5 https://astana.zagranitsa.com/article/3537/top10-prilozhenii-dlia-izucheniia-angliiskogo-iazyka-dlia-ios-i-android
6 https://sputnik.by/technology/20200222/1026832706/3-luchshih-prilozheniya-dlya-izucheniya-inostrannyh-yazykov.html

ОӘЖ 004

## DDOS ШАБУЫЛДАРДЫ АНЫҚТАЙТЫН ӘДІСТЕР МЕН ҚҰРАЛДАРДЫ ЗЕРТТЕУ

**Ж.Н. Манкошев**
Л.Н.Гумилев атындағы Еуразия ұлттық университеті, Нұр-Сұлтан қ., Қазақстан
Ғылыми жетекшісі - К.М.Сагиндыков

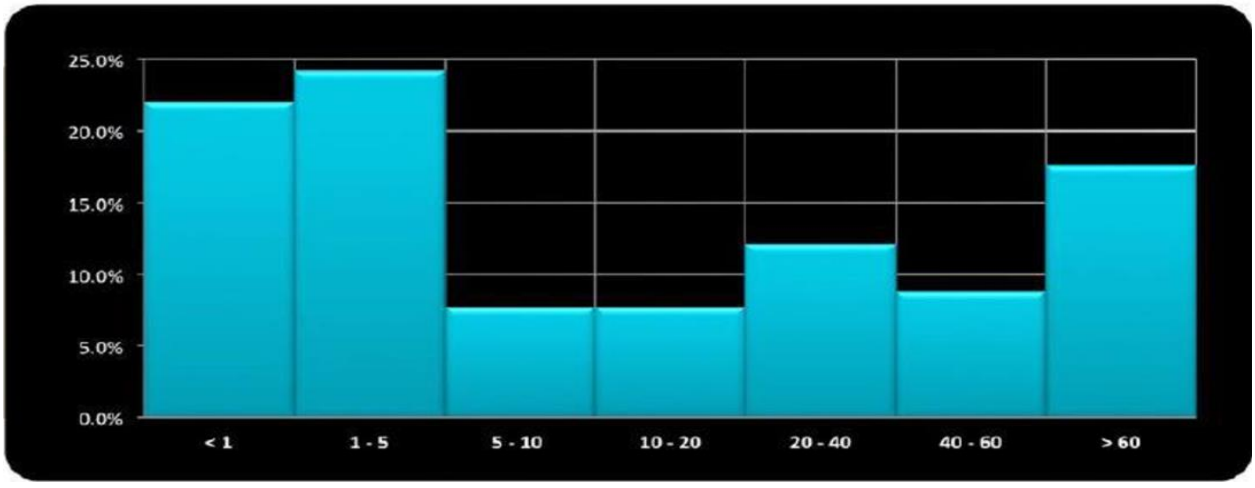
**Кіріспе**

Желілік шабуылдың мәні қаскүнемдердің немесе бағдарламалық қамтамасыз етудің соққы астына түскен құрылғыға зиян келтіруінен тұрады. Бағдарлама зиянын келтіруші рөлінде DoS-шабуыл құралдары, желілік құрттар, зиянды қосымшалар, бірқатар трояндық вирустар пайдаланылады. Шабуыл басталуын сәйкестендірудің және зиянды трафикті анықтаудың үлгілі нұсқасы жүйенің ағымдағы жағдайы оның қалыпты конъюнктурасымен салыстырған кезде аномалияны зерттеуге негізделген технология болып саналады. DDoS-шабуылдар аясында жүйе параметрлерінің картиналарын салыстыруды желі белсенділігінің әртүрлі сипаттамаларын салыстыру арқылы жүзеге асыру ұсынылады. Оларға: сан, сұраныстардың түсуінің түрі мен жылдамдығын және IP - адрестерді жатқызуға болады.

Зиянды технологиялардың түрлері және оларға қарсы әрекет ету әдістері.

Бүгінгі таңда ең көп таралған басып кіру нұсқасы HTTP немесе HTTP-flood түріндегі шабуылдар болып табылады. Олардың мазмұны көптеген HTTP-пакеттерді шабуылдайтын серверге жөнелтуден көрінеді. Мұндай шабуылдар сервердің жұмыс істеуінің іркілісіне де, байланыс арнасының өткізу жолағын асыра толтыруға да есептелуі мүмкін. Мысалы, зиянкестер сайттың әлуетті осал беттеріне шабуыл жасайды, яғни көптеген ресурстарды жұмсайтын скрипттер және көлемі жағынан үлкен берілетін жауаптар. Немесе заңды пайдаланушының әрекеттерін еліктеуге тырысады.

