CONSIDERAȚII ASUPRA PRINCIPIULUI FUNCȚIONAL AL UNUI ATAC CIBERNETIC LA DISTANȚĂ

Dragoş NICOLAU

dragos@ici.ro

Institutul Național de Cercetare - Dezvoltare în Informatică – ICI Bucureşti

Rezumat: La începutul Erei Internetului, comunicațiile nu prezentau nici un pericol, nici pentru servere, nici pentru utilizatori. Acest lucru se explica, în principiu, datorită faptului că informația era vehiculată într-un singur sens, de la server la utilizator, constituind un flux de tip "doar citire". De mulți ani încoace însă, acest lucru nu se mai întâmplă, pentru că şi-au făcut apariția atacurile informatice. În principiu, acestea constau fie în emiterea unui flux foarte intens de cereri către o maşina server victimă pentru blocarea directă sau indirectă a traficului, fie în injectare de cod malițios în speranța că programul cărora le este destinat (aplicație client infectată de server sau aplicație server) va executa de bună credință, în acest fel furând sau viciind informație[1].Trecerea de la aplicațiile inițiale de tip Internet la cele de tip Web (acele aplicații care permit trimiterea de date de la utilizator la server, spre a fi prelucrate) a deschis noi oportunități pentru cyber-infractori de a trimite cod malițios către partea de server a aplicațiilor . În lucrarea de față se va prezenta principiul de funcționare al unei aplicații care execută atacuri la distanță.

Cuvinte cheie: comunicații prin rețea, atac cibernetic, server, injectare de cod malițios.

Abstract: At the beginning of the Internet Era, communications did not pose any threat either to servers or users. This is mainly explained by the fact that the information was conveyed in one sense, from the server to the user, constituting a "read-only" flow. For many years now, however, this is no longer the case, because computer attacks have emmerged. Basically, these consist either in issuing a very high stream of requests to a victim server machine, or in malicious code injection in the hope that the program to which it is destined (client application infected by server or server application) will execute in good faith, thereby stealing or ruining information. The evolution from the original Internet-type applications to the Web type (those applications that allow the user to send data to the server to be processed) opened new opportunities for cyber-criminals to send malicious code to the server side of applications. In this paper we present the principle of running an application that executes remote attacks.

Keywords: network communications, cyber-attack, server, malicious injection.

1. Introducere

Industria software este domeniul de activitate care are nu doar cea mai mare viteză de evoluție şi de diversificare, ci şi cea mai mare uşurință de participare la fenomenul internaționalizării (atât în ceea ce priveşte dezvoltarea de produse soft, cât mai ales, în ceea ce priveşte utilizarea lor).

Progresul tehnologic fără precedent în domeniul transmiterii informațiilor au transformat profund societatea umană, contribuind la modificarea modelului funcțional, adică la trecerea la societatea informațională[1].

Spațiul cibernetic se caracterizează prin lipsa frontierelor, dinamism şi anonimat, generând deopotrivă oportunități de dezvoltare a societății informaționale, dar şi riscuri la adresa funcționării acesteia (la nivel individual, statal şi chiar transfrontalier).

Alături de beneficiile incontestabile pe care tehnologia informației le aduce la nivelul societății moderne, aceasta introduce şi o gamă largă de riscuri şi vulnerabilități. Astfel, din multitudinea de actori ce acționează în spațiul cibernetic, există anumite segmente (grupări) caracterizate printr-un grad ridicat de sofisticare dat de nivelul de resurse umane, materiale si tehnologice pe care le dețin, ce pot fi folosite în exploatarea vulnerabilităților în scopul obținerii frauduloase de informații, resurse financiare şi putere economică, dar şi în cel al afectării vieții cotidiene a milioane de oameni prin dezvoltarea de capacități ce pot perturba, distruge sau amenința furnizarea unor serviciilor esențiale precum cele din domeniul energiei, telecomunicațiilor, bancar, al sănătății sau administrației publice[2].

Atacurile din spațiul cibernetic rămân greu

[1] *** - Strategia de securitate cibernetică a României; https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf

[2] *** - US Dept. of Homeland Security - Cybersecurity Overview; https://www.dhs.gov/cybersecurity-overview

de identificat şi urmărit. Acestea pot fi iniţiate de la distanţă, cu minimum de resurse tehnice, dar cu implicaţii majore asupra activităţilor cotidiene, a economiei şi chiar a securităţii unui stat, de cele mai multe ori sursa lor rămânând anonimă. În spatele acestor atacuri pot fi grupări infracţionale sau teroriste, entităţi statale sau grupuri cu diverse interese economice ori sociale, astfel încât există o plajă largă de obiective ale cyber-infracţionalităţii.

