МОДЕЛИРАНЕ НА ПРОЦЕСИТЕ ПРИ ВЪЗДЕЙСТВИЕ НА КОМПЮТЪРНА МРЕЖА СЪС ЗЛОНАМЕРЕН СОФТУЕР

проф. д.т.н. Андон Лазаров, Петя Иванова Петрова – докторант
Бургаски свободен университет, ЦИТН

MODELING OF IMPACT PROCESSES ON COMPUTER NETWORK WITH MALWARE

Dr.Sc. Prof. Andon Lazarov, Petia Petrova - PhD student
Burgas Free University

Анотация: *Акцентът на настоящото изследване е да се анализират процесите на податливост, експозиция, инфекция и възстановяване на компютърните мрежи в случай на въздействие на злонамерен софтуер. Основните диференциални уравнения, описващи поведението на мрежата, се дефинират като система от диференциални уравнения. Два случая се разглеждат, случаят на равновесие в компютърната мрежа и случаят без равновесие в компютърната мрежа. Решени са нехомогенни диференциални уравнения и система от нехомогенни диференциални уравнения и са получени аналитични изрази за изчисляване на мрежовите характеристики в случай на податливост, експозиция, инфекция и възстановяване (реконструкция) на компютърни възли по време на атака на злонамерен софтуер.*

Ключови думи: *компютърни мрежови атаки, защита от зловреден софтуер, мрежови диференциални уравнения.*

Abstract: *The focus of the present study is to analyze the processes of susceptibility, exposition, infection and recoverability of computer networks in case of malware attacks. The basic differential equations describing the behavior of network are defined as a system of differential equations. Two cases are under consideration, the case of equilibrium in the computer network, and the case without equilibrium in the computer network. Nonhomogeneous differential equations and system of nonhomogeneous differential equations are solved, and analytical expressions are derived to calculate the network characteristics in case of susceptibility, exposition, infection and reconstruction of computer nodes during malware attack.*

Key words: *computer network attacks, malware protection, network differential equations.*

1. Въведение

Компютърният злонамерен софтуер (worm) е самостоятелна компютърна програма, която има свойството да се мултиплицира, т.е. да създава множество копия на самата себе си с цел поразяване на множество компютри в мрежата. Пораженията на злонамерения софтуер са основно върху мрежата, което се изразява в увеличение на мрежовия трафик и съществено забавяне на предаването на данни по нея. В [1] се обсъжда общата структура на модерните компютърни зловреден софтуер (worms) и общите стратегии, които този софтуер използва, за да порази компютърните мрежи, в

които те се само-възпроизвежда. Математическо моделиране и алгоритми за защита срещу Internet атаки на зловреден софтуер върху компютърни мрежи подробно са анализирани в [2]. Математически модел на процесите на податливост, експозиция, инфекция и възстановяване от въздействие на злонамерен софтуер с графическа илюстрация на решенията на диференциалните уравнения, описващи комплексния процес на въздействие върху възлите от компютърната мрежа е представен [3,4,5]. Съвременните компютърни мрежи са софтуерно дефинирани (Software Defined Network), което определя тяхната уязвимост от въздействие на злонамерен софтуер. Тази уязвимост нараства пропорционално на мобилността на компонентите на мрежата. Динамичен модел, базиран на епидемичните процеси при разпространение на бактерии и вируси с теоретичен анализ и цифрова симулация на епидемичния процес е представен в [6]. Широко-мащабното дигитализиране на основни функции при административно и социално управление, банкиране, комуникации и т.н., като правило Internet-базирани, направи тези функции атрактивна цел за програмисти на зловреден софтуер, като се създават условия за мощни, а понякога и глобални кибернетични атаки с намерение за несанкциониран достъп до информация или да нарушат или прекъснат електронния процес на управление. Тези въздействия върху мрежите са непрекъснати, въпреки усилията за осигуряване на защита чрез въвеждане на нови механизми за противодействие срещу тях. Ефективността на защита и избор на подходяща и ефективна от гледна точка на разходите стратегия за противодействие в случай на кибернетична атака зависи от успешното моделиране на процеса на разпространение на кибернетичната атака, ефективността на техниката за защита и сигурност, което дава възможност да се определи и даже намали броят на поразените машини. В [7] се предлага стохастичен модел, който отчита факта, че различните мрежови пътища имат различни нива на риск, както и оценка на противодействието на защитния софтуер. Динамиката на въздействието на зловреден софтуер (worms) върху Internet се описва с класически модел SIR(Susceptible-Infective-Removed) [3]. В [8] се предлага модел на инфектиране на мрежата под въздействие на злонамерен софтуер, който се описва с диференциално уравнение, описващо процеса на инфектиране и изведено непосредствено от модела на процеса на високо ниво, изразен в стохастична PEPA (Performance Evaluation Process Algebra) алгебра.

Компютърният зловреден софтуер е предназначен само за разпространение и не въздействат върху компютърните системите, през които преминават. Въпреки това, например, известният злонамерен софтуер на Morris и Mydoom, могат да причинят сериозни смущения, като увеличат мрежовия трафик и предизвикат други нежелани ефекти. Злонамереният софтуер Slammer е използвал уязвимост в софтуера на Microsoft за бази данни на SQL и предизвика каскадни ефекти в компютърната инфраструктура, системите за резервации на авиокомпании и банковите автоматизирани банкомати (ATM). Различни концепции, свързани със въздействие на зловреден софтуер и класификация на съществуващите агресивни мултиплициращи се програми в Internet от типа P2P, e-mail и IM (Instant Messaging) въздействащи са разгледани в [9], като акцент е направен върху стратегията за откриване и противодействие на e-mail и IM поразяващи програми.

