Botnet trafikinin aşkarlanmasının bir üsulu haqqında

Gülnarə Qarayeva
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
qarayevagulnare@mail.ru

Xülasə-- **Botnet botmaster tərəfindən əmr və nəzarət zənciri vasitəsi ilə idarə olunan bot zərərverici proqramlarla yoluxmuş kompüterlər sistemidir. Botnet trafikinin normal trafikdən fərqləndirilməsi əsas problemlərdən biridir. Belə yanaşmalardan biri Netflow və IPFIX standartlarının verilənlərindən istifadə edərək botnet şəbəkə trafikinin aşkarlanmasıdır.**

Açar sözlər-- ***botnet, əmr və nəzarət kanalı, şəbəkə axını, Netflow, maşın təlimi***

I. GİRİŞ

Bu gün şəbəkə texnologiyalarının və informasiyanın təhlükəsizliyinin təmin olunması üsul və vasitələrinin yüksək səviyyədə inkişaf etməsinə paralel olaraq zərərverici proqram təminatı da sürətlə inkişaf etməkdə və yeni növləri yaranmaqdadır. Belə zərərverici proqram növlərindən biri bot zərərvericiləri və onlar əsasında qurulmuş botnetlərdir. Digər zərərli proqramlardan fərqli olaraq botnetlər istifadə olunan əmr və nəzarət *(ing. command and control, C&C)* kanalı vasitəsilə daim yenilənə bilir və aşkarlamaya qarşı daha dözümlü metodlar istifadə edirlər. Botnetlər həmçinin “ağıllı zombi ordular” da adlandırılırlar [1].

Botnetlər yarandıqları vaxtdan etibarən daim inkişaf etmiş, arxitekturaları, yayılma və əlaqə texnologiyaları, aşkarlanmaya qarşı istifadə etdikləri dözümlülük metodları da kifayət qədər təkmilləşmişdir. Müasir botnetlər domen adlarının dəyişdirilməsi *(ing. domen flux)*, IP ünvanların dəyişdirilməsi *(ing. IP flux)* və s. kimi DNS və şifrləmə texnologiyaları istifadə etməklə aşkarlama prosesini də çətinləşdirirlər [2]. Bütün bunlar botnetləri kibertəhlükəsizlik sisteminin əsas problemlərindən birinə çevirmişdir. Buna görə də onların daha yaxşı və hərtərəfli öyrənilməsi, bütün botnet növlərinə yönəlmiş aşkarlama üsullarının işlənməsi aktual problem olaraq qalmaqdadır.

Botnetlərin aşkarlanması üsullarının işlənməsi zamanı qarşıya çıxan əsas problemlərdən biri botnet şəbəkə trafikinin aşkarlanması üçün lazım olan axın verilənlərinin toplanmasıdır. Botnetlərin aşkarlanması üçün şəbəkə trafikinin monitorinqi aparılmalı və böyük ölçüdə verilənlər toplanmalıdır. Bu verilənlərin emalı üçün maşın təlimi *(ing. machine learning)* üsullarından istifadə edilir. Şəbəkə trafikinin monitorinqi və verilənlərin toplanması üçün istifadə olunan standartlardan biri Cisco Netflow formatıdır [3]. Netflow axın verilənləri bir çox zərərvericilərin, o cümlədən botnetlərin aşkarlanması üçün istifadə edilir və bir neçə belə aşkarlama üsulu işlənmişdir [4].