Deşi se bazează foarte mult pe şansă, din punct de vedere al efectelor generate, atacul cibernetic la distanţă poate avea probabilitate mare de succes din următoarele considerente:

- atacul se poate executa oricând, din practic orice loc spre practic orice loc, singura condiţionare fiind funcţionarea unui calculator conectat la o reţea funcţională;
- efectul scontat se manifestă practic imediat (blocarea serverului atacat, furtul de informaţie, furtul de bani, compromiterea unei baze de date etc.), ceea ce constituie un suplimentar motiv de încurajare;
- efectul nedorit, cel de tip reactiv, adică expunerea la riscul de a suferi acţiuni punitive, este îndepărtat şi cu şanse foarte mici de materializare – ceea ce constituie un motiv de încurajare.

Dezvoltarea cu viteză crescută a unor instrumente software specializate în atacuri a dus la regândirea standardelor de lucru specifice Internetului, însă, în acelaşi timp, a stimulat şi creativitatea celor care căutau noi breşe de securitate în sisteme de operare, reţele, sisteme de baze de date sau aplicaţii. Succesele repurtate de partea celor atacaţi au însemnat gândirea şi implementarea de noi norme de securitate, actualizate şi eficiente, în timp ce succesele din tabăra opusă au însemnat pierderi financiare / pierderi de date / prejudicii morale aduse victimelor, dar şi ridicarea nivelului de vigilenţă la proiectarea şi exploatarea sistemelor informatice.

Pornind de la aceste considerente, în acest articol vor fi prezentate:

- riscurile la care suntem expuşi în faţa atacurilor cibernetice;
- arhitectura de principiu a unei aplicaţii software de atac la distanţă şi modalitatea prin care aceasta poate efectua un atac asupra unor ţinte alese aleator;
- consideraţii asupra standardizării soluţiilor de prevenire şi răspuns în astfel de cazuri.

Pentru înţelegerea mecanismului de funcţionare a unei astfel de aplicaţii şi implicit a impactului asupra securităţii informatice, este necesară o privire de ansamblu asupra principalelor tipuri de atac la distanţă şi a modului de propagare a acestora prin intermediul protocoalelor de comunicare a datelor.

De asemenea, rezultă necesitatea standardizării măsurilor de securitate cibernetică drept modalitate eficientă de organizare şi corelare a răspunsurilor în cazul unor atacuri informatice. Această necesitate derivă şi din uşurinţa prin care infractorii informatici au acces din ce în ce mai facil la instrumente de atac, tot mai sofisticate.

Aplicaţia de atac informatic prezentată în interiorul acestui articol, nu reprezintă o încurajare de a prelua un model şi a-l utiliza în scopuri distructive, ci este pur principială cu rol exclusiv demonstrativ, însă funcţională elementar.

2. Motivaţii ale atacurilor informatice

Infracţionalitatea cibernetică, fenomen nedorit care se întinde de la furt de personalitate şi furt financiar până la răspândire de viruşi şi viciere de trafic sau de servere, reprezintă un domeniu întins şi complex (este bazat pe creativitate şi performanţă tehnologică) care câştigă tot mai multă atenţie din cauza faptului că Internetul a devenit practic o componentă a existenţei. Deşi este greu de trasat un contur motivaţional generalizant al infractorului informatic, câteva trăsături de profil par totuşi să se distingă[3].

Motivarea financiară. Aşa cum este în cazul multor ilegalităţi comise pe Internet, banii constituie o motivaţie importantă pentru mulţi ciber-infractori, mai cu seamă din cauza

[3] Mercer, Edward - Causes of Cyber Crime; http://techin.oureverydaylife.com/causes-cyber-crime-1846.html

faptului că percepția asupra riscului scade în acuitate în spatele protecției iluzorii oferite de anonimatul din spatele unui calculator aflat undeva departe de victimă.

Motivații personale. De multe ori, în spatele cyber-infracțiunilor stau motivațiile personale, cazurile începând cu angajatul frustrat care instalează un virus şi cu liceanul care sparge baza de date cu note şi terminând cu specialistul care doreşte să-şi dovedească priceperea (atacurile din perioada de început a deceniului 1990 erau mai curând inofensive, însă situația s-a schimbat odată cu apariția viermilor, spionilor sau troienilor). Cu toate acestea, daunele provocate de cyber-infracțiuni alimentate de motive personale pot fi considerabile.

Motivații ideologice. Aceste atacuri sunt executate invocându-se de către atacatori motive morale / ideologice / etice şi vătămează activitatea on-line a aplicațiilor sau rețelelor pentru a exprima dezaprobarea față de anumite persoane, organizații, agenții, instituții, guverne.

Când victimele sunt din mediul de afaceri, "complicitatea" lor involuntară este asigurată însă şi de cauze structurale, cum ar fi:

- neglijența în protejarea sistemelor împotriva atacurilor informatice;
- dificultatea strângerii dovezilor incriminatoare, căci ori companiile neglijează rularea pe serverele proprii de programe care să jurnalizeze intruziunile[4], ori, dacă o fac, nu acordă importanță (sau nu au resurse umane destinate) studierii acestor jurnale; lipsa de inter-operare şi coordonare a mecanismelor penale naționale;
- lipsa de colaborare între victime şi poențiale victime, foarte puțini procedând la împărtăşirea experiențelor avute; ideea răspândită că infracțiunile cibernetice oricum sunt mici dezavantaje inerente ale extrem de avantajoasei lumi a Internetului;
- absența monitorizării traficului de ieşire, scanarea acestuia din urmă fiind o modalitate eficientă de a trage alarma că în sistem s-a instalat un intrus.