Келесі танымалдығы бойынша SYN-flood шабуылы (сур. 1.). Олар қосылысты орнату нәтижесінде "үштік қол алысу" нюанстарына негізделеді. Зомби-компьютерлер серверде "жартылай ашық қосылыстардан"кезек қалыптастыра отырып, жауап талаптарына назар аудармай, SYN-қосылуға сұраныстарды жібереді. Әдістеменің кең таралуы зиянды сұраныстарды анықтауға қабілетті пәрменді технологиялардың болмауымен түсіндіріледі.




Сурет 1.

UDP және TCP-flood түрінің шабуылдары UDP және TCP-пакеттердің жиынының шабуылданатын серверіне бағытталуымен көрсетіледі. Шабуыл анықталғаннан кейін сервер оны бейнелеуге кіріседі. Сервердің және желі учаскесінің жүктелуіне мұқият талдау жасау алдында трафикті сүзгілеу және ресурстарды шоғырландыру қарсы іс-қимылдың негізгі шаралары болып табылады. Мысалы, сервер штаттық режимде байланыс арнасының едәуір бөлігін пайдаланғанда, онда қауіп төнген жағдайда қылмыскер оны жойқын сұраныстармен толық жүктеуге тырысады. Сондықтан осы байланыс арнасында оның өткізу қабілетін алдын ала ұлғайтудың мағынасы бар. Егер Web-сервер шабуылдау бірлігі ретінде қарауды жалғастырса, онда деректер базасынан басқа, жоғары жүктемені веб-ресурстың өзі немесе онда орналасқан скрипттер жасай алады. Бұл жағдайда сервердің өзінің ресурстарын ұлғайту қажет: процессордың қуатын арттыру, қосымша жадты орнату және т.б. Немесе арнайы құралдар арқылы веб-серверді жеке кластерге бөлу. Мысалы, оны Apache және Nginx web-серверлерінің байланыстыруын пайдалану арқылы жасауға болады.

Ресурстарды арттырудан тұратын бұл әдістеме желілік шабуылдардан тамаша дәрі болмайды және қосымша кемшіліктерге ие:

- қуаттардың шоғырлануы дереу орындала алмайды, себебі ол аппараттық кешеннің трансформациясымен өзара байланысты;
- ресурстардың шекті саны ұзақ уақытты ұстап тұру тиімді емес, әсіресе шабуылдың нақты күні белгісіз болған жағдайда.

Осы әлсіз жерлерді еңсерудің жақсы ұсынылған нұсқасы қажет болған жағдайда қуатты шоғырландыруға мүмкіндік беретін бұлтты технологияларды қолдану болып табылады. Қазір көптеген хостинг-провайдерлер оларды ұсынылатын қызметтер тізіміне қосады. Клиенттер қажеттілігіне қарай белгілі бір уақытта оларға қажетті ресурстар санын алады. Мысалы, заңды пайдаланушылар саны күрт өскен кезде немесе зиянды сұраныстар саны өсуде, провайдер әрбір талапты өңдеуге мүмкіндік беретін резервтік қуаттарды ұсынады. Нәтижесінде сервер жұмысы бұзылмайды. Бұл тәсілдің маңызды кемшілігі оның қымбат болуы болып табылады. Клиент өз қалтасынан қосымша ресурстарды төлеуге тура келеді.

Шабуылдарды болдырмау мақсатын көздейтін әдістердің келесі тобы трафикті сүзумен байланысты болып табылады. Зиянды сұраныстарды бұғаттау сенімсіз және күдікті өңдеумен қатар, ресурстық базаны ұлғайтуда үнемдеуге мүмкіндік береді.

Сүзгілеу мақсатында трафикті талдаудың екі түріне негізделген кейбір бағдарламалық-аппараттық құралдар қолданылады: сандық және сапалық. Бұл құралдарды талдау негізіне кластерлік, мінез-құлық әдісі, математикалық статистика және ықтималдық теориясы әдісі, басқа да әдістер салынған.

