Malware

What is Malware?

Kinds of Malware

- Virus / Worm: spread infection to additional computers
- Rootkit: hide the existence of malware
- Spyware: collect information and send it to the attacker
  - Keyloggers, password hash grabbers, screen scrapers, use the webcam
- Backdoor: provide the attacker with access to the computer
- Botnet: infected computers communicate and coordinate actions
- {ad,scare,ransom,dox}ware: extract money from the victim

Andromeda bot webpanel - Opera

Menu
- Bots
- Black list
- Tasks
- Service

Plugins
- Formgrabber
- Socks4

General statistic

Total:	16
Online:	5
Online per hour:	5
Online per day:	16
Online per week:	16
New bots at last day:	16
Dead bots:	0

Statistics by system

Win7	12.5% (2)
WinVista	25% (4)
WinXP	62.5% (10)

x86/x64 statistic

x86	100% (16)

Statistics by Build ID

21032012	100% (16)

Statistics by country

Canada	6.3% (1)
France	12.5% (2)
Germany	6.3% (1)
Italy	25% (4)
Latvia	6.3% (1)
Poland	6.3% (1)
Portugal	6.3% (1)
Senegal	6.3% (1)
Spain	25% (4)

Filter

Status: ☐ Online
NAT: ☐ Only real IP's
Records limit: 30
Sort by: Last response
Apply

Search

Bot ID:
IP address:
Search

Select all | Unselect all | Add task for selected | Ban selected | Delete selected

Bot ID	Build ID	IP address	Country	Install date	Last response	Task	Bot ver.	OS version	Status
2446DBDA	21032012	[redacted] (NAT)	(IT)	23:37:10 19 Apr	14:12:53 20 Apr	#0	02.05	WinVista x86 (U)	Online
28E3854F	21032012	[redacted]39 (NAT)	(PL)	22:13:27 19 Apr	14:10:45 20 Apr	#0	02.05	WinVista x86 (U)	Online
BCE872D3	21032012	[redacted]220 (NAT)	(ES)	16:23:11 19 Apr	14:08:35 20 Apr	#0	02.05	WinXP x86 (A)	Online
8C0F331C	21032012	[redacted]164 (NAT)	(FR)	16:22:24 19 Apr	14:08:05 20 Apr	#0	02.05	WinXP x86 (A)	Online
5A003357	21032012	[redacted]78 (NAT)	(ES)	16:22:22 19 Apr	14:07:55 20 Apr	#0	02.05	WinVista x86 (U)	Online
6C01D618	21032012	[redacted]52 (NAT)	(CA)	21:38:15 19 Apr	09:21:17 20 Apr	#0	02.05	WinXP x86 (A)	Offline
0CFC241C	21032012	[redacted]4 (NAT)	(IT)	18:51:48 19 Apr	08:25:03 20 Apr	#0	02.05	WinXP x86 (A)	Offline
18FCF3B4	21032012	[redacted]50 (NAT)	(ES)	16:26:15 19 Apr	07:52:04 20 Apr	#0	02.05	WinXP x86 (A)	Offline
845758B7	21032012	[redacted]7 (NAT)	(FR)	07:18:23 20 Apr	07:45:26 20 Apr	#0	02.05	WinXP x86 (A)	Offline
EA48FED1	21032012	[redacted]1 (NAT)	(ES)	17:33:45 19 Apr	07:04:14 20 Apr	#0	02.05	Win7 x86 (A)	Offline
BC1C5B2E	21032012	[redacted]3 (NAT)	(SN)	05:09:58 20 Apr	06:30:56 20 Apr	#0	02.05	WinXP x86 (A)	Offline
6CC1B786	21032012	[redacted] (NAT)	(IT)	16:21:03 19 Apr	06:06:44 20 Apr	#0	02.05	WinXP x86 (A)	Offline
38326154	21032012	[redacted] (NAT)	(PT)	04:51:35 20 Apr	05:37:06 20 Apr	#0	02.05	WinXP x86 (A)	Offline
20EB4AB3	21032012	[redacted]186	(LV)	04:44:47 20 Apr	05:20:50 20 Apr	#0	02.05	WinXP x86 (A)	Offline
26136A15	21032012	[redacted] (NAT)	(IT)	01:17:14 20 Apr	05:20:25 20 Apr	#0	02.05	Win7 x86 (U)	Offline
64B2ACC1	21032012	[redacted] (NAT)	(DE)	20:41:50 19 Apr	02:15:09 20 Apr	#0	02.05	WinVista x86 (U)	Offline