II. ŞƏBƏKƏ TRAFİKİNİNN MONİTORİNQİ

Şəbəkələrdə verilənlərin ötürülməsinə nəzarət və monitorinq üçün müxtəlif şəbəkə avadanlıq və tətbiq satıcılarının hazırladıqları standart protokollar mövcuddur. Bunlara misal olaraq Cisco Netflow (Cisco Inc, 2012), Juniper-jflow [5] (Juniper Networks Inc, 2011), Huawei-Netstream [6] (Huawei Texnologies Co Ltd, 2012), Alcatel-Cflow (Alcatel-Lucent Inc.,), Ericsson-Rflow (Ericsson Inc.) və s. göstərilə bilər. Şəbəkə trafikinə nəzarət və verilənlərin toplanması üçün istifadə olunan belə protokollardan ən məşhuru Netflow formatıdır. Netflow protokolu vasitəsilə şəbəkə isifadəçiləri, müxtəlif səviyyələrdə fəaliyyət göstərən şəbəkə protokolları və tətbiqləri, axın marşrutlayıcıları və s. haqqında məlumatları əldə etmək mümkündür. Hazırda istifadə olunan ən son versiyası Netflow v9 və onun eyni məqsədlə istifadə olunan digər protokollardan əsas fərqi şablon-əsaslı *(ing. template-based)* olmasıdır. Bu xüsusiyyət seçilmiş şablona görə eyni vaxtda müxtəlif tip axın məlumatlarını toplamağa imkan verir.

Netflow protokolu vasitəsilə nəzarət olunan marşrutlayıcılardan axın məlumatları toplanılır və bu informasiya Netflow axın toplayıcısında *(ing. Netflow Collector)* cəmlənir. Axın toplayıcısı bu verilənləri istifadəçi üçün daha rahat formata gətirir və təqdim edir.

Toplanmış Netflow verilənləri UDP (User Datagram Protocol) və ya SCTP (Stream Control Transmission Protocol) dəstəkli olur və aşağıdakı kimi əsas bilikləri özündə saxlayır [7, 8]:

- Netflow versiyasının nömrəsi;
- Paketin sıra nömrəsi (sequence number);
- Giriş və çıxış interfeysləri (SNMP dəstəkli);
- Axın ölçüsü və paket sayı;
- Axının başlaması və bitməsi haqqında məlumatlar;
- 3-cü səviyyə paket başlıqları (mənbə və hədəf IP ünvanlar və portlar, IP protokolu, xidmətin tipi və s.);
- 3-cü səviyyə marşrutlama məlumatları.

Netflow protokolu vasitəsilə toplanmış şəbəkə axın bilikləri bir çox zərərli proqramların, o cümlədən botnet şəbəkə trafikinin aşkarlanması üçün lazım olan bütün

DOI: 10.25045/NCInfoSec.2018.49

verilənləri özündə saxlayır. Xüsusilə, IETF (Internet Engineering Task Force) tərəfindən standartlaşdırılmış Netflow v9 digər versiyalardan şablon-əsaslı olması ilə fərqlənir. Şablonlar axın verilənlərinin formatını genişləndirməyə və baza axın formatını dəyişmədən paralel olaraq bir neçə şablona görə verilənləri toplamağa imkan verir.

III. BOTNET TRAFİKİNİN AŞKARLANMASI

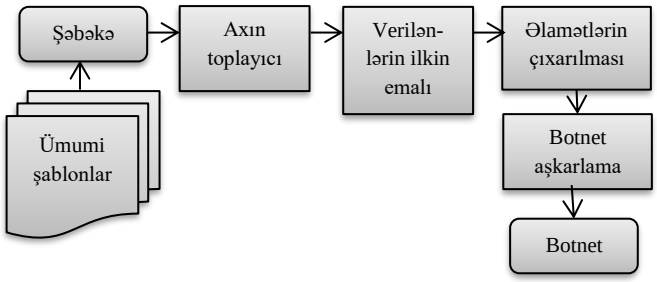
Bütün əvvəlcədən proqramlanmış sistemlərdə olduğu kimi botnetlər də fəaliyyət göstərdikləri müddətdə dövrü olaraq avtomatik alqoritmləri icra edirlər. Buna görə də botmasterlər fəaliyyətlərini təsadüfiləşdirmək üçün maksimum enerji sərf edirlər. Aparılan araşdırmalar göstərir ki, botnetləri aşkarlamaq üçün hələ də onları bir neçə standart sinifdə qruplaşdırmaq olar:

- IRC, HTTP və DNS-əsaslı botnetlərin əsas xarakteristik xüsusiyyəti C&C təlimatlar və botların bu təlimatlara necə cavab verməsidir.

