UOT 004.056

İmamverdiyev Y.N.[1], Qarayeva G.B.[2]
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]yadigar@lan.ab.az, [2]qarayevagulnare@mail.ru

BOTNETLƏRLƏ MÜBARİZƏDƏ YANAŞMALARIN ANALİZİ

Botnetlər zərərli proqramlarla yoluxdurulmuş və uzaqdan idarə edilən kompüterlərin şəbəkəsidir. Son dövrlər botnetlərin miqyasının sürətlə artması, onların istifadə olunduqları kibercinayətkarlıq məqsədləri və səbəb olduqları maddi və qeyri-maddi zərərlər onlarla kompleks mübarizənin vacibliyini göstərir. Məqalədə botnetlərlə mübarizənin istiqamətləri və iştirakçı tərəfləri araşdırılmış, beynəlxalq, milli, ictimai və fərdi səviyyələrdə botnetlərlə mübarizəyə yanaşmalar analiz olunmuşdur.

Açar sözlər: *botnet, kibertəhlükəsizlik, kiberfəza, İnternet xidməti provayderləri, botnetlərlə mübarizə təşəbbüsləri.*

Giriş

Botnetlər botmasterlər tərəfindən xüsusi zərərli proqramlarla – botlarla yoluxdurulmuş kompüterlərin şəbəkəsidir. Bu proqramlar kompüterləri uzaqdan idarə etmək üçün yoluxdurur və botmasterlərə onları özlərinin təhlükəli və qeyri-qanuni məqsədləri üçün istifadə etməyə imkan verir. Buraya paylanmış xidmətdən imtina hücumları (*ing. Distributed Denial of Service, DDoS*), spam göndərilməsi, informasiya oğurluğu və s. kimi kifayət qədər təhlükəli hərəkətlər daxildir. Yoluxmuş kompüterlərin sayı və dəyən maddi ziyan botnet təhlükəsinin ölçüsünü xarakterizə edir.

Botnetlərin sayının sürətlə artmasına səbəb genişzolaqlı İnternet xidmətlərinin çeşidlərinin artması və zərərli proqram təminatının yaradılmasında yeni istiqamətlərin inkişafıdır. Bu da kriminal fəalliyyətin artmasına şərait yaradır. Zərərli proqramların törətdiyi hadisələr nəticəsində dəyən zərər milyonlarla ABŞ dolları ilə ölçülür. Bu da botnetlərlə mübarizənin vacibliyini bir daha aktuallaşdırır. Botnetlərlə mübarizəyə müxtəlif aspektlərdən – fərdi, ictimai, iqtisadi, milli, regional və beynəlxalq səviyyədə yanaşmalar mövcuddur [1]. 2007-ci ildə Estoniya [2], 2008-ci ildə Gürcüstan, 2009-cu ildə isə İrana qarşı törədilmiş botnet əsaslı kiberhücumlar milli təhlükəsizlik baxımından botnetlərlə mübarizənin əhəmiyyətini bir daha sübut edir. Bu da birbaşa dövlətlərin kibertəhlükəsizlik siyasətləri ilə əlaqədardır [3].

Bu gün dövlətlər kiberfəzaya maliyyə köçürmələrindən hərbi əməliyyatlara qədər bütün sahələrdə etibar edirlər. Lakin İnternet təhlükəsizlik üçün deyil, sürətli məlumat mübadiləsi üçün yaradılmışdı. Son illərdə həyata keçirilən kiberhücumların məqsədi və ölçüsü bu sahədə beynəlxalq əməkdaşlığın vacibliyini göstərir [4].

Botnetlərlə mübarizənin bu və ya digər səviyyəsində, birbaşa və ya dolayı olaraq iştirak edən maraqlı tərəflər vardır. Bunlar qanunverici və hüquq-mühafizə orqanları, İnternet provayderləri, kibertəhlükəsizlik həllərinin vendorları, elmi-tədqiqat institutları və tədqiqatçılar, İnternet istehlakçıları və son istifadəçilərdir. Botnetlərlə mübarizə məqsədilə beynəlxalq və dövlətlər səviyyəsində bir çox işçi qrupları yaradılmış, qabaqcıl təcrübə və tövsiyə kodeksləri hazırlanmış, qanunvericiliklə dəstəklənən layihələr həyata keçirilmişdir. Lakin botnet təhlükəsi hər gün artmaqda davam edir. Bu da botnet iqtisadiyyatının gətirdiyi gəlir və botnet idarəçilərinin çox az hallarda cinayət məsuliyyətinə cəlb olunması ilə bağlıdır [5].

Bütün bunlara baxmayaraq, dünyanın bir çox inkişaf etmiş və inkişaf etməkdə olan ölkələrində həyata keçirilən mübarizə tədbirləri botnetlərin gələcəkdə sayının və vurduğu ziyanın azalacağına olan inamı artırır.

Botnetlərlə mübarizənin əsas aspektləri

Botnetlərlə mübarizə tədbirlərinin istiqamətini müəyyənləşdirmək üçün əvvəlcə onların cari vəziyyəti ilə bağlı problemlər öyrənilməlidir [6]. Botnetlərlə bağlı əsasən aşağıdakı problemlər vardır:

Hazırda mövcud olan botnetlərin real sayının dəqiq təyin edilməsi. Belə ki, real botnetlərin sayı haqqında söylənilən rəqəmlər həqiqətə uyğun deyil və onlar elmi şəkildə əsaslandırılmır, eləcə də botnetlərin səbəb olduğu təhlükələri qiymətləndirməsi üçün onların sayı yeganə faktor deyildir.

Botnet təhlükəsinin qiymətləndirilməsi üçün əməkdaşlığın vacibliyi. Uzaqdan idarə edilə və yenilənə bilən zərərli bot proqramları botnetlərin coğrafi əhatə dairəsini də sürətlə genişləndirir. Buna görə də, coğrafi regionlar arasında müxtəlif sahələrdə (informasiya, təcrübə və tövsiyə kodeksləri və s. kimi) əməkdaşlığın həyata keçirilməsi məqsədəuyğundur.