Компютърният злонамерен софтуер се разглежда като вид компютърен вирус, но има няколко характеристики, които отличават компютърния злонамерен софтуер от вирусния софтуер. Основната разлика се състои това, че вирусният софтуер се разпространяват чрез дейност на оператора (потребителя) (стартиране на програма, отваряне на файл и т.н.), докато компютърният злонамерен софтуер има способността да се мултиплицира и разпространява автоматично без човешка намеса. Освен, че мо-

гат да се разпространява без намеса на оператора, компютърният злонамерен софтуер има способността да се само-размножава. Това означава, този софтуер създават няколко копия от себе си, за да порази и други компютри. Това се постига чрез изпращането на масови имейли към имейл адреси на заразени със злонамерен софтуер компютър в мрежата.

Примери на компютърен злонамерен софтуер са Stuxnet, Duqu и Flame, които продължават да правят свои нови копия от злонамерен софтуер с основно предназначение провеждане на кибернетична война. Способността на зловредните програми да се разпространяват и мултиплицират с високи скорости, преодолявайки защитните механизми, ги прави основна заплаха за сигурността на разпределените компютърни системи. В [10] е представен софтуерен сензорен комплекс за автоматично откриване на потенциални вектори (посоки) за инфектиране на мрежата и противодействие. Обща характеристика на различни видове зловреден софтуер, вируси и ботове (автоматично генериране на данни, които заливат IP адреси в мрежата) и методите на въздействие върху приложенията и мрежовите устройства и средствата за противодействие са представени в [11].

Internet е основната среда, използвана за извършване на компютърни престъпления. Атаките със зловреден софтуер се определят с най-висок риск за сигурността в компютърната мрежа. Този софтуер е създаден да се разпространяват без предупреждение или взаимодействие с потребителите. Той предизвиква увеличаване на заявките за трафик, което от своя страна осигурява осъществяване на кибернетична атака. Оценка и топологичен анализ на уязвимостта на мрежите, като и алгоритми за превенция от въздействие на кибернетични атаки с цел несанкциониран достъп до данни, както и роботизирана програма за пълно неутрализиране на зловреден софтуер са представени в [12]. Съвременните информационни и комуникационни системи стават все по-разнообразни и по-сложни, което ги прави привилегирована цел за мрежови и компютърни атаки, чийто брой неимоверно нараства, а тяхното поражение не предсказуемо. В [13] е представен модел на атака, наречен AIDD (Attack Identification And Defence). Пълна характеристика на процесите при откриване и превенция на атаки със зловреден софтуер в съвременните компютърни мрежи е направена в [14]. За ефективно противодействие на зловреден софтуер от съществено значение познаването на неговия source code. Характеристика и описание на някои основни source codes със злонамерено въздействие върху приложенията и мрежовите компоненти са представени в [15]. Подробно описание на зловредния софтуер Stuxnet Worm е направено [16].

Цел на настоящото изследване е изграждане на математически модел на поведението на компютърната мрежа и динамиката на нейните възли, които са податливи, експонирани, инфектирани и възстановени след атака на зловреден софтуер, дефиниране на основните диференциални уравнения, описващи състоянието на мрежата, т.е. определяне на броя на звената в компютърната мрежа предразположени към атака, експонирани на въздействие, инфектирани и възстановени след въздействие.

Статията е организирана по следния начин. В част 2 се представя математически модел на кибернетична атака. В част 3 е представено решение на системата от диференциални уравнения при равновесно състояние на компютърна мрежа**.** В част 4 се определят оптималните (екстремални) стойности на характеристиките на компютърната мрежа при атака от злонамерен софтуер при равновесие на системата. В част 5 е изведено решение на системата от диференциални уравнения при неравновесно състояние на компютърната система. В част 6 е дадено заключение и са направени изводи за приложимостта на анализа на уязвимостта на компютърната мрежа.

2. Математически модел на кибернетична атака

Предлага се епидемичен модел SEIR (Susceptible-Exposed-Infectious-Recovered) за предаване на класически вирус, който илюстрира динамиката на прякото предаване на злонамерен софтуер сред възприемчивите (податливи) – Susceptible (*S*), изложените (незащитени) – Exposed (*E*), заразените (инфектираните) – Infectious (*I*) и възстановените – Recovered (*R*) класове на компютърната мрежа. Означава се с *I* и *R* съответно инфектираният и възстановеният клас мрежи. Със символа *b* се означава степен на включване на нови възли (nodes) във възприемчивия клас, μ е степента на смъртност, дължаща се на атака на злонамерения софтуер (вирус), β е степента на инфекциозен контакт, δ е степента на пропадане възлите (nodes) в мрежата в резултат на инфекция, τ е степента на инфектиране на експонирания незащитен клас, изложен на инфекция.

