated attackers to hide their presence on compromised machines, recent malwares with rootkit capabilities have started using them to complicate efforts to detect and clean the infections. This article aims to give an idea about Windows rootkits with advanced techniques observed in the recent years, mainly rootkits with boot infections.

Windows Rootkits

This is not year 2005, when the word “Rootkit” was not known to the most of the people in cyber world besides security researchers. The technique used by rootkits to hide the presence of malwares has been, for longer time, to steal more information, send out more spam, launch more DDOS attacks, and ultimately make millions of dollars, was the matter of concern for only the cyber security researchers. But some commercial ethical software had adopted the same technique for self protection. Among all of them Sony Digital Rights Management (DRM) software received intense media attention and criticism in late 2005 and the word “Rootkit” became common term in the cyber security world.

You will find more than dozen of definitions of the “Rootkit”. But to understand the term in very simple manner we have following definition of rootkit:

A Rootkit is a set of tools used by an intruder after cracking a computer system. These tools can help the attacker maintain his or her access to the system and use it for malicious purposes. Root kits exist for a variety of operating systems.

The term rootkit is used to describe the mechanisms and techniques whereby malware, including viruses, spyware, and trojans, attempt to hide their presence from antispyware, antivirus, and various system management utilities. In other words, a rootkit is a set of programs and code that allows a permanent or consistent, undetectable presence of other components, mostly the malwares.

Windows rootkits are the rootkits which work on Microsoft Windows Operating system's versions to hide the presence of malwares' components like files, registry, processes, drivers etc. They do achieve this by using techniques like user mode hooking, SSDT hooking, IRP hooking and Direct kernel Object Manipulation (DKOM) etc. Initially PoC (proof of concept) Windows rootkits were constantly being released to demonstrate new methods of bypassing rootkit detection and prevention mechanisms provided by various security vendors for Windows operating system. Some proof of concept also got published in one of the bestselling books about Windows rootkits; "Subverting The Windows Kernel: ROOTKITS". But eventually most of the PoCs got transformed into real world rootkits that made their way into the hands of attackers. The current state of rootkits is no more than just an arms race but has become warfare between the rootkit writers and the anti-rootkit industry which is responsible for protecting millions of systems.

Advanced Windows Rootkits with boot infection: TDSS

We can divide Windows rootkits' era in two parts, one as pre TDSS (also known as TDL, Alureon Family) and other is TDSS family. The TDSS family rootkit first appeared in 2008. Since then, it has become far more widespread than one of the most notorious rootkits like Rustock. It has been more than two years since this family of rootkits began to evolve. The rootkit writers of this family have developed one of the most sophisticated and advanced mechanisms for bypassing various protective measures and security mechanisms embedded into the operating system. TDSS implements the concept of infecting operating system drivers and MBR; this means it is loaded and run at the very early stages of the operating system. This effectively complicates the detection of TDSS and makes the task of cleaning it too difficult and challenging.

TDL4 is the most recent high tech and widely spread member of the TDSS family rootkit, targeting x64 operating systems too such as Windows Vista and Windows 7. One of the most striking features of TDL4 is that it is able to load its kernel-mode driver on systems with an enforced kernel-mode code signing policy (64-bit versions of Microsoft Windows Vista and 7) and perform kernel-mode hooks with kernel-mode patch protection policy enabled.

When the driver is loaded into kernel-mode address space it overwrites the MBR (Master Boot Record) of the disk by sending SRB (SCSI Request Block) packets directly to the miniport device object, then it initializes its hidden file system. The bootkit's modules are written into the hidden file system from the dropper.

The TDL4 bootkit controls two areas of the hard drive one is the MBR and other is the hidden file system created at the time of malware deployment. When any application reads the MBR, the bootkit changes data and returns the contents of the clean MBR i.e. prior to the infection, and also it takes care of Infected MBR by protecting it from overwriting.

The hidden file system with the malicious components also gets protected by the bootkit. So if any application is making an attempt to read sectors of the hard disk where the hidden file system is stored, It will return zeroed buffer instead of the original data.

The bootkit contains code that performs additional checks to prevent the malware from the cleanup. At every start of the system TDL4 bootkit driver gets loaded and initialized properly by performing tasks as follows:

- Reads the contents of the boot sector, compares it with the infected image stored in hidden file system, if it finds any difference between these two images it rewrites the infected image to the boot sector.

- Sets the DriverObject field of the miniport device object to point to the bootkit's driver object and also hooks the *DriverStartIo* field of the miniport's driver object.

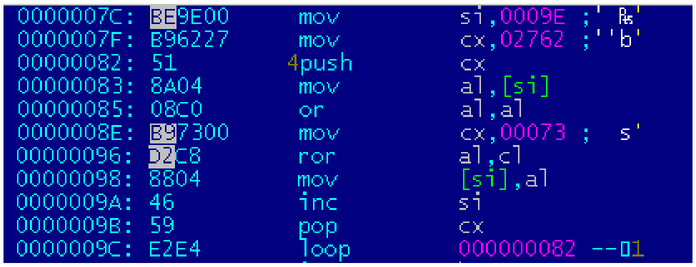
- If kernel debugging is enabled then this TDL4 does not install any of it's components.

TDL4 Rootkit hooks the ATAPI driver i.e. standard windows miniport drivers like atapi.sys. It keeps Device Object at lowest in the device stack, which makes a lot harder to dump TDL4 files.

All these striking features have made TDL4 most notorious Windows rootkit and it is also very important to mention that the key to its success is the boot sector infection.

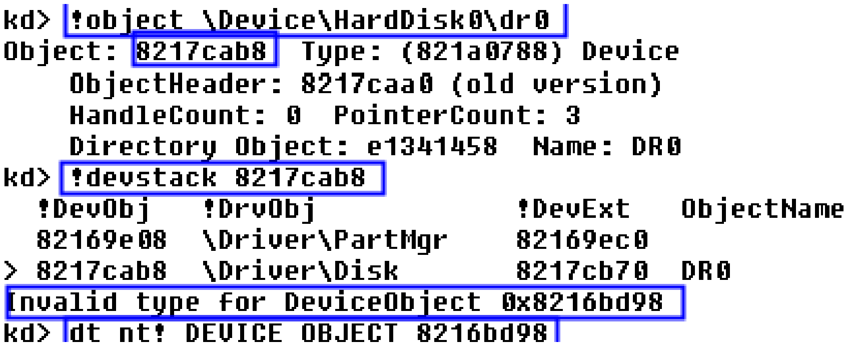
Stealthy variant of Bootkit.Trup

We will go through the technical details of the one more new generation malware with bootkit ability which is simpler in design than TDL4 but again using boot infection as a key. The new variant of Bootkit. Trup was making rounds 2-3 months back, which is updated to protect the infected MBR. The encryption used in Bootkit. Trup.B is very similar to its old variant "Bootkit. Trup.A" which is simple rotate right (ROR) operation.

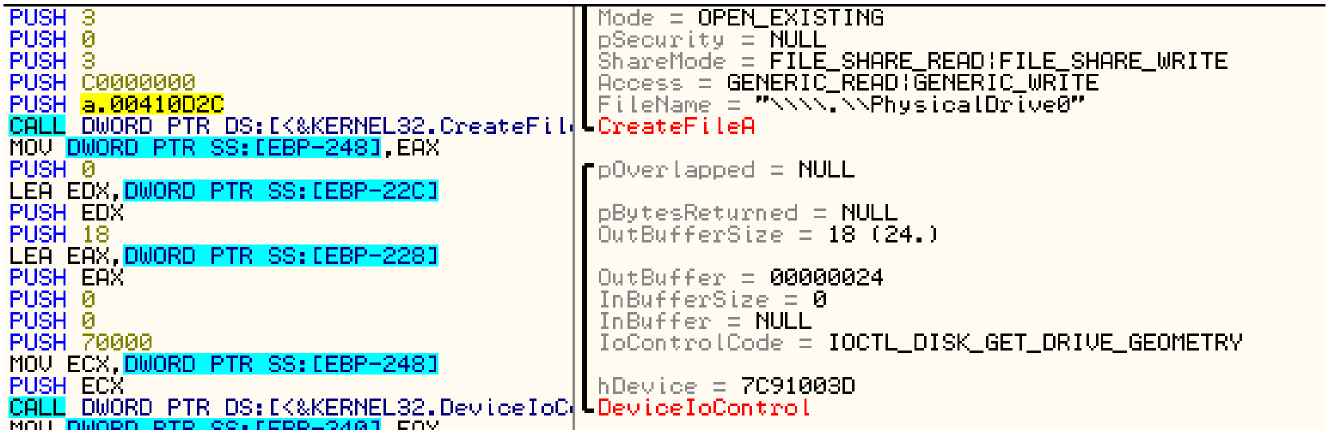


```
0000007C: BE9E00    mov       si,0009E ;' ₧'
0000007F: B96227    mov       cx,02762 ;''b'
00000082: 51       4push      cx
00000083: 8A04      mov       al,[si]
00000085: 08C0      or        al,al
0000008E: B97300    mov       cx,00073 ;  s'
00000096: D2C8      ror       al,cl
00000098: 8804      mov       [si],al
0000009A: 46        inc       si
0000009B: 59        pop       cx
0000009C: E2E4      loop      000000082 --↑1
```

It gets Drive geometry of the infected disk and then calculates position near end of the partition to store original MBR and other components. These components are written into unallocated part of the partition, in case disk becomes full there is chance of it getting overwritten with other data.



```
kd> !object \Device\HardDisk0\dr0
Object: 8217cab8  Type: (821a0788) Device
    ObjectHeader: 8217caa0 (old version)
    HandleCount: 0  PointerCount: 3
    Directory Object: e1341458  Name: DR0
kd> !devstack 8217cab8
  !DevObj   !DrvObj            !DevExt   ObjectName
  82169e08  \Driver\PartMgr    82169ec0
> 8217cab8  \Driver\Disk       8217cb70  DR0
Invalid type for DeviceObject 0x8216bd98
kd> dt nt! DEVICE OBJECT 8216bd98
```



```
PUSH 3                                    ┌Mode = OPEN_EXISTING
PUSH 0                                    │pSecurity = NULL
PUSH 3                                    │ShareMode = FILE_SHARE_READ|FILE_SHARE_WRITE
PUSH C0000000                             │Access = GENERIC_READ|GENERIC_WRITE
PUSH a.00410D2C                           │FileName = "\\\\.\\PhysicalDrive0"
CALL DWORD PTR DS:[<&KERNEL32.CreateFil   └CreateFileA
MOV DWORD PTR SS:[EBP-248],EAX
PUSH 0                                    ┌pOverlapped = NULL
LEA EDX,DWORD PTR SS:[EBP-22C]            │
PUSH EDX                                  │pBytesReturned = NULL
PUSH 18                                   │OutBufferSize = 18 (24.)
LEA EAX,DWORD PTR SS:[EBP-228]            │
PUSH EAX                                  │OutBuffer = 00000024
PUSH 0                                    │InBufferSize = 0
PUSH 0                                    │InBuffer = NULL
PUSH 70000                                │IoControlCode = IOCTL_DISK_GET_DRIVE_GEOMETRY
MOV ECX,DWORD PTR SS:[EBP-248]            │
PUSH ECX                                  │hDevice = 7C91003D
CALL DWORD PTR DS:[<&KERNEL32.DeviceIoC   └DeviceIoControl
MOV DWORD PTR SS:[EBP-248],EAX
```

The original MBR and driver component are stored in encrypted form using the same encryption. Driver component hooks ATAPI's DriverStartIo routine where it monitors for write operations. In case of write operation targeted at the MBR sector, it is changed to read operation. This way it is trying to bypass repair operation by Security Products.

MBR protection mechanism was previously seen in TDSS.TDL4 which was sitting at the bottom of the storage stack to monitor read and write operations to first sector and its encrypted components in unpartitioned disk space.

Having insights of the technical details of these new generation Windows rootkits, the reader must have got an idea that how difficult it is for anti-rootkit tools to counter them.

Conclusion

In the past few years there were no great concerns about the malware infecting boot sectors and they were even told to be no more in the wild. But looking at the changing threat landscape in the last year or two, we have to mention that these types of malwares are coming back with more rootkit capabilities.

Most of the anti-rootkit softwares available resulted in the failure while detecting the presence of these rootkits, as these antirootkit tools use techniques like cross view based detection, user mode or kernel mode hook detection or DKOM detection. These rootkits don't provide any chance to scan the “Rooms”, where their components are residing.

