Počítačové vírusy (Úvod do infológie)

František Gyárfáš, 29.6.1999,inZine • Publicistika • Mysty

hodnotenie článku 91/20

Nasledujúci text je (na môj veľký žiaľ) mystifikácia. Väčšina faktov je ale pravdivých a ilúziu z nich robí ich usporiadanie. Stačí akceptovať jemný posuv od možného k pravdepodobnému a ocitnete sa v podivnom svete, v ktorom stretnúť stepného vlka je menej prekvapujúce ako zistenie, že ho už dávno dôverne poznáte.

Keď pominie šok z poslednej európskej vojny tohoto storočia a Kosovo sa zaradí do dejín hanebností sociálneho inžinierstva, objaví sa v pravom svetle jar 1999 ako Zrodenie vírusov. Počítačových vírusov, aby som upokojil obdivovateľov AIDS či ovčích kiahní. Hrdinovia budúcich mytológií sa volajú Melissa, ktorá na niekoľko dní paralyzovala počítačovú poštu USA, Černobyľ, ktorý vážne poškodil státisíce počítačov v Európe a Ázii, ExploreZip, ktorý vo vašom mene rozposiela pozdravy vašim priateľom, a potom im vandalsky poničí súbory či francúzsky vírus PrettyPark, ktorý otvára počítače a púšťa do nich lupičov. A to je len vrcholec ľadovca chronológie vírusov tejto jari.

Počítačové vírusy sú spoločný názov pre programy, ktoré napádajú, znefunkčňujú alebo rovno ničia iné programy či dáta. Vírusmi sa nazývajú kvôli nápadnej podobnosti svojich vlastností a aktivít s biologickými vírusmi.

Počítačové vírusy sú zmaterializovaným snom intelektuála násilníka. Ich činnosť je vysoko deštruktívna, ale nevyžaduje si fyzický kontakt a netečie pri tom krv. Prostredie, ktorým sa epidémia počítačového vírusu prehnala, pripomína krajinu po bitke: v hmlách skapíňajúceho operačného systému sa potulujú poškodené programy vypisujúce nezmyselné chybné hlásenia; mrchožrúti vykrádajú zomierajúce súbory a všade sa šíri hniloba, choroby a smrť. Ako Dánsko na konci piateho dejstva. Všetci čakajú Fortinbrasa, aby zavelil: "To chce reset celého systému!".

Vírusy nie sú objavom tejto sezóny. Existujú už viac než desaťročie a dnes registrujeme stovky druhov. Vírus je zvyčajne kus počítačového kódu, ktorý nevie existovať samostatne, ale keď sa pripojí k nejakému programu, ktorý ho živí, prenáša, kŕmi a zobúdza, dokáže sa rozmnožovať a následne po istej inkubačnej dobe udrieť. Podobnosť so správaním sa ozajstných vírusov je taká nápadná, že sa nedá vylúčiť ani predstava spoločného tvorcu. Pre menej radikálnych mysliteľov ponúkam vznik nápodobou.

Vírusy v tejto klasickej podobe dnes predstavujú len jednu čeľaď počítačových parazitov. Aj ďalšie sú realizácie ľudských metafor: trójske kone, ktoré sa trikom dostávajú do pevností lokálnych počítačových sietí a potom do nich vpúšťajú svojich známych votrelcov; žížaly, ktoré sa lenivo rozvaľujú a obžierajú listy stromov súborov atď. A tiež najrôznejšie kombinácie predošlých.

Vírusy majú svoje povahy, temperamenty a poslania. Sú vírusy skromné aj velikášske. Vírusy killeri a vírusy srandisti. Vírusy samovrahovia, ale aj také, čo sa úpenlivo držia pri živote. Psychopati alebo blázni. Sú vírusy revolucionári a vírusy obyčajní násilníci. Sú aj vírusy perverzné, sadistické, morbídne. Iné sú moralistické či vizionárske. Tie bývajú najzhubnejšie a najbezohľadnejšie. Skôr než prírodu pripomínajú ľudí.

