MRLAB

“Domen adı generator alqorithmi” və zərərvericilər tərəfindən istifadəsi

Azərbaycan Respublikası Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti – Kompüter İnsidentlərinə qarşı Mübarizə Mərkəzi - Malware Research Lab – F. Cəfərov - 25 Aprel 2022

Giriş

Qlobal internet təhdidləri yalnız infrastrukturu sıradan çıxarmaq üçün nəzərdə tutulmuş hücumlardan, insanları və təşkilatları hədəf alan köklü dəyişikliklərə məruz qalıb. Yeni hücumlar insanların həyatlarına birbaşa təsir edir, biznes və hökümətləri təhlükə altına qoyur. Bu məqaləmizdə botnetlərdə istifadə olunan domen yaratma alqoritmi, ASLR (address space layout randomization) və DEP (data execution prevention) haqqında məlumat verəcəyik.

Botnet nədir?

Botnet – zərərli proqramların gizli şəkildə quraşdırıldığı, çoxlu sayda kompüterdən ibarət şəbəkədir və xakerlərə yoluxmuş maşınlarda uzaqdan istənilən hərəkəti yerinə yetirməyə imkan verir. Botnetlərin əsas hədəfləri spam, virus yaymaq, şəxsi məlumatların ələ keçirilməsi və ya DdoS hücum etməkdir. Kompüter yoluxandan sonra, botnet server ilə əlaqə yaratmağa çalışır və əlaqə qurulandan sonra serverdən komandalar alır. Botnetlər əsasən İnternet Chat Relay şəbəkələri, domenlər və ya veb saytlar vasitəsi ilə fəaliyyət göstərir. Ən çox istifadə olunan üsul domen üzərindən yaradılan qoşulmalardır. Bəs bu domenlər necə qenerasiya olur?

Domen adı yaratma alqoritmi

Statik domen və ya IP ünvanından asılı olan botnet, tez aşkar olunur və bloklanır. Domen və ya İP ünvan bloklanandan sonra xakerlə zərərçəkənin əlaqəsi itir, yəni botnet təlimatlar əldə edə bilmir. Beləliklə zərərli proqram təminatı yenidən hazırlanmalıdır və zərərçəkənin kompüterinə yüklənilməlidir. Bu işləri görməmək üçün xakerllər domen yaratma alqoritmindən istifadə edirlər. Domen yaratma alqoritmi əmr və idarəetmə (command and control) serveri üçün çoxlu sayda domen adı yaraatmaq üçün, zərərli proqram təminatına yazılan texnikadır. Bu üsul əmr və idarəetmə server ünvanlarının qara siyahıya düşnəsinin qarşısını almaq üçün istifadə olunur. Domen yaratma alqoritminə sahib olan xaker öncədən yaradılan domenlərin siyahısını qenerasiya edib, həmin adları serverdə

yaradır. Yəni, botnetin yaradacağı domenlərin siyahısını xaker əvvəlcədən bilir. Botnet yaradılan domenlərdən biri əmr və idarəetmə serverinin İP ünvanına həll olunana qədər DNS sorğular göndərir. Server sorğuya cavab verdiyi andan zərərli ona göndərilən sorğuları icra etməyə başlayır. Domen adları əsasən 1 saat əvvəl yaradılır və 24 saat ərzində aktiv olur, daha sonra isə ləğv edilir.
Domen yaratma alqoritmləri ilkin verilənlər əsasında minlərlə domen adı qenerasiya edir. İlkin verilənlər xaker tərəfindən təyin olunur. İlkin verilənlər iki növ olur: statik və dinamik. Statik verilənlər təsadüfi stringlər, rəqəmlər və ya xakein təyin etdiyi domen adları ola bilər. Dinamik növdə isə verilənlər zamanla dəyişir. Çox vaxt domen adı yaratmaq üçün cari tarix və vaxt istifadə olunur. Bu kibertəhlükəsizlik işçiləri üçün çətinliklər yaradır. Əsas domen yaradan alqoritmlər kimi **bamital**, **banjori**, **blackhole**, **ccleaner**, **chinad**, **conficker**, **cryptolocker**, **dircrypt**, **dyre**, **emotet**, **feodo**, **fobber**, **gameover**, **gspy**, **locky**, **madmax**, **matsnu**, **mirai**, **murofet**, **mydoom**, **necurs**, **nymaim**, **omexo**, **padcrypt**, **proslikefan**, **pykspa**, **qadars**, **ramnit**, **ranbyus**, **rovnix**, **shifu**, **shiotob**, **simda**, **suppobox**, **symmi**, **tempedreve**, **tinba**, **tinynuke**, **tofsee**, **vawtrak**, **vidro**, **virut**, **xshellghost** göstərə bilərik.