Andromeda bot webpanel v06 (c) 2012
Generation time 0.0119 sec.


iPhone - Wikipedia, the fr
en.wikipedia.org/wiki/IPhone
Create account
Log in
Article
Talk
Read
View source
View history
Search
WIKIPEDIA
The Free Encyclopedia
Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page
Toolbox
iPhone
From Wikipedia, the free encyclopedia
Looking For free encyclopedi...
Find What You Need. Look For free encyclopedia Here Now
MonsterMarketplace.com
click here
The user interface is built around the device's multi-touch screen, including a virtual keyboard. The iPhone has Wi-Fi and cellular connectivity (2G, 3G, 4G, and LTE). An iPhone can shoot video (though this was
The 5S (left) and 5C (right) to scale.

Personal Antivirus

Our best-solution software has been already registered by 876,130 US citizens

DANGER! Your PC is threatened by 1 potentially severe trojans and worms!

Viruses are programmed to damage the computer by damaging programs, deleting files, or reformatting the hard disk. As a result, they cause erratic behavior and can result in system crashes. In addition, many viruses are bug-ridden, and these bugs lead to system crashes and data loss.

Optimize and protect your system with advanced antivirus technology.

Before you register this program, please read the following carefully:

This is a one-time charge. Your credit card will never be rebilled and you will receive UPGRADES FOR FREE! Registration is immediate, and once registered, Personal Antivirus will remove all viruses, spyware, adware and other security risks and block them from accessing your system.

YOU CAN ALSO MAKE YOUR PC UP-TO-DATE!

Register now
for only
$ 59.95
You save $ 33.30
Click Here!

You have an exclusive **40% discount**, since US citizens are our most frequent buyers.

VISA MasterCard

Malware “steps”

1. **Infect** the user’s computer (drive-by-download, trojan, email attachment)
2. Perform some **malicious operation** (steal/encrypted data, install a rootkit, etc)
3. **Persist** within the system (file, autorun, registry, powershell scripts, etc)
4. **Spread** to other systems (local network, via email clients, etc)

Ransomware

Malware authors realized they can extract money directly from users by removing access to their data

1. Encrypt all user .doc/.pdf/.png/.jpg/etc files with a generated public key
2. Force users to pay you in bitcoin
3. Decrypt their files with their private key

Security is ensured by crypto (if properly implemented)

Your files are encrypted.

To get the key to decrypt files you have to pay **750 USD/EUR**. If payment is not made before the cost of decrypting files will increase **2** times and will be **1500 USD/EUR**

Prior to increasing the amount left:

42h 48m 35s

Your system: Windows 7 (x64) First connect IP: Total encrypted files.

Refresh | **Payment** | FAQ | **Decrypt 1 file for FREE** | Support

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

bitcoin

1. **You should register Bitcon wallet (click here for more information with pictures)**
2. **Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.**

Here are our recommendations:

Warning Message!!

We are sorry to say that your computer and **your files have been encrypted**,
but wait, don't worry. There is a way that you can restore your computer and all of your files

0 years, 6 days, 00 hours, 45 min and 58 sec

Time remain when your files will lost forever!