- SpyEye [9] və Zeus botnetinin bir neçə versiyası botların aşkarlanması üçün siqnaturaların yaradılmasında istifadə oluna biləcək unikal axın davranışlarına malikdir.

- P2P botnetlərdə sorğu və təlimat kimi əlaqələr digər qanuni P2P əlaqələrdə olduğu kimi çox kiçik ölçüdə paketlərlə həyata keçirilir. Paketlərin ilkin mübadiləsinin vahid formatı var, bu da qanuni trafikdən asanlıqla fərqlənir.

İstənilən sinif botnetlərin aşkarlanmasında istifadə olunan əsas əlamətlər və xüsusi sinif botları aşkarlamaq üçün istifadə olunan xüsusi əlamətlər vardır. Mənbə və hədəf ünvanlar və portlar istənilən sinif botnetlərin aşkarlanması üçün ümumi xüsusiyyətlərdir. Netflow v9 verilənlərinin istifadə edilməsinin əsas üstünlüklərindən biri də ümumi obrazı dəyişmədən xüsusi sinif botları aşkarlayan obrazların qurula bilməsidir. Bu standart 3-cü səviyyədə fəaliyyət göstərən bütün tip qurğuları (switch və marşrutlayıcıları) dəstəkləyə bilir. Netflow verilənləri əsasında botnet trafikinin aşkarlanması üçün aşağıdakı kimi mərhələlərdən ibarət üsul təklif edilir.



Şəkil 1. Botnet şəbəkə trafikinin aşkarlanması modeli

A. Trafik axınının toplanması

Bot trafikinin aşkarlanması üçün üsulun işlənməsi zamanı əsas problemlərdən biri lazımi verilənlərin əldə olunmasıdır. Düzgün verilənlərin seçilməsi üsulun effektivliyinin artırılması üçün vacib amillərdən biridir. Belə biliklərin əldə edilməsi üçün birinci mərhələdə Netflow axın verilənlərinin toplanması həyata keçirilir. Bu məqsədlə xüsusi virtual test şəbəkəsi yaradılaraq axın məlumatları toplanılır. Botnet aşkarlamanın keyfiyyətini artırmaq üçün bir neçə maşın xüsusi bot proqramlarla yoluxdurulur, C&C server yaradılır və süni bot şəbəkəsi qurulur [10].

Ümumi şablonlar şəbəkə trafik axının toplanması üçün istifadə olunur. IPv4 və IPv6 axın verilənlərinin hər ikisi paralel olaraq toplanıla bilər. Axın mənbə və hədəf IP ünvan, mənbə və hədəf port, xidmət növü, IP protokol və interfeys kimi atributları saxlayan paketlər şəklində təyin olunur. Bu atributlar qəbul edilən paketin mövcud və ya yeni axına aid olduğunu müəyyənləşdirməyə imkan verir. Aşkarlamanın dəqiqliyinin yoxlanması üçün daha çox biliklərin toplanması əhəmiyyətlidir. Lakin atributların sayı artdıqca verilənlər bazasının ölçüsü də böyüyür. Bu problemi həll etmək üçün dəyişkən sahə ölçülərindən istifadə olunur [11].

Axın toplayıcı müxtəlif qurğular tərəfindən yaradılan trafik axın verilənlərini saxlamaq üçün istifadə olunur. Burada xüsusi proqram təminatı vasitəsilə axın verilənləri nizamlanır və istifadəçi üçün uyğun formatda təqdim olunur. Verilənlər trafikin tipinə, istiqamətinə, il, ay, vaxt və tarixə görə qovluqlarda saxlanıla bilər. Axın toplayıcı da verilənlərin sıxlaşdırılması, axtarılması və s. funksiyaları yerinə yetirir, lazımsız axının aradan qaldırılması və botnetlərin aşkarlanması alətlərinin istifadəsini yaxşılaşdırır.