Mövcud qanunvericiliyin yetərsizliyi. Xüsusilə Avropa Birliyinə üzv ölkələrin kibercinayətkarlıq haqqında qəbul etdiyi müxtəlif məzmunlu sənədlər botnetlərlə mübarizənin də effektivliyini artırır. Lakin buna baxmayaraq, bötnetlərin hazırkı miqyası hələ də belə sənədlərin beynəlxalq səviyyədə yetərsizliyini göstərir [7, 8].

Bundan əlavə, qlobal botnetin ən yaxşı həlli dövlətlər, texniki və qanunverici təşkilatlar arasında beynəlxalq əməkdaşlıqla bağlıdır. Beynəlxalq əməkdaşlıq strategiyasının effektiv işləməsi üçün iştirakçı tərəflər arasında möhkəm siyasi dəstək olmalıdır. Buraya hücumlar haqqında etibarlı hesabatlar, məlum təhlükələr haqqında əsaslı informasiya, kibercinayətkarlara qarşı onların həbsinə imkan verəcək dəlil və sübutlar və s. daxildir.

Botnetlərlə mübarizənin aşağıdakı əsas istiqamətləri vardır [6]:

1. Mövcud botnetlərin sayının və təsirinin azaldılması. Botnetlərin sayının azaldılması məqsədilə aşağıdakı kimi tədbirlərin həyata keçirilməsi vacibdir:

- yoluxmuş kompüter sahiblərinin botun təmizlənməsi prosesinin bütün mərhələlərində şərtsiz dəstəklənməsi;
- botnetlərin monitorinqi və aşkarlanması prosesinin, zərərli proqramların analizinin inkişaf etdirilməsi;
- botnetlərin məhv edilməsi cəhdlərinin davam etdirilməsi;
- botnetlərin azaldılması prosesinin iştirakçı tərəfləri arasında informasiya mübadiləsinin təşkili;
- kibercinayətkarlığa qarşı qanunların beynəlxalq səviyyəyə uyğunlaşdırılması;
- botnetləri məhvetmə prosesinin bütün botnet infrastrukturu aşkarlanana qədər davam etdirilməsi.

2. Yeni yoluxmaların qarşısının alınması. Botnetlərlə yeni yoluxmaların qarşısının alınması tədbirlərinin həyata keçirilməsi vacibdir. Buraya aşağıdakı kimi tədbirlər daxildir:

- botnetlərin yayılması sürətini azaltmaq məqsədilə yoluxmanın ilkin mərhələsində aşkarlama;
- ictimai maarifləndirmə tədbirlərinin həyata keçirilməsi;
- əməliyyat sistemlərində boşluqların aradan qaldırılması;
- sistem təhlükəsizliyinin artırılması və s.

Botnetlərlə mübarizə prosesində proqram istehsalçılarının iştirakı və istifadəçilərin maarifləndirilməsi ilə botla yoluxmanı ləngitmək və ya qarşısını tamamilə almaq olar.

3. Botnetlərin istifadəsindən əldə edilən gəlirlərin azaldılması. Zərərli proqramların istifadə olunmasının səbəblərindən biri də əldə olunan maddi gəlirlərdir. Əks-tədbirlər ilk növbədə kibercinayətkarlıqdan və xüsusən də, botnetlərdən əldə edilən gəlirlərin azaldılmasına yönəldilməlidir. Bu məqsədlə:

- zərərli proqramların istifadəsinə qanunvericilikdə təsbit edilmiş qadağaların qoyulması;
- ictimai maarifləndirmə və s. tədbirlər həyata keçirilməlidir.

Hazırda botnetlərin sürətlə yayılmasına təsir edən aşağıdakı kimi faktorlar vardır:

- fərdi kompüterlərin zərərli bot proqramları ilə asan və ucuz yoluxdurulması;

- botnetlərin fəaliyyətindən əldə olunan gəlirin kifayət qədər cəlbedici olması;
- botmasterlərə qarşı tətbiq olunan cəza sanksiyaları ehtimalının az olması.

Botnetlərlə mübarizənin iştirakçı tərəfləri

Botnetlərin azaldılması və məhv edilməsində maraqlı olan, birbaşa və ya dolayı olaraq bu prosesdə iştirak edən tərəflər vardır [8]:

1) ***Qanunvericilik və hüquq-mühafizə orqanları*****.** Dövlətin kibertəhlükəsizlik siyasətini formalaşdıran qanunvericilik orqanları və hüquq-mühafizə orqanları botnetlərlə mübarizədə mühüm yer tuturlar. Qanunvericilik orqanlarının vəzifələri aşağıdakı kimidir:

- milli səviyyədə mövcud qanuni sənədləri müasirləşdirmək və kibercinayətkarlığın müxtəlif aspektləri ilə məşğul olmaq üçün praktik əsas yaratmaq;
- botnetləri azaltma prosesini və beynəlxalq səviyyədə əməkdaşlığı yaxşılaşdırmaq üçün mövcud qanunları uyğunlaşdırmaq və ya yeni sənədlər qəbul etmək;
- əməkdaşlıq çərçivəsində üzv dövlətlər arasında öhdəlik və rolları dəqiq təyin edən əlaqələrin yaradılmasını təmin etmək və s.

2) ***Kibertəhlükəsizlik həllərinin vendorları (antivirus firmaları və s.).*** Botla yoluxmanın qarşısının alınması, həmçinin botların təmizlənməsi prosesinin həyata keçirilməsini təmin edən proqram təminatı istehsalçıları botnetlərin azaldılması prosesinin maraqlı tərəflərindən biridir.

