

## Вируси, црви и тројански коњи (вовед) Кадриу Арбен

### 1. Феноменот наречен компјутерски вирус

Дваесетиот век е несомнено еден од пресвртните точки на човековото постоење. Луѓето се фасцинирани од машините. Многу луѓе веќе заборавиле што е тоа конвенционална пошта, електронската пошта го зазема нејзиното место со своите предности - доставување на пораките со огромни брзини (најмногу неколку минути) било каде во светот. Современото општество не може да се замисли без компјутери кои овозможуваат повеќекратно зголемување на ефективноста на трудот и добивање огромно количество на информации. Што се однесува до компјутерите при крајот на векот се појавува уште еден феномен - компјутерските вируси.

Првите обиди за истражување на мултилицирачки вештачки ентитети биле направени во средината на овој век. Von Neumann, Wiener и други автори дале дефиниција и математички ги анализирале конечните машини, вклучувајќи ги самомултилицирачките. Терминот “компјутерски вирус” станува познат подоцна - сега официален, најпрво бил користен од F.Cohen (USA), во 1984 год. на седмата конференција за компјутерска безбедност, одржана во САД.

Главна тешкотија за да се даде прецизна дефиниција за терминот компјутерски вирус е што, виртуелно, сите карактеристики на вирусите (инкорпорирање во други објекти, прикривање, потенцијални опасности итн.), можат да се најдат и кај други програми што не се вируси, но постојат и вируси што ги немаат овие карактеристики (освен да се распространуваат). Ако на пр. се земе како определувачка карактеристика на вирусите нивната способност за прикривање, тогаш лесно може да се даде пример што би го негирал ова. Така, може да постои вирус кој пред да инфицира некоја дадотека, испишува соодветен коментар на екранот. Ако се земе способноста за деструктивно однесување на вирусите во однос на програмите и податоците на дискот како одлучувачка карактеристика, тогаш може да се наведат огромен број на вируси што ги немаат тоа свойство, туку едноставно си поигруваат со графиката и звукот на компјутерот. Исто така главната карактеристика на вирусите, да се инкорпорираат во различни објекти од оперативниот систем - може да се најдат и кај многу конвенционални програми што не се вируси.

Првата причина што оневозможува да се даде прецизна дефиниција за компјутерските вируси е неможноста да се набројат сите карактеристики што би ги имале вирусите и само тие.

Втората причина произлегува од фактот дека дефиницијата треба да е специфична за секој оперативен систем. Теориски, може да постојат оперативни системи во кои вирусите не можат да постојат. Тоа можат да бидат такви системи кои ќе забрануваат менување на извршните кодови.

Поради тоа, може да се наведат само неопходни услови за да некоја секвенца извршен код се смета за вирус.

НЕОХОДЕН УСЛОВ ЗА ДА НЕКОЈ ИЗВРШЕН КОД СЕ СМЕТА ЗА ВИРУС е способноста да произведе копи од самиот себе си, ид а ги инкорпорира во компјутерските мрежи, датотеките, системските подрачја на компјутерот, ив о други извршни објекти. Копиите исто така да имаат способност за понатамошно распространување.

### **1.1. Што е компјутерски вирус?**

Компјутерскиот вирус е програма која бара домаќин (копјутер) за да може да направи копии на самата таа програма во дисковите на компјутерот. Вирусот може да зарази програмски датотеки (да се копира и да се прошири), програми во секторите на дискот. Можноста тие самите да се множат ги дели вирусите од програмите кои не се вируси и оваа паразитска природа на вирусите не случајна ниту некоја компјутерска грешка. Сите вируси се направени од луѓе кои знаат да напишат компјутерски програми. Вирусот се активира секогаш кога компјутерот ќе изведе инфективна програма односно програма што содржи вирус. Додека е во меморијата тој може да предизвика голема штета како што е реплицирање преку компјутерот, а ако компјутерот е приклучен на компјутерска мрежа тогаш може да ги инфицира сите компјутери што се во мрежа.

#### **1.1.1. Зошто се наречени вируси?**

Првите теории за можноста на креирање на програма која сама се множи датираат назад во 1949, и првите експериментални вируси биле направени и тестирали во 1960. Тие го добија своето име кога универзитетски професор ги нарече “вируси” во 1984, бидејќи како биолошкиот вирус истотака и компјутерскиот е мал, прави копии од себеси, и не може да постои без домаќин. Кога персоналните компјутери станаа популарни почнаа да се појавуваат PC вирусите (во 1986-1987) кои како прво беа наменети како шега или беа направени за истражување или за демонстрирање.