Când victimele sunt persoane private, de cele mai multe ori naivitatea şi ignoranța expun la riscuri de atac cibernetic: setarea de bună credință a datelor personale sau a parolelor pe situri de phishing la care se ajunge prin accesarea unei legături (link) primite pe e-mail, deschiderea unor ataşamente tot în aplicația de e-mail etc.

3. Atacuri informatice şi mediul de afaceri

Companiile de toate mărimile pot fi ținte ale atacurilor informatice, prejudiciile fiind nu doar de natură tehnică (blocarea de servere, infectarea de calculatoare, viciere de date), financiară sau funcțională (atacurile au drept consecință alocări neprevăzute de timp şi personal), ci şi în ceea ce priveşte reputația (de exemplu, cursul acțiunilor la Bursă ale unei companii de carduri de credit poate scadă substanțial în urma unui atac cu efecte de proporții, cum s-a întâmplat în 2009 cu "Heartland Payment Systems "[5]).

Companiile mici sunt expuse din cauza creşterii tendinței ca angajații să-şi aducă la servici propriile lor dispozitive de comunicare electronică, utilizate atât în interes de serviciu, cât şi în interes personal (laptopuri, tablete, telefoane inteligente), ceea ce creează o varietate de riscuri.[6]

Companiile comerciale mari sunt o țintă predilectă pentru cyber-infracționalitate, deşi au puse în funcțiune sisteme de protecție. În mod special, se rețin ca remarcabile atacurile produse cu succes fie asupra companiilor de IT, fie asupra companiilor a căror activitate se bazează substanțial pe componenta de IT. Mai jos se prezintă două exemplificări recente ale atacurilor cibernetice executate asupra mediului de afaceri.[7]

[4] Grimes, Roger - Five reasons Internet crime is worse than ever; http://www.infoworld.com/article/2608631/security/5-reasons-internet-crime-is-worse-than-ever.html

[5] Freed, AM – Another Payment Card Processor Hacked, 2009; http://information-security-resources.com/2009/02/14/another-payment-card-processor-hacked

[6] *** - OpenVPN Technologies Inc - Why Small Businesses are a BIG target for Cyber Criminals; https://www.privatetunnel.com/home/why-small-businesses-are-a-big-target-for-cyber-criminals

[7] *** - Bisk Technolgy Center – 10 Companies Affected by Cyber Attacks;

eBay - În feb.-mar. 2015, eBay a fost victima unui atac soldat cu fraudarea datelor de contact şi a acreditărilor de autentificare a 233 milioane de clienţi.

Firme Britanice – între iulie şi sept. 2017, 55000 de companii mici şi mijlocii din Marea Britanie au fost supuse unor tentative informatice de furt de date[8].

O ţintă tot mai des afectată de atacuri cibernetice o constituie companiile de producere-transport-distribuţie a energiei electrice, un exemplu edificator de infrastructură informatică sensibilă[9] din cauza faptului că sistemele de calcul devin o prezenţă din ce în ce mai activă în acest sector (sarcina optimizării fluxurilor de energie electrică revine unei complexe reţele de sisteme de calcul, implementate să realizeze achiziţiile de date, centralizarea datelor, procesarea / stocarea informaţiei, luarea deciziei - eventual în condiţiile unor avarii neprevăzute! - şi în cele din urmă acţionarea echipamentelor de generare, transformare, compensare, reglaj automat).

4. Ilustrarea principiului de funcţionare al unui atac la distanţă

În cele ce urmează se va ilustra principiul funcţional al unui atac la distanţă.

Atacul executat asupra unei aplicaţii, sistem de operare, sau unei maşini virtuale (Java VM sau .net VM) presupune o studiere prealabilă a victimei, pentru înţelegerea modului de funcţionare şi detectarea breşelor de securitate. În principiu, se utilizează un soft de tip debugger ("depanator de funcţionare") care încarcă executabilul ţintă şi care îi afişează acestuia codul în limbaj assembler; o funcţionalitate suplimentară fiind urmărirea în timp real a execuţiei secvenţiale. Odată găsită vulnerabilitatea, infractorii vor încerca s-o exploateze prin trimiterea de cereri conţinând cod maliţios.

Atacul executat asupra unui sit web sau asupra unei reţele se face prin aplicaţii care primesc drept intrare adresa de www., respectiv cea de IP, şi care apoi scanează situl sau reţeaua, căutând vulnerabilităţi. Un instrument larg uzitat în acest scop este NMAP , Internetul fiind nu doar canalul de colportare a atacurilor ci şi "depozitul" unde infractorii informatici se pot găsi şi accesa softuri de complexitate ridicată, apte de funcţionare şi cu interfaţă prietenoasă. Deşi sunt destule instrumente gratis, există deja formată o piaţă a aplicaţiilor malware, în continuă expansiune.