Your personal unique ID: **0e72bfe849c71dec4a867fe60c78ffa5**

Please send at least **1.0 Bitcoin** to address **1LEiPgvh6S9VEXWV2dZTytSRd7e9B1bWt3**

Click to check your Balance

Restoring your files - The fast and easy way

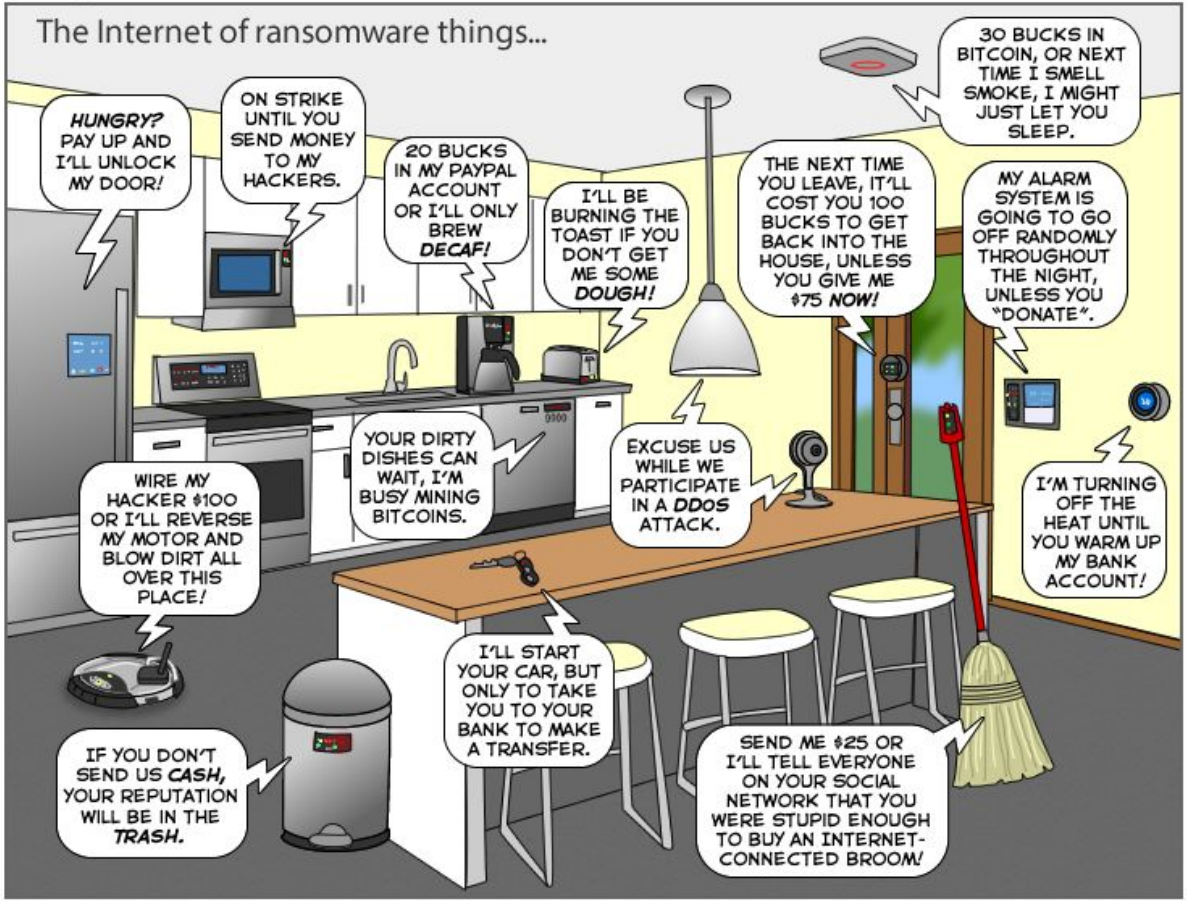
To get your files fast, please transfer **1.0 Bitcoin** to our wallet address **1LEiPgvh6S9VEXWV2dZTytSRd7e9B1bWt3**. When we will get the money, we will immediately give you your private decryption key. Payment should be confirmed in about 2 hours after payment made.