Класове възли, податливите на инфектиране се характеризират с изчислителен капацитет на пренасяне с нарастване $k > 0$, както и свойствен темп на нарастване $r > 0$. Ефективността на антивирусния софтуер в дадена мрежа е ограничена поради времевият интервал на актуализиране на антивирусния софтуер и ефективността на разходите. Предлага се следната функция за възстановяване след атака със злонамерен софтуер [3]

$$\mathrm{Rec}(I) = \begin{cases} \rho I, \ 0 \le I \le I_{\min} \\ m, \ I \ge I_{\min} \end{cases} \tag{1}$$

където ρ е степен на възстановяване след инфектиране на I компютърните възли, когато антивирусната програма не се използва напълно, т.е. $0 \le I \le I_{\min}$, $m = \rho . I_{\min}$, когато $I \ge I_{\min}$, където $I_{\min}$ е минималният брой инфектирани възли, след което се включва антивирусната програма.

Динамиката на възлите от възприемчивия *S* клас се дефинира със скоростта на изменение на S чрез израза

$$\frac{dS}{dt} = r.S - (r.S).\left(\frac{S}{k}\right) - (\beta.I).S - \delta.S \tag{2}$$

Динамиката на възлите от експонирания *E* клас се дефинира със скоростта на изменение на *E* чрез израза

$$\frac{dE}{dt} = (\beta.I).S - (\tau + \delta).E \tag{3}$$

Динамиката на възлите от инфектирания *I* клас се дефинира със скоростта на изменение на *E* чрез израза

$$\frac{dI}{dt} = \tau.E - (\mu + \delta).I - \mathrm{Rec}(I) . \tag{4}$$

Динамиката на възстановяване на възлите от клас *R* се дефинира със скоростта на изменение на *R* чрез израза

$$\frac{dR}{dt} = \mathrm{Re\,c}(I) - \delta R \,. \tag{5}$$

Системата от диференциални уравнения, описващи поведението на компютърна система, атакувана със злонамерен софтуер записана за динамиката на възприемчивостта (susceptibility), S, експозицията (exposed) E, инфекцията I, възстановяването (Recovery) R на мрежата се записва във вида

$$\frac{dS}{dt} = r.S - (r.S).\left(\frac{S}{k}\right) - (\beta.I).S - \delta.S$$

$$\frac{dE}{dt} = (\beta.I).S - (\tau + \delta).E \tag{6}$$

$$\frac{dI}{dt} = \tau.E - (\mu + \delta).I - \mathrm{Re\,c}(I)$$

$$\frac{dR}{dt} = \mathrm{Re\,c}(I) - \delta R$$

Първите три уравнения са независими от класа *R*, което позволява системата от уравнения да се редуцира до три линейни диференциални уравнения, т.е.

$$\frac{dS}{dt} = r.S - (r.S).\left(\frac{S}{k}\right) - (\beta.I).S - \delta.S$$

$$\frac{dE}{dt} = (\beta.I).S - (\tau + \delta).E \tag{7}$$

$$\frac{dI}{dt} = \tau.E - (\mu + \delta).I - \mathrm{Re\,c}(I)$$

3. Решение на системата от диференциални уравнения при равновесно състояние на компютърна мрежа

Равновесно състояние на компютърната мрежа е това, при което променливите дефиниращи различните класове възли в мрежата са константи, т.е.

$$\frac{dS}{dt} = 0 \,,\ \frac{dE}{dt} = 0 \,,\ \frac{dI}{dt} = 0$$

С отчитане на горните условия, системата от уравнения, дефинираща равновесното състояние на компютърната мрежа, се записва във вида

а) при $0 \le I \le I_{\min}$

$$r.S - (r.S).\left(\frac{S}{k}\right) - (\beta.I).S - \delta.S = 0$$

$$(\beta.I).S - (\tau + \delta).E = 0 \qquad (8)$$

$$\tau.E - (\mu + \delta).I - \rho I = 0$$

б) при $I > I_{\min}$

$$r.S - (r.S).\left(\frac{S}{k}\right) - (\beta.I).S - \delta.S = 0$$

$$(\beta.I).S - (\tau + \delta).E = 0 \qquad (9)$$

$$\tau.E - (\mu + \delta).I - m = 0$$

Решението на система (8) при наличие на предразположеност на компютърната мрежа, но отсъствие на експонирани и инфектирани възли в мрежата, т.е. $E = 0$, $I = 0$, има вида

$$S = \frac{k(r - \delta)}{r}. \qquad (10)$$

Решението на система (8) при наличие на ендемично равновесие се записва във вида

$$S' = \frac{a(\delta + \tau)}{\beta.\tau},\ E' = \frac{a.r.(k\beta - a(\delta + \tau)) - k.\delta.\beta.\tau}{\beta^2.\tau^2.k},\ I' = \frac{.r.(k\beta - a(\delta + \tau)) - k.\delta.\beta.\tau}{\beta^2.\tau.k}, \qquad (11)$$

