Botnetlər Aşkarlanması Üsullarının İcmalı

Yadigar İmamverdiyev[1], Gülnarə Qarayeva[2]
[1]AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[2]Azərbaycan Müəllimlər İnstitutunun Şəki filialı, Şəki, Azərbaycan
[1]*yadigar@lan.ab.az*, [2]*qarayevagulnare@mail.ru*

***Xülasə* — Botnetlər kiber-hücum infrastrukturunda mühüm yer tuturlar. Botnet yoluxmuş kompüterlərdən və onları idarə edən botmasterlərin istifadə etdikləri C&C serverlərdən ibarət şəbəkədir, bəzən bu şəbəkəyə milyonlarla kompüter cəlb edilir. Botnetlər daim inkişaf edir, strukturları, istifadə etdikləri protokollar, yoluxdurma üsulları, hücum məqsədləri daim dəyişir. Məqalədə botnetlərin arxitekturası, təsnifatı və aşkarlama üsulları araşdırılmışdır.**

Açar sözlər* — *botnet, C&C server, honeypot, DDoS hücum, şəbəkə əsaslı aşkarlama üsulları

I. GİRİŞ

Botnet – “robot” və “network” sözlərinin birləşməsindən yaranmışdır. Bədniyyətliyə istifadəçinin xəbəri olmadan yoluxmuş kompüteri məsafədən idarə etməyə imkan verən ziyankar proqramlarla (botlarla) yoluxmuş kompüterlərdən ibarət şəbəkədir. Bot istifadəçinin kompüterində gizli quraşdırılan və bədniyyətliyə yoluxmuş kompüterin resurslarından istifadə etməklə müəyyən əməlləri yerinə yetirməyə imkan verən proqramdır. Belə şəbəkələr çox vaxt verilmiş əmrləri avtomatik yerinə yetirən zombi-kompüter şəbəkələri də adlanır.

Botnetlər 2003-cü ildən başlayaraq İnternetdə bir çox təhlükəsizlik problemlərinin meydana çıxmasında əsas rol oynayır. Belə şəbəkələr vasitəsilə həyata keçirilən müxtəlif məqsədli hücumlar müasir ümumdünya şəbəkəsinin əsas və demək olar ki, ən irihəcmli təhlükəsi hesab olunur.

Hücumların həcmi oğurlanmış elektron (rəqəmsal) kimliklərin və yoluxmuş kompüterlərin sayı ilə xarakterizə olunur. Botnetlər bir çox hücum məqsədləri üçün istifadə olunur. Əsasən spamların göndərilməsi (spamming), fişinq, fərdi və konfidensial məlumatların oğurlanması, DDoS (Distributed Denial of Service, paylanmış xidmətdən imtina) hücumları, zərərli proqramların yüklənməsi və yayılması, klikləmə saxtakarlığı (ing. click fraud) və s. məqsədlər üçün istifadə olunur.

Bu gün müxtəlif ölkələrdə milyonlarla yoluxmuş kompüter vardır. Bu şəbəkələr artıq kifayət qədər təhlükəli vəziyyətdədir. Botnetlərin aktiv olaraq yaradıldığı və istifadə olunduğu ölkələr əsasən ABŞ, Cənubi Amerika ölkələri, Avropa ölkələri və bir neçə Asiya ölkəsidir. Botnetləri idarəetmə mərkəzlərinin yerləşdiyi ölkələr ABŞ, Çin, Böyük Britaniya, Rusiya və s.dir (Kasperski şirkətinin 2015-ci ilin I rübü üçün hesbatı).

Kibercinayətkarlar tərəfindən idarə olunan komanda-nəzarət (Command and Control, C&C) serverləri müxtəlif ölkələrdə yerləşir. Serverlərin fiziki olaraq yerləşdiyi ərazi çox vaxt kibercinayətkarların olduğu yer deyildir. Serverlərin yerləşdiyi ölkələr isə ABŞ, Çin, Böyük Britaniya, Rusiya, Cənubi Koreya və s. ölkələrdir.

Botnetlərin yaradılması üsulları, onların istifadəsi, yayılması internet vasitəsilə həyata keçirilir. Kibercinayətkarlığa qarşı görülən tədbirlərə baxmayaraq, botnet “bazar”ları aşkar fəaliyyət göstərməkdədir. Aparılan araşdırmalar və statistik nəticələr onu göstərir ki, botnetlərin istifadə olunduğu əsas məqsəd DDoS hücumlarıdır. Saytların çökdürülməsi nəticəsində vurulan maddi zərər isə milyonlarla ölçülür.

İstər DDoS hücumların sayı, istərsə də botnetlərin səbəb olduğu digər problemlər onların nə qədər təhlükəli olduğunu sübut edir. Botnetlərin qarşısının alınması, zamanında aşkarlanması və onlara qarşı ehtiyat tədbirlərinin həyata keçirilməsi vacibdir.