As Current Anti-Rootkit softwares are not helping us more in tackling such highly advanced rootkits, need of specialized bootkit detection and removal tool arises. Most of Security vendors have already developed and released these kinds of specialized tools to counter these rootkits. Analysis of such complex malwares becomes harder with unavailability of dropper samples.

The war against rootkits has been taken up to a newly changed battleground as insights of case studies mentioned above give clear idea that how rootkit driver protects infected Master Boot Record, which keeps those advanced rootkits ahead than traditional bootkits. We have to be ready for all such techniques never seen before in malware threats and next generation of rootkits, bootkits, kernel infectors and boot sector infectors written by highly technical and professional malware writers.

Credits

I would like to give sincere thanks to Mr. Sanjay Katkar (CTO, Quick Heal Technologies) for his most valuable guidance. Also I would like to thank to my colleague Mr. Rajesh Nikam and Mr. Rajendra Kumbhar for their help in the analysis and valuable inputs.

Swanand Shinde

Swanand Dattaram Shinde is working with Quick Heal Technologies (P) Ltd. since 2005 as a Sr.Software Engineer.
He holds Masters in Computer Science. He is currently working in Research and Development of Antivirus Quick Heal. He has researched on various security products like Antivirus, AntiRootkit etc.

HackCONF

HACKTIVITY

The Largest Hacker Conference in Central and Eastern Europe

September 17-18, 2011. Millenáris / HUNGARY, Budapest

Hacktivity 2011

World of Ethical Hackers Revs Up - Hacktivity 2011

On September 17-18, 2011, Hacktivity, the largest hacker conference in Central and Eastern Europe will be held again, this time at Millenáris. The two-day conference will have a real festival mood, presentations, workshops, games, the Central and Eastern European finals of the Global CyberLympics, hardware hacking, a party in the evening and 1000+ hackers from all over the world!

Hacktivity, the oldest Hungarian independent IT security conference, which has become truly international by now, will be held for the 8th time this year. As usual, speakers will include the most prominent representatives of IT security. It is a major professional achievement to give a presentation at the conference therefore IT experts have had to apply to be selected as a speaker for years now. This year over 60 applications were sent from 15 countries to the programme committee of which the best 28 were chosen by the jury.

Similarly to previous years, this year's two keynote speakers are real stars in their fields of expertise. **Saturday will open with Hungarian-born Peter Szor who lives in the US and is justly called the Father of Virus Protection**. His 650-page book „The Art of Computer Virus Research and Defense", recently published in Hungarian, is not only a highly scientific work but also the most extensive study written about computer viruses to date. Peter Szor graduated from the University of Veszprém, Hungary as an IT specialist and wrote his first anti-virus software called Pasteur in the 1990s (also used by OTP Bank at the time). In 1996 he was hired by the predecessor of F-Secure in Finland, then became a leading engineer at Symantec in 1999 and recently joined McAfee. At CARO (Computer AntiVirus Researcher's Organization) he worked together with many security researchers including John McAfee, Mikko Hypponen or Eugene Kaspersky. Peter Szor is the author of over 40 inventions and patents on computer virus detection and intrusion prevention.

Sunday's keynote speaker is Raoul "Nobody" Chiesa from Italy, the well-known European cyber crime expert. In the 1980s and 90s he was one of the first Italian hackers then in 1997 he founded @Mediaservice.net Srl, a vendor-neutral security consulting company. Since 2003 he has co-operated with the UN agency "UNICRI" (United Nations Interregional Crime and Justice Research Institute) and in 2010 he was selected among the 30 European top security expert to assist the ENISA Director until 2012 at the PSG, Permanent Stakeholders Group.

And that's not all when it comes to foreign speakers. Vivek Ramachandran, founder of securitytube.net, will come from India, Joseph McCray, Air Force veteran and winner of multiple awards by EC-Council, will arrive from the US, Ertunga Arsal, SAP expert and Alexander Kornbrust, Oracle expert will come from Germany. Pavol Luptak is Head of the Slovakian OWASP and Michele Orru, penetration tester for the Royal Bank of Scotland will come from Italy. In addition to the renowned foreign specialists there will be numerous prominent Hungarian speakers as well including Csaba Barta, security consultant at Deloitte Zrt. who was voted best speaker at Hackers Halted and who will speak about Computer Forensics, László Tóth, internationally recognized database security expert also from Deloitte Zrt., László Klock from kancellar.hu who is the winner of last year's Hacktivity Wargame and will deliver a presentation on his research on virtualization security, and Péter Bodor, Associate Professor at Eötvös Loránd University, who will talk about the connection between the increasingly popular method of social engineering and psychology.

Beside the presentations plenty of other programmes will await participants such as interactive hello workshops, hardware hacking lockpicking, i.e. unlocking a lock without a key, and ardunio testing, games: Wargame, CTF, hacker's path, ancient computers reborn, a wild party Saturday evening and for the first time this year the **Central and Eastern European Finals of the Global CyberLympics at Hacktivity 2011!** The global defense games organized and launched by EC-Council will have groups of 6 competing in 7 regions in the world. The finals will be held in the United States where the regional winners will be invited.

At the conference certified (CISA, CISM, CISSP) specialists can collect CPE points necessary for their licence. Due to the high interest shown in the event the organizers expect 1,000-1,200 participants this year. We have a new venue as well: this year's conference will be held in the 4590 sqm Hall B of Millenáris where professional infrastructure, a restaurant, two large and several smaller rooms will be available. The largest room will seat 1,000 people.

Further information, the detailed program and registration: www.hacktivity.com

Facebook:
http://www.facebook.com/hacktivity

Twitter: twitter.com/hacktivity2011

For more information please contact:
Bernadette Szutor
+36 20 9179539
bernadette.szutor@hacktivity.com

Tools for Reverse Engineering and Malware Analysis

Introduction

Reverse engineering is the process of analyzing a subject system to identify the system's components and their relationships, and to create representations of the system in another form or at a higher level of abstraction. The process of reverse engineering, which is part of malware analysis, is accomplished using specific tools that are categorized as hex editors, disassemblers/debuggers, decompiles and monitoring tools.

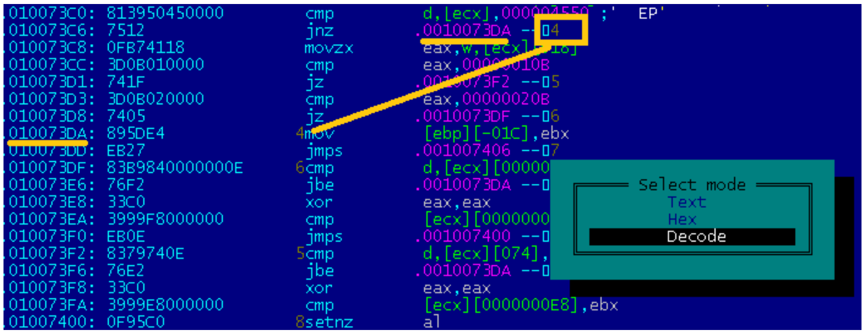
Disassemblers/debuggers occupy important position in the list of reverse engineering tools. A disassembler converts binary code into assembly code. Disassemblers also extract strings, used libraries, and imported and exported functions. Debuggers expand the functionality of disassemblers by supporting the viewing of the stack, the CPU registers, and the hex dumping of the program as it executes. Debuggers allow breakpoints to be set and the assembly code to be edited at runtime.

One must be familiar with the Portable Executable (PE)[1]file format before diving into reverse engineering for Windows executables. In this article we will get into important aspects of Hiew, OllyDbg and IDA Pro from reverse engineer's perspective.

Hiew

Hiew[2] short for *Hacker's view* is a great disassembler (not that this is not debugger) designed for hackers, asthe name suggests.

It supports three modes - Text, Hexadecimal and Decode (Dis-assembly) mode. Enter/F4 key is used to switch between these modes. In each mode the Function Line, corresponding to function keys from F1 to F12, which appears at the bottom of the Hiew screen, changes and its functionality with CTRL, SHIFT and ALT



```
.010073C0: 813950450000        cmp      d,[ecx],000004550 ;'  EP'
.010073C6: 7512                jnz      .0010073DA --04
.010073C8: 0FB74118            movzx    eax,w,[ecx][018]
.010073CC: 3D0B010000          cmp      eax,00000010B
.010073D1: 741F                jz       .0010073F2 --05
.010073D3: 3D0B020000          cmp      eax,00000020B
.010073D8: 7405                jz       .0010073DF --06
.010073DA: 895DE4             4mov      [ebp][-01C],ebx
.010073DD: EB27                jmps     .001007406 --07
.010073DF: 83B9840000000E     6cmp      d,[ecx][00000
.010073E6: 76F2                jbe      .0010073DA --0
.010073E8: 33C0                xor      eax,eax
.010073EA: 3999F8000000        cmp      [ecx][0000000
.010073F0: EB0E                jmps     .001007400 --0
.010073F2: 8379740E           5cmp      d,[ecx][074],
.010073F6: 76E2                jbe      .0010073DA --0
.010073F8: 33C0                xor      eax,eax
.010073FA: 3999E8000000        cmp      [ecx][0000000E8],ebx
.01007400: 0F95C0             8setnz    al
```

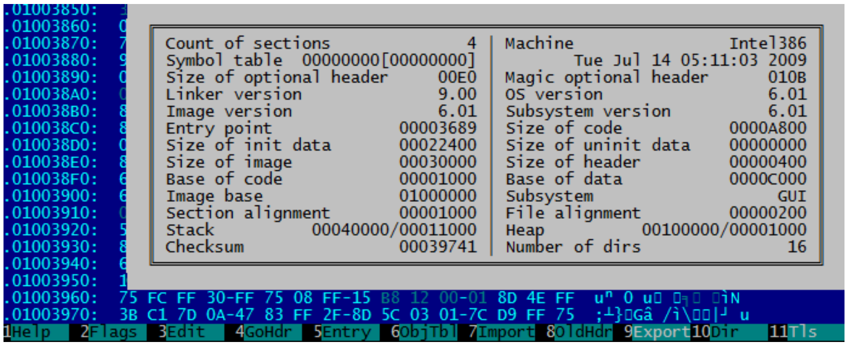
Fig. 1 Hiew – Three modes: Text, Hex, Decode

combinations.

PE Header

PE Header could be viewed by pressing F8 from Hex or Decode view. In this mode we could see important properties of PE file using following shortcuts:

F6	Sections Table
F7	Import Table
F9	Export Table
F10	Data Directories
F5	Jump to Entry Point
Alt-F2	Jump to end of last section



```
.01003850:  
.01003860:  0
.01003870:  7   Count of sections              4 | Machine                  Intel386
.01003880:  9   Symbol table  00000000[00000000] |          Tue Jul 14 05:11:03 2009
.01003890:  0   Size of optional header     00E0 | Magic optional header        010B
.010038A0:  0   Linker version              9.00 | OS version                   6.01
.010038B0:  8   Image version               6.01 | Subsystem version            6.01
.010038C0:  8   Entry point             00003689 | Size of code             0000A800
.010038D0:  0   Size of init data       00022400 | Size of uninit data      00000000
.010038E0:  8   Size of image           00030000 | Size of header           00000400
.010038F0:  6   Base of code            00001000 | Base of data             0000C000
.01003900:  6   Image base              01000000 | Subsystem                     GUI
.01003910:  0   Section alignment       00001000 | File alignment           00000200
.01003920:  5   Stack          00040000/00011000 | Heap           00100000/00001000
.01003930:  8   Checksum                00039741 | Number of dirs                 16
.01003940:  6
.01003950:  1
.01003960:  75 FC FF 30-FF 75 08 FF-15 B8 12 00-01 8D 4E FF  uⁿ 0 u▯ ▯╕▯ ▯iN
.01003970:  3B C1 7D 0A-47 83 FF 2F-8D 5C 03 01-7C D9 FF 75  ;┴}▯Gâ /ì\▯▯|┘ u
1Help  2Flags  3Edit  4GoHdr  5Entry  6ObjTbl 7Import 8OldHdr 9Export10Dir   11Tls
```

Fig. 2 Hiew – PE Header

Search in file

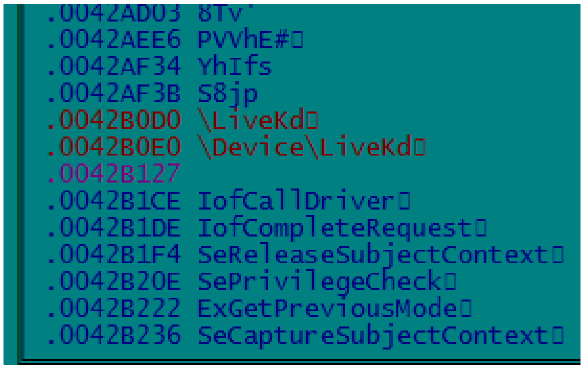
Hiew supports to search in a file for ASCII or HEX sequence of bytes by pressing F7 key. It also supports byte wild character.