където $a = \rho + \mu + \delta$

Като се отчете, че $S \neq 0$, система (9) се записва във вида

$$r - S.\left(\frac{r}{k}\right) - (\beta.I) - \delta = 0$$

$$(\beta.I).S - (\tau + \delta).E = 0 \qquad (12)$$

$$\tau.E - (\mu + \delta).I - m = 0$$

Решението на система (12) при наличие на ендемично равновесие се извършва по следния начин. От първото уравнение се определя S

$$S = \frac{k(r - \beta.I - \delta)}{r} \tag{13}$$

От третото уравнение се определя E

$$E = \frac{(\mu + \delta).I + m}{\tau} \tag{14}$$

Замества се (13) и (14) във второто уравнение на (12). След преобразования се получава следното квадратно уравнение относно инфектираните възли на мрежата в ендемично равновесие I

$$\beta^2 \tau k I^2 - [\beta\tau k(r - \delta) - r(\tau + \delta)(\mu + \delta)].I + m.r.(\tau + \delta) = 0 . \tag{15}$$

Решението за броя на инфектираните компютърни възли I има вида

$$I_{1,2} = \frac{n \pm \sqrt{t}}{2.\tau.k.\beta^2} . \tag{16}$$

Изразът (16) се замества в изразите (13) и (14) за определяне податливите S и експонирани възли E на мрежата в ендемично равновесие

$$S_{1,2} = \frac{2.\tau.k.\beta(r - \delta) - n \pm \sqrt{t}}{2.\tau.r.\beta} . \tag{17}$$

$$E_{1,2} = \frac{(\mu + \delta)(n \pm \sqrt{t}) + 2.m.\tau.k.\beta^2}{2.k.\tau^2..\beta^2} . \tag{18}$$

При ендемично равновесие и включена антивирусна програма, $I_{1,2} > I_{\min}$, т.е.

$$I_{1,2} = \frac{n \pm \sqrt{t}}{2.\tau.k.\beta^2} \geq I_{\min} , \tag{20}$$

откъдето условието за ендемично равновесие при включена антивирусна програма се записва във вида

$$\sqrt{t} \geq I_{\min}.2.\tau.k.\beta^2 - n \tag{21}$$

4. Определяне на оптималните (екстремални стойности) на характеристиките на компютърната мрежа при атака от злонамерен софтуер при равновесие на системата

За тази цел се изчисляват матриците на Jacobian на системите от уравнения (8) и (9) и определят техните характеристични числа, които позволяват тяхното сингулярно разложение. За системата от уравнения (8), чрез левите страни на равенствата се дефинират следните вектори

$$A = r.S - (r.S).\left(\frac{S}{k}\right) - (\beta.I).S - \delta.S$$

$$B = (\beta.I).S - (\tau + \delta).E \tag{22}$$

$$C = \tau.E - (\mu + \delta).I - \rho I$$

За системата от уравнения (9), чрез левите страни на равенствата се дефинират следните вектори

$$A = r.S - (r.S).\left(\frac{S}{k}\right) - (\beta.I).S - \delta.S$$

$$B = (\beta.I).S - (\tau + \delta).E \tag{23}$$

$$C' = \tau.E - (\mu + \delta).I - m$$

Матрицата на Jacobian на системата от уравнения (8) при $0 \le I \le I_{\min}$ има вида

$$J_1 = \begin{bmatrix} \frac{\partial A}{\partial S} & \frac{\partial A}{\partial E} & \frac{\partial A}{\partial I} \\ \frac{\partial B}{\partial S} & \frac{\partial B}{\partial E} & \frac{\partial B}{\partial I} \\ \frac{\partial C}{\partial S} & \frac{\partial C}{\partial E} & \frac{\partial C}{\partial I} \end{bmatrix} = \begin{bmatrix} r - 2.r.\left(\frac{S}{k}\right) - (\beta.I) - \delta & 0 & -\beta S \\ \beta.I & -(\tau + \delta) & \beta.S \\ 0 & \tau & -(\mu + \delta + \rho) \end{bmatrix} \tag{24}$$

Матрицата на Jacobian на системата от уравнения (9) при $I > I_{\min}$ има вида

$$J_2 = \begin{bmatrix} \frac{\partial A}{\partial S} & \frac{\partial A}{\partial E} & \frac{\partial A}{\partial I} \\ \frac{\partial B}{\partial S} & \frac{\partial B}{\partial E} & \frac{\partial B}{\partial I} \\ \frac{\partial C'}{\partial S} & \frac{\partial C'}{\partial E} & \frac{\partial C'}{\partial I} \end{bmatrix} = \begin{bmatrix} r - 2.r.\left(\frac{S}{k}\right) - (\beta.I) - \delta & 0 & -\beta S \\ \beta.I & -(\tau + \delta) & \beta.S \\ 0 & \tau & -(\mu + \delta) \end{bmatrix}. \tag{25}$$

1. В случай на пълно равновесие на компютърната мрежа, т.е. S = 0, E = 0, I = 0 (отсъствие на предразположеност, експозиция за инфекция и инфекция на възлите) характеристичните числа на матрицата J_1 имат следните стойности, които са елементи на диагонала на екстремалната матрица $\hat{J}_1$ от сингулярното разложение на J_1

$$\hat{J}_1 = \begin{bmatrix} r-\delta & 0 & 0 \\ 0 & -(\tau+\delta) & 0 \\ 0 & 0 & -(\mu+\delta+\rho) \end{bmatrix}. \tag{26}$$

За да се постигне асимптотическо равновесие и глобална стабилност в компютърната мрежа при $0 \le I \le I_{\min}$ с течение на времето характеристичните числа следва да бъдат отрицателни, което поставя условието $r < \delta$.