3) ***Akademik qurumlar (elmi-tədqiqat institutları və s.).*** Uyğun səlahiyyət verilmiş tədqiqat institutları botnetlərlə mübarizədə daha effektiv nəticələr əldə etməyə imkan verirlər. İşlənmiş aşkarlama üsulları mürəkkəb təhlükələrin azaldılması və yeni yaradılmış təhlükələrlə mübarizədə yararlı alət olmalı, araşdırmaların nəticələrinin nəşr edilməsi və yayılması məsul qurumlar tərəfindən təşkil olunmalıdır.

4) ***İnternet xidməti provayderləri*** **(*ing. Internet Service Provider, ISP*).** ISP-lər botnetlərin aşkarlanması və azaldılması prosesində "açar" rolunu oynayırlar. Bir çox ölkələrdə ISP milli mübarizə təşəbbüsləri mövcuddur. ISP-lər ümumilikdə aşağıdakı problemləri həll edə bilərlər [9]:

- son istifadəçilərin zərərli proqramlarla yoluxmasının qarşısının alınması;
- mülki səviyyədə kibertəhlükəsizlik üzrə maarifləndirmənin artırılması;
- aşkarlama üçün vacib olan məlumatların asan əldə edilməsinin təmin olunması;
- son istifadəçilərin uzaqdan idarə edilən yoluxma haqqında xəbərdar edilməsi və s.

5) ***İnternet istehlakçıları və son istifadəçilər*****.** Botnetlərlə mübarizənin bütün səviyyələrində son istifadəçilər bu və ya başqa şəkildə iştirakçıya çevrilirlər. Botnetlərin yayılması prosesinin iştirakçıları olan istifadəçilər, həm də ən çox maddi və mənəvi zərər çəkən tərəflər kimi çıxış edirlər. Buna görə də botnetlərin azaldılmasının maraqlı tərəflərindən biri də son İnternet istehlakçılarıdır.

Botnetlərlə mübarizə təşəbbüsləri

Botnetlərlə mübarizə problemlərinə qlobal (regional), milli (dövlətlər), ictimai (sosial), iqtisadi və fərdi səviyyələrdə həllər axtarılır.

Qlobal mübarizə təşəbbüsləri

Kiberfəzanın qlobal və regional səviyyədə hər hansı pozulmaları ən ağır nəticələrlə müşahidə olunur. Regional və ya qlobal səviyyədə siyasi əməkdaşlıq vacib olduğu kimi, kiber əməkdaşlıq da vacibdir. Belə ki, kiber-infrastrukturun regional stabilliyi iqtisadi və siyasi münasibətlərin stabilliyinə əsaslanır. Bu səviyyədə mübarizə mexanizmləri beynəlxalq təşkilatlar, dövlətlər, İKT sektoru ilə əlaqəli maraqlı tərəflər və s. tərəfindən formalaşdırılmalı və hər hansı qlobal müdaxilə ilə mübarizənin idarə edilməsinə zəmanət verməlidir [10, 11].

Qlobal botnet təhlükəsinin artması ilə əlaqədar olaraq bir çox əməkdaşlıq təşəbbüsləri milli və beynəlxalq səviyyədə işə başlamış və mövcud təşkilatlar bu sahədəki fəaliyyətlərini intensivləşdirmişdir. Bu təşkilatların əsas məqsədi botnetlərlə mübarizə fəaliyyətlərini sürətləndirmək üçün müxtəlif təşkilatlar arasında inam əlaqələrinin yaradılması və qorunması,

kritik informasiya və biliklərin mübadiləsi prosesinin sadələşdirilməsi və bütün tərəflər arasında səlahiyyətlərin tənzimlənməsidir.

Botnetlərlə mübarizədə ilk belə beynəlxalq təşəbbüs 2007-ci ildə ITU (*ing. International Telecommunication Union, Beynəlxalq Telekomunikasiya Birliyi*) tərəfindən yaradılmış Botnet Mitigation Toolkit layihəsidir [12]. Bu layihə ümumilikdə botnet təhlükəsini xarakterizə edir və müxtəlif səviyyələrdə − siyasi, texniki və sosial aspektlərdə problemin həlli üçün tövsiyələri təmin edir:

- Siyasi aspekt kiber-cinayətkarlıqla mübarizə üzrə qanunvericilik sənədlərinin yayılmasını, iştirakçı tərəflər arasında əməkdaşlığı dəstəkləyir, istifadəçinin gizliliyi və təhlükəsizlik arasında balansı təmin edir;
- Texniki aspektdə botnetlərin aşkarlanması İnternet xidməti provayderlərinin, domen adlarının qeydiyyatı prosesinə və qeydiyyatçılarına nəzarətin, botnetlərin azaldılması prosesində iştirak edən maliyyə institutlarının rolu aydınlaşdırılır;
- Nəhayət, sosial aspekt istifadəçilərin maarifləndirilməsi işinin təşkili və vizual media istifadə etməklə onların daha da əlçatan olmasını təmin edir, həmçinin təhlükəsizlik proqram təminatının yayılması və vaxtaşırı yenilənməsi işini təşkil edir.

Botnetlərlə mübarizədə qlobal standartlaşma sahəsində işlər CYBEX (*ing. Cybersecurity Information Exchange Framework*) mübadilə standartı ilə tənzimlənir [13]. Standart müxtəlif kibertəhlükəsizlik təşkilatları arasında eyni səviyyədə əlaqələrin yaradılmasına, yaranmış səhvlərin aradan qaldırılmasına xidmət edir. Botnetlərin aşkarlanması sahəsində müxtəlif maraq dairələrinə aid məlumatlar toplanır və strukturlaşdırılır. Təşkilatlar arasında mübadilə maneələrinin aradan qaldırılması, xidmət və resursların asan tapılması məqsədilə unikal obyekt identifikatoru istifadə edilir.