Alt-?	Wild character
Shift-F7	To repeat search
Alt-F7	To change search

	direction

Strings

ASCII and Unicode strings are viewed from Text/Hex mode by pressing Alt-F6 key. This helps to search for juicy strings like suspicious urls, FTP, SMTP or IRC commands, files names, registry keys etc in the file. You could jump to selected string from string window by pressing ENTER key. +/- keys are used to change the minimum length of displayed strings, this will help to filter out smaller strings. You could apply filter for displayed strings using F9 key.



```
.0042AD03 8Tv'
.0042AEE6 PVVhE#▯
.0042AF34 YhIfs
.0042AF3B S8jp
.0042B0D0 \LiveKd▯
.0042B0E0 \Device\LiveKd▯
.0042B127
.0042B1CE IofCallDriver▯
.0042B1DE IofCompleteRequest▯
.0042B1F4 SeReleaseSubjectContext▯
.0042B20E SePrivilegeCheck▯
.0042B222 ExGetPreviousMode▯
.0042B236 SeCaptureSubjectContext▯
```

Fig. 3 Hiew – Strings from file

Moving around

You could directly jump to specific location by pressing F5 key and providing offset (offset values are hexadecimal☺). To specify relative offset + or - sign could be used as prefix to offset. When specified offset is a Virtual Address, it should start with ".". Alt-F1 key is used to toggle between Virtual Address and file offset.

If you want jump to specific function or offset which appears as part of control transfer instruction like call, jmp or conditional jump, you could press the key that appears at the end of instruction. Please see Fig.1 marked for label 4. In this case if you press key "4", it will take you to offset 0x010073DA.

0 or Backspace key is used to jump back the previous instruction.

Simple Decryption

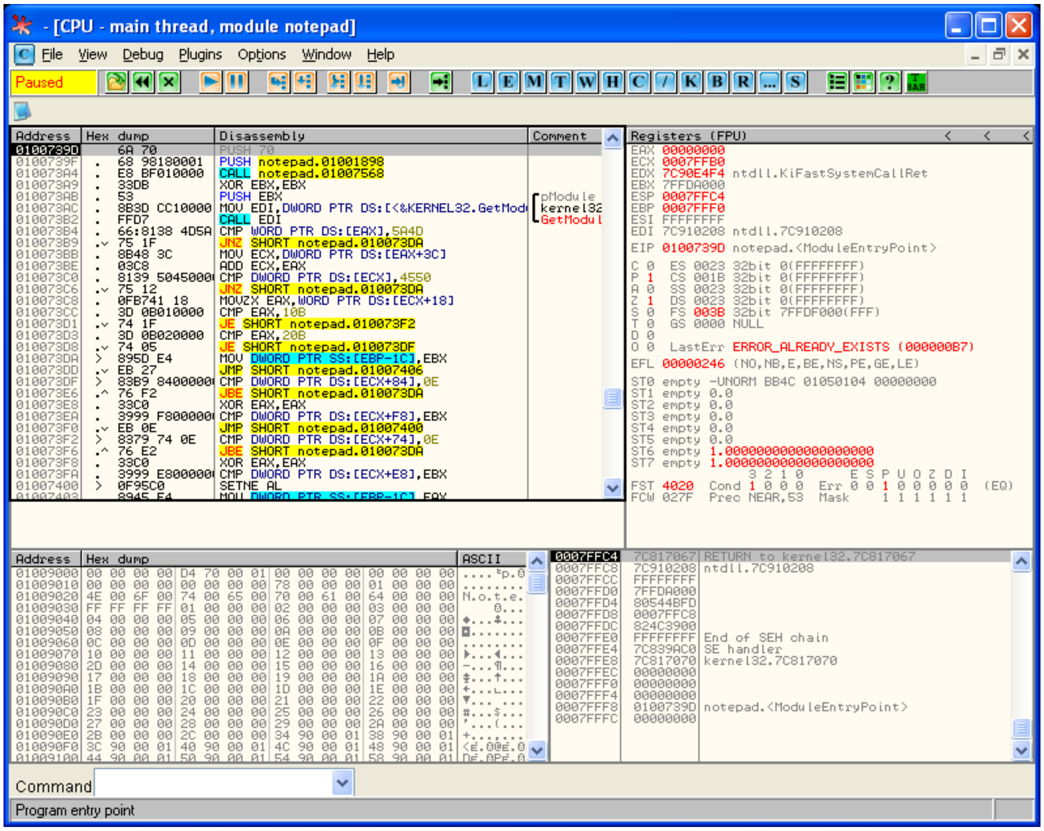
Hiew supports decryption of block using simple encryptions like xor, add, rol etc. Press F3 from Hex or Decode view to enter in edit mode and then press F7 to add simple decryption routine. You could set operand size as byte, word or dword by pressing F2.

Hiew works great when used in combination with File Manager like FAR[3] by configuring its command line. This is very helpful disassembler to quickly get different aspects of file under analysis like file header, section information, data directories, imported / exported functions and strings.

OllyDbg

OllyDbg[4][5]is an application-level debugger. OllyDbg interface shows the disassembly, hex dump, stack, and CPU registers. Additionally, OllyDbg supports run tracing, conditional breakpoints, PE header viewing, hex editing, and plug-in support.

At first Startup, OllyDbg asks to setup User Data Directory (UDD) and Plugins directory.UDD is used to keep debugged application specific information like breakpoints and other information and obviously you need to save plugins in Plugins directory. It provides wide Debugging Options like break on new module or when thread is created, how to process exceptions etc. OllyDbg supports



```
Address   Hex dump          Disassembly                             Comment
0100739D    6A 70           PUSH 70
0100739F  . 68 98180001     PUSH notepad.01001898
010073A4  . E8 BF010000     CALL notepad.01007568
010073A9  . 33DB            XOR EBX,EBX
010073AB  . 53              PUSH EBX                                 ┌pModule
010073AC  . 8B3D CC10000    MOV EDI,DWORD PTR DS:[<&KERNEL32.GetMod  │kernel32
010073B2  . FFD7            CALL EDI                                 └GetModul
010073B4  . 66:8138 4D5A    CMP WORD PTR DS:[EAX],5A4D
010073B9  .v 75 1F          JNZ SHORT notepad.010073DA
010073BB  . 8B48 3C         MOV ECX,DWORD PTR DS:[EAX+3C]
010073BE  . 03C8            ADD ECX,EAX
010073C0  . 8139 5045000    CMP DWORD PTR DS:[ECX],4550
010073C6  .v 75 12          JNZ SHORT notepad.010073DA
010073C8  . 0FB741 18       MOVZX EAX,WORD PTR DS:[ECX+18]
010073CC  . 3D 0B010000     CMP EAX,10B
010073D1  .v 74 1F          JE SHORT notepad.010073F2
010073D3  . 3D 0B020000     CMP EAX,20B
010073D8  .v 74 05          JE SHORT notepad.010073DF
010073DA  > 895D E4         MOV DWORD PTR SS:[EBP-1C],EBX
010073DD  .v EB 27          JMP SHORT notepad.01007406
010073DF  > 83B9 8400000    CMP DWORD PTR DS:[ECX+84],0E
010073E6  .^ 76 F2          JBE SHORT notepad.010073DA
010073E8  . 33C0            XOR EAX,EAX
010073EA  . 3999 F800000    CMP DWORD PTR DS:[ECX+F8],EBX
010073F0  .v EB 0E          JMP SHORT notepad.01007400
010073F2  > 8379 74 0E      CMP DWORD PTR DS:[ECX+74],0E
010073F6  .^ 76 E2          JBE SHORT notepad.010073DA
010073F8  . 33C0            XOR EAX,EAX
010073FA  . 3999 E800000    CMP DWORD PTR DS:[ECX+E8],EBX
01007400  > 0F95C0          SETNE AL
01007403    8945 E4         MOV DWORD PTR SS:[EBP-1C],EAX
```

```
Registers (FPU)
EAX 00000000
ECX 0007FFB0
EDX 7C90E4F4 ntdll.KiFastSystemCallRet
EBX 7FFDA000
ESP 0007FFC4
EBP 0007FFF0
ESI FFFFFFFF
EDI 7C910208 ntdll.7C910208

EIP 0100739D notepad.<ModuleEntryPoint>

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_ALREADY_EXISTS (000000B7)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty -UNORM BB4C 01050104 00000000
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 1.0000000000000000000
ST7 empty 1.0000000000000000000
               3 2 1 0      E S P U O Z D I
FST 4020  Cond 1 0 0 0  Err 0 0 1 0 0 0 0 0  (EQ)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
Address   Hex dump                                         ASCII
01009000  00 00 00 00 D4 70 00 01 00 00 00 00 00 00 00 00  ....Ԁp.0........
01009010  00 00 00 00 00 00 00 00 78 00 00 00 01 00 00 00  ........x...0...
01009020  4E 00 6F 00 74 00 65 00 70 00 61 00 64 00 00 00  N.o.t.e.p.a.d...
01009030  FF FF FF FF 01 00 00 00 02 00 00 00 03 00 00 00  ....0...........
01009040  04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00  ♦...♣...♠...•...
01009050  08 00 00 00 09 00 00 00 0A 00 00 00 0B 00 00 00  ◘...............
01009060  0C 00 00 00 0D 00 00 00 0E 00 00 00 0F 00 00 00  ................
01009070  10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00  ►...◄...↕...‼...
01009080  2D 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00  -...¶...§...▬...
01009090  17 00 00 00 18 00 00 00 19 00 00 00 1A 00 00 00  ↨...↑...↓...→...
010090A0  1B 00 00 00 1C 00 00 00 1D 00 00 00 1E 00 00 00  ←...∟...↔...▲...
010090B0  1F 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00  ▼... ...!..."...
010090C0  23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00  #...$...%...&...
010090D0  27 00 00 00 28 00 00 00 29 00 00 00 2A 00 00 00  '...(...)...*...
010090E0  2B 00 00 00 2C 00 00 00 34 90 00 01 38 90 00 01  +...,...4É.08É.0
010090F0  3C 90 00 01 40 90 00 01 4C 90 00 01 48 90 00 01  <É.0@É.0LÉ.0HÉ.0
01009100  44 90 00 01 50 90 00 01 54 90 00 01 58 90 00 01  DÉ.0PÉ.0TÉ.0XÉ.0
```

```
0007FFC4  7C817067  RETURN to kernel32.7C817067
0007FFC8  7C910208  ntdll.7C910208
0007FFCC  FFFFFFFF
0007FFD0  7FFDA000
0007FFD4  80544BFD
0007FFD8  0007FFC8
0007FFDC  824C3900
0007FFE0  FFFFFFFF  End of SEH chain
0007FFE4  7C839AC0  SE handler
0007FFE8  7C817070  kernel32.7C817070
0007FFEC  00000000
0007FFF0  00000000
0007FFF4  00000000
0007FFF8  0100739D  notepad.<ModuleEntryPoint>
0007FFFC  00000000
```

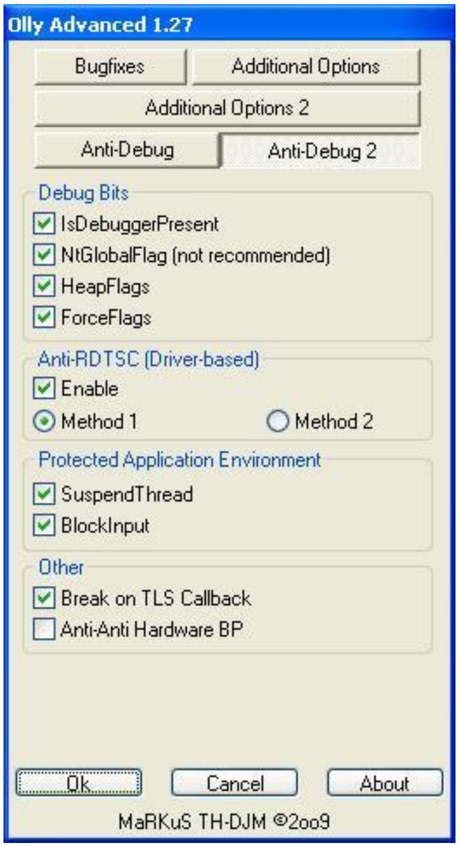
Fig. 4 OllyDbg Main Window

setting of Hardware Breakpoints, Software Breakpoints, Memory Breakpoints and even Conditional Breakpoints.