Трафикті сүзу және қарсы әрекет өнімділігін арттыру үшін жұптасқан міндеттердің жұптарын шешу талап етіледі. Олардың бірі шабуылдың басталу фактісін іздестірумен, екіншісі зиянды трафик көзін сәйкестендірумен байланысты. Аталған міндеттерді шешудің дәлдігіне көбінесе қарсы іс-қимыл шараларының өнімділігі байланысты. Шабуылдың басталуын анықтауға байланысты екі тәсіл бөлінеді: теріс пайдалану фактілерін талдауға негізделген, сондай-ақ аномалияны зерттеуге негізделген. Бірінші тәсіл жүйенің ағымдағы жай-күйін сипаттайтын ақпаратты үлгі шабуылдарға тән ақпаратпен салыстыру арқылы анықтауды көздейді. Екіншісі ағымдағы жағдайды бағалау және қалыпты көрсеткіштермен салыстыру арқылы шабуылдарды анықтауды болжайды. Аталған тәсілдердің әрқайсысы кейбір кемшіліктермен сипатталады. Бірінші, мысалы, шабуылдардың жаңа түрлерін табу үшін тиімсіз. Тиімсіздік проблемасы DDoS-шабуылдардың контекстінің шеңберінде ерекше өткір болып отыр, өйткені зиянкестер нақты пайдаланушылардың іс-әрекетін симуляциялауға тырысады. Екіншіден, оны тиімді пайдалану үшін жүйенің жұмыс істеуінің қалыпты көрсеткіштері туралы айтуға мүмкіндік беретін статистика деректерін жинақтау талап етіледі. Осылайша, табудың өнімді жүйесін құру мақсатында екі тәсілді жиынтық пайдалану ұсынылады.

Мұндай жүйенің жұмыс істеу нәтижесінде оның жай – күйін сипаттайтын деректерді үздіксіз жинау, бұдан әрі-деректерді берілген модельдік параметрлерден айырмашылығы

мәніне өңдеу және талдау жүзеге асырылады. Шабуыл жасалған жағдайда зиянды трафик көзін анықтау тетіктері іске қосылады. Деректерді модельдермен салыстыруды әртүрлі әдістермен жүзеге асыруға болады.

Әсіресе қарапайым адамдардың арасында ережелер қағидаттарында іске асырылғанын атап өту керек. Мұндай қарапайым әдістердің мәні жүйенің қалыпты және аномальды жағдайын сипаттайтын кейбір ережелерді тапсырмада жатыр. Бұл ережелер жүйенің жалпы мінез-құлқы мен жай-күйін немесе жекелеген элементтердің мінез-құлқы мен жай-күйін (сұрау жиілігін, сұрау өрістерін және т.б.) сипаттай алады. Қолдану оңай болғанда, бұл әдістер өте тиімді.

Әсіресе кең таралған әдістердің жиынтығында сандық талдауға негізделгенін атап өткен жөн. Осы шартты топ жүктеменің ұлғаю белгісі бойынша шабуыл фактісін анықтау мақсатын көздейді:

1. MULTOPS - Алынған және жіберілген деректер пакеттерінің арақатынасын талдауға арналған.
2. MIB variables - Пакеттердің санын, олардың түрін және сұраныс санын есепке алуды жүргізуге арналған.
3. ACC - Әртүрлі ішкі желілерден пакеттер санын есепке алуды жүргізеді.
4. Network-Aware Clustering - Кіші желілер бойынша келіп түскен сұрау салуларды топтастырады және оларды салыстыруды жүзеге асырады.
5. Hop-Count Filtering - Дұрыс емес мекен-жайлары бар пакеттерді сүзу мақсатында секіру қашықтықтарын қосалқы желілерге дейін есепке алады.
6. Gateway Based - Деректерді ағынға бөледі.
7. D-Ward - Хаттамалар бойынша трафиктің заңдылығын тексеруді жүзеге асырады:

- TCP (TCP-ACK пакеттерінің саны);
- ICMP (ICMP пакеттерінің саны);
- UDP (олардың әрқайсысында қосылыстар мен пакеттер саны).

Перспективалы әдістердің арасында деректердің ықтималдық параметрлеріндегі өзгерістер бойынша ауытқуларды анықтауға негізделген. Мұндай әдістердің мәні күзетілетін жүйенің жай-күй параметрлерінің кейбір уақытша қатары алынады, содан кейін параметр мәні кейбір тарату заңы бойынша алынған кездейсоқ шамалар түрінде талданады. Осыдан кейін шабуыл фактісі бойынша үлестіруді ұсыну өзгерістерге ұшырайды (сонымен бірге жиынтықтың ықтимал параметрлері де өзгереді). Айта кету керек, бірнеше анықтау әдістері бар "өту нүктелері" (change-point detection) деп аталады.