Könüllü işçi qruplar

Botnetlərlə mübarizədə bir sıra təşkilatlar tərəfindən yaradılmış könüllü işçi qruplarının da böyük rolu vardır. Belə qruplardan biri OECD (*ing. Organisation for Economic Co-operation and Development, İqtisadi Əməkdaşlıq və İnkişaf Təşkilatı*) tərəfindən 2010-cu ildə fəaliyyətə başlamış WPISP (*ing. Working Party on Information Security and Privacy, İnformasiya təhlükəsizliyi və gizlilik üzrə işçi qrupu*) könüllü işçi qrupudur [14]. WPISP beynəlxalq səviyyədə işləyən mübadilə platformasıdır. Qrupun maraq dairəsinə zərərli proqramlar, kibertəhlükəsizlik siyasəti, kritik informasiya infrastrukturlarının qorunması kimi məsələlər daxildir.

Qrup xüsusilə ISP-lərin botnetlərin azaldılması və dövlətlərin İnternetin sabitliyi və təhlükəsizliyinin artırılması sahəsindəki rolunu analiz edir. Qrupun beynəlxalq səviyyədə həyata keçirdiyi təlimləri, dövlət-özəl sektor tərəfdaşlığı sahəsində fəaliyyəti qənaətbəxş hesab edilir.

Conficker, Mariposa və Waledac kimi kifayət qədər təhlükəli botnetlərin məhv edilməsində iştirak etmiş könüllü hədəf işçi qrupların rolu da qeyd olunmalıdır. "Conficker işçi qrupu" 2008-ci ildə Conficker bot zərərli proqram təminatı ilə yaradılmış botnetə qarşı mübarizəyə başlamışdır, daha effektiv və koordinasiya edilmiş əks-tədbirlər üçün bir neçə beynəlxalq institut və təşkilat arasında əməkdaşlığı əlaqələndirmişdir [15, 16].

2009-cu ilin mayında Mariposa botnetinin aşkarlanmasından sonra Corciya Texnologiya İnstitutunun İnformasiya Təhlükəsizliyi Mərkəzi, Panda Security, Neustar, Directi və bir neçə anonim təhlükəsizlik tədqiqatçısı tərəfindən "Mariposa işçi qrupu" yaradılmışdı [17, 18]. Məhz bu qrupun fəaliyyəti və əməkdaşlığı nəticəsində botnet çökdürüldü, hətta botmasterləri və zərərli bot proqramının yaradıcılarını məsuliyyətə cəlb etmək mümkün oldu.

B49 əməliyyatı adı ilə Waledac botnetinə qarşı mübarizə aparan "Waledac işçi qrupu" Mannheim Universiteti, Vyana Texnologiya Universiteti, Bonn və Vaşinqton Universitetlərinin əməkdaşlığı nəticəsində botnetin aşkarlanmasına nail olunmuşdur [19]. Son botnet çökdürülmələri isə Çin milli CERT-i (*ing. Computer Emergency Response Team*) tərəfindən həyata keçirilmişdir.

Botnetlərlə milli səviyyədə mübarizə təşəbbüsləri

Hazırda kibertəhlükəsizlik siyasətinin əsasını milli sərhədlər daxilində tətbiq olunan təhlükəsizlik tədbirləri təşkil edir. Təəssüfedici haldır ki, bir çox dövlətlər kiberfəzanı əsl kibermüharibə məkanına çeviriblər və bu işdə botnetlərin imkanlarından istifadə etməkdən çəkinmirlər. Bunun nəticəsidir ki, beynəlxalq səviyyədə mübarizə cəhdləri yalnız bir neçə dövlət və ya region səviyyəsində məhdudlaşır.

Kiberfəzadakı ən məşhur konfliktlərdən biri hər hansı ölkənin kritik infrastrukturlarına fiziki müdaxilə ilə yanaşı kibermüdaxilələrin də həyata keçirilməsidir ki, burada ən böyük problem kibercinayətkarların tapılmasıdır. Xüsusilə real müharibə şəraiti olduqda və botnetlərin imkanlarından istifadə edildikdə bu məsələ daha da çətinləşir. Bu da dövlətlərin kibertəhlükəsizlik siyasəti ilə yanaşı beynəlxalq səviyyəli mübarizə təşəbbüslərinə qoşulmasını vacib edir [20, 21].

Botnetlərlə mübarizədə dövlətlər səviyyəsində tətbiq olunan və kifayət qədər effektiv nəticələr əldə etməyə imkan verən yanaşmalar mövcuddur. Botnetlərlə mübarizədə ən yaxşı təcrübəyə malik ölkələrdən Almaniya, Hollandiya, Yaponiya, Cənubi Koreya, ABŞ, Avstraliya, Braziliya, Ruminiya və s. misal göstərmək olar.

Almaniya

Almaniyada Anti-Botnet Kömək Bürosu Almaniya İnformasiya Təhlükəsizliyi Agentliyi (*ing. German Federal Office for Information Security (BSI)*) və İnternet Sənayesi Assosiasiyasının (*ing. Association of the German Internet Industry*) əməkdaşlığı və dəstəyi ilə fəaliyyətə başlamışdır [22, 23]. Büronun yaradılmasının əsas məqsədi Almaniyanı ən çox botnet yaradılan 10 ölkə siyahısından çıxarmaq idi. Hal-hazırda da işini davam etdirən mübarizə layihəsi bir çox ölkə üçün təcrübə örnəyi rolunu oynayır. ISP əsaslı informasiyaya əsaslanan botnet təmizləmə prosesi 3 mərhələdə həyata keçirilir:

1. Yoluxmuş kompüterlər spam-tələlər (*ing. spamtrap*) və ya honeypotlar vasitəsilə dolayı olaraq təyin edilir;
2. Yoluxmuş kompüter istifadəçiləri ISP-lər tərəfindən müxtəlif yollarla (e-mail, ənənəvi poçt və s.) xəbərdar edilir. Xəbərdarlıq yoluxmuş zərərli proqram haqqında ümumi informasiyadan, bu zərərli proqramı təmizləmək üçün lazım olan proqram təminatına linkdən və məxfi nömrədən ibarətdir;
3. Məxfi nömrə vasitəsilə istifadəçilər əlavə interaktiv dəstək əldə edə bilərlər. Həmçinin bu səviyyədə qazanılmış biliklər sonrakı təcrübə üçün toplanılır.