B. Verilənlərin ilkin emalı

Süzgəcləmə prosesinin əsas məqsədi verilənlər bazasının ölçüsünü botnet trafiki ilə əlaqəsi olmayan axını ayırmaqla azaltmaqdır. Bu prosesin özü bir neçə mərhələdə aparılır və maşın təlimi üsullarından istifadə olunur. İlk addımda TCP və UDP protokollu axın seçilir. Bu onunla əlaqədardır ki, bir çox botnet sinifləri C&C əlaqə kanalı yaratmaq üçün məhz qanuni DNS trafikinə oxşar trafikdən istifadə edirlər.

Botnetlər status yoxlama, kodların yenilənməsi, əmrlərin verilməsi və s. əlaqələrdə adətən kiçik ölçülü paketlərdən istifadə edirlər. Halbuki, proqram təminatının yenilənməsi və qanuni P2P ötürmələr kifayət qədər böyük ölçülü axın yaradır. Bunu nəzərə alaraq böyük ölçülü verilənlər süzgəclənir. Bu zaman paketlərin ölçüsü və sayı qəbul edilmiş həddən böyük olan axın verilənləri bazadan çıxarılır.

C. Bot trafikin aşkarlanması

Botnetlərin aşkarlanması zamanı əsasən 3 tip davranışlar araşdırılır: bot davranışları, botnet davranışları və müvəqqəti davranışlar. Bot davranışları dedikdə, yalnız bir botun C&C əlaqələri və ya hücum cəhdləri araşdırılır. Botnet davranışları dedikdə, qrup şəklində botlar tərəfindən yaradılan axın müəyyənləşdirilir. Müvəqqəti davranışlar isə hər hansı vaxt ərzində bot və ya botlar tərəfindən yaradılan trafikin analizi nəticəsində aşkarlanır.

IRC, HTTP, P2P və hybrid botnetlərin araşdırılması nəticəsində məlum olmuşdur ki, bütün botnet sinifləri fəaliyyətləri dövrünün müxtəlif fazalarında müxtəlif davranış xüsusiyyətlərinə malikdirlər. [12] İlkin yoluxma fazasında botmasterlər yoluxdurulacaq qurğuların boşluqları yoxlayır və bu işi bütün fəaliyyət dövründə vaxtaşırı təkrarlayır. Mərkəzləşmiş arxitekturada bu birbaşa bot-server tərəfindən həyata keçirilirdisə, P2P botnetlər üçün botlar arasında yayılma vasitəsilə mümkün olur. Botlar daim yeni “qurbanlar” üçün axtarış edir, kiçik ölçülü paketlərdən istifadə etməklə botnetin ölçüsünü genişləndirməyə çalışırlar.

Təkrar yoluxma fazasında yoluxmuş qurğunun idarəsini tamamilə ələ keçirmək üçün zərərli proqramlar yüklənir və bot öz C&C serveri ilə botnetə üzv olmaq üçün əlaqə saxlayır. Əlaqə və yeniləmə fazalarında bot, serverdən gələcək hücum və ya digər zərərli fəaliyyətlərin koordinantlarını gözləyir, onları yerinə yetirir, yeni qurğuların yoluxdurulması ilə məşğul olur, aşkarlama və neytrallaşdırma cəhdlərinə qarşı dözümlülüyü artırmaq üçün botmasterlər tərəfindən bot zərərvericiləri yenilənir.

Birbaşa C&C əlaqəli IRC və HTTP botnetlərdə botlar bot-serverlə, P2P və hibrid arxitekturada isə öz *proxy* botları ilə əlaqə saxlamağa çalışırlar. Aşkarlamadan yayınmaq və DNS və ya IP ünvanlarını gizlətmək üçün C&C serverlər öz əlaqələrində domen flux, IP flux kimi texnologiyalardan istifadə edirlər. Həmçinin bəzi botnetlər zərərli tapşırığın yerinə yetirilməsi haqqında daim hesabat verirlər. Məsələn, Zeus botnetində hər 20 dəqiqədən bir botlar avtomatik yoxlanılır və yenilənir.