В случай на пълно равновесие на компютърната мрежа, т.е. S = 0, E = 0, I = 0 (отсъствие на предразположеност, експозиция за инфекция и инфекция на възлите) характеристичните числа на матрицата J_2 имат следните стойности, които са елементи на диагонала на екстремалната матрица $\hat{J}_2$ от сингулярното разложение на J_2

$$\hat{J}_2 = \begin{bmatrix} r-\delta & 0 & 0 \\ 0 & -(\tau+\delta) & 0 \\ 0 & 0 & -(\mu+\delta) \end{bmatrix}. \tag{26}$$

За да се постигне асимптотическо равновесие и глобална стабилност в компютърната мрежа при $I > I_{\min}$ с течение на времето характеристичните числа следва да бъдат отрицателни, което поставя отново условието $r < \delta$.

2. При наличие на предразположеност на компютърната мрежа при времево условие $t \ge t_0$, където t_0 определя момента на асимптотическа константна предразположеност S и отсъствие на експонирани и инфектирани възли в мрежата, т.е.

$$S = \frac{k(r-\delta)}{r},\ E = 0,\ I = 0,$$

матрицата на Jacobian

$$J_3 = \begin{bmatrix} r - 2.r.\left(\frac{S}{k}\right) - \delta & 0 & -\beta S \\ 0 & -(\tau+\delta) & \beta.S \\ 0 & \tau & -(\mu+\delta) \end{bmatrix}, \tag{27}$$

се записва във вида

$$J_3 = \begin{bmatrix} -(\delta - r) & 0 & -\beta\dfrac{k(r-\delta)}{r} \\ 0 & -(\tau+\delta) & \beta.\dfrac{k(r-\delta)}{r} \\ 0 & \tau & -(\mu+\delta) \end{bmatrix}. \tag{28}$$

Характеристичните числа на матрицата J_3 имат следните стойности, които са елементи на диагонала на екстремалната матрица $\hat{J}_3$ от сингулярното разложение на J_3

$$\hat{J}_3 = \begin{bmatrix} -(\delta - r) & 0 & 0 \\ 0 & \dfrac{-f - \sqrt{g^2 - 4f}}{2} & 0 \\ 0 & 0 & \dfrac{-f + \sqrt{g^2 - 4f}}{2} \end{bmatrix}, \tag{29}$$

където $f = 2\delta + \mu + \tau$, $g = (\delta + \tau)(\mu + \delta) - \dfrac{\beta.\tau.k(r-\delta)}{r}$.

Характеристичните числа на J_3 следва да бъдат отрицателни, което поставя отново условието $r < \delta$ и $f > \sqrt{g^2 - 4f}$.

3. При наличие на фиксирана предразположеност на компютърната мрежа към атака със злонамерен софтуер, асимптотически дефинирана с израза $S = \dfrac{k(r-\delta)}{r}$ при времево условие $t \geq t_0$ и динамика на експонирани и инфектирани възли в мрежата, т.е. $E = var \neq 0$, $I = var \neq 0$, системата от диференциала уравнение за E и I се записва във вида

$$\frac{dE}{dt} = -(\tau + \delta).E + \beta.\frac{k.(r-\delta)}{r}.I \tag{30}$$

$$\frac{dI}{dt} = \tau.E - (\mu + \delta + \rho).I \tag{31}$$

Матрицата от коефициенти на системата от диференциални уравнения се записва във вида

$$\begin{bmatrix} -(\tau+\delta) & \beta.\dfrac{k.(r-\delta)}{r} \\ \tau & -(\mu+\delta+\rho) \end{bmatrix} \tag{32}$$

Характеристичните числа λ на матрицата с коефициентите на диференциалните уравнения (32) се изчисляват от следното уравнение

$$\det\begin{bmatrix} -(\tau+\delta)-\lambda & \beta.\dfrac{k.(r-\delta)}{r} \\ \tau & -(\mu+\delta+\rho)-\lambda \end{bmatrix} = 0, \tag{33}$$

откъдето се получава следното квадратно уравнение относно характеристичните числа λ на матрица (32)

$$\lambda^2 + (\tau+2\delta+\mu+\rho)\lambda + (\tau+\delta)(\mu+\delta+\rho) - \frac{\tau.\beta.k(r-\delta)}{r}. \tag{34}$$

За да се получат асимптотично намаляващи стойности на възлите от класове *E* и *I*, следва характеристичните числа да имат реални отрицателни стойности, което се постига в два случая, при $r<\delta$, а когато $r>\delta$ и при $(\tau+\delta)(\mu+\delta+\rho) \geq \dfrac{\tau.\beta.k(r-\delta)}{r}$, откъдето следва

$$\frac{\tau.\beta.k(r-\delta)}{r.(\tau+\delta)(\mu+\delta+\rho)} \leq 1. \tag{35}$$

Дясната част на неравенство (35) се означава с

$$R_0 = \frac{\tau.\beta.k(r-\delta)}{r.(\tau+\delta)(\mu+\delta+\rho)} \tag{36}$$

и определя базовия репродукционен брой от нови инфектирани компютърни възли, причинени от инфекция на предразположената към инфекция популация от компютърни възли в мрежата.