În secţiunea de mai jos se va prezenta un exemplu foarte concret de cod C utilizat la emularea unei aplicaţii destinate hack-ing-ului la distanţă. Aplicaţia rulează pe principiul "descoperire automată a ţintei", în ipoteza că nu ştie apriori cine, unde, ce găzduieşte. Se vor crea mai multe fire de execuţie care trimit cereri (requests) către adrese IP generate automat, fiecare răspuns fiind jurnalizat şi ulterior, în funcţie de rezultatul obţinut, utilizat pentru simularea creării şi trimiterii unor cereri maliţioase. Aplicaţia, rulabilă sub Windows, este pur principială, cu rol exclusiv demonstrativ, însă funcţională elementar. Reprezentarea schematică a aplicaţiei se face în Figura 1.

---

https://www.villanovau.com/resources/iss/companies-affected-by-cyber-attacks/#.WBx_uvQvvZ_

[8] *** - *Cyber criminals increase attacks on remote working technologies; http://continuitycentral.com/index.php/news/technology/2363-cyber-criminals-increase-attacks-on-remote-working-technologies, oct 2017*

[9] Low, Steven – Smart Grid Research: Potential Cyber Threats and Mitigation; https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/critical-infrastructures-west-hemisphere.pdf

```
// functia principala
int main()
{
#define NUMAR_FIRE 12

HANDLE hFire[NUMAR_FIRE];
     ZeroMemory(hFire, sizeof(HANDLE) * NUMAR_FIRE);
     int IdFire[NUMAR_FIRE];
     DWORD flag = THREAD_QUERY_INFORMATION|
CREATE_SUSPENDED|THREAD_SUSPEND_RESUME;
     for(int i = 0; i <= NUMAR_FIRE - 1; ++i)
     {
          hFire[i] = ::CreateThread(NULL, 0, (Func)ScaneazaProc, 0,
                      flag, &IdFire[i]);
     }
     for(i = 0; i <= NUMAR_FIRE - 1; ++i) if(hFire[i]) ResumeThread(hFire[i]);
     return 0;
}

// functie asociata fiecarui fir de executie; executa generare de
// adrese IP, conectare, trimitere de cereri, procesare raspunsuri.
UINT ScaneazaProc(LPVOID pParam)
{
     string ipCurent = "";

     while (TRUE)
     {
          // IESIRE DIN BUCLA
          if(Semnalizat(semafor)) break;

          // generare automata IP Adresa Victima
          string IPAdresa = GenereazaIP("85", ipCurent);

          // memorare adresa curenta pentru a NU mai fi folosita
          // in generari ulterioare
          ipCurent = IPAdresa;

          int codProtocolCurent = 0;
          string reqCurent = "";
          while (TRUE)
          {
               // IESIRE DIN BUCLA
               if(Semnalizat(semafor)) break;

               // stabilite automata a unui protocol de APLICATIE
               // pe care se SCONTEAZA ca se va realiza atacul
               int CodProtocol = GenereazaProtoc(codProtocolCurent);

               // memorare adresa curenta pentru a NU mai fi folosita
               // in generari ulterioare
               codProtocolCurent = CodProtocol;

               // genereaza Request
               string Req = GenereazaRequest(CodProtocol, reqCurent);
               reqCurent = Req;
               SOCKET priza = Conecteaza(IPAdresa);
               Trimite(priza, Req);

               // citeste raspuns
               string rasp = Primeste(priza);

               // utilizeaza raspuns
               Jurnalizeaza("D:\\TRMISE\\RESP\\Jurnal.txt", rasp);

               // efectueza atac
               Atac(priza, rasp);

               Deconectez(priza);
          }
     }
}
```

Acesta este codul de principiu care ilustrează posibilitatea de a testa pe ce protocol funcționează pe un anume **port** (aici, se presupune că s-a ales implicit :8080) o maşină anume (daca acea maşină există şi e conectată la Internet !), ceea ce se poate afla urmărind răspunsurile primite la o gamă de cereri trimise. Ulterior, în funcție de răspuns, programul încearcă pe maşina curentă un atac (tot sub forma unei cereri). Mai jos se vor explica succint conceptele de **port** şi protocol.

Prin **port** se înțelege un număr natural între 1 şi 65 535 asociat în mod unic, pe o maşină server, cu o aplicație (proces) care "ascultă" rețeaua (care citeşte periodic informațiile venite prin rețea, pe care i le depune într-un buffer un serviciu specializat al Sistemului de Operare). Trebuie menționat că în terminologia de specialitate de limbă engleză există expresia consacrată de "network listener", adică aplicație care "ascultă", adică verifică periodic informația care îi este destinată, venită prin rețea. Valoarea **portului**, stabilită în mod liber de către aplicația (procesul) care ascultă rețeaua, rămîne constantă, odată aleasă. Fiecărei aplicații, indiferent de rol sau complexitate, Sistemul de Operare gazdă îi asociază în mod unic un identificator numeric creat aleatoriu la startare, şi anume **ID Proces**.