Botnetlər zərərli fəaliyyətlərin növündən asılı olaraq da müxtəlif davranış xüsusiyyətlərinə malik olurlar. DDoS hücumlar zamanı şəbəkədə naməlum ünvanlara yönəlmiş TCP Syn paketlərin aktivliyi müşahidə olunur , bu da obrazın qurulması zamanı onların sayının nəzərə alınmasını tələb edir. Spam e-mail göndərilməsi zamanı isə xarici mail serverlər istifadə edilərək böyük ölçüdə məktublar göndərilir. Belə ki, şəbəkədə qeyri-adi SMTP aktivlik botların aşkarlanması üçün əsas ola bilər.

Bütün bu davranış xüsusiyyətləri botnetlərin aşkarlanması üçün obrazların qurulmasında aparıcı rol oynayır [13]. Botnetin bütün fəaliyyəti dövründə, müxtəlif davranış əlamətlərinə görə ümumi obrazın qurulması üçün maşın təlimi üsullarından istifadə olunur. Müxtəlif maşın təlimi üsullarının tətbiqi nəticəsində məlum olmuşdur ki, botnetlərin növündən və fəaliyyət məqsədindən asılı olaraq tətbiq olunan üsul da dəyişir. Məsələn, qərar ağacları *(ing. Decision Tree)* klasifikatoru P2P botnetlərin aşkarlanması üçün axın intervallarına görə, SVM və Bayes şəbəkələri HTTP və IRC əsaslı mərkəzləşmiş botnetlərdə C&C əlaqələri aşkarlamaqda daha effektiv nəticə əldə etməyə imkan verir.

IV. EKSPERİMENTLƏRİN NƏTİCƏLƏRİ

Eksperimentlərin aparılması üçün CTU-13 verilənlər bazasından 7-ci ssenari üzrə toplanmış verilənlər seçilmişdir. CTU-13 verilənlər bazası 2011-ci ildə Çexiya Texniki Universitetində *(ing. Czech Technical University, CTU)* botnet, normal və arxa fon trafikin birlikdə ssenari adlanan 13 bazada toplanması ilə yaradılmışdır. Hər bir ssenari üzrə xüsusi protokol istifadə etməklə xüsusi zərərli fəaliyyətlər həyata keçirən müxtəlif bot proqramlardan istifadə olunmuşdur.

Hər ssenari üç tip trafikin paketlərindən ibarət olub nişanlanmış və *.pcap* fayllarda toplanmışdır. Axınlar biristiqamətli və ikiistiqamətli NetFlow şəbəkə verilənlərindən ibarətdir. İkiistiqamətli verilənlərin istifadəsi bir çox səbəbdən daha məqsəduyğundur. Çünki, klient və serverləri fərqləndirir, axın haqqında daha çox informasiya saxlayır və daha detallı sinifləndirmə aparmağa imkan verir.

CTU-13 verilənlər bazasının fərqləndirici xüsusiyyətlərindən biri də bütün ssenarilər üzrə bazaların əllə analiz olunması və nişanlanmasıdır. Nişanlanma prosesi NetFlow fayllarının daxilində aparılmışdır və hər bir ssenari Arxa fon, Botnet, C&C kanal və Normal trafik olaraq adlandırılmışdır [14].

Bazadakı hər bir ssenari müxtəlif formatlı fayllar şəklində işlənmişdir, lakin gizlilik problemləri baxımından bütün verilənləri özündə saxlayan *pcap* faylı yoxdur. Buna baxmayaraq digər fayllar əlçatandır və aşağıdakı kimi tərkibə malikdir:

- ***.pcap*** genişlənməli yalnız botnet axından ibarət fayl;
- ikiistiqamətli ***.biargus*** genişlənməli bütün tip axın verilənlərini özündə saxlayan NetFlow faylları;
- orijinal icra oluna bilən fayl.

Nişanlanmış NetFlow verilənlər faylı bir çox axın əlamətləri ilə xarakterizə olunur (cədvəl 1).