Botnetlərlə mübarizə iki mərhələdə aparıla bilər. Birincisi, botla yoluxmadan qorunmaq (bu birbaşa istifadəçilərin üzərinə düşür), ikincisi isə, yoluxmuş qurğuların aşkarlanması və botnetin fəaliyyətinin dayandırılması. Botnetlərin istifadə etdiyi yoluxma üsullarının müxtəlifliyi, onların arxitekturasının kifayət qədər öyrənilməməsi, istifadəçilərin qorunma yollarından məlumatsızlığı botnetlərin yaranmasının əsas səbəblərindəndir.

Hazırda botnetlər və onların istifadə olunduğu sahələr sürətlə artmaqdadır. Botnetlərin qurulma və idarəetmə üsulları, həmçinin hücumların növləri artdıqca onlarla yeni mübarizə üsullarının işlənməsi də aktual olaraq qalır.

II. BOTNETLƏRİN QISA XARAKTERİSTİKASI

Botnet zərərli proqramlarla yoluxmuş və bədniyyətli tərəfindən idarə edilə bilən kompüterlər şəbəkəsidir. Belə şəbəkədəki hər bir botu və bütövlükdə botneti idarə edən bədniyyətlilər “botmaster” adlanır. Botmasterlər botnetləri müxtəlif məqsədlər üçün istifadə edirlər. Botmasterlər işə bot toplamaqla, yəni yeni kompüterləri ələ keçirməklə başlayırlar. Bunun üçün müxtəlif üsullardan istifadə olunur. Məsələn; viruslar və ya digər zərərli proqramlar, e-poçt, spamlar, müxtəlif məqsədli cəlbedici şəkillər, reklamlar və s. vasitəsilə. Botmasterlər tərəfindən yayılan belə vasitələrin istifadəçi tərəfindən yüklənməsi nəticəsində həmin proqram kompüterdə qurulmuş olur. Kompüter botla bir dəfə yoluxduqda o, botnet idarəetmə mərkəzinə bağlanır və əmr gözləyir. Yoluxmuş kompüterin açıq vəziyyətdə olması onun botmaster tərəfindən

idarə edilməsi üçün kifayətdir. Belə istifadə istifadəçinin icazəsi olmadan yerinə yetirilir.

Botnetlər müxtəlif məqsədlər üçün istifadə olunurlar. Ən çox istifadə olunduqları məqsədlər aşağıdakılardır:

1) Spam göndərilməsi (Spamming). Bildiyimiz kimi internet trafikinin 90%-dən çoxunu spamlar təşkil edir. Belə spamların 95%-dən çoxu botnetlər tərəfindən göndərilir. Spamların botnetlər tərəfindən yayılmasının botmasterlər üçün əsas üstünlükləri spamları qəbul edən tərəflərin leqal yolla spamı göndərən tərəfə dönə bilməməsi və daha böyük ölçüdə spamların yayıla bilməsidir;

2) DDoS (Distributed Denial of Service, Paylanmış Xidmətdən İmtina) hücumlar. Botmasterlər botnetlərdən istifadə edərək böyük sayda istifadəçisi olan veb saytlara eyni anda müraciəti təşkil edirlər. Belə olduqda veb serverdə gecikmə və ya tamamilə xidmətdən imtina vəziyyəti yaranır. Ən çox istifadə olunan DDoS hücumlarının bir növü də Syn hücumlarıdır (Syn Flood);

3) Kliklәmə saxtakarlığı (Click fraud). Veb saytların, şəxsi bloqların, sosial şəbəkə səhifələrinin istifadəçi sayını süni olaraq artırmaq məqsədilə, həmçinin elektron səsvermə sistemlərində klik sayı artırmaq (və ya azaltmaq) üçün botnetlərdən geniş istifadə olunur;

4) İnformasiya oğurluğu. Belə informasiyaya plastik kartlar haqqında məlumatlar (son istifadə tarixi, CVV2 və s.), ünvan, telefon nömrəsi, istifadəçi adı/parol, SSN (Social Security Number), ATM PIN və s. məlumatlar daxildir;

5) Fişinq hücumları üçün infrastruktur yaratmaq;

6) Digər zərərli proqramları yaymaq, məsələn, casus proqramların yayılması, reklam materiallarının yayılması və s.