### **1.2. Што е компјутерски црв?**

Со порастот на популярноста на Интранетот и Интернетот, e-mail-от еволвира од улужност во потребност. Тоа го знаат програмерите на вирусите и тие направија нов начин како преку e-mail да ги пренесат нивните вируси и црви. Црв-програмата е многу слична на вирусот дури од некои се мисли дека е подгрупа од вирусот бидејќи ја има истата функција на правење копии од себе од еден до друг компјутер преку мрежа (пр. преку e-mail) но тоа го прави без да направи измени кај домаќинот.

### **1.3. Што е тројански коњ?**

Овие програми се именети според легендата на големиот дрвен коњ во кого беа скриени грчките војници кои го употребија да за да ја нападнат Троја. Исто како познатиот трик што е употребен на легендата така и оваа програма содржи во себе скриен програмски код. Скриената функција може да биде само шега, но многу често ги употребуваат тројаните за да уништат податоци знаејќи дека некои луѓе ќе отворат било каква датотека која содржи интересно име или вика дека прави некоја корисна функција.

#### **1.4. Дали сите овие програми се штетни?**

Тие трошат меморија во дискот, ги успоруваат операциите на компјутерот, и ја зголемуваат веројатноста на паѓање на системот. Тие се многу често напишани лошо и се однесуваат на погрешен начин, бришат податоци и ги тераат другите програми да се однесуваат на недозволен начин. Многу од нив имаат деструктивни рутини кои променуваат податоци или ги бришат.

#### **1.5. Кој ги прави овие програми и зошто?**

Пишувачи на вируси се од истражувачи до шегации па до криминални вандали. Типичниот пишувач на вируси е интелигентен човек, помеѓу 15 и 23 години. Тој можеби тоа го прави од досада или од интерес или со намера да направи недозволени работи само да ги заплаши другите. Некои вируси припаѓаат на групи кои работат заедно и тие групи најчесто реагираат од притисок, трудејќи се да ги надминат другите. Без разлика дали се во група или не, некои добиваат сatisфакција од предизвикот, додека други се мислат себеси како бунтовници против “системот”.

#### **1.6. Како се шират овие програми?**

Вирусите и Тројаните се шират од еден компјутер во друг употребувајќи една или повеќе методи, од кои сите зависат од недоволната грижа на корисникот. Некои луѓе никогаш немаат проблем, но некои кои не се толку претпазливи (или среќни) го заразуваат својот диск со симнување на датотеки, или со помош на снимање од заразена дискета или било каков вид на пренослив диск. Вирусите и Црвите најбрзо се шират во LAN межите особено кога се работи за е-майл-ови кои имаат закачени датотеки на нив.

### **2. Класификација на компјутерските вируси**

Вирусите може да се поделат во класи според следниве карактеристики:

- околина
- оперативен систем
- различни алгоритми на функционирање
- деструктивни способности

Според ОКОЛИНАТА вирусите се делат на:

- датотечни вируси (file)
- бут вируси (boot)
- макро вируси (macro)
- мрежни вируси (network)

Датотечните вируси ги инфицираат извршните датотеки на разни начини (паразитски-најчести вируси) или креират копија на датотеката (компањон вируси) или користат некои специфични карактеристика на датотечниот систем (линк вирус).

Бут вирусите се сместуваат во бут секторот (почетниот сектор) на дискот или во т.н. Master Boot Record или го менуваат покажувачот на активниот бут сектор.

Макро вирусите ги инфицираат датотеките на познати софтверски пакети (документи,табели,бази на податоци).

Мрежните вируси користат протоколи и команди на мрежата или системот на електронската пошта да се прошируваат и во други системи.

Постојат и разни комбинирани вируси, на пример датотечни-бут вируси кои инфицираат и датотеки и бут секторот на дискот или мрежни-макро вируси, кои не само што ги напаѓаат документите туку и се шират сами преку мрежата.

Според ОПЕРАТИВНИОТ СИСТЕМ во кој дејствуваат, компјутерските вируси исто така можат да се поделат на повеќе класи. Секој датотечен или мрежен вирус инфицира датотеки на еден или повеќе оперативни системи - DOS, Win95/98/ME, Win2000, OS/2 итн. Макро вирусите инфицираат датотеки од Word, Excel т.е. Office2000. Бут вирусите се исто така ориентирани на различни формати - секој од нив напаѓа еден специфичен формат или системски податоци во бут секторите на дисковите.