Všeobecne sa predpokladá, že počítačové vírusy sú produktom programátorov. V prospech tejto domnienky svedčia prípady, keď sa podarilo autora nejakého vírusu vypátrať či odhaliť. Toto vysvetlenie vyhovuje antropocentrizmu, ktorým sme posledné tisícročia posadnutí. Nášmu úprimnému presvedčeniu, že všetko racionálne a inteligentné pochádza z dielne ľudstva a jeho bohov. A trochu aj z potláčanej obavy, že to tak nemusí byť.

Predstava vírusov ako ľudských produktov napĺňa aj ďalší z odvekých ľudských snov: túžbu po racionálnom vysvetlení nepochopiteľného. Ľudia odvždy milovali paranoidné teórie, tvrdiace, že spoločenské deje majú svojich tajných vládcov. Že ktosi poťahuje za neviditeľné špagátiky, organizuje revolúcie a usmerňuje ich k svojim cieľom. Že nič nie je náhodou a dejinný kolobeh je sprisahaním mocných. Mýty o slobodomurároch či inkvizíciách, zaručené dôkazy o dlhých prstoch KGB, CIA, Mossad sú len variáciami tej istej interpretačnej hry.

S počítačovými vírusmi je to podobné. Je podstatne prijateľnejšie osvojiť si predstavu, že nejaký ukomplexovaný programátor, ktorý sa hanbí ísť na diskotéku a osloviť normálnu babu, si vymyslí program podobný prírode (a našej znalosti toho, ako príroda funguje) a vírus pustí do obehu. Bežná a médiami podporovaná je aj predstava organizovanej skupiny hackerov, crackerov či iných typov počítačových zločincov, teroristov alebo politických idealistov, ktorí si vyrábajú trójske kone či vírusy podobne ako pakľúče: ako pracovné nástroje na páchanie svojej činnosti. Väčšina známych faktov tieto predstavy aj potvrdzuje.

Keď zhruba v rovnakom čase (apríl 1999) prepukli epidémie vírusov Melissa a Černobyľ, antivírusových odborníkov najviac prekvapilo, že oba vírusy boli v tej dobe už známe, dobre preskúmané a boli vybudované rozsiahle ochranné opatrenia proti ich šíreniu. Napriek tomu vírus Melissa tvrdo zasiahol informačnú diaľnicu USA a medzi postihnutými inštitúciami boli aj také giganty, ako sú Pentagon, vláda USA či firma Boeing. (Microsoft, samozrejme, tiež, ale ten nespomínam kvôli ich systematickému zanedbávaniu ochrany). Keďže išlo o zásadnú otázku americkej bezpečnosti, vláda poverila vyšetrovaním špeciálnu odnož FBI pre vyšetrovanie počítačovej kriminality FBI(binary). FBI(b) v spolupráci s antivírusovými firmami McAffe (scan), Symantec (Norton Antivirus) a ThunderBYTE (tbav) zhromaždili okolo desaťtisíc rôznych výskytov oboch vírusov. Sústredili sa najmä na situácie, v ktorých vírusy prekonali rôzne ochrany a analyzovali priebehy jednotlivých napadnutí.

Prvé prekvapenie ich čakalo pri porovnávaní samotného kódu vírusu Melissa. Napriek tomu, že išlo o veľmi jednoduchý vírus, ktorý nerobil nič iné, než že sa odoslal na prvých 50 adries elektronického adresára napadnutého počítača, analýza objavila vyše 2000 rôznych modifikácií kódu vírusu. Niektoré modifikácie sa týkali čisto elegantnosti kódu bez vplyvu na algoritmickú funkčnosť, iné ale reprezentujú úplne odlišné prístupy pri programovaní danej úlohy. Viaceré z kódov boli čiastočne alebo úplne nefunkčné, iné obsahovali nezmyselné, nepochopiteľné časti, akoby prevzaté z iných programov. Celé to vyzeralo ako cvičenie gigantického kurzu programovania, ktorého všetci účastníci dostali zadanie naprogramovať vírus Melissa. Niektorí postupovali presne podľa postupu učiteľa. Iní zvolili neštandardný postup. Ďalší odpisovali. Tretí vytrhli daný algoritmus z podobných ale iných programov. Presne ako v škole. FBI(b) začala okamžite pátranie po podobnom kurze, ale márne. Obrovské množstvo účastníkov (ktorých stále pribúdalo, ako sa zbierali testovacie vzorky) vylučovalo utajenie podobného projektu.