III. BOTNETLƏRİN TƏSNİFATI

Botnetlərin təsnifatı onların arxitekturasına və botları idarə etmək üçün istifadə edilən protokollara əsaslanır. Botnetləri xarakterizə edən əsas kateqoriyalardan biri də C&C (Command & Control, Əmr və Nəzarət) serverlərdir. Botmasterlər botlarla əlaqə saxlamaq üçün belə xüsusi serverlərdən istifadə edirlər. C&C server olaraq çox vaxt leqal olaraq yerləşdiyi coğrafi ərazi məlum olmayan gizli serverlərdən istifadə olunur. Botmaster botneti idarə etmək üçün C&C server qurur və yoluxmuş kompüter hər hansı bir kanalla (məs; IRC) bu serverə bağlanır və ondan əmr gözləyir. Botnetləri arxitekturasına görə bir neçə formada təsnif etmək olar. [5]-də botnetlər 3 arxitekturada – mərkəzləşmiş, P2P (peer – to – peer) və hibrid (ağacvari) olaraq təsnif edilmişdir. Lakin, bəzi mənbələrdə, məs; [8]-də C&C sistemlər aşağıdakı kimi təsnif edilmişdir:

- *1) Mərkəzləşmiş C&C modeli (Centralized C&C Model).*

Mərkəzləşmiş C&C modeli botnetlərdə istifadə olunan əsas modellərdən biridir. Ən çox tanınan botnetlərdən AgoBot, SDBot, Rbot və s. mərkəzləşmiş modelə aiddir. Belə modeldə botmaster botlarla əlaqə saxlamaq üçün bir yüksəksürətli kanal seçir. Adətən, belə modeldə C&C server IRC (Internet Relay Chat), HTTP kimi şəbəkə protokollarını istifadə edərək kompüteri razı salır. Yeni kompüter botla yoluxduqda o, C&C serverlə əlaqə yaradaraq botnetə qoşulur. Müvafiq C&C serverə bir dəfə qoşulduqdan sonra botmasterin əmrlərini gözləyir.

Mərkəzləşmiş C&C modelin istifadə edilməsinin aşağıdakı kimi üstün cəhətləri var:

- daha asan əldə olunan proqramlar (məs; IRC skriptlər və IRC botlar) səbəbindən mərkəzləşmiş C&C modelində yoluxdurma və xüsusiləşdirmə daha sadədir. Belə modeli istifadə edərək botmaster eyni vaxtda minlərlə botu idarə edə bilər. Mənfəət məqsədli botnetlər yaradılarkən daha çox botu idarə etməyə imkan verən və maksimum qazanc gətirən mərkəzləşmiş C&C modeli seçilir;
- mərkəzləşmiş modeldə mesajların gecikmə vaxtı çox kiçikdir. Bu da botmasterə botları rahat idarə etməyə və hücumlar təşkil etməyə imkan verir.

Lakin, bu modelin də zəif cəhətləri vardır. Belə ki, mərkəzləşmiş modeldə bütün mübadilələr server üzərindən aparıldığından, C&C server zəif halqa təşkil edir. Əgər C&C server aşkarlanarsa, bütün botnet çökmüş olur.

2) P2P əsaslı (mərkəzi olmayan) C&C modeli (P2P-Based C&C Model).

Şəbəkədə aşkarlanmalara daha davamlı hesab olunan botnet modellərindən biri də P2P (nöqtə-nöqtə birləşmiş) əsaslı C&C modelidir. P2P əsaslı botnetlər olduqca az olmasına baxmayaraq, mərkəzləşmiş modellə müqayisədə aşkarlanması və dağıdılması daha çətindir. Mərkəzi olmayan botnetlərdə botlar idarəetmə mərkəzinə deyil, zombi-şəbəkənin bir neçə yoluxmuş maşınına qoşulur. Əmrlər botdan bota göndərilir, hər botda bir neçə “qonşusunun” ünvanı olan siyahı olur və onların hər hansı birindən əmr alınan zaman o, əmri digər qonşularına ötürür, bununla da əmri yayır. Bu halda, botneti idarə etmək üçün botmasterin botnetə daxil olan ən azı bir kompüterə birbaşa çıxışı olmalıdır.

Bu modellə qurulmuş botnetlərin getdikcə artmasına və daha çətin aşkarlanmasına baxmayaraq mənfi cəhətləri də vardır. Birincisi, P2P sistemlər çox kiçik saylı istifadəçi qrupları arasında əlaqəyə imkan verir (10 – 50 arası). Bu ölçü mərkəzləşmiş modellə müqayisədə olduqca kiçikdir. İkincisi, P2P sistemlər mesajların vaxtında çatmasına və yayılmanın gecikməməsinə zamanət verə bilmir. Aktiv olmayan bir və ya bir neçə bot şəbəkədə yayılmanı kifayət qədər zəiflədə bilər. Ona görə də belə botnetləri idarə etmək çətindir. Bu iki səbəb P2P modelin daha geniş yayılmasını və istifadəsini məhdudlaşdırır.

3) Təsadüfi C&C modeli (Random C&C Model).

Təsadüfi C&C modellər real botnetlər üçün çox da istifadə olunmur. Daha çox gələcəyə istiqamətlənmiş dözümlü botnetlər üçün düşünülmüşdür. Belə modeldə bot digər botlarla və ya botmasterlə birbaşa əlaqə saxlamır. Adətən, bot öz botmasterindən gələcək əlaqəni gözləyir. Botmaster lazım olduqda öz aktiv botlarını tapmaq üçün internetdə axtarış edir.