CƏDVƏL 1. NETFLOW AXIN ƏLAMƏTLƏRİ

Say	Əlamətin adı	Əlamətin izahatı
1	StartTime-EndTime	Axının başlama və bitmə vaxtı (tarix, vaxt)
2	Duration	Axının davametmə müddəti (mksan)
3	Protocol	İstifadə olunmuş protokol (tcp, udp, ıcmp və s.)
4	Source IP Addres	Mənbə IP ünvan
5	Source port	Mənbə port
6	Direction	Axın istiqaməti (<-, <->, ->)
7	Destination IP Addres	Çatdırılma IP ünvan
8	Destination port	Çatdırılma port
9	State	Axın statusu (CON, FSPA və s.)
10	Source ToS	Mənbə xidmət tipi (0,1)
11	Destination ToS	Çatdırılma xidmət tipi (0,1)
12	Total Packets	Axın tərkibindəki paketlərin sayı
13	Total Bytes	Axın tərkibindəki baytların sayı
14	Source Bytes	Mənbədən çatdırılma ünvana kimi

		baytların sayı
15	Label	Sinif (Background, Normal, Botnet və s.)

7-ci ssenari üzrə verilənlər 22 dəqiqə ərzində toplanmış və ümumi ölçüsü 5.8 Gb-dır. Verilənlərin ilkin emalı mərhələsində TCP və UDP protokollu axınlardan başqa digər protokol axınları filtrlənmişdir. Eksperimentlər üçün bazadan 65 botnet və 65 normal axın verilənləri seçilmişdir. IP ünvan verilənləri kodlanmış və onluq formata çevrilmişdir. Analizlər nəticəsində məlum olmuşdur ki, bazadakı əlamətlər daha yaxşı sinifləndirmə aparmaq üçün kifayət etmir. Daha yaxşı nəticələrin əldə edilməsi üçün iki yeni əlamət çıxarılmışdır: nisbi paket faizi və nisbi bayt faizi. Nisbi paket faizi axındakı paketlərin ümumi sayının *(Total Packets)*, axının davametmə müddətinə *(Duration)* nisbəti kimi təyin edilir və müxtəlif zaman intervallarında ötürülən paketlərin orta qiymətini müəyyən etməyə imkan verir.

Nisbi paket faizi= Total Packets/ Duration

Nisbi bayt faizi isə ötürülən axındakı baytların ümumi miqdarının, axının davametmə müddətinə nisbəti kimi hesablanır.

Nisbi bayt faizi=Total Bytes/ Duration

BayesNet (Bayes şəbəkələri), NaiveBayes, SVM (Dəstək vektor maşınları), Random Tree (Təsadüfi ağaclar) və Random Forest (Təsadüfi meşələr) maşın təlimi üsullarının tətbiqi ilə aparılan təcrübələrin nəticələri aşağıdakı cədvəldə göstərilmişdir (cədvəl 2). Üsulların qiymətləndirilməsi üçün üç meyar (Recall, Precision, F-Measure) istifadə olunmuşdur.

Cədvəl 2. Klassifikatorların müqayisəsi

Qiymətləndirmə meyarları	**Klassifikatorlar**				
	BN	**NB**	**SVM**	**RT**	**RF**
Recall (%)	100	98,5	99,2	93,1	100
Precision (%)	100	98,5	99,2	93,2	100
F-measure (%)	100	98,5	99,2	93,1	100

Recall (tamlıq) klassifikatorun müsbət sinfin bütün obyektlərindən hansı hissəsini tapdığını göstərir:

$$Recall = \frac{TP}{TP + FN}$$

Precision (dəqiqlik) – klassifikatorun müsbət adlandırdığı və həqiqətən də müsbət olan obyektlərin nisbi sayıdır:

$$Precision = \frac{TP}{TP + FP}$$

F-measure (F-ölçü) dəqiqlik və tamlığın harmonik ortasıdır:

$$F - measure = 2\frac{precision \times recall}{precision + recall}$$

Burada, TP – doğru klassifikasiya olunan müsbətlərin sayı, TN – doğru klassifikasiya olunan mənfilərin sayı, FP – səhv klassifikasiya olunan müsbətlərin sayı, FN – səhv klassifikasiya olunan mənfilərin sayıdır.