Принципі іске асырылды:

- Active Distributed Defense System
- Improved D-Ward
- Source IP address monitoring
- SYN flooding CUSUM detection

Мысалы, бірінші IP кіріс қосылыстарының сандық өзгерістерін зерттейді. Қалғандары CUSUM әдісіне негізделген, бұл "өту нүктелерін"анықтай отырып, берілген параметрдің ауысуын итеративті бақылауға мүмкіндік береді. Мәні, кейбір уақыт аралығында қандай да бір параметрдің мәнін арттыру жағдайында қорғаныс шаралары іске қосылады. Сонымен, Improved D-Ward үшін мұндай параметр ретінде TCP пакеттердің көзінен алушының растау ағыны, Source IP address monitoring үшін жаңа IP саны, SYN flooding CUSUM detection үшін TCP SYN-FIN (RST) пакеттерінің қатынасы болады.

Деректерді алу (Data Mining) принциптерінде жұмыс істейтін әдістер аз таралған. Оларға өзін-өзі оқытатын жіктеуіштердің иерархиялық жүйелерін қолданатын әдістер жатады.

Модельдік ақпаратты қолданатын сипатталған жүйелердің көптігі екі функциялық режимдерге ие: оқыту және табу. Бүгінгі таңда аталған әдістерді практикалық енгізу мен қолданудың кейбір нұсқалары бар. Мысалы, ақпаратты есепке алу мен зерттеуді қорғалатын

серверге орнатылған бағдарламалық модульдер арқылы жүзеге асыруға болады. Бұл рөлді серверден тыс орналасқан ақпаратты талдау мен жинаудың физикалық құралдары да атқара алады. Мысалы, Cisco Guard жекелеген желілік сегменттерде орналасқан трафик талдағыштарымен ұштасқан бағдарламалық-аппараттық кешен болып табылады.

Қарсы іс-қимыл құралдарын орналастыруға келетін болсақ, оларды шартты түрде топтарға бөлу керек:

- зиянды трафик көзі желісінде;
- дерек көзі мен тағайындау желісі арасында;
- тағайындау желісінде

Қорғау құралдарының өнімділігі олардың жақындауы жағдайында, яғни көз желісіне тікелей жақын орналасқан жағдайда өседі. Осы аспектіде шабуылдарға қарсы іс-қимылдың әсіресе тиімді әдістерімен байланыс көзі желісіндегі трафикті бұғаттайды деп санауға болады. Айта кету керек, бұл әдістер интеграцияға байланысты ұйымдастыру міндеттерінің күрделілігіне байланысты аз дамыған. Бұл ретте қорғаныс құралдарын желіде орналастыру аз таралған, бұл толыққанды қорғауды ұйымдастырумен ұштасқан бірқатар шығындарға негізделген:

- бірінші деңгейдегі провайдерлердің кейбір санына қосылу қажеттілігі;
- шабуылдарды тәулік бойы көрсетуге дайын қызметкерлердің болу қажеттілігі;
- қорғау үшін ерекше жабдықты пайдалану қажеттілігі.

Шабуылдарды болдырмау және сүзу үшін жабдық тақырыбын қозғағанда, IBM жасаған Proventia Network IPS жүйесін атап өткен жөн. Бұл аппараттық және бағдарламалық құралдар кешенінің мынадай мүмкіндіктері бар:

- түрі мен деңгейіне қарамастан 200 хаттамадан бастап өңдеу;
- деректердің ағып кетуін бақылау;
- 3 мың астам аналитикалық алгоритмдерді пайдалану;
- IBM Proventia Desktop агенті арқылы корпоративтік желі шеңберінде өзара іс-қимыл жасайтын жүйелерді қорғауды қамтамасыз ету;

Шабуылдаушы желі ішінде қорғауға келетін болсақ, желі шекарасында емес, шабуылдаушы жүйе шеңберінде орналасқан әдістер мен құралдардың шартты кіші тобын атап өткен жөн. Дислокация нюанстарын ескере отырып, бұл құралдар массалық шабуылдарды көрсету үшін тиімділігі жоғары болып саналмайды. Мысалы, олар ірі шабуылдарды және олардың ішінен байланыс арнасын өткізу жолағын артық жүктеуді мақсат еткендерін нәтижелі етіп көрсете алмайды. Осы себепті мұндай құралдар әлсіз дамыған.

Осы контексте бағдарламалық құралдардың бірнеше тобын бөлеміз:

- шабуылданатын серверлердің операциялық жүйе деңгейінде жұмыс істеуі;
- бағдарлама деңгейінде жұмыс істеуі;

1. Біріншісіне - firewalls (файерволлдар) және ұқсас құралдар:

- Conlimit - Iptables үшін жасалған, *nix-жүйелерде қосылуды шектеуге мүмкіндік береді. Мысалы, шарт қою: бір мекенжайдан бір ғана қосылымнан артық емес.
- DDoS deflate - Conlimit аналогы, бұл лимиттер бұзылған жағдайда белгілі бір уақытқа қолжетімділікті шектейді.