Bot tapıldıqda botmaster əmr verir. Belə modeldə hücumu həyata keçirmək asandır, botneti aşkarlama və dağıtma cəhdləri isə olduqca çətindir. Həmçinin böyük ölçülü hücumlarda istifadə etmək mümkün deyil.

Botnetlər üçün xarakteristik kateqoriyalardan biri də C&C serverlərin işləmə mexanizmidir. Bu mexanizmlər yeni botlar kəşf etmək və onları botmasterdən asılı salmaq üçün vacibdir. Ən çox istifadə olunan mexanizmlər aşağıdakılardır:

Sabit (statik) IP ünvanlar (Hard-coded IP address). Bu üsulda bot ilk yoluxduğu anda sabit IP ünvanlı C&C serverlə əlaqə saxlayır. Bu üsulun mənfi cəhəti odur ki, sabit IP ünvan istifadə edən C&C serverləri asanlıqla aşkarlamaq və əlaqəni bloklamaq olar. Bu vaxt əgər serverlə botlar arasında əlaqə kəsilirsə, botnet tamamilə məhv edilmiş olur. Ona görə də bu üsul müasir botnetlərdə demək olar ki, istifadə olunmur.

Dinamik DNS (DNS flux). Botnetlər DGA (Domain Generation Algorithm, Domen Yaratma Alqoritmi) istifadə edərək kriptoqrafik olaraq yaradılmış domen adlar istifadə edirlər. Bu texnologiya statik sistemlər üçün bütün mümkün C&C ünvanları tapmağı olduqca çətinləşdirir. Əgər C&C server sahibi tərəfindən bağlanarsa, idarəetmə asanlıqla yeni serverə ötürülür. Köhnə serverlə əlaqəni itirən bot DNS sorğu göndərir və yeni C&C serverə qoşulur. Dinamik DNS adlar istifadə etməklə botmaster C&C server funksiyasını itirdikdə onu bərpa edə bilir. Həmçinin çox vaxt aşkarlamanı çətinləşdirmək üçün C&C serverlər tez-tez bilərəkdən dəyişdirilir.

Dinamik IP (IP flux). Bu texnologiya FFSN (Fast Flux Service Networks, Xidmət şəbəkələrinin sürətli dəyişməsi) kimi də tanınır. Fast flux botnetlərin şəbəkədəki zərərli fəaliyyət göstərən serverlərini gizlətmək üçün istifadə olunan bir DNS texnologiyasıdır. Bu texnologiyanın əsasını bir domen adı üçün birdən çox IP ünvan saxlamaq və bu ünvanların DNS yaddaşlarının daimi olaraq dəyişdirilməsi təşkil edir. İki cür fast flux texnologiyası məlumdur: tək və double (ikiqat) flux.

Bot kompüterə botnet sahibinin əmrlərini ötürmək üçün bot və əmr göndərən kompüter arasında şəbəkə bağlantısı yaratmaq lazımdır. Bütün şəbəkə qarşılıqlı əlaqəsi şəbəkə daxilində kompüterlərin ünsiyyət qaydalarını müəyyən edən şəbəkə protokollarına əsaslanır. Buna görə də, botnetləri istifadə olunan ünsiyyət protokolu əsasında təsnif etmək olar. İstifadə edilən şəbəkə protokollarının növünə görə botnetlər IRC, IM (Instant Messaging), veb və digər (TCP, ICMP, UDP və s.) yönümlü qruplara bölünür.

Cədvəl 1-də köhnə və yeni botnetlərin istifadə etdiyi arxitektura və protokollara görə müqayisəsi verilmişdir:

CƏDVƏL 1 BOTNETLƏRİN MÜQAYİSƏSİ

Əlaqə	Köhnə	Yeni
Topologiya	mərkəzləşmiş	paylanmış və ya hibrid, bəziləri hələ də mərkəzləşmiş
Protokollar	IRC və ya HTTP	P2P
Qurulması	asan	çətin
Aşkarlanması	asan	çətin
Əlaqə	kiçik gecikməli	kiçik – orta gecikməli
Dözümlülük	pis	yaxşı
Anonimlik	pis	yaxşı

IV. BOTNETLƏRİN AŞKARLANMASI ÜSULLARI

Yoluxmuş kompüterləri bir çox əlamətlərinə görə digər kompüterlərdən fərqləndirmək olar. Məsələn; istifadə olunan IRC trafik, C&C serverlərə qoşulma cəhdləri, şəbəkədəki bir neçə maşının eyni DNS sorğu göndərməsi, yüksək SMTP (Simple Mail Transfer Protocol) trafiki (spam göndərilməsinin nəticəsi kimi), yavaş hesablama/yüksək CPU istifadəsi, istifadəçi tərəfindən göndərilməyən e-poçt, sosial media, ani mesajlar, internetə giriş problemləri və s. Bir çox şəbəkə müdaxilələrinin aşkarlanması sistemləri (Network Intrusion Detection System, NIDS) bu və ya digər xüsusiyyətlərə əsaslanır və 3 kateqoriyaya bölünürlər [7]:

- host-əsaslı (host -based);
- şəbəkə-əsaslı (network -based);
- hibrid (host- və şəbəkə-əsaslı birlikdə).