Rolul portului: etichetează un unic canal de comunicare (conexiune) stabilit între aplicația server şi un client oarecare. Sistemul de Operare de pe maşina server menține un tabel de corespondență [**port** : **ID Proces**], creat la pornirea serverului şi actualizat la închiderea unei aplicații sau la startarea cu succes a uneia noi. Orice aplicație rețea care intenționează să "asculte" pe un **port** deja ocupat nu va fi lansată în execuție, astfel că pe o maşină server, pe un **port** oarecare nu poate rula ("asculta") decât o singură aplicație la un moment dat.

Orice aplicație client începe dialogul (stabileşte o conexiune) cu o aplicație server specificînd, printre altele, IP-ul maşinii server şi **portul** pe care rulează pe server aplicația "conlocutoare" aleasă.

Portul **:80** este consacrat pe plan internațional ca destinat aplicațiilor Internet (cele care rulează pe protocolul de aplicație HTTP).

Prin protocol se înțelege un regulament care guvernează dialogul dintre două aplicații, astfel încât fiecare să înțeleagă "ce a vrut să spună cealaltă" şi să execute întocmai ceea ce i se cere. În acest context, protocol = un vocabular + acțiuni asociate cu elementele vocabularului.

Strict pentru exemplificarea conceptului, vom presupune o situație ipotetică: o aplicație client (rulând într-o sucursală bancară) trimite unei aplicații server (rulând la sediul central) următoarea informație: SCRIECONT AAAA/DEP/900,YYY/ECO/4100,ZZZZZ/CRE/700.

Aplicație server execută ceea ce i s-a transmis şi trimite la aplicația client confirmarea de executare: CFRMCONT 0, 0, -1.

In acest exemplu, ipotetica SCRIECONT reprezintă comanda de consemnare în baza de date a unei sume de bani în contul unui anume client.

Aplicația server execută următoarele operațiuni (imediat mai jos se va vedea asocierea explicită între *acțiuni* şi *elemente de vocabular*):

- partiționează şirul total cu ajutorul separatorului blank şi obține comanda **SCRIECONT** plus un şir de tip argument;
- citeşte şirul aflat la dreapta caracterului blank de după **elementul de vocabular SCRIECONT** (chiar şirul argument) şi obține o listă de 3 sub-şiruri rezultate din partiționarea şirului argument cu ajutorul separatorului ",";
- fiecare sub-şir este la rîndul lui partiționat cu ajutorul separatorului "/";
- pentru clientul AAAA, va introduce în contul de depozit curent (indicat de **elementul de vocabular DEP**) suma de 900 lei; *scrierea în baza de date* este o *acțiune asociată* cu **elementele de vocabular SCRIECONT** şi **DEP;**
- în mod asemănător va proceda în cazul celorlalți 2 clienți (**elementul de vocabular ECO** înseamnă cont de economii, iar **elementul de vocabular CRE** înseamnă cont de credit);
- trimite la aplicație client confirmarea scrierii în cont cu indicativul Succes = 0, respectiv Esec = -1 (banca refuză să-l crediteze pe ZZZZZ cu 700 lei).

Aplicația client, la primirea informației

"**CFRMCONT** 0, 0, -1" (confirmare operaţiune pe cont), execută următoarele operaţiuni (imediat mai jos se va vedea asocierea explicită între *acţiuni* şi *elemente de vocabular*):

- partiţionează şirul total cu ajutorul separatorului blank şi obţine comanda **CFRMCONT** plus un şir de tip argument;
- citeşte şirul aflat la dreapta caracterului blank de după **elementul de vocabular CFRMCONT** (chiar şirul argument) şi obţine o listă de 3 subşiruri rezultate din partiţionarea şirului argument cu ajutorul separatorului ",";
- pentru clientul AAAA, va afişa pe ecran succesul operaţiunii; *afişarea* este o *acţiune asociată* cu **elementul de vocabular CFRMCONT** şi codul 0.

În continuare se dau 3 exemple de dialoguri de tip protocol (**FTP, SMTP, HTTP**):

FTP: dialog de tip **"conect, utilizator, prezint parola, solicit lista cu fişierele din folderul meu"**:

```
Status:Connecting to
ftp.oarecare.org ...
Status:Connected with ftp.oarecare.org.
Response:220 ProFTPD 1.2.4 Server
(ProFTPD) [109.41.xx.xxx]
Command:USER UnulCineva
Response:331 Password required for
UnulCineva.
Command:PASS **********
Response:230 User UnulCineva logged in.
Status:Connected
Status:Retrieving directory listing...
Command:PWD
Response:257 "/users/ UnulCineva" is
current directory.
Command:LIST
Response:150 Opening ASCII mode data
connection for file list.
Response:226 Transfer complete.
Status:Directory listing successful
```