При $R_0<1$ злонамереният софтуер не може да въздейства върху мрежата, която остава асимптотически локално стабилна. При $R_0>1$ злонамереният софтуер атакува компютърната мрежа, която става нестабилна.

Решението на квадратното уравнение (34) има вида

$$\lambda_{1,2} = \frac{-(\tau+2\delta+\mu+\rho) \pm \sqrt{(\tau+2\delta+\mu+\rho)^2 - 4\left[(\tau+\delta)(\mu+\delta+\rho) - \dfrac{\tau.\beta.k(r-\delta)}{r}\right]}}{2} \tag{37}$$

Доминиращото характеристично число от сингулярното разложение на матрицата (32) определя динамиката на изменение на класовете *E* и *I*. При $t=t_0$ се регистрира максимум в класа *E* на експозиция на зловреден софтуер. При $t=t_1>t_0$ се регистрира максимум в класа *I* на инфекция при въздействие на зловреден софтуер.

5. Решение на системата от диференциални уравнения при неравновесно състояние на компютърната система

Поведението на компютърна мрежа, атакувана със злонамерен софтуер, представена с динамиката на възприемчивостта (susceptibility), S, експозицията (exposed) E, инфекцията I, възстановяването (Recovery) R на възлите на мрежата се изразява с диференциални уравнения от вида

$$\frac{dS}{dt} \neq 0\ ,\ \frac{dE}{dt} \neq 0\ ,\ \frac{dI}{dt} \neq 0\ , \tag{38}$$

което с отчитане на функционалната зависимост на параметрите на поведение на компютърната мрежа, S, E, I се записва чрез пълната системата от диференциални уравнения

$$\begin{aligned}
\frac{dS}{dt} &= r.S - (r.S).\left(\frac{S}{k}\right) - (\beta.I).S - \delta.S \\
\frac{dE}{dt} &= (\beta.I).S - (\tau + \delta).E \\
\frac{dI}{dt} &= \tau.E - (\mu + \delta).I - \rho.I \\
\frac{dR}{dt} &= \mathrm{Re\,c}(I) - \delta R
\end{aligned} \tag{39}$$

При $0 \le I \le I_{\min}$ системата от диференциални уравнения (39) се записва във вида

$$\begin{aligned}
\frac{dS}{dt} &= r.S - (r.S).\left(\frac{S}{k}\right) - (\beta.I).S - \delta.S \\
\frac{dE}{dt} &= (\beta.I).S - (\tau + \delta).E \\
\frac{dI}{dt} &= \tau.E - (\mu + \delta).I - \rho I \\
\frac{dR}{dt} &= \rho.I - \delta.R
\end{aligned} \tag{40}$$

б) при $I > I_{\min}$ системата от диференциални уравнения (39) се записва във вида

$$\frac{dS}{dt} = r.S - (r.S).\left(\frac{S}{k}\right) - (\beta.I).S - \delta.S$$

$$\frac{dE}{dt} = (\beta.I).S - (\tau + \delta).E \tag{41}$$

$$\frac{dI}{dt} = \tau.E - (\mu + \delta).I - m$$

$$\frac{dR}{dt} = m - \delta.R$$

Системите от уравнения (40) и (41) могат да бъдат обединени при условие $I = I_{\min}$, при което $m = \rho.I_{\min}$. При тези условия първото и четвъртото диференциални уравнения могат да бъдат решени по отделно.

Решението на първото диференциално уравнение, записано във вида

$$\frac{dS}{dt} = (r - \beta.I_{\min} - \delta).S - \frac{r}{k}.S^2 \tag{42}$$

се извършва в съответствие с решението на диференциалното уравнение на Bernoulli.

Прави се следната субституция

$$a = (r - \beta.I_{\min} - \delta),\ b = \left(-\frac{r}{k}\right), \tag{43}$$

при което уравнение (42) се записва във вида

$$\frac{dS}{dt} = S' = a.S + b.S^2 \tag{44}$$

Допуска се, че S = const, тогава лявата и дясна част на (44) се разделя на S, при което се получава

$$\frac{S'}{S^2} - \frac{a}{S} = b \tag{45}$$

Въвежда се нова функция $z = z(t)$ и определя нейната първа производна $z' = z'(t)$, т.е.

$$z = z(t) = \frac{1}{S} = S^{-1},\ z' = z'(t) = \frac{dz(t)}{dt} = -\frac{S'}{S^2}. \tag{46}$$

Уравнение (45) получава вида

$$z' + a.z = -b, \tag{47}$$

чието решение се записва по следния начин

$$z = \exp\left(\int a.dt\right)\left(C + \int b.\exp\left(\int a.dt\right)dt\right)$$

Като се отчете, че $S = z^{-1}$, решението на диференциалното уравнение за *S* се получава във вида

$$S = \frac{\exp\left(-\int a.dt\right)}{\left(C + \int b.\exp\left(\int a.dt\right)dt\right)} \tag{48}$$

Като се отчете, че *a* и *b* константни величини, решението на (48) може да се запише

$$S = \frac{\exp(-a.t)}{C + (b/a).\exp(a.t)} \tag{49}$$

При $t = 0,\ S(t_0) = S_0$, откъдето интеграционната константа се получава $C = (S_0)^{-1}$. За класа предразположени компютърни възли се получава следният израз

$$S(t) = \frac{E_0.e^{-a.t}}{1 + E_0.(b/a).e^{a.t}}, \tag{50}$$

където $a = (r - \beta.I_{\min} - \delta)$, $b = \left(-\frac{r}{k}\right)$.