NƏTİCƏ

Aparılan araşdırmalar belə qənaətə gəlməyə imkan verir ki, bot şəbəkələr fəaliyyəti dövrlərinin bütün fazalarında, istifadə etdikləri əlaqə və nəzarət kanalının tipinə, həyata keçirdikləri zərərli fəaliyyətin növünə və s. görə müxtəlif davranış xüsusiyyətlərinə malik olurlar. Botnet davranış əlamətlərindən istifadə etməklə, Netflow axın verilənlərinin və maşın təlimi üsullarının tətbiqi ilə daha effektiv aşkarlama üsullarının işlənməsi mümkündür. Məqalədə belə bir üsulun ümumi modeli verilmişdir.

ƏDƏBİYYAT

[1] Y.N. İmamverdiyev, G.B. Qarayeva, “Botnetlər və onların aşkarlanması üsulları,” İnformasiya texnologiyaları problemləri, №1, s. 100–111, 2017.

[2] R. Sharifnya, M. Abadi, “DFBotKiller: Domain-flux botnet detection based on the history of group activities and failures in DNS traffic,” Digital Investigation, Vol. 12, pp. 15-26, March 2015.

[3] Cisco Inc 2012, Introduction to Cisco IOS® NetFlow, <http://www.cisco.com/c/en/us/products/collateral/ios-nx-ossoftware/ios netflow/prod_white_paper.

[4] J. Francois, S. Wang, R. State, & T. Engel, “BotTrack: Tracking Botnets Using NetFlow and PageRank,” 2011.

[5] Juniper Flow Monitoring, J-Flow on J Series Services Routers and Branch SRX Series Services Gateways, www.juniper.net/us/en/local/pdf/app-notes/3500204-en.pdf

[6] NetStream (Integrated) Technology White Paper, Huawei Technologies Co., Ltd. , 2012.

[7] D. Zhao, I. Traore, B. Sayed, W. Lu, S. Saad, A. Ghorbani, & D. Garant, 'Botnet detection based on traffic behavior analysis and flow intervals, Computers & Security, vol. 39, Part A, no. 0, pp. 2-16, 2013.

[8] W.T. Strayer, D. Lapsely, R. Walsh, & C. Livadas, “Botnet Detection Based on Network Behavior,” W Lee, C Wang & D Dagon (eds), Botnet Detection, Springer US, vol. 36, pp. 1-24, 2008.

[9] A. K. Sood, R.J. Enbody, & R. Bansal, “Dissecting SpyEye – Understanding the design of third generation botnets,” Computer Networks, vol. 57, no.2, pp. 436-50, 2013.

[10] U. Wijesinghe, U. Tupakula, V. Varadharajan, “An enhanced model for network flow based botnet detection,” Proceedings of the 38th Australasian Computer Science Conference, 2015.

[11] C. Livadas, R. Walsh, D. Lapsley. W. T. Strayer, “Using Machine Learning Techniques to Identify Botnet Traffic,” Internetwork Research Department, BBN Technologies.

[12] D. Andriesse, C. Rossow, B. Stone-Gross, D. Plohmann, & H. Bos, 2013, “Highly resilient peer-to-peer botnets are here: An analysis of Gameover Zeus,” 8th International Conference on Malicious and Unwanted Software, pp. 116-123, 22-24 Oct. 2013.

[13] Tarng, W., Den L-Z, Ou K-L & Chen M. “'The analysis and identification of P2P botnet's traffic flows”, International Journal of

Communication Networks and Information Security (IJCNIS), vol. 3, no. 2, pp. 138-148, 2011.

[14] P.Kalaivani, M.S.Vijaya. Mining Based Detection of botnet traffic in Network Flow. IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol. 6, No 1, pp. 535-541, Jan-Feb 2016.

ABOUT ONE METHOD OF BOTNET TRAFFİC DETECTİON

Gulnara Garayeva
Institute of Information Technology of ANAS,
Baku, Azerbaijan
qarayevagulnare@mail.ru

Abstract - Botnet is a system of infected computers controlled with the command and control chain by botmaster. One of the main problems is to distinguish between botnet traffic and normal traffic. One such approach is to detect botnet network traffic using Netflow and IPFIX standards.

Keywords- botnet, command and control channel, network flow, Netflow, machine learning