Murofet alqoritminin mənbə kodu:

```
import hashlib
from datetime import datetime, timedelta
import argparse


def dga(date):

    for index in range(1020):
        seed = 7*[0]
        seed[0] = ((date.year & 0xFF) + 0x30) & 0xFF
        seed[1] = date.month
        seed[2] = (date.day//7)*7
        r = index
        for i in range(4):
            seed[3+i] = r & 0xFF
            r >>= 8

        seed_str = ""
        for i in range(7):
            seed_str += chr((seed[i]))

        m = hashlib.md5()
```

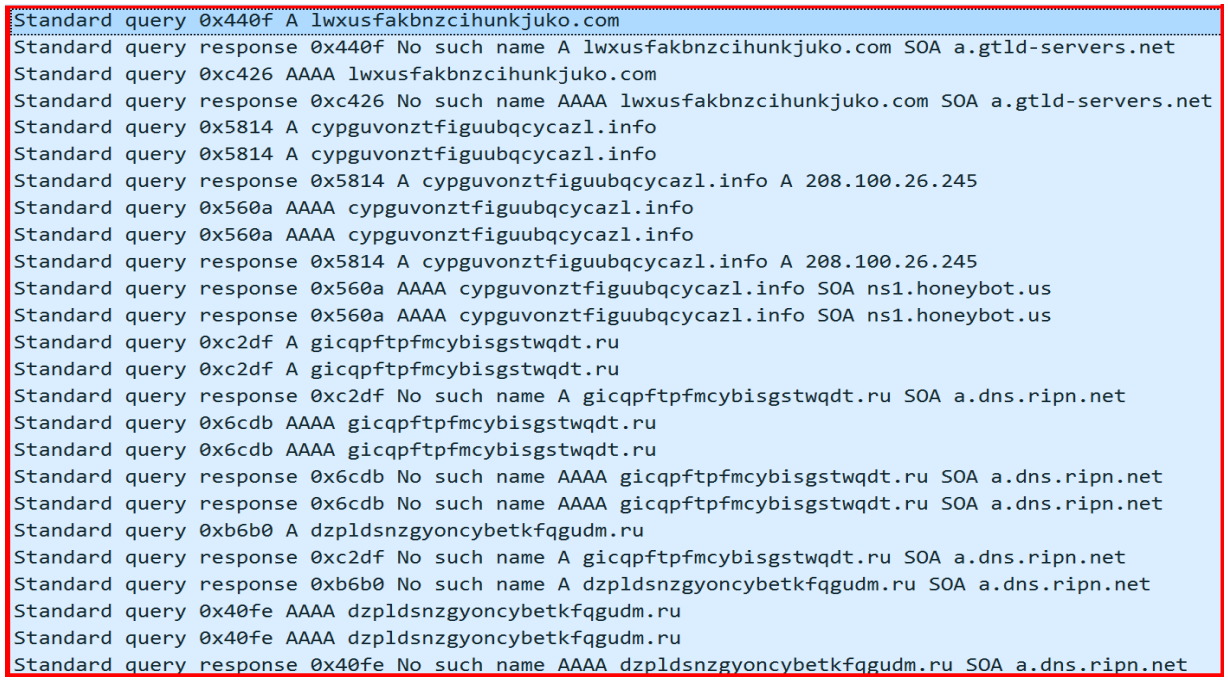
```
        m.update(seed_str.encode('latin1'))
        md5 = m.digest()

        domain = ""
        for m in md5:
            d = (m & 0x1F) + ord('a')
            c = (m >> 3) + ord('a')
            if d != c:
                if d <= ord('z'):
                    domain += chr(d)
                if c <= ord('z'):
                    domain += chr(c)

        tlds = [".ru", ".biz", ".info", ".org", ".net", ".com"]
        for i, tld in enumerate(tlds):
            m = len(tlds) - i
            if not index % m:
                domain += tld
                break
        print(domain)

if __name__=="__main__":
    parser = argparse.ArgumentParser()
    parser.add_argument("-d", "--date", help="date for which to generate domains")
    args = parser.parse_args()
    if args.date:
        d = datetime.strptime(args.date, "%Y-%m-%d")
    else:
        d = datetime.now()
    dga(d)
```

