İnformasiya kommunikasiya texnologiyalarının inkişafında internet şəbəkəsində kibertəhlükəsizliyin rolu

Elçin Qafar oğlu Həsənov
Azərbaycan Respublikası Prezidenti yanında Dövlət İdarəçilik Akademiyasının dosenti
E-mail: elgafgas@yahoo.com
Bəhram Bəhlul oğlu Əzizov
Azərbaycan Universitetinin dosenti
E-mail: bah-aziz@rambler.ru
Zakir Habil oğlu Babazadə
Azərbaycan Universiteti
E-mail: zakirbabazade@gm

Rəyçilər: r.ü.e.d., prof. A.X. Xanməmmədov,
t.ü.f.d., dos. Ç.M. Həmzəyev

Açar sözlər: İKT, kiber hücum, internet şəbəkə, xakerlərin məqsədi, saytların yarılması
Ключевые слова: ИКТ, кибер атаки, хакеры и их цели, интернет сети, взламывание сайтов
Key words: ICT, cyber attacks, hackers and their goals, Internet networks, hacking sites

Bu mövzu kompüter və ya proqramlaşdırma ilə maraqlananlar üçün asan deyil. Bu ixtisas fərdi məlumatların və ya hər hansı digər məlumatların qorunmasına zəmanət verməyi hədəfləyir. Bir tələbənin aldığı dərəcənin ümumi adı Kompüter və İnformasiya Elmləri kimi səslənə bilər

"Kiber təhlükəsizlik" ixtisası işə demək olar ki, hər hansı bir şirkətin qapısını açır, çünki bugünkü dünyada informasiya təhlükəsizliyi ən vacib problem və əsas vəzifədir. Tələbələr verilənlər bazalarını saxlama metodlarını, şəbəkə fəaliyyətini izləmə üslublarını, məlumatları qorumaq prinsiplərini, haker hücumlarını dəf etmək üçün texnologiyaları öyrənirlər. Kompüterlərin həyata nüfuz etməsinin mövcud səviyyəsi ilə şəbəkə texnologiyaları, cihazlarda təhlükəsizliyin təmin edilməsi, İnternet təhlükəsizliyi, kriptoqrafiyaya, kriptovalyutaların öyrənilməsinə, "bulud" təhlükəsizliyinə, hər hansı bir "istifadəçinin" informasiya təhlükəsizliyinə diqqət yetirilir. Məlumat mənbəyi kimi proqramlaşdırma prosesində təhlükəsizlik nəzəriyyəsi və praktikası öyrənilir.

Ümumiyyətlə, ABŞ və Avropadakı müasir universitetlərdə əsas fənlər bunlardır: kompüter təhlükəsizliyi, şəbəkə təhlükəsizliyi, rəqəmsal məhkəmə ekspertizası, təhlükəsizlik sistemlə-

rindəki risklərin idarəedilməsi və kiber cinayətlərin araşdırılması.

Tələbələr hansı proqramdan (softlardan) istifadə edirlər?

Kiber Təhlükəsizliyi öyrənərkən tələbələr aşağıdakılardan istifadə edir və öyrənirlər: ENCASE; Nessus paketləri, MetaSploit, Kali Linux, OpenSSH, SSL və s. Tələbələr davamlı olaraq görünən və yenilənən ən yeni və inkişaf etmiş proqramı öyrənir və istifadə edirlər.

Cyber Security, əmək bazarında aktuallığı və tələbi zamanla artacaq olan super müasir bir peşədir. Bu peşə (ixtisas) zatən çox böyükdür və ABŞ kimi bir ölkədə belə son dərəcə yetkin mütəxəssis çatışmazlığı var! ABŞ-da və dünyanın bütün ən böyük İT şirkətləri (Facebook, Google, Pixar, Twitter, IBM, eBay, Amazon), daha kiçiklərdən danışmırıq, davamlı olaraq müvafiq peşələrini genişləndirərək bu peşə üzrə işçilər götürürlər.

Rəsmi statistikaya görə, ABŞ Əmək Statistika Bürosu, CIS (Beynəlxalq Məktəblər Şurası)) və Comodo İnternet Təhlükəsizliyi işçilərinin orta əmək haqqı 2017-ci ildə ildə 160.000 ABŞ dollarını keçdi! Yalnız bir nisbi dar çərçivədə olan "kiber təhlükəsizlik" ixtisası üçün 2021-ci ilədək iş sayı eyni ABŞ Statistika Bürosunun proqnozuna görə 210.000 olacaqdır!