Host-əsaslı sistemlər yoluxmuş botları aşkarlamaq üçün adətən fərdi hostlarda siqnatura və ya davranış əsaslı üsullar istifadə edir. Belə ki, şəbəkə trafiki və ya sistem tarixçəsi, bot imzaları və ya davranış informasiyaları ilə öyrənilir. Host əsaslı IDS-lər tək botun aşkarlanmasına imkan verir, ona görə də daha çox digər üsullarla birlikdə tətbiq olunurlar.

Şəbəkə əsaslı üsullar şəbəkəni izləyərək bir neçə hostun oxşar davranışlarına əsasən yoluxmanı aşkarlamağa cəhd edir. Belə üsullar zamanı hostun əvvəlki siqnaturaları və ya davranış məlumatları lazım deyil, çünki, eyni botlar şəbəkədə özlərini yoluxmamış kompüterlərə görə fərqli aparırlar. Şəbəkə əsaslı aşkarlama zamanı eyni şəbəkədə bir neçə yoluxmuş kompüterin olması kifayətdir. Həmçinin belə üsullar şəbəkə administratoru ilə əməkdaşlıq tələb edir ki, bu zaman şəbəkə istifadəçilərinin təhlükəsizliyi təmin olunmalıdır.

Şəbəkə əsaslı üsullarda botnetlər şəbəkə trafikinin müxtəlif xarakteristikalarını istifadə etməklə aşkarlanır. Məsələn, istifadə olunan şəbəkə statistikası, əlaqə protokolları, şübhəli trafik davranışları, davranışların qrafik təsviri, honeypotların (bal küpü) qurulması və izlənməsi, davranış xüsusiyyətləri və s. Şəbəkə əsaslı botnet aşkarlama üsulları özü də 2 sinfə ayrılır: honeynetlər və passiv trafikə əsasən. Honeypotların qurulması və onların davranışlarının izlənməsi ilə aparılan müşahidələr daha aktiv xarakter daşıyır.

Aşkarlama texnologiyaları aşağıdakı siniflərə də bölünür:

- siqnatura əsasında;
- anomaliya əsasında;
- DNS əsasında (Domain Name System, DNS);
- intellektual analiz əsasında (mining-based).

Müdaxilələri aşkarlama üsulları olduqca müxtəlifdir. Bir çox müdaxilələri aşkarlama sistemləri botnet şəbəkəsinin normal şəbəkə ilə müqayisədə daha çox trafik istifadə etməsinə, bəziləri isə botları aşkarlamaq üçün anomaliyaların

aşkarlanmasına əsaslanır. Anomaliyanın aşkarlanması normal davranışlardan əhəmiyyətli dərəcədə sapmalara əsaslanır. Məsələn; şəbəkə davranışları, sistem səviyyəsində davranışlar, CPU istifadəsi və ya fayl sisteminin dəyişməsi kimi. Anomal aşkarlamanın əsas üstünlüyü odur ki, dəyişikliyin məqsədindən asılı olmayaraq yoluxmanı daha tez təyin etmək mümkündür.

BotMiner

Şəbəkə əsaslı müdaxiləni aşkarlama sistemlərindən biri BotMiner-dir [1]. Bütün üsulların üstün cəhətləri olsa da, bir sıra problemlər də vardır. Aşkarlamanı çətinləşdirən əsas problemlər aşağıdakılardır:

- Rutkitlərdən istifadə edərək sistem səviyyəsində analizlərin gizlədilməsi;
- Botnetlərin çox dəyişkən və fərqli C&C strukturlarının olması;
- Botlar və onların davranışlarının daim inkişaf etməsi;
- Tək strukturlu şəbəkəyə baxaraq ümumi bir aşkarlama modeli qurmağın çətinliyi və s.