45-ci sətirdə dga funksiyasına cari dövrün tarix və vaxtı göndərilir. 6-cı sətirdə for dövrü bizə domen sayının 1020 ədəd olacağını göstərir. İlkin parametrlər olaraq ölçüsü 7 olan seed list yaradılır. İlkin parametrlər 8-14-cü sətrlərdə təyin olunur. 17-18-ci sətrlərdə ilkin parametrlərin chr funksiyası ilə əldə olunmuş xarakterləri seed_str stringinə birləşdirilir. Alınan stringin md5 xeş funksiyası hesablanır. 25-ci sətrdə hər bir md5 xeşin xarakterinin üzərində dəyişikliklər edilir. d və c dəyişəninə xarakter üzərində olunan

dəyişikliklər yazılır. Əgər d və c eyni olmasa, sayı 122-dən (ord('z') = 122) az olan dəyişənlər domain dəyişəninə yazılacaq. tlds listninə istifadə olunan domen adları təyin olunub. 36-cı sətirdə m dəyişəninə domen sayından hazırki domenin sıra nömrəsi çıxılır və sonra əgər index dəyişəni qalıqsız m dəyişəninə bölünürsə domain dəyişəninə domen adı əlavə edilir.Nəticədə 1020 saxta domen adı alır .Bu üsul nə qədər mürəkkəb olsada təhlükəsizlik əməkdaşları üçün faydalıdır. Program təminatı revers edilsə domen qeneratoru alqoritminin yaradacağı domenləri öncədən hesablayıb qara siyahıya əlavə etmək olar.
Digər maraqlı bir üsul zərərvericilərin xüsusi DNS serverlərin istifadəsidir. Xüsusi DNS serverlərin üstünlükləri xakerlərin nəzarəti altında olmasıdır və təhlükəsizlik işçiləri proqram təminatından domen adlarını əldə edəndən sonra həmin domenə müraciət edəndə, həmin domenə müraciət getməyəcək. Bu o anlama gəlirki xakerlər hamının tanıdığı domen adlarından istifadə edə bilər, məsələn google.com, facebook.com və s. Bu zaman xakerlərin əldə etdiyi üstünlük sandbox-un qaytardığı cavab, məsələn google.com, yanlış müsbətlərə (false positive) səbəb olur.

Saxta domenləri necə aşkar etmək olar?

Domen yaratma alqoritminin yaratdığı saxta domenləri şəbəkə paketlərinin tutulub təhlil edildikdən sonra müəyyən etmək olar. Bunun üçün, virtual məkanda, şəkil 2-də göstərilən alqoritm vasitəsilə bir domen gotürüb DNS sorğu göndərək. DNS əsas internet protokollarından biridir və bu protokol üçün 53-cü port istifadə olunur.
Ancaq xakerlər DNS mesaj formatına riayət etmədən, 53-cü portdan öz trafikini göndərmək üçün istifadə edirlər. DNS sorğuların analizi "Wireshark" proqramı vasitəsi ilə aparılacaq. "Wireshark" işə saldıqdan sonra "dns" filteri vasitəsilə DNS sorğulara diqqət yetirək:



Şəkil 4.

Şəkil 4-də qırmızı çərçivəyə alınan hissəyə nəzər yetirsək, saxta domen adlarına oxşar, DNS sorğular görəcəyik. İlk addımlarımızdan biri domenin qeydiyyatda olmasının təyin edilməsidir. Əgər domen qeydiyyatda deyilsə dərhal qara siyahıya əlavə olunmalıdır, əks halda analiz davam edilməlidir. Domen adlarının saxta olduğuna əmin olmaq üçün, vacib suallardan biri: gostərilən domen ünvanına hər hansı bir məlumatın ötürülüb? Göndərilən sorğunu pars edək:

Şəkil 5.

Şəkil 5-də, botun id-si, ip ünvan, ölkə, botun aktiv olmağına dair status, vaxt və versiya kimi məlumatlar HTTP protokolu üzərindən ötürülür. Müşahidə aparsaq görərik ki bu sorğular 30 saniyə aralıqla davamlı şəkildə aparılır. Bu cürə sorğuların normal olmamasına görə göstərilən domenləri qara siyahıya əlavə edib bloklamaq lazımdır. Göstərilən üsul ilə saxta domenlər zərərlinin analizi zamanı və ya şəbəkənin analizi zamanı əldə oluna bilər. Göstərilən üsullarla saxta domenlərin təyini təhlükəsizlik əməkdaşları üçün olduqca çətindir və çox vaxt aparır. Bu isə öz növbəsində maşın öyrənmənin inkişafına yol açır. İstifadə olunan alqoritmlardan biri klaster korrelyasiyasından istifadə edərəksaxta domenlərin aşkarlanmasıdır. Domen adının xüsusiyyətləri və uzunluğu, simvol tezliyi, leksik iyerarxik strukturunun təhlilini nəzərdə tutur.

İstinadlar

https://blog.malwarebytes.com/security-world/2016/12/explained-domain-generating-algorithm
https://hackersterminal.com/domain-generation-algorithm-dga-in-malware
https://www.techtarget.com/searchsecurity/definition/domain-generation-algorithm-DGA
https://www.avast.ru/c-botnet
https://www.techtarget.com/searchsecurity/definition/botnet
https://github.com/baderj/domain_generation_algorithms/blob/master/murofet/v2/dga.py