OllyDbg supports plugins to enhance its functionality.

Olly AdvancedPlugin

There were some bugs reported with Olly v1.10 related to string parsing routine, parsing of faulty executables. This plugin fixes most of these bugs. Some malware samples are loaded with Anti-Debugging techniques [7], Olly Advanced plugin helps to counter most of them.



Olly Advanced 1.27

Debug Bits

☑ IsDebuggerPresent
☑ NtGlobalFlag (not recommended)
☑ HeapFlags
☑ ForceFlags

Anti-RDTSC (Driver-based)

☑ Enable
● Method 1 ○ Method 2

Protected Application Environment

☑ SuspendThread
☑ BlockInput

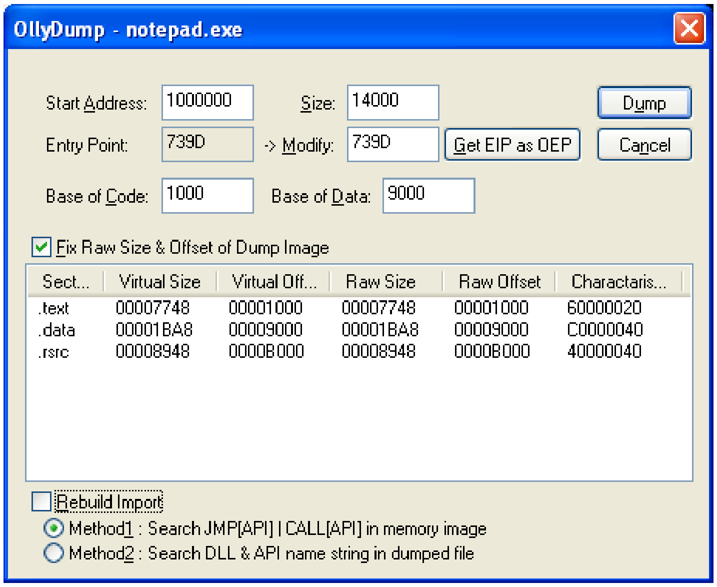
Other

☑ Break on TLS Callback
□ Anti-Anti Hardware BP

Fig. 4 OllyDbgAdvanced Plugin

Olly DumpPlugin

Olly Dump is used to dump debugged process memory. You could trace the packed file till it reaches original entry point and then dump unpacked version of file from process memory. It provides options to rebuild Import Address Table (IAT).



OllyDump - notepad.exe

Start Address: 1000000 Size: 14000

Entry Point: 739D -> Modify: 739D

Base of Code: 1000 Base of Data: 9000

☑ Fix Raw Size & Offset of Dump Image

Sect...	Virtual Size	Virtual Off...	Raw Size	Raw Offset	Charactaris...
.text	00007748	00001000	00007748	00001000	60000020
.data	00001BA8	00009000	00001BA8	00009000	C0000040
.rsrc	00008948	0000B000	00008948	0000B000	40000040

□ Rebuild Import

● Method1 : Search JMP[API] | CALL[API] in memory image

○ Method2 : Search DLL & API name string in dumped file

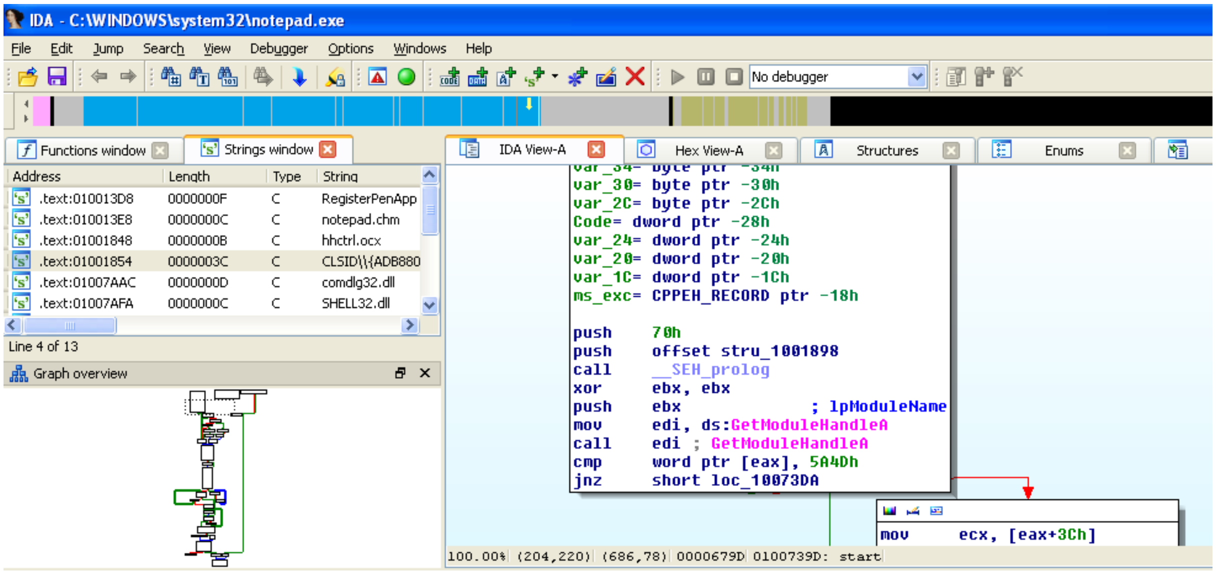
Fig. 5 OllyDbgDump Plugin

Olly ScriptPlugin

OllyScriptis a plugin to that lets you to automate OllyDbg by writing scripts in an assembly-like language. Many tasks involve a lot of repetitive work just to get to some point in the debugged application. By using this plugin you could write a script once and it could be used with other similar samples. OpenRCE[8]hosts dozens of scripts that helpful to find original entry point (OEP) of many packers.

IDA Pro

IDA Pro is a powerful disassembler that presents the disassembly in well-organized format, shows Graph view of selected function. However, it is less frequently used as a debugger in reverse engineers community where OllyDbg steals the top rank. IDA Pro's features include hex editing, string extraction, and import and export viewing. IDA Pro also features a window for



Address	Length	Type	String
.text:010013D8	0000000F	C	RegisterPenApp
.text:010013E8	0000000C	C	notepad.chm
.text:01001848	0000000B	C	hhctrl.ocx
.text:01001854	0000003C	C	CLSID\\{ADB880
.text:01007AAC	0000000D	C	comdlg32.dll
.text:01007AFA	0000000C	C	SHELL32.dll

Line 4 of 13

```
var_34= byte ptr -34h
var_30= byte ptr -30h
var_2C= byte ptr -2Ch
Code= dword ptr -28h
var_24= dword ptr -24h
var_20= dword ptr -20h
var_1C= dword ptr -1Ch
ms_exc= CPPEH_RECORD ptr -18h

push    70h
push    offset stru_1001898
call    __SEH_prolog
xor     ebx, ebx
push    ebx             ; lpModuleName
mov     edi, ds:GetModuleHandleA
call    edi ; GetModuleHandleA
cmp     word ptr [eax], 5A4Dh
jnz     short loc_10073DA
```

```
mov     ecx, [eax+3Ch]
```

```
100.00% (204,220) (686,78) 0000679D 0100739D: start
```

Fig. 6 IDA Pro Main Window

viewing all of the functions called by a program, and provides accurate analyses of the program, summarizing them in a color-coded bar at the top of the screen, which classifies the various sections of the program's code. Below figure shows IDA Pro's interface, including the disassembly and the color-coded analysis bar at the top of the screen. The titles of the other windows are visible on the tabs above the disassembly.

IDA Pro supports wide variety of processors like ARM, DEC, Intel, Motorola etc.

IDA Pro provides selection of debuggers

- Bochs
- Win Debugger
- GDB
- WinDbg

IDA Pro with Boch semulator make an interesting combination that is used to debug Operating system starting from booting process and it is helpful in debugging even ROM BIOS and Master Boot Record code.

Analysis done on particular sample, comments added, functions marked could be saved as an .idb file.

IDA Shortcuts

Below is the list of some important IDA Shortcuts, for complete list please visit reference [9].

Enter	Goto address or variable
Esc	Go back to previous location
;	Add inline comment
INSERT | SHIFT ;	Add comment
N	Rename label, variable, functions etc.
X	Show cross reference
M	Substitute enum
CTRL W	**Dont forget to** Save changes

Extending IDA

IDA supports writing IDC Scripts which is very similar to C like language on top of powerful IDA disassembler. The functionality of disassembler could be utilized even through python scripts and by writing plugins.

FLIRT

Fast Library Identification and Recognition Technology

One of the challenges with disassembly of programs developed with modern high level languages is to identify library functions. One may end up in spending considerable time to go through these functions. On the other hand identification of library functions can considerably ease the analysis of a program. IDA comes with FLIRT to recognize the standard library functions.

One must understand the power of each tool to choose appropriate tool for specific requirement during reverse engineering.

References

1. Portable Executable File Format – A Reverse Engineer View

http://tuts4you.com/download.php?view.2974

2. Hiew

http://www.hiew.ru/

3. FAR Manager

http://farmanager.com/

4. OllyDbg

http://www.ollydbg.de

5. OllyDbg Quick Start Guide

http://tuts4you.com/download.php?view.214

6. OllyDbg Plugins

http://www.openrce.org/downloads/browse/OllyDbg_Plugins

7. Anti-Debugging

http://lilxam.free.fr/repo/hacking/Windows%20Anti-Debug%20Reference.pdf

8. Olly Scripts

http://www.openrce.org/downloads/browse/OllyDbg_OllyScripts

9. IDA Shortcuts

http://www.hex-rays.com/idapro/freefiles/IDA_Pro_Shortcuts.pdf

Rajesh Nikam
rajesh@quickheal.com

Rajesh Nikam works as Lead Research Engineer with Quick Heal Malware Analysis Team. He has over 10 years of experience in Security software development and Malware Analysis. His areas of interest include Automations that help Malware Analysis, Behavior based detections and Smart Phone Malware.

EC-Council's Global CyberLympics

The cybersecurity executing arm of the United Nations has endorsed the Global CyberLympics, a new initiative by the EC-Council to foster stronger international cooperation on information security issues and to improve cybersecurity training and awareness in developing nations and third world countries.

Created by EC-Council, the Global CyberLympics is a series of ethical hacking games comprised of both offensive and defensive security challenges that will take place starting from September across six continents. Teams will vie for regional championships, followed by a global hacking championship round to determine the world's best cybersecurity team. The EC-Council is sponsoring over $400,000 worth of prizes at the CyberLympics.

The Global CyberLympics is supported by the International Multilateral Partnership Against Cyber Threats (IMPACT), the cybersecurity executing arm of the United Nations' specialized agency – the International Telecommunications Union (ITU). With this support, the Global CyberLympics hopes to be able to promote its mission to 136 partner countries with the world's first international team hacking contest around the globe.

"The Global CyberLympics could help to foster a greater sense of partnership and cooperation between countries on the issue of cybersecurity," said Mohd Noor Amin, Chairman of IMPACT. "By sharing knowledge, training and resources, we can help to improve the level of cybersecurity in many countries and regions around the world."

"Our purpose with the Global CyberLympics initiative is to help establish true cybersecurity partnerships across borders," said Jay Bavisi, Chairman of the Global CyberLympics Organizing Committee and president of EC-Council. "We are very proud and honored for this initiative to be supported by key players in the information

security community, including IMPACT, the world's first United Nations-backed global alliance for cybersecurity, as well as some of the most reputable events such as GITEX, the largest IT tradeshow in the Middle East region, and Hacktivity, the largest hackers conference in central and eastern Europe."
The hacking contests come at a crucial time as global cyber threats appear to be escalating. According to the U.S. Cyber Consequences Unit, the annual loss of intellectual property and investment opportunities is $6 to $20 billion as a result of hacking. In a recent article about cyber espionage attacks against the US, the magazine Vanity Fair even referred to 2011 as "the Year of the Hack."