Според АЛГОРИТМИТЕ НА ФУНКЦИОНИРАЊЕ ги има следниве класи:

- TSR карактерисика
- Користење на Stealth алгоритми
- Самоенкриптирање и полиморфни карактеристики
- Користење на нестандардни техники

TSR вирусите додека го инфицираат компјутерот оставаат еден свој дел резидентен во RAM, кој потоа ги попречува системските повици до целните објекти и се инкорпорира во нив. Резидентните вируси остануваат во меморијата и се активни до исклучувањето на компјутерот или до неговото ресетирање. Нерезидентните оставаат свој мал дел резидентен во RAM, но не се шират, па се сметаат за нерезидентни. *Макро вирусите се резидентни, бидејќи осигнуваат во меморијата за цело време додека работи инфицираната единица програма. Овде единицата игра улога на "оперативен систем".*

Stealth алгоритмите овозможуваат целосно или делумно покривање на прагите од вирусот во оперативниот систем. Најчест ваков алгоритам е попречување на системските повици за читање и запишување во инфицираните објекти. Кај макро вирусите најпопуларна техника на криење е оневозможување на менито ViewMacro. Еден од првите вируси е "Frodo", а вирусот "Brain" е прв бут вирус.

Нестандардни техники има многу и се користат за криење на вирусот што подлабоко во јадрото (кернелот) на оперативниот систем, заштита на резидентните копии од детектирање, отежнувањето на нивното чистење итн.

Според ДЕСТРУКТИВНИТЕ СПОСОБНОСТИ вирусите се делат на:

- не штетни, што немаат ефект во процесирањето (освен што пропагираат намалување на слободниот процесор на дискот);

- безопасни, со ограничени ефекти како намалување на слободниот процтор на дискот или некои графички, звучни или други ефекти;
- многу опасни вируси чии алгоритми на дејствување водат до губење или оштетување на податоците, бришење на витални информации од системските подрачја, и дури оштетување на некои подвижни механички делови со предизвикување резонанса во некои видови хард дискови.

Често може да се случи на изглед да нема штетни дејствија, но со сигурност тоа не може да се тврди бидејќи самото инфильтрирање на вирусот во компјутерот може да биде со непредвидливи последици. Имено како и секоја друга програма.

### **3. Историја на компјутерските вируси - Хронологија на настаниата**

Постојат различни мислења околу датата на раѓањето на првиот компјутерски вирус. Посната е дека немало вируси во машината Babbage, но компјутерите Univac 1108 и IBM 360/370 беќе ги имаа (“Pervading”, “Animal” и “Christmas tree”). Поради тоа може да се каже дека првиот вирус се родил во раните 70-ти или дури и при крајот на 60-тите, иако никој тогаш тие програми не ги менувал како вируси.

Првиот “невидлив” (Stealth) вирус бил Frodo.4096. Од оваа класа вируси подоцна се појавуваат Beast.512 и Dir II. Првиот полиморфен вирус бил наречен Chameleon и се појавува во раните 90-ти, но проблемот со полиморфните вируси станува сериозен само година подоцна, во април 1991 со глобалната епидемија на полиморфниот вирус Tequila. Понатамошниот развој на вирусите оди во насока на усвршување на полиморфниот механизам.

#### *Доцниот 1960-ти - раниот 1970-ти*

Првиот инцидент кој може да се нарече епидемија на компјутерски вирус се случил на Uniax 1108 систем. Вирусот наречен “Pervading Animal” се поставувал себе син а извршните датотеки - виртуелно правел нешто што го прават и денешните вируси.

#### *Доцниот 1970-ти - раниот 1980-ти*

Бил креиран вирусот The Creeper под оперативниот систем Tenex, кој ги искористил глобалните компјутерски мрежи за да се прошири. Вирусот бил способен да навлезе во мрежата преку модем ид а префрли своја копија на оддалечен систем. За борба против овој вирус била креирана антивирусна програма The Ripper, прва позната антивирусна програма.

#### *1980-ти години*

Комјутерите стануваат се популарни. Се појавуваат многу програми пишувани не само од софтверски куки, но и од приватни лица. Како резултат на тоа се појавуваат многубројни програми што прават некакви штети на компјутерските системи, познати како Trojan Horses (тројани).