Restoring your files - The nasty way

Send the link below to other people, if two or more people will install this file and pay, we will decrypt your files for free.

https://3hnuhydu4pd247qb.onion.to/r/0e72bfe849c71dec4a867fe60c78ffa5

The Joy of Tech™ by Nitrozac & Snaggy



You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech

joyoftech.com

Defending against malware

- Antivirus
- Dynamic Analysis

Signatures

- File has been identified by at least one AntiVirus on VirusTotal as malicious
- Tries to unhook Windows functions monitored by Cuckoo
- Executed a process and injected code into it, probably while unpacking
- Installs itself for autorun at Windows startup

Windows PowerShell

```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\> get-childitem C:\CD-DVD\w*iso | get-filehash

Path                                    MD5 Hash
----                                    --------
C:\CD-DVD\W2KSvrStd_x86.iso             9DDD017E995E66263109DA9A924AE789
C:\CD-DVD\Win7Pro_x64.iso               7B7AF5FE3A01E9FD76DE4DACB45A796B
C:\CD-DVD\Win7Pro_x86.iso               7D7F567E5684C8FC7C5C81EC0D9A42DB
C:\CD-DVD\WS03R2Std_x86_CD1.iso         69F8E0C297C1814582838A379909366A
C:\CD-DVD\WS03R2Std_x86_CD2.iso         75B3D8877F2993152C9A4B6A73815179
C:\CD-DVD\WS03_Std_x64.iso              D688D6AC0986A32D45B26E437A4259D2
C:\CD-DVD\WS08R2StdEnt_x64.iso          0207EF392C60EFDDA92071B0559CA0F9


PS C:\> _
```

```
[cberman@MS-DOS ~]$ sha256sum
hello there.
d874711a0f5b480f86181c76d969e0193e67c950be5dcf311d66ea1d4031ac8b  -
[cberman@MS-DOS ~]$ sha256sum
hello there!
be3825966f46b982841ba286a10c0974427e7b3f6dc2fa20205ff59ecb3b43c0  -
```

```
[cberman@MS-DOS ~/cns/malware]$ strings malware | grep "^<.*>\( \|$\)"
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
<security>
<requestedPrivileges>
<requestedExecutionLevel level="requireAdministrator"/>
</requestedPrivileges>
</security>
</trustInfo>
</assembly>
```