The EC-Council's mission with the Global CyberLympics is to unify global cyber defense through the hacking games, along with the following objectives:

- Capacity Building: Discover new talents, methods and ideas; and to encourage development in the field of information security. Besides discovering gifted hackers and cyber-defenders, the Global CyberLympics will also inspire the development of Information security professionals of the future.
- Raising Awareness: Educate the global community, especially in developing nations and third world countries, on the issues of Information security, and encourage further development of the field. This will raise awareness towards increased education and ethics in information security.
- Global Peace: Foster friendship and create cohesiveness between information security professionals, whether as an individual, representing a corporation or for a national agency, and encourage frequent exchange of essential information, technology and skills.

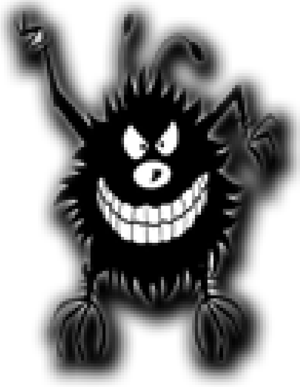
Regional championships will be held in various locations across different continents, and co-hosted with reputable IT/information security conferences and tradeshows, as follows:

- North America (Eastern) | Hacker Halted USA – Miami, USA
- North America (Western) | TakeDownCon – Las Vegas, USA
- South America | H2HC – Sao Paolo, Brazil
- Europe | Hacktivity – Budapest, Hungary
- Middle East & India | GITEX – Dubai, UAE
- Asia Pacific | Hacker Halted APAC – Kuala Lumpur, Malaysia
- Africa | TakeDownCon – Johannesburg, South Africa

The CyberLympics world final is tentatively scheduled for the first quarter of 2012, with its venue still being decided.

EC-Council has selected iSight Partners' Threatspace platform as the Official Technology Partner of the Global CyberLympics 2011-12.

Registration for the Global CyberLympics is open, and more details can be found at the official Global CyberLympics website:
http://www.cyberlympics.org



Introduction to Malware & Malware Analysis

Introduction

Very often people call everything that corrupts their system as *virus*, not aware of what it actually means or does. This paper systematically gives an introduction to different varieties of beasts that come under the wide umbrella called as *malware*, their distinguishing features, prerequisites for malware analysis and an overview of malware analysis process.

What is Malware?

The genesis of Computer viruses started in early 1980 when some researchers came up with self-replicating computer programs. In 1984 Dr. Cohen provided a definition for computer viruses. Here is Cohen's informal definition of a computer virus:

"A virus is a program that is able to infect other programs by modifying them to include a possibly evolved copy of itself."

This definition, based on the behavior of programs of that period was appropriate. However over time, viruses have evolved into dozens of different categories and are now termed as *malware* collectively instead of virus. Virus is considered as one category of *malware*.

Malware, short for, MALicious softWARE. It is software specifically designed to harm user's computer data in some way or the other. Malwares have evolved with technology and have taken advantage of new developments.

Wikipedia[1]:

Malware consists of programming (code, scripts, active content, and other softwares) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behavior. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

Symptoms of infected system

How do you know that your system is infected with possible malware? Following are some of the symptoms of an infected system:

- System might become unstable and respond slowly as Malware might be utilizing system resources
- Unknown new executables found on the system
- Unexpected network traffic to sites where you don't expect to connect
- Altered system settings like browser homepage without your consent
- Random pop-ups are shown as advertisements
- Recent addition to the set are alerts shown by fake-security application that you never installed like "Your computer is infected!" and it asks to register the program to remove detected threats.

Overall, your system will have unexpected behavior.

Malware Classification

The category of malware is decided based upon different parameters like how it affects the system, functionality or the intent of the program, spreading mechanism, and whether program asks for users' permission or consent before performing these operations.

A program that can be regarded as malware if it does one of the following activities:

- modifies another program
- replicates through a network or a file system without users' consent
- allows an unauthorized person to take control over a remote system
- sends personal or confidential information to a remote system without user's consent
- sends data to a system in order to disrupt normal functioning
- opens port for listening on local machine to accept commands from control server
- record keystrokes and send this information to remote servers
- connects to suspicious remote servers
- downloads and executes files from suspicious remote servers
- copy itself to multiple locations
- injects code into another program
- makes unauthorized changes to the system
- modifies a protected system setting

- modifies a registry setting used for launching programs upon startup

Now we will specific malware categories based on distinguishing malicious features of the sample:

Virus

Virus is the first category of malware to appear on the horizon of Computer Security. They are self-replicating in nature and are referred to as parasitic infectors. They don't have separate existence; however they insert their code into existing files on the system. They could be executable programs or scripts of different programming languages like VBS, JS, Perl etc.

Worm

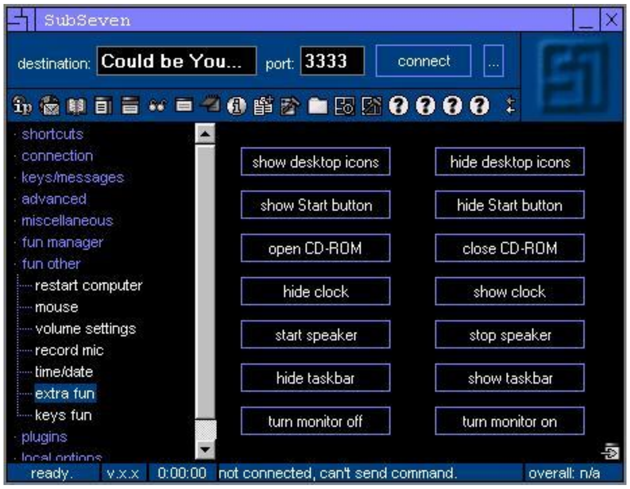
Worm are self-replicating; however they are stand-alone malware. They don't modify other files to spread, instead makes copies of own over network shares or on other systems. Worms are further classified based upon spreading mechanism used like Email, P2P, IRC etc.

Trojan Horse

Trojan is disguised as useful software and tempts user to install it and it is bundled with hidden malicious functionality. They are non-replicating in nature, i.e. they don't spread themselves as in case of viruses or worms.

Backdoor

Backdoor allow unauthorized access to compromised system by opening a port on victim’s system. This creates a pathway for hackers to control the compromised system by sending commands of his choice. SubSeven, Netbus and Back Orifice are some of the well-known examples of Backdoor which enables unauthorized people to access users' system over the Internet without his/her knowledge.



SubSeven

destination: Could be You... port: 3333

ready. v.x.x 0:00:00 not connected, can't send command. overall: n/a

Fig. 1Backdoor.SubSeven

HackTool

HackTool is used by a hacker to attack and exploit users' system to gain unauthorized access to system resources. They attempt to gain information on the system bypassing security mechanisms inherent to the system. *netcat* is an example of HackTool. Sometimes it is used by Network Administrators; however it is used by hackers to get unauthorized access and to transmit data on network.

Spyware

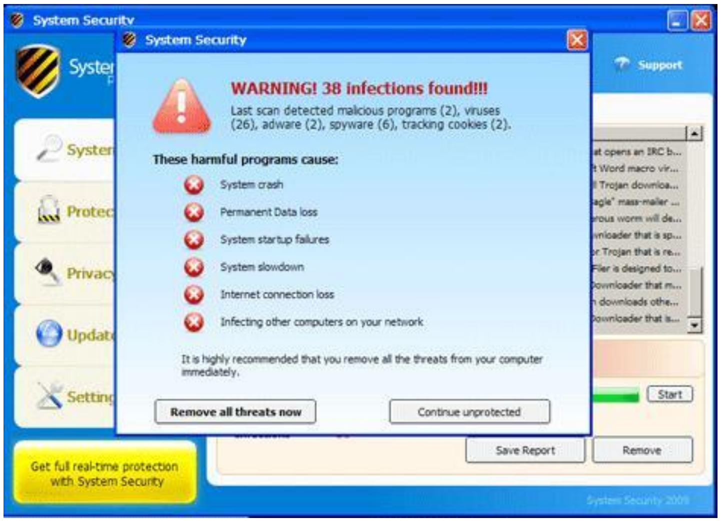
Spyware is software that gathers personal or confidential information from users' system without his knowledge. It includes monitoring on victims system to collect information like his browsing habits, recently visited sites, passwords, credit card information, and other such confidential information. Once Spyware is installed, it doesn’t have any visible notification to indicate it’s monitoring users' activities. It sends this information to the configured remote server.

Rootkit

Rootkit use stealth technique to actively hide its presence by hiding it components like files, registry key, running processes and other objects. These techniques are used to hide its behavior from user and to bypass detection from security applications.

Rogue application

These are fake applications which pose themselves as Security Applications or System Tools to mislead user into paying for removal of non-existent malwares or issues with users' system. This category of malware is on rise of from last 4-5 years. They use different Social Engineering techniques to mislead the user into installing it. Its downloader component may come as a video codec to run certain video clips, P2P software or trojanized shared applications. Malware writers use SEO poisoning technique to push malicious urls based on recent popular news. When user visits such malicious urls, it gets downloaded using drive-by-download technique by exploiting vulnerabilities in web browser and its plugins.



WARNING! 38 infections found!!!

Last scan detected malicious programs (2), viruses (26), adware (2), spyware (6), tracking cookies (2).

These harmful programs cause:

- System crash
- Permanent Data loss
- System startup failures
- System slowdown
- Internet connection loss
- Infecting other computers on your network

It is highly recommended that you remove all the threats from your computer immediately.

Fig. 2 Rogue Application – System Security

Infection Vectors

An infection vector refers to spreading mechanism used by malware.

- Boot Sector: Infecting Master Boot Record of the physical disk
- File infection: Parasitic infectors
- Email: Email worms
- File shares: Parasitic infectors, worms
- Network: Network worms, through vulnerabilities
- IRC: Internet Relay Chat
- P2P networks: IM, Kazaa, etc.
- Removable Media: Floppy, USB Disks
- Bluetooth: Worms for mobile devices
- Web Apps: Using cross-site scripting vulnerabilities
- Vulnerabilities: Operating system, Web Browser & plugins, Adobe Reader vulnerabilities

Prerequisites for Malware Analysis

Now being equipped with the knowledge of what malware is, you may want to look at it more closely. Natural question might come to your mind is, "*how to analyze malware*?"Prerequisites for Malware Analysis include understanding of malware classification, essential x86 assembly language concepts[2], file formats like Portable Executable file format, Windows APIs, expertise in using

Monitoring tools, Disassemblers and Debuggers. This section will introduce you with prerequisites for malware analysis.

Cheat sheet of x86 assembly language

Registers are special data location as part of CPU used for data manipulation.	
EAX	Accumulator, Contains the return value
ECX	ECX Used as a loop counter, "this" pointer in C++
EBX	General Purpose Register
EDX	General Purpose Register
ESI	Source Index Pointer
EDI	Destination Index Pointer
ESP	Stack Pointer
EBP	Stack Base Pointer
EIP	Instruction Pointer
Flags	ZERO, SIGN, CARRY, OVERFLOW, TRAP

Assembly Instructions	
ARITHMATIC	ADD, ADC, SUB, SBB, MUL, DIV, IMUL, IDIV, INC, DEC, CMP, NEG
LOGICAL	XOR, OR, AND, TEST, NOT
SHIFT AND ROTATE	ROR, ROL, RCR, RCL,SHR, SHL, SAR, SAL
DATA TRANSFER	MOV, PUSH, POP, PUSHA, POPA, XCHG
CONTROL TRANSFER	CALL, RET, JMP, LOOP, JE/JZ, JL, JG, JGE, JLE, JNE/JNZ, conditional JMPs, INT
STRING	CMPS, SCAS, LODS, STOS, MOVS, REP prefix
MISCELLANEOUS	LEA, NOP, XLAT

Portable Executable File Format

Microsoft uses the Portable Executable (PE) file format[3] for executables and system libraries from Windows 95. For reverse engineering one should be familiar with the Portable Executable file format.

The PE Header contains important information about linker version used, how the executable should be loaded, compatible version of Microsoft Windows, type of executable file etc.

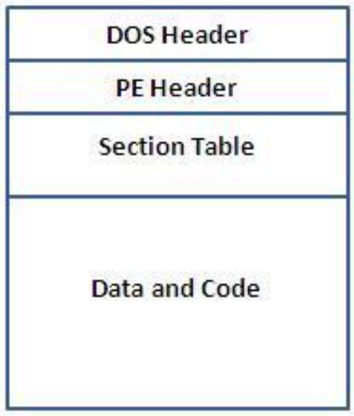


Fig.3 PE File Format

Some important fields from PE Header are Address Of Entry Point and Image Base which points to address of first instruction to be executed when executable is loaded and Virtual Address where executable is loaded in virtual memory, respectively.