Започнува пандемија на првиот IBM PC вирус наречен Brain. Тој ги инфицира 360 KB дискети кој бил креиран во Пакистан.

Во Петок 13-ти 1988 год. некои компании и универзитети во многу земји биле зафатени со вирусот Jerusalem. На тој ден вирусот ги уништувал сите датотеки кои се стартувале, предизвикувајќи вистинска пандемија.

Во Ноември истата година, тотална епидемија на мрежниот вирус Morris (Internet Worm – црв). Овој вирус инфицирал повеќе од 6000 компјутерски системи во САД (вклучувајќи ја и НАСА). Поради некој грешен код што го содржи, овој вирус испраша не ограничен број свои копи на другите компјутери во мрежата со тоа практично ја парализира. Овој вирус предизвикал штета од 96 милиони долари. Вирусот ги користел пропустите во оперативниот систем Unix за Vax и Sun Microsystems за да се шири, но ги користел и корисничките лозинки.

*1990-тие години* Оваа година е значајна по неколку настани:

- Појавата на полиморфните вируси - прв претставник вирусот Chameleon
- Појавата на бугарската “фабрика за производство на вируси”: голем број нови вируси се креирани во Бугарија. Примери за тоа се цели фамилии вируси: Murphy, Nomenclatura, Beast итн.
- Проблемот на CD вирусите добива на значење. Брзо стекнувајќи популарност, CD дисковите стануваат значаен фактор во ширењето на компјутерските вируси.
- Linux.Blis вирус за Linux (клон на Unix).
- - Homer – прв мрежен вирус, прв кој го користи FTP(File Transfer Protocol) за сопствено проширување
- Се појавува нов вид на вируси “mIRC Worms” или mIRC црви. Се покажува дека најраспространетата Windows програма за IRC, mIRC е ”дупка” преку која слободно може да навлегуваат вирус скрипти ид а се пренесуваат преку IRC каналите.
- Се појавуваат многу нови вируси со покомплексни карактеристики, посебно вируси со напредни методи за навлегување во компјутер преку мрежа. Покрај т.н. тројани кои ги крадат лозинките за пристап на Интернет, се појавуваат и многу алатки за скриено управување со компјутер.

#### Top 12 Viruses For December 2002

1. Worm/Klez.E (incl. G variant)	40.1%
2. W32/Yaha.E	14.7%
3. Worm/BugBear	8.6%
4. W32/Elkern.C	7.4%
5. Worm/W32.Sircam	6.8%
6. W32/Magistr.B	2.9%
7. W32/Nimda	2.3%
8. W32/Funlove	1.6%
9. W95/Hybris	1.1%
10. W32/Yaha.M	0.9%
11. Worm/Bride.C	0.8%
12. W95/CIH	0.6%
Others	12.2%

## **4. Детекција и отстранување**

Еден од најдобрите методи за борба против вирусите е навремено преземање на превентивни мерки, што подразбира следење на некои правила што значително ја намалуваат можноста за вирусна инфекција и губење на податоците. Како прво треба да се разгледат можните начини за навлегување на вирусите во компјутерот и компјутерските мрежи.

### **4.1. Од каде доаѓаат компјутерските вируси?**

*Глобални мрежи и електронска пошта* - Денес, еден од примарните извори за инфекција со компјутерски вирус е Интернет. Најмногу случаи на инфекција се појавуваат при размената на пораки во Word формат.

*E-mail конференции, датотечни сервери (FTP)* - Датотечните сервери со општпристап и e-mail конференциите се исто така еден од главните извори за ширење на вирусите.

*Локални мрежи* - Друг начин за брза инфекција е преку локалните мрежи. Ако не се пресемени безбедносни мерки, инфицираната работна станица по логирањето на мрежата инфицира една или повеќе системски датотеки на мрежниот сервер.

*Пиратски софтвер* - Илегалните копи на различен софтвер остануваат најголема опасна зона. Честопати ваков софтвер на дискети или компакт дискови содржи многу видови вируси.

## **5. Антивирусни Програми**

Антивирусните програми се најефикасниот начин за борба против вирусите, но не постојат антивирусни програми програми што гарантираат 100% заштита од вируси. Ова е и математички докажано со помош на теоријата на конечните машини. Затоа секогаш треба да се има последната верзија на некоја антивирусна програма. Иако не постои 100% заштита од компјутерските вируси, пожелно е да се има во секое време резидентна антивирусна програма.