Fəaliyyət göstərən layihə Almaniyada sürətlə artmaqda olan ISP-lər, İT təhlükəsizlik və sosial şəbəkə servisləri arasında əlaqələndirici rolunu oynayır, lakin əsas problem bu ölkədə mövcud olan kifayət qədər sərt gizlilik və fərdi informasiyanın qorunması qanunlarıdır ki, bu da əlaqələrin kontent səviyyəsində izlənməsinə imkan vermir. Yalnız spam-tələlərin və "bal küpələrinin" (*ing. honeypot*) tətbiqi ilə aşkarlama texnologiyaları nəzərdə tutulur.

Hollandiya

2009-cu ildə Hollandiya İnternet bazarının 98%-dən çoxunu əhatə edən 14 ISP-nin əməkdaşlığı nəticəsində botnetlərlə mübarizə üçün yeni bir layihə hazırlanmışdır [24]. Mübarizə layihəsi üzv ISP-lər arasında yoluxmuş sistemlər haqqında informasiya mübadiləsinə və ən yaxşı təcrübə kodekslərinə əsaslanır. Layihə müştəri xəbərdarlıq sistemi, mübarizə üsulları haqqında dəstək və aşkarlanmış sistemlərin təmizlənməsi xidmətlərindən ibarətdir.

Avstraliya

2005-ci ildə Avstraliya Kommunikasiyalar və Media Agentliyi tərəfindən ölkədə yoluxmuş kompüterlərin sayının azaldılması məqsədilə Avstraliya İnternet Təhlükəsizliyi Təşəbbüsünə start verildi [25, 26]. Təşəbbüs Avstraliya CERT-i tərəfindən hazırlanmış ən yaxşı təcrübə kodeksinə əsaslanır. Proqramın könüllü olmasına baxmayaraq, 2005-ci ildən indiyədək qoşulmuş ISP-lərin sayı 6-dan 100-ə yüksəlib. Layihənin əsas ideyası zərərli proqram təminatı və hərəkətlər haqqında istifadəçilərin bilik səviyyəsinin artırılması, yoluxmuş qurğuların məsafədən müəyyən edilməsi və

məsul şəbəkə provayderlərinin xəbərdar edilməsidir. Şəbəkə provayderi tərəfindən istifadəçi verilənlərinin qorunması və daha çox zərərin qarşısının alınması məqsədilə yoluxmuş qurğunun İnternetə girişi məhdudlaşdırılır. Daha sonra uyğun proqram təminatı vasitələri ilə botun təmizlənməsi prosesi həyata keçirilir. Həmçinin şübhəli hallar haqqında müvafiq tədbirlərin görülməsi üçün məsul dövlət agentliklərinə hesabat verilir.

Amerika Birləşmiş Ştatları

2012-ci ildə ABŞ Rabitənin Təhlükəsizliyi, Etibarlılığı və Əməkdaşlıq Şurası (*ing. Communications Security, Reliability and Interoperability Council*) tərəfindən botnetlərin sayının azaldılması məqsədilə ISP-lər üçün könüllü proqram olan anti-botnet tövsiyələr kodeksi (*ing. U.S. Anti-Bot Code of Conduct for ISPs*) hazırlanmışdır [27]. Kodeks İnternetdə daha etibarlı mübadilə üçün şəbəkə təhlükəsizliyi və xidmət təminatçıları ilə son istifadəçilər arasında əməkdaşlığı və bu işdə ISP-lərin rolunu aydınlaşdırır. Botnetlərə qarşı mübarizənin effektivliyini artırmaq üçün kodeks İnternet mühitində bütün maraqlı tərəflərin – antivirus və təhlükəsizlik vendorları, proqram və texniki təminat istehsalçıları, domen adı qeydiyyatçıları, son istifadəçilər, İT-departamentlər, veb-sahibkarlar və s. arasında əməkdaşlığı nəzərdə tutur. Kodeks könüllü xarakter daşıyır və iştirakçı ISP-lərin əsas vəzifələri aşağıdakı kimi müəyyən edilir:

- ***Maarifləndirmə.*** Botnet təhlükəsi və ondan qorunma yolları haqqında istifadəçilərin məlumatlandırılması;
- ***Aşkarlama.*** ISP-lər səviyyəsində bot fəaliyyətlərinin aşkarlanması;
- ***Xəbərdarlıq.*** İstifadəçilərin yoluxma şübhəsi və ya yoluxma baş verdiyi hallarda bu haqda məlumatlandırılması;
- ***Təmizləmə.*** Yoluxmuş qurğu istifadəçilərinə botun təmizlənməsi üçün kömək göstərilməsi və ya bu işdə birbaşa iştirak edilməsi;
- ***Əməkdaşlıq.*** Digər iştirakçı ISP-lər arasında informasiya mübadiləsi və vaxtaşırı məlumatlandırmanın təmin edilməsi.

Yaponiya

2006-cı ildə Yaponiyada botnetlərə qarşı mübarizə üçün Kiber Təmizləmə Mərkəzi (*ing. Cyber Clean Center, CCC*) yaradılmışdır və hal-hazırda fəaliyyət göstərir. Qurumun fəaliyyəti dövlət səviyyəsində dəstəklənir və bir neçə institut və təşkilatın əməkdaşlığı nəzərdə tutulur [28]. Ölkədəki İnternet xidmətlərinin təqribən 90 %-nə məsul olan 70-dən çox ISP layihəyə qoşulmuşdur. Layihənin iştirakçıları 3 əsas qrupda birləşirlər:

- Bot əks-tədbir sisteminə məsul Telekommmunikasiya İnformasiya Mübadiləsi və Analiz Mərkəzi;
- Bot proqramlarının analizinə məsul JP-CERT (Yaponiya milli CERT-i);
- Botla yoluxmadan qorunmaq üçün istifadəçilərin maarifləndirilməsinə məsul İnformasiya Texnologiyalarının Təşviqi Agentliyi (*ing. Information Technology Promotion Agency, IPA*).