SMTP: de tip **"sunt eu, am contul meu, de pe el trimit acum ceva la adresa de destinaţie"**:

```
$ /usr/lib/sendmail -v
oarecare@exemplu.com < /tmp/mtest
someuser@pobox.com... Connecting to
mx1b.exemplu.com. via esmtp...
220 ilustrativ.exemplu.com ESMTP
Postfix
>>> EHLO GAZDA.3x.com
250- ilustrativ.exemplu.com
250-PIPELINING
250-SIZE 10240000
250-ETRN
250 8BITMIME
>>> MAIL From: SIZE=51
250 Ok
>>> RCPT To:
250 Ok
>>> DATA
354 End data with .
>>> .
250 Ok: queued as 0E3EA1D216
oarecare@exemplu.com... Sent (Ok:
queued as 0E3EA1D216)
Closing connection to mx1b.pobox.com.
>>> QUIT
221 Bye
```

Răspunsurile sunt, în funcţie de fiecare protocol exemplificat:

HTTP REQUEST de tip **"doresc să primesc (GET) acest fişier de la *Serverul specificat* !"**:

```
GET /ceva.htm HTTP/1.1
User-Agent: Mozilla/4.0 (compatible;
MSIE5.01; Windows NT)
Host: www.undeva.com
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Connection: Keep-Alive
```

HTTP REQUEST de tip **"doresc să trimit (POST) un şir de octeţi la *Serverul specificat* !"**:

```
POST /cgi-bin/process.cgi HTTP/1.1
User-Agent: Mozilla/4.0 (compatible;
MSIE5.01; Windows NT)
Host: www.undeva.com
Content-Type: application/x-www-form-
urlencoded
Content-Length: 497
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Connection: Keep-Alive
```

HTTP RĂSPUNS de tip **"de acord (OK) ! poftim fişierul pe care l-ai solicitat *Serverului*"**:

```
HTTP/1.1 200 OK
Date: Mon, 27 Jul 2009 12:28:53 GMT
Server: Apache/2.2.14 (Win32)
Last-Modified: Wed, 22 Jul 2009
19:15:56 GMT
Content-Length: 88
Content-Type: text/html
Connection: Closed
```

Protocol FTP = VOCABULARUL şi acţiunile asociate, ca suport pentru dialogul dintre o aplicaţie şi un server de fişiere

Protocol SMTP = VOCABULARUL şi acţiunile asociate, ca suport pentru dialogul dintre o aplicaţie şi un server de poştă electronică

Protocol HTTP = VOCABULARUL şi acţiunile asociate, ca suport pentru dialogul dintre o aplicaţie şi un server de aplicaţii Internet sau Web