Решението на четвъртото диференциално уравнение, записано във вида

$$\frac{dR}{dt} + \delta.R = m, \tag{51}$$

се решава в съответствие с решението на нехомогенни диференциални уравнения от първи ред при начални условия $R(t = 0) = 0$, което е сума от решението за свободната компонента и решението за принудителната компонента, т.е.

$$R(t) = R_0(t) + R_c \tag{52}$$

Първо, намира се решението на хомогенното диференциално уравнение, записано за свободната компонента R_0 на *R* във вида

$$\frac{dR_0}{dt} + \delta.R_0 = 0 \text{ или } \frac{dR_0}{R_0} = -\delta.dt, \tag{53}$$

откъдето след интегриране се получава

$$\ln R_0 = -\delta.t + C \text{ или } R_0(t) = C.e^{-\delta.t}, \tag{54}$$

където C е интеграционна константа, определяща се от началните условия за R.

Определя се принудителната компонента R_c на R от диференциалното уравнение

$$\frac{dR_c}{dt} + R_c = m. \tag{55}$$

По дефиниция свободният член на диференциалното уравнение е константна величина, т.е. принудителната компонента R_c е константна величина, т.е. $\frac{dR_c}{dt} = 0$. Тогава като резултат от (55) следва

$$R_c = m. \tag{56}$$

Изразите (54) и (56) се поставят в (52)

$$R(t) = C.e^{-\delta.t} + m. \tag{57}$$

При $t = 0$, $R(0) = 0$, откъдето $C = -m$.

Решението на нехомогенното диференциално уравнение получава вида

$$R(t) = m\left(1 - e^{-\delta.t}\right). \tag{58}$$

Изразът (58) описва динамиката на възстановяване на компютърните възли. Максималният брой компютърни възли от класа възстановени при $t \to \infty$ е m.

Намира се решението на съвместната система от второто и третото диференциални уравнения при известна времева зависимост на S, дефинирана с (50), която се записва във вида

$$\frac{dE}{dt} = \dot{E} = -(\tau + \delta).E + \frac{E_0.e^{-a.t}}{1 + E_0.b.e^{a.t}}.\beta.I, \tag{59}$$

$$\frac{dI}{dt} = \dot{I} = \tau.E - (\mu + \delta + \rho).I. \tag{60}$$

От уравнение (60) се определя E и $\dot{E}$ както следва

$$E = \frac{\dot{I} + (\mu + \delta + \rho).I}{\tau}, \ \dot{E} = \frac{\ddot{I} + (\mu + \delta + \rho).\dot{I}}{\tau} \tag{61}$$

Изразите (61) се заместват в (59), при което се получава

$$\ddot{I} + (\tau + \mu + 2.\delta + \rho).\dot{I} + \left[(\tau + \delta)(\mu + \delta + \rho) - \frac{\tau.\beta.E_0.e^{-a.t}}{1 + E_0.(b/a).e^{a.t}} \right].I = 0 \tag{62}$$

Характеристичното уравнение на (62) се записва във вида

$$\omega^2 + (\tau + \mu + 2.\delta + \rho).\omega + \left[(\tau + \delta)(\mu + \delta + \rho) - \frac{\tau.\beta.E_0.e^{-a.t}}{1 + E_0.(b/a).e^{a.t}} \right]. = 0 \tag{63}$$

За да се получат решения за E и I асимптотически намаляващи се при $t \to \infty$ следва да се удовлетворява условието

$$(\tau + \delta)(\mu + \delta + \rho) \geq \frac{\tau.\beta.E_0.e^{-a.t}}{1 + E_0.(b/a).e^{a.t}} \tag{64}$$

Решението на (63) има вида

$$\omega_{1,2} = \frac{-(\tau + 2\delta + \mu + \rho) \pm \sqrt{(\tau + 2\delta + \mu + \rho)^2 - 4\left[(\tau + \delta)(\mu + \delta + \rho) - \frac{\tau.\beta.E_0.e^{-a.t}}{1 + E_0.(b/a).e^{a.t}} \right]}}{2} \tag{65}$$

За решение на характеристичното уравнени (63) се избира коренът с по голяма абсолютна стойност, който се означава с $(-\omega)$.

Решението на диференциалните уравнения (60) се записва във вида

$$I = C.e^{-\omega.t}. \tag{66}$$

Интеграционната константа се определя от условие $C = I(0) = I_0 = I_{\min}$ при $t = 0$, т.е. $I = I_0.e^{-\omega.t}$

Замества се (66) в $E = \frac{\dot{I} + (\mu + \delta + \rho).I}{\tau}$ при което се получава

$$E = \frac{(\mu + \delta + \rho - \omega).C.e^{-\omega.t}}{\tau}. \quad (67)$$

Интеграционната константа се определя от условие $E = E(0) = E_0$ при $t = 0$, откъдето се получава

$$C = \frac{E_0.\tau}{\mu + \delta + \rho - \omega}. \quad (68)$$

Изразът в (67) се записва във вида

$$E = E_0.e^{-\omega.t}. \quad (69)$$

Изведените аналитични изрази за определяне на динамиката на основните процеси при въздействие на злонамерен софтуер могат да бъда използване за изграждане на симулационни модели на поведение на компютърните мрежи, на базата на които да се разработят защитни стратегии за противодействие.