Cənubi Koreya

Koreyaya qarşı törədilmiş DDoS hücumların və yoluxmuş kompüterlərin sayının artması ilə Koreya İnternet Təhlükəsizliyi Agentliyi (*ing. Korean Internet Security Agency, KISA*) və Koreya milli CERT-i tərəfindən geniş anti-botnet kampaniyası başlamışdır [29, 30]. Mübarizə yanaşması 3 əsas hissədən ibarətdir:

- Şübhəli sorğu və əlaqələri qeydə alan xüsusi ixtisaslaşmış DNS (*ing. Domain Name System*) serverlər istifadə edilərək yoluxmuş qurğular təyin edilir. Daha geniş məlumat isə zərərli proqramların analizi və müdaxilələrin aşkarlanması sistemlərinin hesabatından əldə edilir.
- KR CERT mərkəzi DNS idarəetmə servisindən istifadə etməklə botnetlərin aşkarlanması və azaldılması prosesini həyata keçirir. Zərərli məqsədlər üçün istifadə olunan domen adlar asanlıqla gizlədilə və dəyişdirilə bilər (*ing. sinkholed*). Bunun üçün də xüsusi DNS

Resurs yazıları (*ing. DNS Resource Records*) vasitəsilə aldatma məqsədilə istifadə olunan domen adları və IP ünvanlar qeydiyyata alınır.

- Botnetləri azaltma cəhdlərini tamamlamaq üçün KR-CERT, ISP-lər və İT-vendorları yoluxmuş istifadəçilərin xəbərdar edilməsi və sistemin təmizlənməsinin təmin edilməsi üçün əməkdaşlıq həyata keçirirlər.

Bundan əlavə, İnternetlə bağlı təhlükəsizlik insidentləri zamanı müraciət üçün elektron çağrı mərkəzi (118) xidmət göstərir.

Braziliya

Braziliya milli CERT-i bir çox ölkələrin təcrübəsinə əsaslanaraq botnetlərin azaldılması layihələri həyata keçirir. Layihə çərçivəsində bir neçə nazirlik, İT agentliyi, ISP-lər, qeyri-hökumət təşkilatları, akademik qurumların birgə əməkdaşlığı təşkil olunur [31]. Əsas məqsəd kiberinfrastrukturun təhlükəsizliyinin artırılması, botnet əsaslı fəaliyyətlərin və botnetlərin azaldılmasıdır. Əsasən aşağıdakı 3 istiqamətdə fəaliyyət həyata keçirilir:

1) İnsidentlər haqqında məlumat toplanması (statistik məlumatlar, dəstək və s.);
2) Təlim və maarifləndirmə tədbirlərinin təşkili (kurslar, sənədlər, təqdimatlar və s.);
3) Şəbəkə monitorinqinin aparılması (paylanmış honey-pot və spam-potlar).

İctimai (sosial) mübarizə təşəbbüsləri

Kibertəhlükəsizlik həllərinin üçüncü səviyyəsi İnternetdə zərərli fəaliyyətlərə qarşı ictimai münasibətin yaradılmasıdır. Bu gün ən çox tətbiq olunan üsullardan biri olan sosial mühəndislik insanlar arasında inamın azalmasına, sosial fərdlər və ya qruplar arasında dezinformasiyanın yayılmasına, kiberterrorizmin artmasına səbəb olmuşdur. Sürətlə inkişaf edən informasiya və kommunikasiya texnologiyaları sosial əlaqələrin həcmini artırır və bununla yanaşı olaraq sosial şəbəkələrdən identifikatorların oğurlanması halları da artmaqdadır. Sosial şəbəkə və platformalarda xüsusilə botnetlərin imkanlarından istifadə edərək mədəni, dini və ya etnik hücumların həyata keçirilməsi məlumdur.

Sosial səviyyədə kibertəhlükəsizliyin inkişaf etdirilməsi üçün sosial platformaların imkanlarından istifadə edərək daha çox kütləyə çata bilən sosial maarifləndirmə kampaniyalarının təşkili əhəmiyyətli yer tutur. Bunun üçün dövlətlər və beynəlxalq səviyyədə həyata keçirilən dövlət-özəl sektor tərəfdaşlıq qruplarının fəaliyyəti vacibdir.

Belə fəaliyyət qruplarından biri 2009-cu ildə Avropa Komissiyası tərəfindən yaradılmış Avropa Dövlət Özəl sektor Tərəfdaşlıq (*ing. European Public Private Partnership for Resilience, EP3R*) təşkilatıdır [32]. Yanaşmanın məqsədi dövlət və özəl sektordan olan tərəflər arasında hökümətlər səviyyəsində əməkdaşlıq çərçivəsi yaratmaqdır.

Fərdi səviyyədə mübarizə

Kibertəhlükəsizlik həllərinin həyata keçirildiyi sonuncu səviyyə zərərli fəaliyyətin artması və yayılmasında birbaşa iştirak edən kompüter istifadəçilərinə fərdi səviyyədə yanaşmadır. Bir çox kiber-hücumlarda fərdlər bu və ya digər formada zərərçəkən qismində iştirak edirlər, gündəlik həyatlarına təsir edən xidmətlərin pozulmasına, şəxsi məlumatlarının konfidensiallığının və ya tamlığının pozulmasına, əlyetərlik problemlərinə məruz qalırlar. Xüsusilə, botnetlərin yaradılması və fəaliyyəti prosesinin bütün mərhələlərində istifadəçilərin imkanlarından sui-istifadə edilir. Fərdi səviyyədə maarifləndirmə tədbirləri həyata keçirmədən kibertəhlükəsizlik həllərinin digər səviyyələrdə uğurlu fəaliyyətindən danışmaq olmaz.