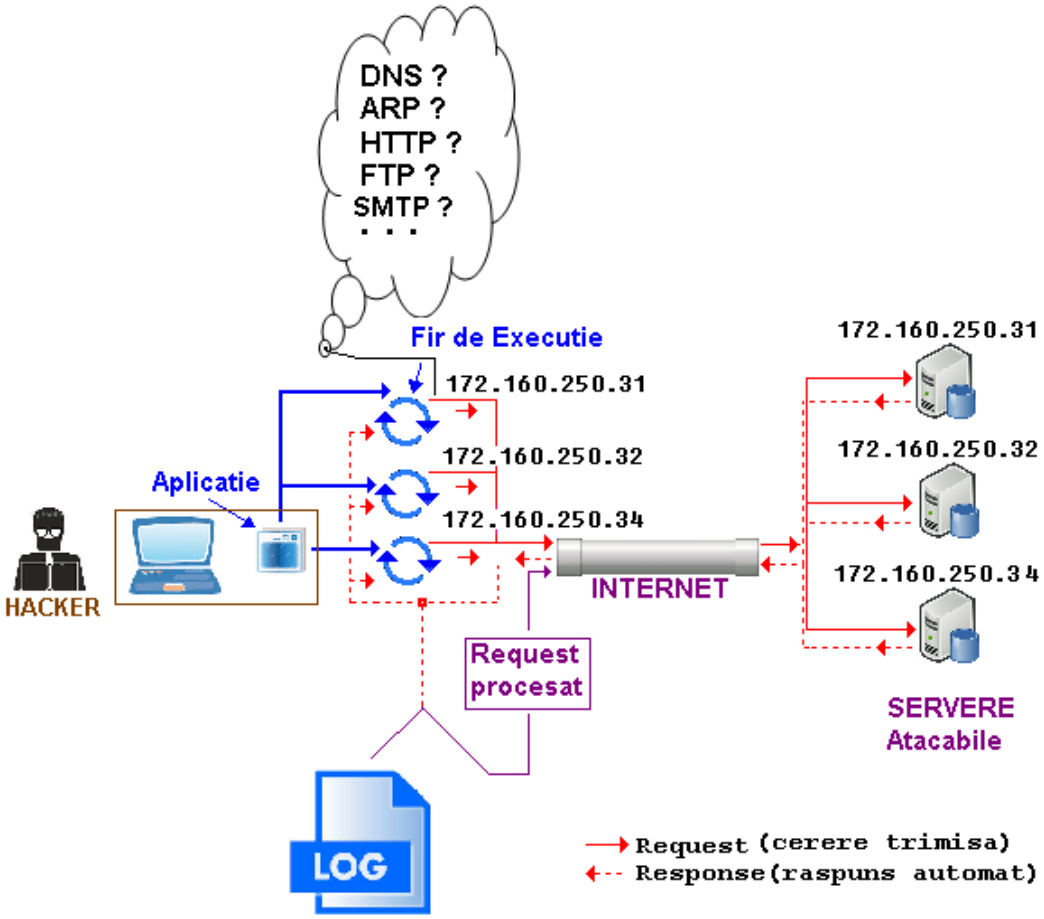

Figura 1. O posibilă schemă de principiu a unui atac la distanță

Această aplicație ilustrativă poate fi îmbogățită prin următoare trăsături funcționale:

- organizare a atacurilor deja efectuate într-o bază de date;
- trimiterea de segmente funcționale destinate instalării executabilului pe alte maşini;
- organizarea atacurilor după criterii de clasificare;
- algoritmi pentru accelerarea generării de IP valide;
- reluarea ulterioară a unor atacuri etc.

5. O soluție *de principiu* în sprijinul contracarării atacurilor la distanță: standardizarea

După cum se observă, efectuarea unui atac cibernetic este departe de a fi dificilă; tocmai de aceea standardizarea politicilor de securitate duce la creşterea şanselor unei apărări eficace.

În procesul de dialog automat prin rețea, esențială este protejarea informației vehiculate, fără ca acest lucru să depindă de sistemul de operare emitor / receptor, tipul aplicațiilor care dialoghează, locul si modalitatea de memorare ulterioară a informației.

Standardul ISO/IEC 17799 recomandă ca protejarea informațiilor să îndeplinească 3 cerințe:

- confidențialitate – informația poate fi accesată doar de emitor / destinatar şi de nimeni altcineva;
- integritate – datele care ajung sa fie riguros aceleaşi de la punctul de plecare;
- disponibilitatea – destinatarul să poată accesa oricând informația solicitată.

Pentru a asigura o strategie eficientă de protejare sunt necesare standardele, procedurile şi ghidurile de bună practică puse în serviciul unei structurări bine determinate a apărării cibernetice. Condiții vitale ale succesului cu

care se previn cyber-atacurile sunt coerența şi consecvența cu care se defineşte şi se clădeşte în practică o arhitectură de securitate. Standardizarea reprezintă un pas important către îndeplinirea acestor condiții.

Standardul înseamnă o colecție de norme, reguli cu valoare de reper, jaloane generale de lucru, criterii la care se raportează acțiunile care au un anumit scop. Standardele specifică utilizarea anumitor tehnologii, într-o viziune uniformă. În cazul cyber-securizării, ele se referă la rețele, aplicații, servicii, medii de stocare, medii de vehiculare, dispozitive. De regulă, standardele sunt obligatorii şi sunt implementate la nivel de unitate, tocmai pentru asigurarea uniformității. Elementele principale ale unui standard de securitate informațională sunt:

- scopul şi aria de aplicare - prin care se oferă o descriere a intenției standardului (realizarea unui tip de server pe o anumită platformă);
- roluri şi responsabilități - la nivel de instituție/companie pe linia definirii, execuției şi promovării standardului;
- standardele cadrului de bază - prin care sunt prezentate declarațiile de pe cel mai înalt nivel, aplicabile platformelor şi aplicațiilor;
- standardele tehnologiei - conțin declarațiile şi descrierile aferente (configurația sistemului sau serviciile nesolicitate de sistem);
- standardele administrării reglementează administrarea inițială şi în timpul exploatării platformei şi aplicațiilor[10].

Procedura reprezintă schema concretă de aplicare practică a unui standard. Ea înseamnă ansamblul de acțiuni specifice care trebuie executate pentru îndeplinirea unui scop bine determinat, cu specificarea atribuțiunilor fiecărui participant.

Prin conformare cu procesul de standardizare se obține coordonarea eforturilor pentru prevenirea cyber-infracționalității şi, prin urmare, creşte sensibil probabilitatea de succes. Este benefică dezvoltarea de strategii şi politici autonome de apărare informatică (adică la nivel de companie sau instituție), însă armonizarea practicilor la nivel național promite efecte mult îmbunătățite față de cele oferite de "atomizarea" soluțiilor. Cu atât mai mult se impune sincronizarea eforturilor şi pe plan supra-național, pentru că, aşa cum se întâmplă în realitate, pe lume există o mare varietate de aplicații conectate la Internet care rulează pe diverse sisteme de operare, iar infracțiunea informatică se diversifică şi modernizează cu cea mai mare viteză, în condițiile în care este cea care nu cunoaşte nici un fel de frontieră de nici o natură; guvernele însele sunt primele entități interesate în prevenirea, limitarea propagării şi descurajarea cyber-infracțiunilor.