YARA

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        threat_level = 3
        in_the_wild = true
    strings:
        $a = “<requestedExecutionLevel level="requireAdministrator"/>”
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"
    condition:
        $a or $b or $c
}
```

Traditional Antivirus

Scan executable files on disk, in memory, downloads, etc for **signatures**, which are (ostensibly) unique identifiers for a piece of malware

When detected, attempt to either **defuse** the malware or **quarantine** it

If a fix is known, try to fix the system by reverting changes the malware is known to make

AV sucks

Any antivirus is basically a **blacklist** composed of executable signatures

We can have **false positives** if a program unintentionally matches a signature

To bypass an antivirus, all you have to do is change the bytes identified by the signature (add a nop somewhere?)

A blacklist fundamentally cannot be the solution when malware can be **generated programmatically**

Few protections against **unidentified threats** -- signatures cannot match something that the AV company has not encountered

Dynamic Analysis

Analyze executable operations at runtime to determine risk of being malicious

Usually performed in a VM so everything can be instrumented

Check for malicious URLs, files accessed, suspicious behavior, etc

https://malwr.com/analysis/YjI2OWE3Yzc1Y2Q0NDNhN2I5MTc1ZTY1MDZiMmVkZWY/

Network Analysis

http://malware-traffic-analysis.net/2016/10/12/index.html

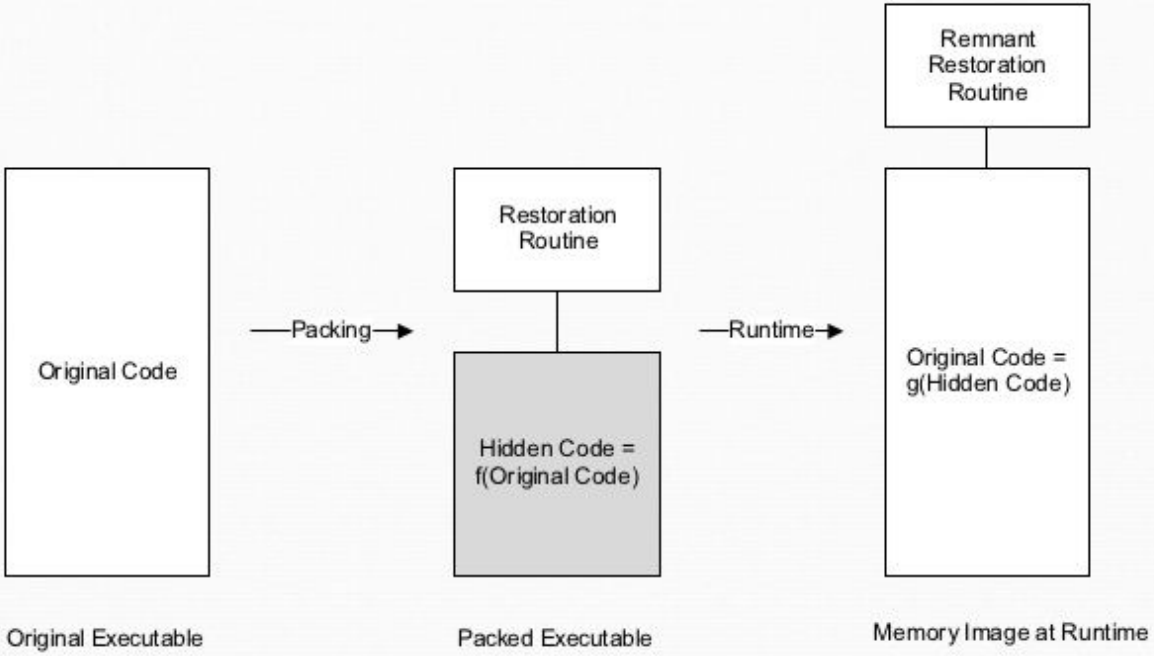
```
alert tcp any any -> 192.168.1.35 any (msg:"Traffic to 192.168.1.35";)