Botlarla yoluxma prosesinin 90%-dən çoxu məhz fərdi kompüter istifadəçilərinin səhlənkarlığı və ya yoluxma metodları haqqında məlumatsızlığı səbəbindən baş verir ki, bu da həmin istifadəçiləri bot "qoşun"unun "əsgər"inə çevirir. İstifadəçilərin maarifləndirilməsi prosesinə, botnetlər haqqında məlumatlar, onların təhlükələri, fəsadları, yoluxmanın istifadəçi səviyyəsində aşkarlanması üsulları və s. daxildir. Demək olar ki, bütün qeyd olunmuş beynəlxalq və milli mübarizə cəhdləri fərdi səviyyədə tədbirləri də müəyyən dərəcədə nəzərə almağa çalışır.

Lakin bütün bunlar müasir kiberfəzadakı real vəziyyətlə müqayisədə yetərsiz qalır və daha çox fərdi maarifləndirmə tədbirlərinin keçirilməsinə ehtiyac vardır. Bu iş xüsusilə dövlətlərin kibertəhlüksizlik siyasətlərinin əsas aspektlərindən biri olmalıdır.

Botnetlərlə mübarizənin ümumi xarakteristikası

Botnetlərə qarşı müxtəlif səviyyələrdə həyata keçirilən əks-tədbirlərin effektivliyinin qiymətləndirilməsi üçün əvvəlcə müvəffəqiyyət meyarları müəyyən olunmalıdır. Mübarizə yanaşmalarının keyfiyyətinin ölçülməsi üçün aşağıdakı kimi meyarlar nəzərdə tutulmuşdur [6]:

1) Botmasterin C&C infrastruktura giriş imkanının və botnetin məhdudlaşması səviyyəsi;
2) Botnet daxilində fəaliyyət göstərən botların dəqiq sayının müəyyənləşdirilməsi, bu sonrakı təmizləmə işlərinin həyata keçirilməsi üçün vacibdir;
3) Botmasterlərin gəlir mənbəyinin müəyyənləşdirilməsi, ən yaxşı halda bot yaradıcıların və botnet sifarişçilərinin məsuliyyətə cəlb olunması.

Botnetlərin C&C mərkəzinin bağlanması botnetlərin azaldılması üçün əsas müvəffəqiyyət sayıla bilər, lakin nəzərə almaq lazımdır ki, botlar hələ də yoluxmuş haldadır. Bu zaman yalnız botmasterin botnetə girişi məhdudlaşmış olur. Deməli, C&C serverin aşkarlanması, problemi yoluxmuş qurğular səviyyəsində həll etmir.

Zərərli bot proqramlardan təmizlənməmiş qurğular təkrar yeni botnetlərə cəlb edilə bilər. Botnetlərin azaldılması cəhdlərinin müvəffəqiyyətinin qiymətləndirilməsi yoluxmuş qurğuların təmizlənməsi ilə birbaşa əlaqəlidir. Lakin bəzən bu da effektiv nəticə vermir, çünki eyni bir qurğu bir neçə botnetin tərkib hissəsi ola bilər.

Bundan başqa, aşkarlanmamış və ya məhv edilməmiş bir C&C serverin qalması əvvəlkindən də güclü yeni botnetin qurulmasına səbəb ola bilər.

Nəticə

Demək olar ki, bütün dövlətlərdə kompüter sistemlərinin uzaqdan idarə edilməsinin qanunla qadağan olunmasına baxmayaraq, praktikada bu tələbə əməl edilmir, bu yalnız tələb olaraq qalmaqdadır. Getdikcə artan botların sayı və bot-əsaslı fəaliyyətlər onu göstərir ki, mövcud yanaşmaların həyata keçirilməsinin daha da intensivləşdirilməsinə və yeni yanaşmaların işlənməsinə ehtiyac vardır. Yalnız mövcud botnetlərin təsirinin və sayının azaldılması, yeni yoluxmaların qarşısının alınması və botnetlərdən əldə edilən maddi gəlirlərin azaldılması istiqamətində beynəlxalq səviyyədə uzunmüddətli fəaliyyətlər effektiv nəticələrin əldə edilməsini təmin edə bilər.

Ədəbiyyat

1. Tiirmaa-Klaar H. Cyber security threats and responses at global, nation-state, industry and individual levels. Ceri SciencesPo. 2011, pp.1–10.
2. Schmidt A. At the boundaries of peer production: The organization of Internet security production in the cases of Estonia 2007 and Conficker // Telecommunications Policy, 2012, vol.36, no.6, pp.451–461.
3. Wilson C. Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress. Library of Congress Washington DC Congressional Research Service. 2008, 43 p.
4. Herzog S. Revisiting the Estonian cyber attacks: Digital threats and multinational responses // Journal of Strategic Security, 2011, vol.4, no.2, pp.49–60.
5. Tiirmaa-Klaar H., Gassen J., Gerhards-Padilla E., Martini P. Botnets, cybercrime and national security. Botnets. Springer London, 2013, pp.1–40.
6. Plohmann D., Gerhards-Padilla E., Leder F. Botnets: Detection, measurement, disinfection & defence. ENISA Report. 2011, 154 p.
7. Plohmann D., Gerhards-Padilla E., Leder F. 10 Hard questions on botnet mitigation. ENISA Report, 2011, 18 p.