2. Екінші топқа қосымшалар деңгейінде жұмыс істейтін құралдарды жатқызуға болады. Плагиндер, Модульдер (web серверлер, деректер қоры үшін):

- mod_evasive - Apache web-Сервері үшін жасалған. Берілген ережелер қатары бойынша блоктауды жүзеге асыруға мүмкіндік береді: мекенжай, сұраныстар саны қағидаты бойынша. Құлыптау ұзақтығын және басқа параметрлерді орнатуға болады.
- ngx_http_limit_zone_module - mod_evasive аналогы, бірақ Nginx web-Сервері үшін.

Аталған құралдардың жұмысының мәні белгілі бір ережелер жиынтығына сәйкес болу принципі бойынша блоктауда жатыр. Бұл ретте трафикті талдау жүргізілмейді. Басқаша айтқанда, бұл бағдарламалар бөлінген шабуылдарға қарсы іс-қимыл үшін тиімсіз.

**Қорытынды:** Қызмет көрсетуден бас тартуға бағытталған таратылған желілік шабуылдардың принциптері зерттелді. Сондай-ақ соңғы уақытта жүргізілетін кейбір DDoS-шабуылдарға мониторинг жүргізілді. Эксперимент нәтижелері кестеде көрсетілген.

| Жүйе | Жалған іске қосу, % | Анықталмаған зиянды сұраулар, % | Шабуылдың басталуы мен табылуы арасындағы орташа уақыт |
|---|---|---|---|
| Kaspersky Anti-Haker | 0,7 | 11 | 44 минут |
| Snort | 3,8 | 10,9 | 17 минут |
| Symantec | 4,3 | 8,4 | 12 минут |

**Қолданылған әдебиеттер тізімі**


1. DDOS атаки [Электронный ресурс]. — URL: http:// localname.ru/soft/ataki-tipa-otkaz-v-obsluzhivanii-dos-iraspredelennyiy-otkaz-v-obsluzhivanii-ddos.html.
2. Предотвращение атак с распределенным отказом в обслуживании (DDoS) [Электронный ресурс] / Официальный сайт компании Cisco. — URL: http:// www.cisco.com/web/RU/products/ps5887/products_white_ paper0900aecd8011e927_.html.
3. Методы защиты от DDOS нападений [Электронный ресурс]. — URL: http://www.securitylab.ru/analytics/216251.php.
4. Терновой О.С., Шатохин А.С. Снижение ошибки обнаружения DDOS атак статистическими методами при учете сезонности // Ползуновский вестник. — 2012. — №3/2.
5. Бенкен Е.С. PHP, MySQL, XML. Программирование для Интернета. — СПб., 2011.


ӘОЖ 004.454

## ТҮРЛІ ОПЕРАЦИЯЛЫҚ ЖҮЙЕЛЕР ДРАЙВЕРЛЕРІН ВЕРИФИКАЦИЯЛАУ ЖҮЙЕЛЕРІ


**Мухамедиева Лаура Сеилхановна**
*l-muhamedieva@mail.ru*
Л.Н.Гумилев атындағы ЕҰУ Информатика және ақпараттық жүйе магистранты, Астана, Қазақстан
Ғылыми жетекшісі – т.ғ.к., доц. Р.Д. Туребаева


Операциялық жүйе (ОЖ) драйверлерін верификациялаудың барлық жүйелері ОЖ ядросымен драйверлердің өзара әрекеттесу ережелерін бұзумен байланысты қателерді іздеуге арналған. Осыған байланысты, драйвердің арнайы ортасын дайындау қажет, бұл драйверді өңдеушінің шақыру тәртібіне қойылатын шектеулерді ескеруге мүмкіндік береді. Верификациялау үшін бағдарламаның еркін нүктесінің жетістіктерін тексеруге мүмкіндік беретін статикалық верификация құралдары қолданылады. Әр түрлі ОЖ ядросының модульдерін верификациялау процесін автоматтандыру үшін статикалық верификация жүйесі әзірленеді.

Операциялық жүйелердің драйверлерін верификациялаудың ең дамыған жүйесі *Microsoft Static Driver Verifier (SDV) жүйесі* болып табылады [1], ол Microsoft Windows операциялық жүйесінің драйверлерін статикалық верификациялауды жүргізуге асыруға мүмкіндік береді. Ол драйверлерді сертификаттау процесінде қолданылады және 2006 жылдан бастап Microsoft Windows Driver Developer Kit құрамына енгізілді. Microsoft SDV жүйесі нақты бағдарламаларды верификациялауды қолдану мүмкіндігін көрнекі көрсетеді.