Standardizarea la nivelul Uniunii Europene mai prezintă un avantaj important: oferă celor interesați surse cuprinzătoare, obținute din sintetizarea celor mai bune şi actuale soluții, multe dintre ele primind confirmarea prin aplicarea în practică. O situație în care standardizarea se dovedeşte importantă este realizarea platformei europene de interoperare, magistrală performantă de informație în servicul cetățenilor, companiilor şi instituțiilor europene. Cadrul European de Interoperare oferă un un set comun de concepte de bază materializate în politici, strategii, orientări şi planuri de acțiune pentru proiectarea şi actualizarea cadrelor naționale de interoperare, scopul concret fiind găsirea de răspunsuri la nevoia de a accesa rapid şi coerent informații administrative, juridice, economice, financiare de mare varietate la nivelul continentului.

Standardizarea prezintă avantaje directe pentru companii şi instituții: reducerea costurilor şi creşterea productivității prin simplificarea procesului de alegere a unei soluții de securitate cât mai adecvate, prin minimizarea riscurilor sau efectelor unui atac, prin acces direct şi instantaneu la informație de calitate, prin optimizarea utilizării resurselor. În general, standardizarea stimulează creativitatea şi creşte gradul de implicare a experților.

6. Concluzii

Efectuarea unui atac cibernetic este posibilă prin operațiunea de trimitere a unei familii de cereri către adrese generate aleatoriu.

[10] Popa, Sorin Eugen - Securitatea sistemelor informatice, note de curs şi aplicații pentru studenții Facultății de Inginerie, Universitatea din Bacău

Atacurile exploatează fisuri în securizarea aplicațiilor care "ascultă" rețeaua funcționând după un anume protocol. Atacurile se pot efectua asupra aplicațiilor de tip server de baze de date, server de fișiere, server de mail, nucleu de comenzi ("shell") al sistemului de operare –gadză etc – prin acțiuni de tip "inundație" (flooding) sau cod malițios.

Articolul şi-a propus să prezinte modelul de principiu al unei aplicații capabile să execute astfel de atacuri prin trimiterea de cereri către adrese de tip IP generate după un algoritm bine determinat. Codul ilustrativ este formulat în limbajul C++.

Pentru securizarea unei aplicații server se utilizează instrumente specifice al căror punct comun îl reprezintă echiparea cu informație profilactică a componentei care dialoghează cu rețeaua.

Standardele, procedurile şi ghidurile de bună practică reprezintă o soluție eficientă în sprijinul unei strategii organizate de apărare cibernetică. Actualizarea cunoaşterii tipologiilor de atac şi consecvența cu care se implementează măsurile de prevenire sînt elemente care contribuie la definirea unei arhitecturi de securitate eficiente. Standardizarea ajută la crearea unei politici coerente de apărare cibernetică, capabile să facă față unei tipologii vaste de atacuri şi țină pasul cu ritmul de dezvoltare a acestora.

BIBLIOGRAFIE

1. *** - Bisk Technolgy Center – 10 Companies Affected by Cyber Attacks; https://www.villanovau.com/resources/iss/companies-affected-by-cyber-attacks/#.WBx_uvQvvZ_
2. *** - Cyber criminals increase attacks on remote working technologies; http://continuitycentral.com/index.php/news/technology/2363-cyber-criminals-increase-attacks-on-remote-working-technologies, oct 2017
3. *** - OpenVPN Technologies Inc - Why Small Businesses are a BIG target for Cyber Criminals; https://www.privatetunnel.com/home/why-small-businesses-are-a-big-target-for-cyber-criminals
4. *** - Strategia de securitate cibernetică a României; https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf
5. *** - US Dept. of Homeland Security - Cybersecurity Overview; https://www.dhs.gov/cybersecurity-overview
6. **FREED, A. M.:** Another Payment Card Processor Hacked, 2009; http://information-security-resources.com/2009/02/ 14/another-payment-card-processor-hacked
7. **GRIMES, R.:** Five reasons Internet crime is worse than ever; http://www.infoworld.com/article/2608631/security/5-reasons-internet-crime-is-worse-than-ever.html
8. **LOW, S.:** Smart Grid Research: Potential Cyber Threats and Mitigation; https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/critical-infrastructures-west-hemisphere.pdf
9. **MARINESCU, I. A.; NICOLAU D.; BĂJENARU, L.:** Considerații asupra atacurilor cibernetice, executate în contextul comunicațiilor prin rețea; RRIA, Art. 01, Vol. 26, Nr. 4, 2016.
10. **MERCER, E.:** Causes of Cyber Crime; http://techin.oureverydaylife.com/causes-cyber-crime-1846.html
11. **POPA, S. E.:** Securitatea sistemelor informatice, note de curs şi aplicații pentru studenții Facultății de Inginerie, Universitatea din Bacău.