8. Vihul L., Czosseck C., Ziolkowski K., Aasmann L., et al. Legal implications of countering botnets. Joint report from the NATO Cooperative Cyber Defence Centre of Excellence and the European Network and Information Security Agency (ENISA), 2012, 67 p.
9. Van Eeten M., Bauer J.M., Asghari H., Tabatabaie S., Rand D. The role of Internet Service Providers in botnet mitigation: an empirical analysis based on spam data / Workshop on the Economics of Information Security (WEIS), 2010, pp.1–31.
10. Sood A.K., Enbody R.J. Crimeware-as-a-service − survey of commoditized crimeware in the underground market // International Journal of Critical Infrastructure Protection, 2013, vol.6, no.1, pp.28–38.
11. Leder F., Werner T., Martini P. Proactive botnet countermeasures: an offensive approach. The Virtual Battlefield: Perspectives on cyber warfare. IoS Press. 2009, vol.3, pp.211–225.
12. ITU Botnet Mitigation Toolkit: Background Information. ITU Telecommunication Development Sector, ICT Applications and Cybersecurity Division, 2008, 78 p.
13. Rutkowski A., Kadobayashi Y., Furey I., Rajnovic D., Martin R., Takahashi T., Schultz C., Reid G., Schudel G., Hird M., Adegbite S. CYBEX: the cybersecurity information exchange framework (x.1500) // ACM SIGCOMM Computer Communication Review, 2010, vol.40, no.5, pp.59–64.
14. Pijpker J., Vranken H. The role of Internet Service Providers in botnet mitigation / European Intelligence and Security Informatics Conference, 2016, pp.24–31.
15. Nadji Y., Antonakakis M., Perdisci R., Dagon D., Lee W. Beheading hydras: performing effective botnet takedowns / Proc. of the ACM SIGSAC conference on Computer & communications security, 2013, pp.121–132.
16. Asghari H., Ciere M., Van Eeten M.J. Post-mortem of a zombie: Conficker cleanup after six years / Proc. of the 24th USENIX Security Symposium, 2015, pp.1–16.
17. Sully M., Thompson M. The deconstruction of the Mariposa botnet. Defence Intelligence. 2010, 32 p.
18. Sinha P., Boukhtouta A., Belarde V.H., Debbabi M. Insights from the analysis of the Mariposa botnet / Proc. of the 5th International Conference on Risks and Security of Internet and Systems (CRiSIS), 2010, pp.1–9.
19. Gold S. Taking down botnets // Network Security, 2011, vol.2011, no.5, pp.13–15.
20. Shirazi R. Botnet Takedown Initiatives: A Taxonomy and Performance Model // Technology Innovation Management Review, 2015, vol.5, no.1, pp.15–20.
21. Salles R., Gu G., Swimmer M. Editorial for Computer Networks special issue on ‘‘Botnet Activity: Analysis, Detection and Shutdown’’ // Computer Networks, 2013, vol.57, no.2, pp.375–377.
22. German Anti-Botnet Initiative. www.botfrei.de
23. Karge S. The German Anti-Botnet Initiative / OECD Workshop: The role of Internet intermediaries in advancing public policy objectives, 2011, pp.1–4.
24. Schless T., Vranken H. Counter botnet activities in the Netherlands: a study on organisation and effectiveness / Proc. of the 8th International Conference for Internet Technology and Secured Transactions (ICITST), 2013, pp.442–447.
25. Editors: “The Australian Internet Security Initiative – Internet triage in action?” // ACMAsphere Newsletter, 2010, Issue 51, pp.14–15.
26. The Australian Internet Security Initiative: Interviews with industry Participants. Australian Communications and Media Authority (ACMA) Report. October 2015, 62 p.
27. U.S. Anti-Bot Code of Conduct (ABC) for Internet Services Providers (ISPs): Barrier and Metric Considerations. The Communications Security, Reliability and Interoperability Council (CSRIC) Final Report, March 2013, 99 p.
28. Cyber Clean Center Japan. https://telecom-isac.jp/ccc/en_index.html
29. Krebs B. PCs Used in Korean DDoS Attacks May Self Destruct. Washington Post Security Fix Blog, 2009.

30. Information Security in Korea – “Safe Internet, Happy Future!”. Korea Internet Security Agency (KISA) Report, 2015, 55 p.
31. Opperman D. Internet Governance and Cybersecurity in Brazil. In book: Multilateral Security Governance. KAS Rio de Janeiro, 2014, pp.167–181.
32. Irion K. The governance of network and information security in the European Union: the European Public-Private Partnership for Resilience (EP3R). In book: The Secure Information Society. Springer London, 2013, pp.83–116.

УДК 004.056

Имамвердиев Ядигар Н.[1], Гараева Гульнара Б.[2]
Институт Информационных Технологий НАНА, Баку, Азербайджан
[1]yadigar@lan.ab.az, [2]qarayevagulnare@mail.ru

Анализ подходов к борьбе с ботнетами

Ботнет – это сеть, зараженная вредоносными программами и дистанционно управляемыми компьютерами. В последнее время наблюдается быстрое увеличение масштаба ботнетов, целей их использования в киберпреступлениях и потерь, вызванных ими, показана важность комплексной борьбы с ними. В статье исследованы направления и заинтересованные стороны борьбы с ботнетами и проанализированы инициативы по борьбе с ботнетами на международном, национальном, общественном и индивидуальном уровнях.
Ключевые слова: *ботнет, кибербезопасность, киберпространство, интернет-провайдеры, инициатива по борьбе с ботнетом.*

Yadigar N. Imamverdiyev[1], Gulnara B. Garayeva[2]
Institute of Information Technology of ANAS, Baku, Azerbaijan
[1]yadigar@lan.ab.az, [2]qarayevagulnare@mail.ru

Analysis of initiatives in the fight against botnets

Botnet is a network of infected with malware and remotely controlled computers. In recent times, rapid increases in the scale of botnets, their use in cybercrime purposes and material and non-material damages stemming from botnets demonstrate the importance of a complex struggle with them. The paper studied directions and stakeholders of fight against botnets and analyzed anti-botnet initiatives at international, national, social and individual levels.
Keywords: *botnet, cybersecurity, cyberspace, Internet Service Providers, anti-botnet initiatives.*