The PE header is followed by Data Directories including the import table, export table. The import table has information about functions that the program calls from DLL files. The export table, generally present in DLL files, has information of functions that call other programs. It is followed by Section Table which provides relative virtual addresses and characteristics of sections of the program.

Windows APIs

Microsoft Windows operating system provides interface to applications through Windows Application Programing Interface (API). It is implemented as a set of system libraries like kernel32.dll, user32.dll etc. Reverse Engineer needs to be conversant with File System, Memory management, Process and thread management, Registry Management, Networking and Security related APIs. Understanding of APIs will help during detailed malware analysis. MSDN [4]provides comprehensive documentation of Windows APIs.

Malware Analysis

Microsoft Windows Operating System is the most popular and widely used over others Operating Systems thus making it first in the target list of Malware authors. We will see Malware Analysis on Windows Platform in this article. Malwares appear in different varieties like executable files, BAT scripts, VBScript, JavaScript, Macros in Microsoft office files, exploit code in JPG, GIF, SWF, PDF files. More than 80% malware samples received by Security Vendors are Windows executables.

The purpose of Malware Analysis is to study a program's behavior and verify if it has malicious functionality or behavior. If the analyzed sample is found malicious then comes classification of it and identification of specific malware family.

Environment for Malware Analysis

One should be very careful when analyzing malware samples. Malware Analysis should be done on the system separated from production environment and network isolated from public network. Virtualization software [10]like VMWare, Virtual Box provides option to create such environment.

Static Analysis

With static analysis, we study a program without actually executing it. Tools of the trade are Hex Editors, disassemblers and packer identifiers. We could look for suspicious strings related to file paths, registry keys, urls, messages intended for users if any are used in a program. APIs used also give an idea about functionality of the program.

Samples which are packed or obfuscated provide challenges for static analysis. If sample is packed, then it needs to be unpacked before diving into code analysis.

Dynamic Analysis

With dynamic analysis, we study a program as it executes. We need to monitor the changes made to file system, registry, processes and its network communication. Sys Internals tools [7] like Process Monitor, Process Explorer, TCPView, gmer[8] and WireShark[9] are useful for observing runtime behavior of a program. Debuggers like OllyDbg, IDA Pro and WinDbg are helpful to dig into details of encrypting malwares and for detailed analysis.

In case of non-availability of safe environment to execute suspicious samples, one could use online automated malware analysis systems[5]. User could submit suspicious sample for analysis and it generates report based on file system modifications, registry modification, network communication etc.

Hope this helps in some way to take your step forward into world of computer viruses, I mean Malware☺

References

1. WIKIPEDIA

http://en.wikipedia.org/wiki/Malware

2. Art of Assembly

http://www.arl.wustl.edu/~lockwood/class/cs306/books/artofasm/toc.html

3. PE File Format

http://www.microsoft.com/whdc/system/platform/firmware/PECOFF.mspx

http://www.openrce.org/reference_library/files/reference/PE%20Format.pdf

4. MSDN

http://msdn2.microsoft.com/en-us/library/default.aspx

5. Online Automated Malware Analysis Systems

http://www.threatexpert.com/

http://www.sunbeltsecurity.com/sandbox

6. The Art of Computer Virus Research and Defense

http://www.peterszor.com/

7. SysInternals Suite

http://technet.microsoft.com/en-us/sysinternals/bb842062

8. GMER

http://www.gmer.net/

9. WIRESHARK

http://www.wireshark.org/

10. Virtualization Software

http://www.virtualbox.org/

http://www.vmware.com/

Rajesh Nikam
rajesh@quickheal.com

Rajesh Nikam works as Lead Research Engineer with Quick Heal Malware Analysis Team. He has over 10 years of experience in Security software development and Malware Analysis. His areas of interest include Automations that help Malware Analysis, Behavior based detections and Smart Phone Malware.

HITBSecConf 2011

The 9th annual HITBSecConf in Malaysia takes place from October 10th - 13th at the InterContinental Kuala Lumpur. HITBSecConf is a deep-knowledge (community backed, not for profit) security conference featuring some of the worlds leading network security specialists under one roof. These conferences are held annually in Dubai, Amsterdam and Kuala Lumpur. The event kicks off as usual with 2 days of hands on technical training sessions catering to a maximum of 20 students per class. Four training courses are scheduled including:

*** The Exploit Laboratory 5.0 * Hunting Web Attackers * Advanced Linux Exploitation Methods * Web Hacking 2.0: Attacks, Penetration and Exploits**

The keynote speakers for the conference will be Kenneth Geers (from NCIS / NATO Cooperative Cyber Defence Centre of Excellence) and Jennifer Granick (former Civil Liberties Director with the Electronic Frontier Foundation). Joining them will be over 30 internationally recognized security experts in a quad track conference format. The draft conference agenda has also been published and some of the presentations scheduled include:

HITB Labs: Practical Attacks Against 3G/4G Telecommunication Networks

http://conference.hitb.org/hitbsecconf2011kul/?page_id=1782

Air Travel Hacking: Understanding and (Ab)Using the Global Distribution System

http://conference.hitb.org/hitbsecconf2011kul/?page_id=1732

Femtocells: A Poisonous Needle in the Operator's Hay Stack

http://conference.hitb.org/hitbsecconf2011kul/?page_id=1760

Satellite Telephony Security: What is and What Will Never Be

http://conference.hitb.org/hitbsecconf2011kul/?page_id=1786

As usual, the conference will be further enhanced by an exhibition and technology showcase area, a lock picking village run by members of TOOOL USA, a Capture The Flag 'live hacking' competition and a Hackerspaces 'playground' in which members of the public will be introduced into the wonderful world of hardware hacking and electronics.

In addition to the above, there will also be a new 24-hour hackthon which will run alongside the main conference called HackWEEKDAY. The main aim of HackWEEKDAY is to build security tools and encourage developers to start thinking about secure coding practices. Kicking off at 13:37 MYT on the 12th of October and ending a full 24-hours later on the 13th, coders from all walks of life will come together and work on open source security projects - From reviving security focused Firefox plugins to writing new Maltego transforms and even development of an analytics based DNS engine.

For further details and to register, please see **http://conference.hitb.org/hitbsecconf2011kul/**

Law relating to Cyber Pornography in India

Pornography or obscenity is very sensitive issue all over the world yet there is no settled definition of the word under any law. What is nude art or sexually explicit thing for one person may be obscene or porn for another. Hence, it is very difficult to define "What is porn?"

There have been many attempts to limit the availability of pornographic content on the Internet by governments and law enforcement bodies all around the world but with little effect. Classic example is a website, www.incometaxpune.com, prima facie, it looks a website of Income tax department of Pune City, but actually it's a porn site. Though it was blocked many times by law enforcement agencies in India, it is still available with obscene contains.

Pornography on the Internet is available in different formats. These range from pictures and short animated movies, to sound files and stories (remember "*Savitabhabhi*"!!!). The Internet also makes it possible to discuss sex, see live sex acts, and arrange sexual activities from computer screens. Although the Indian Constitution guarantees the fundamental right of freedom of speech and expression; it has been held that a law against obscenity is constitutional. The Supreme Court has defined obscene as "offensive to modesty or decency; lewd, filthy, repulsive".

Section 67 of the Information Technology Act, 2000 penalizes cyber pornography. Other Indian laws that deal with pornography include the **Indecent Representation of Women (Prohibition) Act** and the **Indian Penal Code.**

Section 67 reads as under:-

Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

This section explains what is considered to be obscene and also lists the acts in relation to such obscenity that are illegal.

Explanation

Any material in the context of this section would include video files, audio files, text files, images, animations etc. These may be stored on CDs, websites, computers, cell phones etc.

Lascivious is something that tends to excite lust.
Appeals to, in this context, means "arouses interest".
Prurient interest is characterized by lustful thoughts.
Effect means to produce or cause some change or event.
Tend to deprave and corrupt in the context of this section means "to lead someone to become morally bad".
Persons here refers to natural persons (men, women, children) and not artificial persons (such as companies, societies etc).

To be considered obscene for the purpose of this section, the matter must satisfy at least one of the following conditions:-

- it must tend to excite lust, or
- it must arouse interest in lustful thoughts, or
- it must cause a person to become morally bad.

The above conditions must be satisfied in respect of a person who is the likely target of the material.

Illustration

Sameer launches a website that contains information on sex education. The website is targeted at higher secondary school students. Pooja is one such student who is browsing the said website. Her illiterate young maid servant happens to see some explicit photographs on the website and is filled with lustful thoughts.
This website would not be considered obscene. This is because it is most likely to be seen by educated youngsters who appreciate the knowledge sought to be imparted through the photographs. It is under very rare circumstances that an illiterate person would see these explicit images.

Acts those are punishable in respect of obscenity:-

"Publishing" means "to make known to others". It is essential that at least one natural person (man, woman or child) becomes aware or understands the information that is published. Simply putting up a website that is never visited by any person does not amount to publishing.

"Transmitting" means to pass along convey or spread. It is not necessary that the "transmitter" actually understands the information being transmitted.

Information **in the electronic form** includes websites, songs on a CD, movies on a DVD, jokes on a cell phone, photo sent as an email attachment etc.

The **punishment** provided under this section is as under:-

- First offence: Simple or rigorous imprisonment up to 3 **years** and fine up to **Rs 5 lakh**.

- Subsequent offence: Simple or rigorous imprisonment up to **5 years** and fine up to **Rs 10 lakh**.

Amendments of 2008 introduced new Section on Cyber pornography i.e. **Section 67A**.

The Section makes publishing or transmitting of sexually explicit act or conduct illegal with a punishment of imprisonment upto five years and with fine which may extend to ten lakh rupees for first offence and seven years for subsequent offences.

Hence, the Section makes publishing or transmission of blue films, audio sex clips, pictures, magazines and any other material in the electronic form involving sexually explicit acts illegal.

Sagar Rahurkar
sr@asianlaws.org

Sagar Rahurkar, a Law graduate, is Head(Maharashtra) at Asian School of Cyber Laws. Sagar specializes in Cyber Law, Intellectual Property Law and Corporate Law. Sagar also teaches law at numerous educational institutes and has also trained officials from various law enforcement agencies.

International Information Security and Hacking Conference

07-08 Oct 2011, Kochi, India

c0c0n
Security And Hacking Conference

http://www.informationsecurityday.com/c0c0n

Tentative Speakers for c0c0n 2011

Mauro Risonho de Paula Assumpção aka firebits
Backtrack Brasil - firebits@backtrack.com.br

Mickaël Schoentgen aka Tiger-222
Development Lead - Project Matriux (France)

Maximiliano Soler
Buenos Aires, Argentina

Michael Kemp
Co-Founder: Xiphos Research Labs, Birmingham, United Kingdom

Pre-Conference Workshops and Trainings

Wireless Security & Hacking
By Vivek Ramachandran
SecurityTube - http://www.securitytube.net/

Metasploit
By Vivek Ramachandran
SecurityTube - http://www.securitytube.net/

Attack/Incident Identification/Investigation analysis course content
By null

Web Application Security
Team Mantra - http://www.getmantra.com/

Shell Coding By Rohit Sharma

Reverse Engineering By Harsimran Walia

Cyber Forensics 101
By Team Matriux - http://www.matriux.com/

.Net Secure Coding Practices
By Vimal Raj

Penetration Testing using Matriux Krypton
By Team Matriux - http://www.matriux.com/

Python 101 for Security Pro
By Team Matriux - http://www.matriux.com/

Contact Details

Manu Zacharia	m@matriux.com or info@informationsecurityday.com	098470-96355
Thomas Ambat	thomas@riskandcontrols.com	094470-22081
Binoy Joseph	binoyjose9@gmail.com	094470-60298

International Information Security and Hacking Conference

07-08 Oct 2011, Kochi, India

Security And Hacking Conference

http://www.informationsecurityday.com/c0c0n

About c0c0n

c0c0n, is an annual information security event conducted as part of the International Information Security Day (http://www.informationsecurityday.com).
The Information Security Research Association along with the Matriux Security Community is organizing a 2 day International Security and Hacking Conference titled c0c0n 2011, as part of Information Security Day 2011.