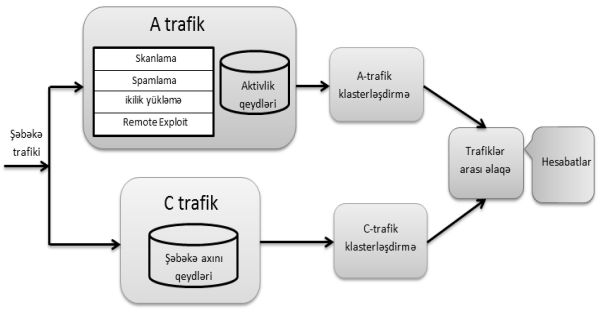
Botnetlər müxtəlif protokol və C&C infrastruktur istifadə etdiklərinə görə elə yanaşma təklif etmək lazımdır ki, protokol və strukturu müstəqil şəkildə aşkarlamağa imkan versin. BotMiner botnetlərin sabit qalan xassələrinə əsaslanır. Belə ki, botlar botmasterə uzunmüddətli istifadə üçün lazımdır. Ona görə də daimi müşahidə onu göstərir ki, eyni botnetdəki botlar adətən eyni C&C serverə bağlanır və botmasterlə eyni üsulla əlaqə saxlayırlar. Həmçinin botlar əmrləri oxşar koordinasiyalı şəkildə cavablandırırlar.

BotMiner şəbəkə aktivliyini iki hissədə araşdırır: əlaqə aktivliyi və zərərli aktivliklər. BotMinerin sistem arxitekturası aşağıdakı kimidir (Şəkil 1):

- C-trafik (C&C əlaqələr): "Kim kimlə danışır?"
- A-trafik (zərərli fəaliyyət): "Kim nə edir?".

BotMiner hostları oxşar əlaqə aktivlikləri və oxşar zərərli aktivliklərə görə klasterləşdirir. C-trafik aşağıdakıları qeyd edir:

- Şəbəkə axınını izləyir, bu iş nüvə səviyyəsində itən paketləri aşkar etmək üçün çox səmərəli şəkildə qurulmalıdır;
- Başlama vaxtı, müddəti, srcIP (çıxış ünvanı), srcPort (çıxış portu), dstIP (son ünvan), dstPort (son port), paketlərin sayı, hər iki istiqamətdə transfer olunan baytların sayı.



Şəkil 1. BotMinerin sistem arxitekturası

BotMiner üsulu ilə aşkarlama zamanı müşahidə olunan botnetlərdə (IRC, HTTP və P2P protokollarına uyğun) müşahidə olunan paketlərin ölçüsü, müddəti, miqdarı və s. xarakteristikalar qeyd edilir.

BotSniffer

BotSniffer anomaliyalara əsaslanan şəbəkə əsaslı aşkarlama üsuludur [3]. Əvvəlki siqnatura və C&C ünvanları bilmədən zərərli kanalları oxşar xüsusiyyətləri və zaman-məkan əlaqələrinə görə aşkarlamağa imkan verir. Bu üsul şəbəkədə bir neçə bot, hətta bir bot belə olduqda C&C kanalı aşkarlaya bilir. BotSniffer dünya miqyaslı real botnetlərin aşkarlanması zamanı tətbiq olunmuşdur və xəta faizi 0,18-dir.

Bildiyimiz kimi, botnetləri xarakterizə edən əsas kateqoriya C&C serverlərdir. Botnetin fəaliyyəti müddətində C&C kanalları nisbətən sabit olur və botmasterlər öz botlarını və idarəetmə variantlarını nadir hallarda dəyişirlər. Həmçinin bu əlaqə botmasterə öz bot "ordusuna" əmr vermək üçün lazımdır. Əgər C&C kanal açılarsa, həm C&C serveri, həm də şəbəkədəki botları aşkarlamaq olar. Bu gün botnetlərin əksəriyyəti IRC protokol və IRC PRIVMSG mesajlarını istifadə edirlər. Çox vaxt əmrlər şifrlənməmiş göndərilir, bəzi botnetlər isə sadə şifrləmə üsullarından (XOR, əvəzləmə və s.) istifadə edirlər.

Botnet C&C trafikini aşkarlamaq çox çətindir, çünki:

- normal protokol istifadə edir (IRC və HTTP) və normal trafikə oxşayır;
- aşağı həcmdə trafik istifadə edir və gizlətmək çətin deyil;
- izlənilən şəbəkədə çox az sayda bot ola bilər;
- şifrlənmiş əlaqə istifadə edilə bilər.

BotSniffer alqoritminin aşağıdakı kimi üstün cəhətləri var:

1. C&C serverlərin əvvəlki bilgiləri və ya istifadəçinin siqnaturaları tələb olunmur;
2. Şifrlənmiş kanalları belə aşkarlamağa imkan verir;
3. İzlənilən şəbəkədə çox sayda bot olması tələb edilmir;
4. Böyük həcmdə C&C əlaqə paketi tələb etmir və yanılma ehtimalı çox azdır.
5. Şəbəkələrdə əlaqələr sorğu-cavab texnologiyası əsasında həyata keçirilir. Normal şəbəkələrdə eyni vaxtda bir neçə müştərinin oxşar cavablar verməsi nadir hadisədir. Əgər şəbəkədə bir neçə belə davranış müşahidə olunursa, onların bot olub-olmamasının yoxlanması BotSniffer aşkarlama sisteminin əsasını təşkil edir.