alert tcp any any -> any any (msg:"Possible  exploit"; content:"|90|";)
```

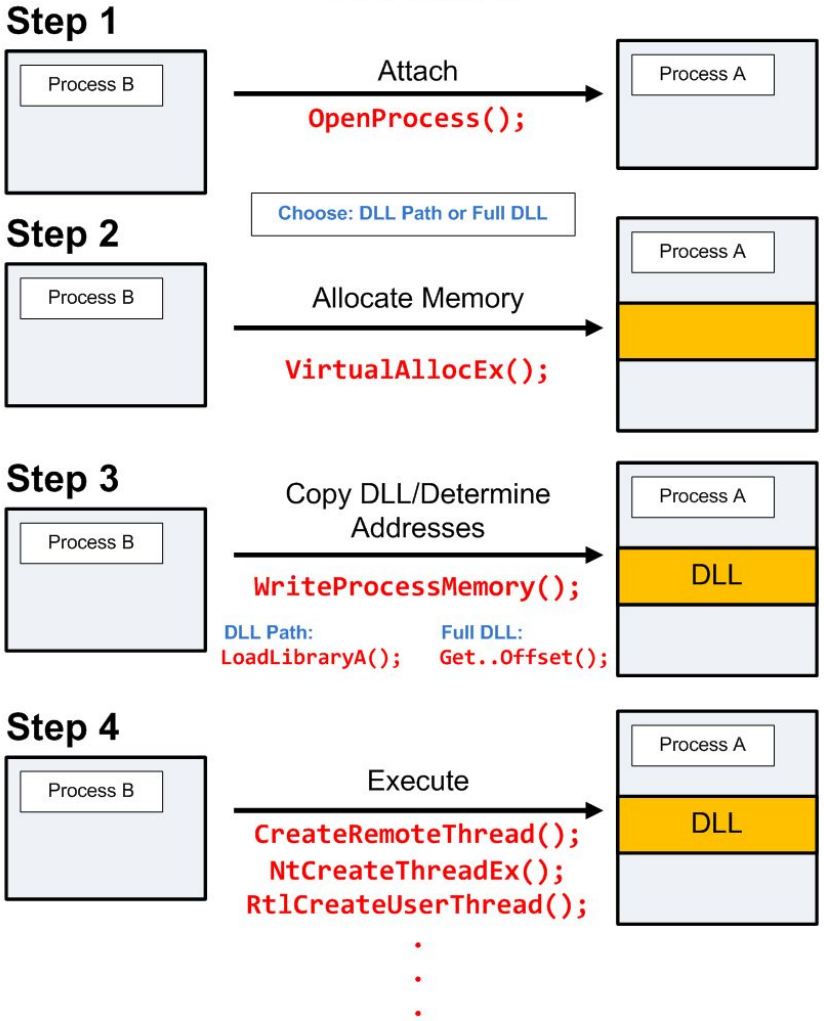
Malware evasion techniques

- Packing
- DLL injection
- System profiling (checking for programs, etc)
- VM detection & escapes
- Polymorphism

Traditional Malware Packing



Overview


Step 1
Process B
Attach
OpenProcess();
Process A
Choose: DLL Path or Full DLL
Step 2
Process B
Allocate Memory
VirtualAllocEx();
Process A
Step 3
Process B
Copy DLL/Determine Addresses
WriteProcessMemory();
DLL Path:
LoadLibraryA();
Full DLL:
Get..Offset();
Process A
DLL
Step 4
Process B
Execute
CreateRemoteThread();
NtCreateThreadEx();
RtlCreateUserThread();
Process A
DLL

System profiling

Malware attempts to identify AV/analyst systems by looking for certain indicators

Presence of reversing tools (IDA), debuggers (WinDBG, Olly), VM software, etc can cause malware to not trigger to avoid dynamic analysis

Malware aimed at specific targets may require certain system details to trigger

ex: Stuxnet/Flame malware checked all files on the system against a given MD5 hash to identify the target system

VM Detection and escaping

Malware often checks for common **artifacts** on a system to detect whether they are running in a VM

Common artifacts include fingerprinting VM hardware, looking for specific files/registry keys, timings of certain operations, unimplemented API calls, etc

Malware can also leverage exploits to escape from a VM and infect the host system

Polymorphism

To avoid detection by signatures, malware will randomly permute its code each time it spreads itself

Malware can change which registers it uses, add dummy operations or nops, rearrange functions in memory, add layers of encryption, etc

```
mov eax, 3
mov ebx, 3
add eax, ebx
```

```
mov eax, 3
nop
mov ebx, 3
nop
add eax, ebx
```

```
mov edx, 9
mov ecx, 3
sub edx, ecx
```

The APT: Advanced Persistent Threats

- What if nation states created malware?
- High level of sophistication
  - Covert communications across air gaps
  - Liberal usage of zero-day exploits
  - Encrypt all the things
- Maintain long-term access
  - “APT1 maintained access to victim networks for an average of 356 days. The longest time period APT1 maintained access to a victim’s network was four years and ten months.” (https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf)

Homework

- You're given some (defused) ransomware and an file that has been encrypted by it
  - https://github.com/cnsatuva/modernsectopics/blob/master/4-6/ransomware.py
- Try to decrypt the file to recover the contents
- Send an email with the recovered data (and a 1-paragraph writeup) to cm7bv@virginia.edu with the subject "MST Assignment 10 - <YOUR_UVA_ID>"
- Tips
  - What *exactly* does the ransomware do?
  - Where does the encryption key come from?
- **Don't hesitate to ask questions**

GitHub repository

- Note: our GitHub page for the class has moved to:

  https://github.com/cnsatuva/modernsectopics

Additional Resources

- A source for pcap files and malware samples, traffic analysis exercises (http://malware-traffic-analysis.net)