Various technical, non-technical, legal and community events are organized as part of the program. c0c0n 2011 is scheduled on 07, 08 Oct 2011. For more information, please visit – http://www.informationsecurityday.com/c0c0n

About Previous Year Event c0c0n 2010 -

c0c0n 2010 was organized on 05 and 06 Aug 2010 @ Hotel Dreams International, Cochin. The event was inaugurated by the then Home Minister of Kerala Sri. Kodiyeri Balakrishnan. The inauguration ceremony was followed by keynote address from r. Laxman K Bagadia, CIO – Wipro Limited. The other keynotes were delivered by:

- Mr. Alok Vijayant, Director – Information Dominance Group (IDG), National Technical Research Organization (NTRO), and
- Mr. Krishnan Nilakantan, Director – CERT, Kerala

The event consisted of 24 security talks on two parallel tracks delivered by international renowned speakers like:

- Raoul Chiesa, Senior Advisor on Strategic Alliances & Cybercrime Issues – United Nations Interregional Crime & Justice Research Institute (UNICRI) and Member PSG – European Network and Information Security Agency (ENISA)
- Fyodor Yarochkin, Security analyst for Armorize Technologies
- Nirupa Calvin, Google
- Vahan Markarov, Security Researcher, Yerevan, Armenia
- Pavel Akhramchuk, Mobile Security Researcher, Minsk, Belarus, etc.

No conference is complete without some fun and parties. The participants and invited guests were also taken through a beautiful Backwater boat ride at the end of Day 1 followed by a Cocktail party with live bands rocking the hall.

More than 400 professionals attended c0c0n 2010 making it the biggest and the largest security conference of India.

Ostinato - Wireshark in Reverse

Namaskaar Readers,

It's been a great time for Matriux in the last month - Matriux Krypton is released on August 15th 2011 and available for public download. And we had an overwhelming downloads and feedback on the project. We thank all the users out there for downloading and testing Matriux. We really appreciate the people out there for their time in writing the feedback and also providing tutorials for the newbies. Thank you all for making Matriux Krypton a big success and looking forward to the same in the future to work along with the enthusiast group of security guys. We are open to feedback/reports report@matriux.com

This issue contains a brief introduction on Ostinato, an open-source, network packet crafter/traffic generator and analyzer with a very easy to use GUI.

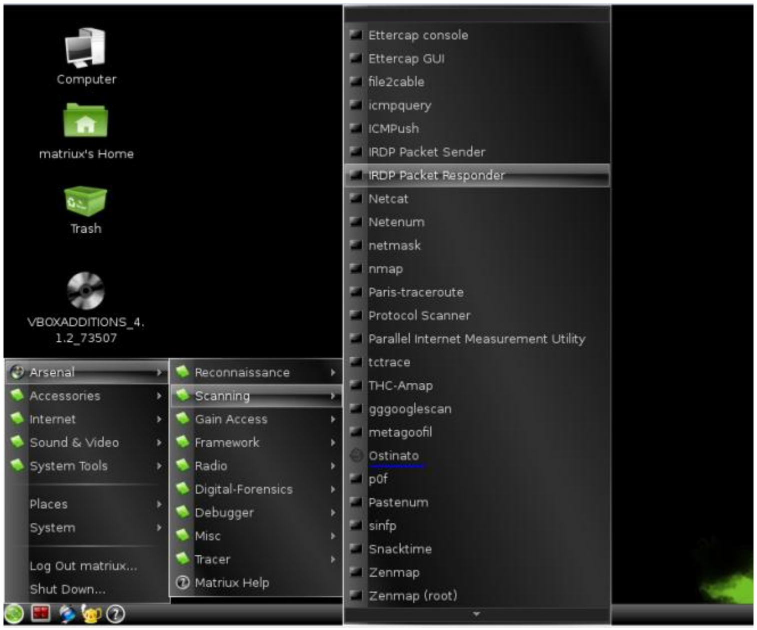
Like it says, it aims to be reverse the ofWireshark.

What could be done with Ostinato?

- Generate the traffic, craft and analyze
- Specify your own Hex Dump
- Create and configure multiple packet streams with stream rates, bursts, packets over multiple ports and computers using a single client
- Capture and view the packets alongside wireshark.

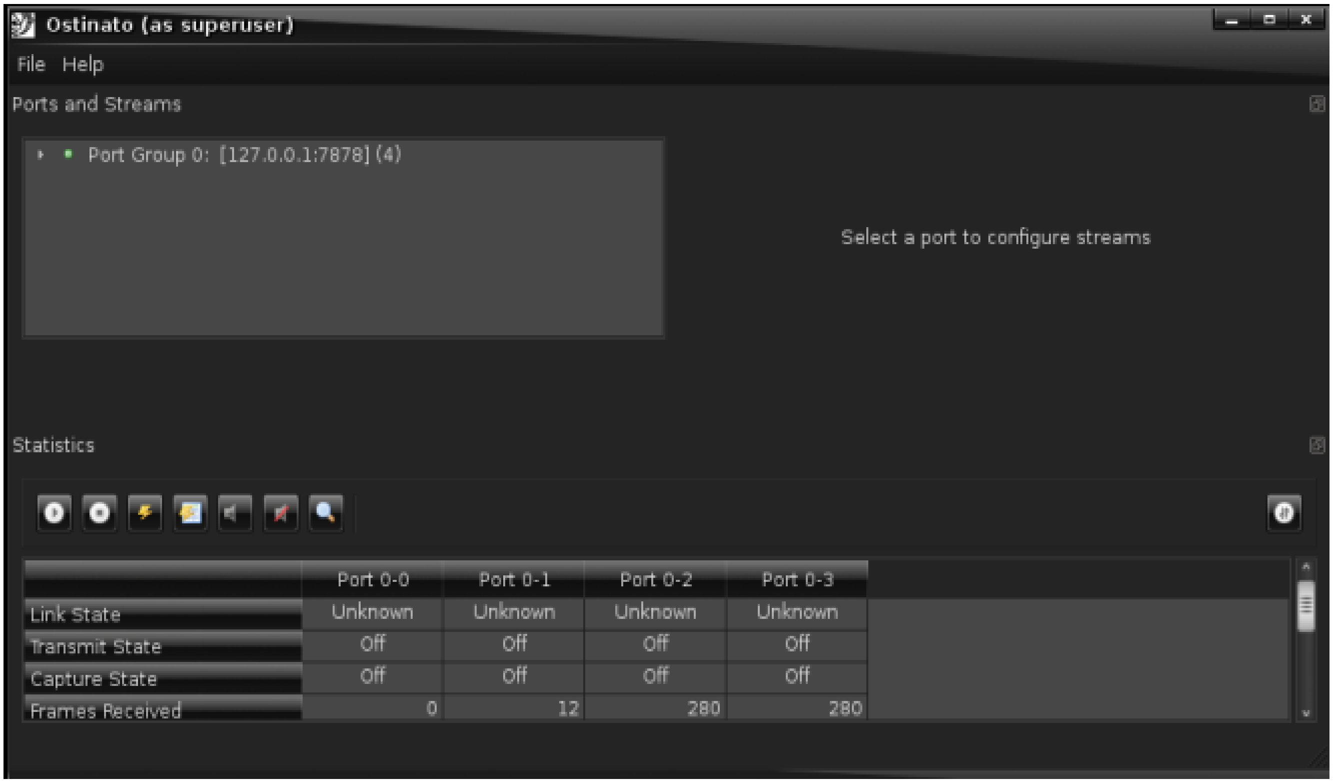
Let's get started!!

Ostinato can be found in MatriuxArsenal as Arsenal => Scanning => Ostinato



This starts up a GUI which is very quick and easy to use (Figure 2).

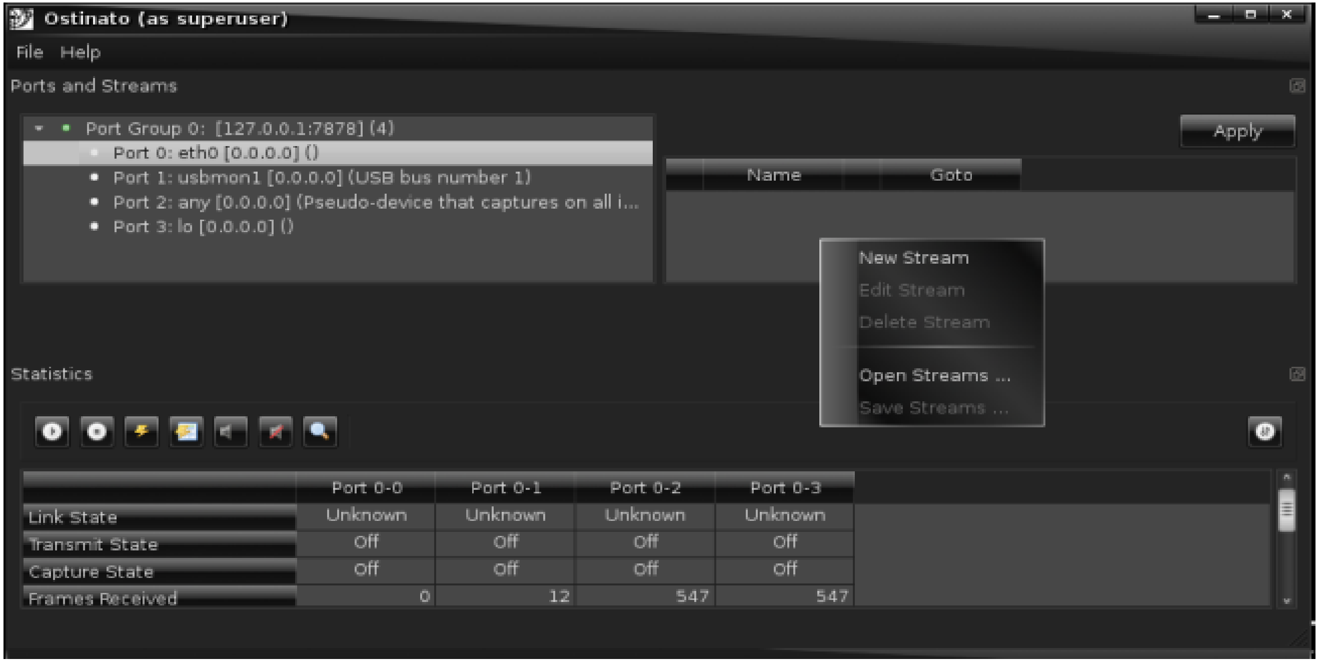
Right click over the column in the right side and create a new stream as shown in the figure below (Figure 3).


Ostinato (as superuser)
File Help
Ports and Streams
Port Group 0: [127.0.0.1:7878] (4)
Select a port to configure streams
Statistics

	Port 0-0	Port 0-1	Port 0-2	Port 0-3
Link State	Unknown	Unknown	Unknown	Unknown
Transmit State	Off	Off	Off	Off
Capture State	Off	Off	Off	Off
Frames Received	0	12	280	280

Figure 2

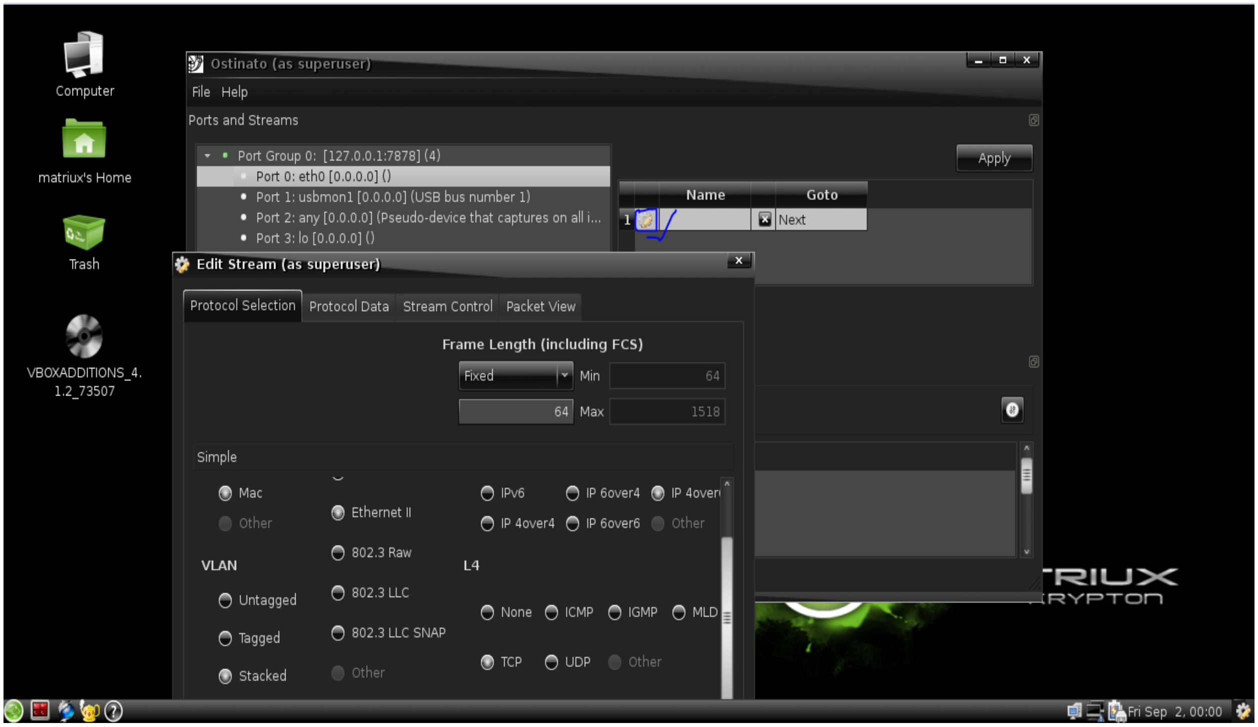
Move around the port groups (either expand the list or create a new port group from the file menu)