BotSnifferin əsas komponentləri izləmə mexanizmi (Monitor Engine) və korrelyasiya mexanizmidir (Correlation Engine).

İzləmə mexanizmi şəbəkə trafikini araşdırır, şübhəli C&C protokollarla əlaqələri qeyd edir və aktiv cavab davranışlarını (məs., skanlama, spam və s.) və mesaj cavabları aşkarlayır. Daha sonra bu məlumatlar korrelyasiya mexanizmi tərəfindən məkan-zaman əlaqəsi və fəaliyyətlərin oxşarlığına görə qrup şəklində analiz olunur. Belə mexanizmlər bir neçə şəbəkədə qurulur və korrelyasiya analizi üçün məlumatlar toplanır.

Əvvəlcə lazım olmayan trafik ayrılır. C&C protokolun təyini zamanı C&C əlaqələrdə istifadə olunmayan ICMP, UDP kimi protokollar süzgəclənir. Google, Yahoo və s. kimi C&C

server olma ehtimalı az olan trafiklər isə ağ siyahıya salınır və vaxtaşırı olaraq dəyişdirilir.

Müşahidə edilən müştərilərdən hansıların C&C-yə bənzər protokol istifadə etdiyini müəyyənləşdirmək üçün əsasən IRC və HTTP protokollar izlənilir. Bildiyimiz kimi, bot əmrlərə iki cür cavab verir: aktiv və mesaj şəklində. Bunun üçün də mesaj cavablar kimi IRC PRIVMSG mesajları əlaqələr analizi üçün izlənilir. Burada 2 anomal modul hesablanır: anormal yüksək skan dərəcəsi və itən əlaqələrin həcmi.

Əlaqələr səviyyəsində əvvəlcə müştərilər IP və port cütünə görə qruplaşdırılır və sonra zaman-məkan əlaqəsi və oxşarlıq xüsusiyyətlərinə görə qrup analizi aparılır. Əgər hər hansı şübhəli C&C əlaqəsi aşkar edilərsə, bu bot siqnalı ola bilər.

BotHunter

Şəbəkə əsaslı aşkarlama üsullarından biri də BotHunterdir. BotHunter yoluxmanı və botlar arasında əlaqəli dialoqu ardıcıl yoluxma modelini istifadə edərək tapır [2]. Bu üsul Snort IDS-in dəyişdirilmiş variantını istifadə edərək şəbəkə çıxışında paketləri qeyd edir. Botun yoluxmasını müəyyən etmək üçün çarpaz analizdən istifadə olunur. IDS siqnalları zaman üzrə izlənilir və bütün hostlar üçün hər ana uyğun yoluxma ehtimalı hesablanır. Əgər aşağıdakı iki hal müşahidə olunarsa, onun haqqında bot olma qərarı alınır:

1) Lokal yoluxma haqqında sübut tapıldıqda və botun hər hansı hücum cəhdi sübut olunduqda;
2) Ən azı iki fərqli çıxış siqnaturası və ya bot əlaqəsi tapıldıqda.

NƏTİCƏ

Botnetlər ölkələrin kritik informasiya resurslarına genişmiqyaslı kiber-hücumların həyata keçirilməsində əsas vasitələrdən biridir. Bu işdə aparılmış analizlər göstərir ki, botnetlərin aşkarlanmasına yanaşmalar maşın təlimi və verilənlərin intellektual analizi metodlarına əsaslanır. Big Data texnologiyaları müxtəlif ölkələri əhatə edən geniş coğrafi əraziyə səpələnmiş botların şübhəli fəaliyyətini izləməyə, milyonlarla mənbədən informasiyanı toplayaraq korrelyasiya etməyə, ilk baxışda əlaqəsiz görünən, zamana görə bir-birindən uzaq hadisələr arasında səbəb-nəticə əlaqələri tapmağa imkan verməklə botnetlərin effektiv tapılmasına imkan verə bilər. Gələcək tədqiqatların bu istiqamətdə aparılması planlaşdırılır.

ƏDƏBİYYAT

[1] G. Gu, R. Perdisci, J. Zhang, W. Lee, “BotMiner: clustering analysis of network traffic for protocol- and structure-independent botnet detection,” Proc. of the 17th Conference on Security Symposium (SS’08), pp. 139–154, 2008.

[2] G. Gu, P. Porras, V. Yegneswaran, M. Fong, W. Lee, “Bothunter: detecting malware infection through IDS driven dialog correlation,” Proc.of 16th USENIX Security Symposium, pp. 1–16, 2007.

[3] G. Gu, J. Zhang, W. Lee, “BotSniffer: detecting botnet command and control channels in network traffic,” Proc. of the 15th Network and Distributed System Security Symposium (NDSS), 2008.