6. Заключение

Приведени са основните диференциални уравнения, описващи състоянието на компютърната мрежа при въздействие със злонамерен софтуер. Получени са решения на диференциалните уравнения при равновесие на компютърната система и при отсъствие на равновесие на процесите на податливост, експозиция, инфектиране и възстановяване след атака със злонамерен софтуер. Приложени са оригинални решения на нехомогенните диференциални уравнения и системата от нехомогенни диференциални уравнения. Разработената методика за оценка на поведението на компютърна мрежа може да бъде приложена при априорно известен закон на въздействие, подчиняващо се, като правило, на разпределението на Poisson.

Литература

[1] Chapter 9 – Strategies of Computer Worms, 304543_ch09.qxd 1/7/05 9:05 AM, pp. 314-364 https://cdn.ttgtmedia.com/searchSecurity/downloads/Szor_Ch9.pdf.

[2] Z. Chen, Modeling and defending against Internet worm attacks, Doctor of Philosophy thesis, School of Electrical and Computer Engineering, Georgia Institute of Technology, May 2007.

[3] B. K. Mishra, Ap. Prajapati. Cyber Warfare: Worms' Transmission Model, International Journal of Advanced Science and Technology, Vol.63, (2014), pp.83-94, http://dx.doi.org/10.14257/ijast.2014.63.08

[4] A. F.Joseph, S. E Adewumi, Ih. Olalekan, K. Sunday. COMPUTER VIRUSES: A FRAMEWORK FOR MODELING INFECTION SUSCEPTIBILITY OF

WORKSTATIONS, December 2015Advances in Computer Science and Engineering 14(2):97-109, DOI: 10.17654/ACSEMay2015_097_109.

[5] Pr. Kumar T S, P V. Etrivelan, J. Mohan. Network Intrusion Detection and Prevention Systems on Flooding and Worm Attacks, In book: Combating Security Breaches and Criminal Activity in the Digital Sphere Chapter: Network Intrusion Detection and Prevention Systems on Flooding and Worm Attacks, Publisher: IGI GlobalEditors: Asnath Victy Phamila Y, S Geetha, June 2016, DOI: 10.4018/978-1-5225-0193-0

[6] L. Liu, R. K. L. Ko, G. Ren, X. Xu. Malware Propagation and Prevention Model for Time-Varying Community Networks within Software Defined Networks, Security and Communication Networks, Volume 2017, Article ID 2910310, 8 pages, https://doi.org/10.1155/2017/2910310

[7] K. Gowtham Sricharan, N. R. Kisore. Mathematical model to study propagation of computer worm in a network, 2015 IEEE International Advance Computing Conference (IACC), 12-13 June 2015, DOI: 10.1109/IADCC.2015.7154812.

[8] J.T. Bradley, St. Gilamore. Analyzing distributed Internet worm attacks using continuous state-space approximation of process algebra models, Journal of Computer and System Sciences 74 (2008) 1013–1032.

[9] Y. Tang, J. Luo, B. Xiao, G. Vei. Concept, Characteristics and Defending Mechanism of Worms, Special Section on Information and Communication System Security, IEICE Trans.. Inf.. & Syst., vol. E92–D, No 5, May 2009, http://www4.comp.polyu.edu.hk/~csbxiao/paper/2009/IEICE-2009-worm.pdf

[10] Stelios Sidiroglou, Angelos D. Keromytis. A Network Worm Vaccine Architecture, file:///C:/Users/adlaz/OneDrive/Documents/Computer%20Criminals/worm-vaccine.pdf

[11] S. U. M. Kamal, R. J A. Ali, H. K. Alani, E. S.Abdulmajed. Survey and brief history on malware in network security case study: viruses, worms, and bots, ARPN Journal of Engineering and Applied Sciences, VOL. 11, NO. 1, JANUARY 2016, pp. 683-698.

[12] M.Masthan et al, Detection and prevention of unknown vulnerabilities on enterprise IP networks International Journal of Computer Science and Mobile Computing, Vol.4 Issue.10, October- 2015, pg. 343-352.

[13] S. Souissi, A. Serhrouchni. AIDD: A novel generic attack modeling approach, International Conference on High Performance Computing, Simulation (HPCS), Jul 2014, Bologne, Italy. 2014, <10.1109/HPCSim.2014.6903738>. <hal01205824>

[14] Chapter 16 Attack Detection and Prevention, National Security Telecommunications Advisory Committee (NSTAC) Intrusion Detection Subgroup, [NetSec], WS 2006/2007. http://www.ccs-labs.org/~dressler/teaching/netzwerksicherheit-ws0607/16_AttackDetection-v2.pdf

[15] Puja Bajaj, Arjun Guha Roy. Source Code Analysis of Worms, http://www.micsymposium.org/mics_2004/Bajaj.pdf

[16] Paul Mueller and Babak Yadegari, The Stuxnet Worm, https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/ presentations/ topic9-final/report.pdf