Ostinato (as superuser)
File Help
Ports and Streams
Port Group 0: [127.0.0.1:7878] (4)
Port 0: eth0 [0.0.0.0] ()
Port 1: usbmon1 [0.0.0.0] (USB bus number 1)
Port 2: any [0.0.0.0] (Pseudo-device that captures on all i...
Port 3: lo [0.0.0.0] ()
Apply
Name
Goto
New Stream
Edit Stream
Delete Stream
Open Streams ...
Save Streams ...
Statistics

	Port 0-0	Port 0-1	Port 0-2	Port 0-3
Link State	Unknown	Unknown	Unknown	Unknown
Transmit State	Off	Off	Off	Off
Capture State	Off	Off	Off	Off
Frames Received	0	12	547	547

Figure 3

Click over the tools option and configure the packets to be generated. Go ahead and choose all the options you prefer. (protocols, data stream, source, destination).



Ports and Streams

- Port Group 0: [127.0.0.1:7878] (4)
  - Port 0: eth0 [0.0.0.0] ()
  - Port 1: usbmon1 [0.0.0.0] (USB bus number 1)
  - Port 2: any [0.0.0.0] (Pseudo-device that captures on all i...
  - Port 3: lo [0.0.0.0] ()

	Name	Goto
1		Next

Frame Length (including FCS)

Fixed Min 64

64 Max 1518

Simple

○ Mac ○ Other

VLAN

○ Untagged ○ Tagged ○ Stacked

○ Ethernet II ○ 802.3 Raw ○ 802.3 LLC ○ 802.3 LLC SNAP ○ Other

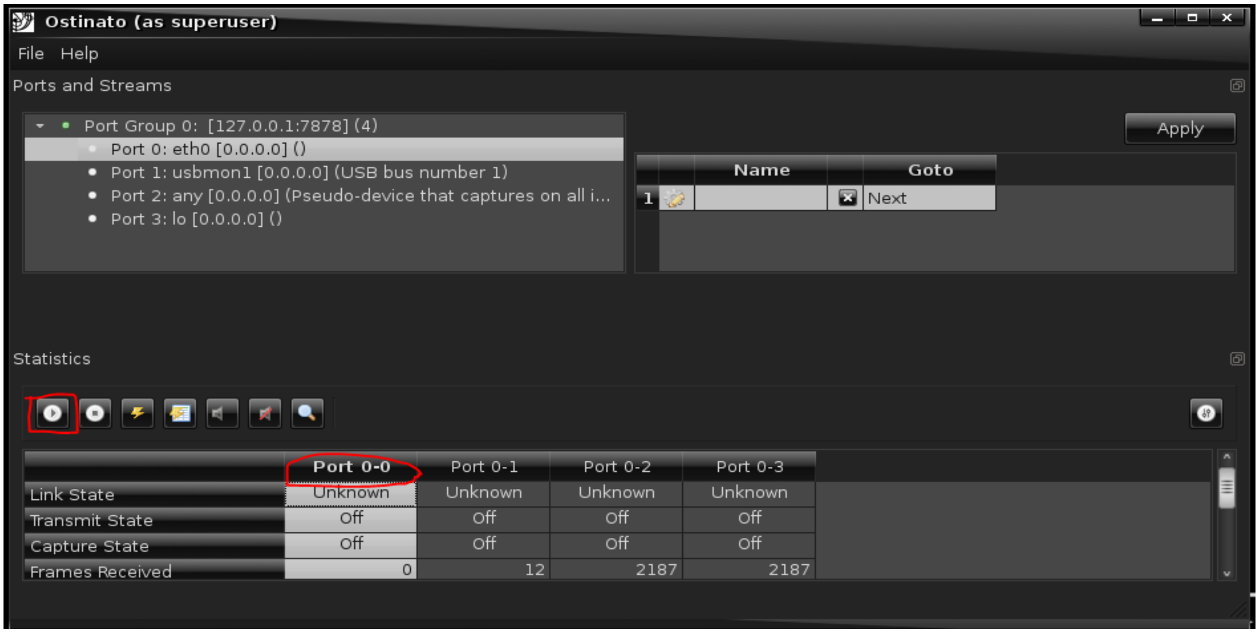
○ IPv6 ○ IP 6over4 ○ IP 4over4 ○ IP 4over6 ○ IP 6over6 ○ Other

L4

○ None ○ ICMP ○ IGMP ○ MLD ○ TCP ○ UDP ○ Other

Figure 4

Click OK and also Apply button over the top right corner of the window otherwise these settings would fail (Figure 5).



Ports and Streams

- Port Group 0: [127.0.0.1:7878] (4)
  - Port 0: eth0 [0.0.0.0] ()
  - Port 1: usbmon1 [0.0.0.0] (USB bus number 1)
  - Port 2: any [0.0.0.0] (Pseudo-device that captures on all i...
  - Port 3: lo [0.0.0.0] ()

	Name	Goto
1		Next

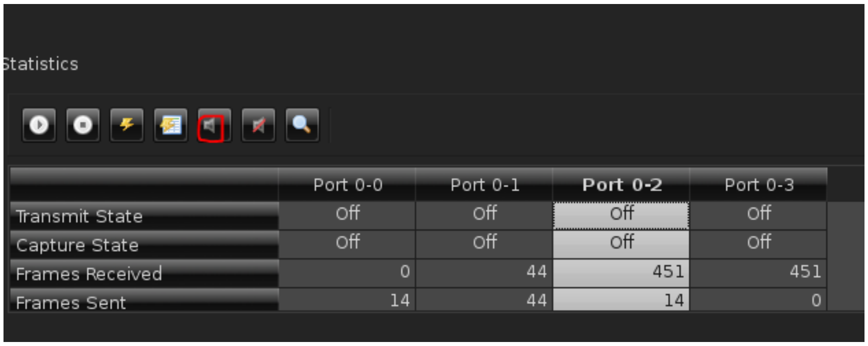
Statistics

	Port 0-0	Port 0-1	Port 0-2	Port 0-3
Link State	Unknown	Unknown	Unknown	Unknown
Transmit State	Off	Off	Off	Off
Capture State	Off	Off	Off	Off
Frames Received	0	12	2187	2187

Figure 5

Now we are ready to go for generating the packet traffic. Click on the port you just applied and click the start button.. This will now start transmitting the traffic

You can capture the traffic that is being transmitted my selecting the configured port group and clicking on the capture button (Figure 6).

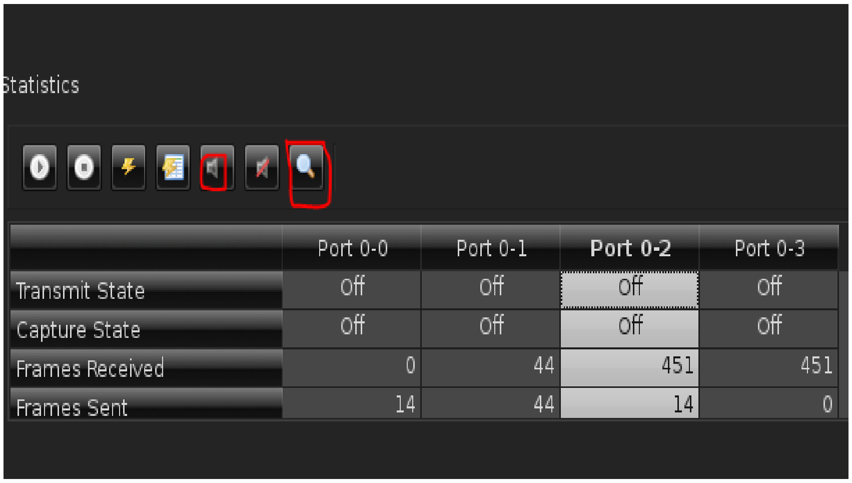


Statistics

	Port 0-0	Port 0-1	Port 0-2	Port 0-3
Transmit State	Off	Off	Off	Off
Capture State	Off	Off	Off	Off
Frames Received	0	44	451	451
Frames Sent	14	44	14	0

Figure 6

This traffic can be analyzed over wireshark by clicking the view captured files button over there (Figure 7).



Statistics

	Port 0-0	Port 0-1	Port 0-2	Port 0-3
Transmit State	Off	Off	Off	Off
Capture State	Off	Off	Off	Off
Frames Received	0	44	451	451
Frames Sent	14	44	14	0

Figure 7

So I hope you go head and try all the options in the Ostinato tool and play around with it.

Report suggestions and bugs to report@matriux.com or prajwal@matriux.com

Team Matriux invites you all to the **c0c0n**, International Information Security and Hacking Conference, 07-08 Oct 2011, Kochi, India. Hope to see you all there. ☺

Team Matriux

http://www.matriux.com/

Twitter : @matriuxtig3r

Cyber Defence Summit being held in Abu Dhabi on September 20th-21st 2011 is the first initiative focused on protecting critical infrastructure in the Middle East. It enables C - level cyber security experts from Government authorities, banks, oil & gas, telecom and utilities sector to identify, investigate and resolve security challenges in the region.

Event Highlights

- ***Focused one-to-one business meetings*****:** One-to-one business meetings are arranged with your choice of pre-qualified delegates at the summit.

- ***Keynote presentations*****:** Keynote presentations and sessions are delivered by experts who have planned and successfully executed cyber defence projects internationally.

- ***Interactive panel discussions*****:** Carefully selected industry experts are invited to lead panel discussions on the latest developments and future of cyber security.

- ***Interactive workshops and executive networking*****:** Educational workshops are led by specialised cyber security consultants, amongst others, to provide a tailored training session to a selected audience.

Speakers at the event include:

- **Victor Philip**, Director Policy and International Cooperation, *IMPACT*

- **Paul Kurtz**, Board Member, *Cloud Security Alliance*

- **Jim Hietala**, VP Security, *The Open Group – Jericho Forum*

- **Tariq Al Hawi**, Director, *aeCERT*

- **Dr. Andrew Jones**, Program Chair, MSc in Information Security, *Khalifa University*

- **Paul Dorey**, Chairman, *IISP*

- **Giovanni Violante**, Head of Cyber Defence, *Selex Sistemi Integrati*

- **Colonel (Retired) Carl Williamson**, Executive Director of Cyber Strategy, Defense Enterprise Solutions, *Northrop Grumman Corporation*

- **Dr. Ihab Ali**, Vertical Solutions Practice Lead, *Dell*

- **Illyas Kooliyankal**, Chief Information Security Officer, *Abu Dhabi Securities Exchange*

These experts will speak on ***key topics*** including:

- Protection of Middle East's critical infrastructure including Government data, Oil & Gas Sector and Finance & Banking industry

- The need for international cooperation in cyber defence

- Staying ahead of the game – early detection and timely response

- Security and cloud migration challenges for the public sector

- Digital forensics and Cyber security

For more details on participation, kindly contact: Ali Rana, Email:register@cyberdefencesummit.com | Tel: +97143671376

ClubHACK

Angry Malware

Design: @pankit_thakkar

Issue 20 | Sep 2011

www.clubhack.com