[4] C. Li, W. Jiang, X. Zou, “Botnet: survey and case study,”Proc. of the 4th International Conference on Innovative Computing Information and Control, Vol. 0, pp. 1184–1187, 2009.

[5] J. Liu, Y. Xiao, K. Ghaboosi, H. Deng, J. Zhang, “Botnet: classification, attacks, detection, tracing, and preventive measures,” EURASIP Journal on Wireless Communications and Networking, Vol. 2009, Article ID 692654, 2009.

[6] S. A. Yeshwantrao, V. J. Jadhav, “Threats of botnet to Internet security and respective defense strategies,” International Journal of Emerging Technology and Advanced Engineering, Vol. 4, No. 1, pp. 121-127, January 2014.

[7] S. García, A. Zunino, M. Campo, “Survey on network-based botnet detection methods,” Security and Communication Networks, Vol. 7, No. 5, pp. 878–903, January 2014.

[8] TrendMicro. Taxonomy of botnet threats. Technical Report, 2006. http://www.cs.ucsb.edu/ kemm/courses/cs595G/TM06.pdf

[9] D. Zhao, I. Traore, B. Sayed, W. Lu, S. Saad, Ali Ghorbani, D. Garant, “Botnet detection based on traffic behavior analysis and flow intervals,” Computers and Security, Vol. 39, pp. 2-16, November 2013.

[10] 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.

[11] OpenDNS Security Whitepaper. The Role of DNS in Botnet Command & Control. http://info.opendns.com/rs/opendns/images/OpenDNS_SecurityWhitepaper-DNSRoleInBotnets.pdf

[12] R. A. Rodríguez-Gómez, G. Maciá-Fernández, P. García-Teodoro, M. Steiner, D. Balzarotti, “Resource monitoring for the detection of parasite P2P botnets,” Computer Networks, Vol. 70, pp. 302-311, 2014.

[13] K. Singh, Sh. Ch. Guntuku, A. Thakur, C. Hota, “Big Data Analytics framework for Peer-to-Peer Botnet detection using Random Forests,” Information Sciences, Vol. 278, pp. 488-497, September 2014.

[14] S. S.C. Silva, R. M.P. Silva, R.C.G. Pinto, R. M. Salles, “Botnets: A survey,” Computer Networks, Vol. 57, No. 2, pp. 378-403, 2013.

[15] L. P. Song, Z. Jin, G.Q. Sun, “Modeling and analyzing of botnet interactions,” Physica A: Statistical Mechanics and its Applications, Vol. 390, Issue 2, pp. 347-358, January 2011.

[16] A. McKewan, “Botnets – zombies get smarter,” Network Security, Vol. 2006, Issue 6, pp. 18-20, June 2006.

[17] J. Jabez, B. Muthukumar, “Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach,” Procedia Computer Science, Vol. 48, pp. 338-346, 2015.

[18] B. McCarty, “Botnets: big and bigger,” IEEE Security & Privacy, Vol. 1, No. 4, pp. 87–90, 2003.

[19] C. Wilson, Botnets, cybercrime, and cyberterrorism: vulnerabilities and policy issues for congress. Congressional Research Service Reports (CRS) and Issue Briefs. 2007.

[20] Y. Zhang, Y. Xiao, K. Ghaboosi, J. Zhang, H. Deng, “A survey of cyber crimes,” Security and Communication Networks, Vol. 5, No. 4, pp. 422–43, 2012.

[21] Ch. Day. Intrusion Prevention and Detection Systems. in Managing Information Security (Second Edition), pp. 119-142, 2013.

[22] A. Patel, M. Taghavi, K. Bakhtiyari, J. Celestino Júnior, An intrusion detection and prevention system in cloud computing: A systematic review,” Journal of Network and Computer Applications, Vol. 36, Issue 1, pp. 25-41, January 2013.

[23] A. Castiglione, R. De Prisco, A. De Santis, U. Fiore, F. Palmieri, “A botnet-based command and control approach relying on swarm intelligence,” Journal of Network and Computer Applications, Vol. 38, pp.22-33, February 2014.

[24] S. Lee, J. Kim, “Fluxing botnet command and control channels with URL shortening services,” Computer Communications, Vol. 36, Issue 3, pp. 320-332, February 2013.

[25] Y. Boshmaf, I. Muslukhov, K. Beznosov, M. Ripeanu, “Design and analysis of a social botnet,” Computer Networks, Vol. 57, Issue 2, pp. 556-578, February 2013.

[26] A. K. Seewald, W. N. Gansterer “On the detection and identification of botnets,” Computers & Security, Vol. 29, Issue 1, pp. 45-58, February 2010.

[27] C. Schiller, J. Binkley, G.Evron, C. Willems, T. Bradley, D. Harley, M. Cross. Botnets: the killer web app. Syngress. 2007.