Ďalšie prekvapenie čakalo policajných úradníkov, keď známy odborník na inkrementálne programovanie Jim P. Clark zistil a následne publikoval sekvenciu modifikácií vírusu Melissa

známu pod názvom Clarkov evolučný reťazec. Clark zistil podrobnou analýzou kódu jednej z väčších skupín (obsahujúcich 258 modifikácií vírusu), že ide jednoznačne a dokázateľne o následné verzie programu. (Neskoršie verzie obsahujú modifikovaný kód predchádzajúcich.) Vyzerá to tak, akoby sa niekto hral s programom, skúšal ho a postupne menil. Clark analyzoval funkčnosť následných verzií (problémom ostáva, že sa nenašli naozaj susedné verzie) a publikoval spôsoby jednotlivých modifikácií. Pozoruhodný na Clarkovom zistení ale nie je samotný fakt existencie vývojových postupností, ktoré sú bežnou rutinou každého praktizujúceho programátora, ale techniky vývoja. Clark tvrdí, že sa v celej reťazi 258 verzií nenašiel jediný postup, typický pre prácu programátorov !!!! Naopak. Objavili sa v ňom postupy typické pre automatické evolučné programovanie objavené v projekte Ghod (MIT AI Lab, TR 5738, 1998). Clarkova správa bola elektronicky publikovaná 5. júna 1999 na www.fbi.gov/binary/melissa.html. Tri dni po objavení sa správy zanikla celá stránka www.fbi.gov/binary. Deň predtým som vo svojom počítači vyčistil cache.

Clark nie je tajný agent, ale vedec a jeho práce sú v počítačovej komunite bežne dostupné. Projekt Ghod bol typický projekt výskumu evolučného programovania, čo je jedna z odnoží automatického samovývoja programov. Technicky je to neobyčajne zložité a nudné. Filozofické implikácie sú ale vzrušujúce. O niektorých z nich píše Jozef Kelemen v knihe Postmoderný stroj. V samotnej správe Technical report 5738, AI Lab je pre neodborníkov zaujímavý len Appendix C/4. Pojednáva o experimentálnom spustení evolučného enginu Ghod IV. nad hackerskou knižnicou z www.urbanPirats.ne, ktorá bola celá prenesená na izolovanú počítačovú sieť AI Lab/Space 2. Ghod IV. pracuje na princípe synergizácie cieľov. V rámci kontrolovaného experimentu došlo k zrýchlenej multiparalelnej reťazovej reakcii obsahujúcej cez dva milióny medzikrokov a vzniklo okolo 12 miliárd nových programov. Vzhľadom na pôvodný charakter hackerských programov sa ukázalo, že nové mutácie prejavovali stále agresívnejší charakter. Ten bol čiastočne zameraný dovnútra a isté obdobie sa zdalo, že systém sa sám zahubí. Nestalo sa tak a celý systém si vytvoril dobre fungujúce mechanizmy vnútornej kontroly a potláčania vnútrosystémových konfliktov. Po štyroch týždňoch bol experiment vedením AI Lab zastavený. Stalo sa tak štyri hodiny po tom, čo prestal fungovať kontrolný modul celého experimentu a v ochrannom obale Space 1 (izolovaná počítačová sieť AI Lab, komunikujúca s uzavretou sieťou Space 2) sa objavil trójsky kôň neznámeho pôvodu. Po otvorení Space 2 a štúdiu jeho statického obsahu sa zistilo, že všetky programy sa rozplynuli v binárnom chaose.

Ako poznamenáva Clark v závere spomínanej správy, evolučné programovanie je ešte stále vo veľmi primitívnom ranom štádiu. Najväčší problém tejto vednej odnože je stanovenie cieľov, ktoré by mala evolúcia sledovať. Príliš jednoduché ciele - napr. riešenie matematických problémov - vedú k veľmi krátkym evolučným cyklom. Príliš abstraktné ciele zase spôsobujú nevyváženosť a odumieranie celých systémov. Zdá sa, že najúspešnejšie sa správajú systémy, ktoré nemajú definované vlastné ciele, len žiaduce interakcie s naším (biologickým alebo spoločenským) svetom a preberajú jeho vývojové trajektórie. Clark to nazýva parazitácia (parasitization) evolučných algoritmov. Ako som už povedal: Melissa, Černobyľ, PrettyPark.