Çox spesifik olmaq üçün İKT tələbələri aşağıdakı səriştələrə sahib olmalıdırlar:

— peşə fəaliyyətində yaranan problemlərin mahiyyətini müəyyənləşdirmək, elmin ümumi qanunlarından istifadə etmək və riyazi aparatı informasiya peşə tapşırıqları sahəsində tətbiq etmək;

— müasir cəmiyyətdə, informasiya texnologiyalarının tətbiqində, müxtəlif mənbələrdə və qlobal kompüter sistemlərində hədəfli məlumat axtarışında məlumatın mahiyyətini və əhəmiyyətini başa düşmək;

— peşə sahəsində hüquqi məsləhətlərdən istifadə;

— qanuni əsaslar, inzibati və texnoloji tətbiqetmə və iqtisadi səmərəliliyi nəzərə alaraq, mümkün təhdidləri müəyyənləşdirərək məlumat təhlükəsizliyini təmin etmək üçün köməkçi tədbirlər kompleksinin idarə olunması;

— dövlət və şirkət siyasətinin tələblərinə uyğun olaraq obyektlərə nəzarət;

— nəzarət, idarəetmə və istismarın alt sisteminin iştirakı və inkişafı;

— kibertəhlükəsizliyin təmin edilməsi üçün texniki və iqtisadi məqsədəuyğunluğun ilkin təhlilində iştirak;

— mövcud informasiya təhlükəsizliyi qaydaları nəzərə alınmaqla texniki göstəricilərin hazırlanması;

— informasiya təhlükəsizliyinin təmin edilməsi və sistem, tətbiq olunan və xüsusi tip proqram təminatlarının istifadəsi üçün ümumi alqoritmlər üçün proqramlaşdırma həlləri;

— tədqiqat zamanı hadisələrin və proseslərin təhlili və dizayn qərarları qəbul edilməsi;

— milli və xarici standartlardan istifadə edərək obyektlərin və sistemlərin informasiya təhlükəsizliyinin təhlili;

— informasiya təhlükəsizliyinin idarə olunması üçün bir sıra tədbirlərin (qaydalar, prosedurlar, praktik tövsiyələr) formalaşdırılması və inkişafı.

İnformasiya texnologiyaları bu gün iqtisadi fəaliyyətin demək olar ki, bütün sahələrində tətbiq edilmişdir. Bunlar işin daha səmərəli və davamlı olmasına kömək edir, inkişaf üçün yeni perspektivlər açır və əslində bir çox iş prosesinin əsası olur. Lakin, eyni zamanda, yeni təhdidlər də gətirirlər. Bu, informasiya texnologiyalarının yalnız ticarət əməliyyatları üçün deyil, həm də haqsız rəqabət üçün istifadə edilməsidir; təcavüzkarlar tərəfindən tez-tez istifadə olunur.

Ən ümumi təhdidlərə aşağıdakılar daxildir:

— saytları və məlumat bazalarını sındırmaq;

— zərərli proqramların paylanması;

— məxfi məlumatların oğurlanması;

— daxili infrastruktura uzaqdan giriş əldə etmək;

— təşkilatın normal fəaliyyətini pozmaq və ya işini tamamilə bloklamaq üçün verilənlər bazalarının redaktə edilməsi və ya məhv edilməsi.

Rəqəmsallaşma kiber təhlükəsizlik mütəxəssislərinə tələbat yaradıb. Ticarət və dövlət üçün yeni kadrların əsas mənbəyi bazarın tələblərini **başa düşməyi bacaran universitetlərdir**.

Yəni təhsil sustemi, xüsusən də ali məktəblər bu mövzunu dərk edərək bacardıqları qədər çalışırlar ki, müdavimlərini müasir biliklərə yiyələndirsinlər.

İnformasiya təhlükəsizliyinin inkişafı kimi kibertəhlükəsizlik, ənənəvi informasiya prosesləri modellərindən fərqli olaraq, xarici amillərin və hədəf dağıdıcı təsirlərin mövcudluğunu nəzərə alan maddənin, enerjinin və informasiyanın işlənməsi üçün müəyyən bir modelə əsaslanır.

Beynəlxalq informasiya təhlükəsizliyi standartlaşdırma qurumları, aparıcı dünya universitetləri, yüksək texnologiyalı aparıcı şirkətlər, innovasiya texnologiyalarının inkişaf perspektivləri, sənayeyönlü bir yanaşmanın yayılması nəzərə alınaraq ayrı bir elm olaraq informasiya təhlükəsizliyi sənayesinin perspektivli bir mənzərəsini meydana gətirirlər. Həm təhsildə, həmdə iqtisadiyyatın rəqəmsallaşdırılmasında. Eyni zamanda, informasiya təhlükəsizliyi çox vaxt rəqəmsallaşdırma istiqamətini müəyyənləşdirir, lakin özü buna əməl etmir.

Bu tendensiyanın tanınmış nümunələri pilotsuz nəqliyyat vasitələrinin maşın-arası (maşınaltı) şəbəkələri, birləşdirilmiş şəbəkə platformaları, 6G rabitə texnologiyaları və antropomorf robotlardır. Onlarda informasiya təhlükəsizliyi və kiber təhlükəsizlik məsələləri, tələbləri, standartları və metodları ön plana çıxır, informasiya və sənaye texnologiyalarının texnoloji imicini və tətbiq profilini formalaşdırır.

Bu səbəbdən kiber təhlükəsizlik mütəxəssislərindən yalnız ixtisaslaşmış şirkətlərdə və ya dövlət xidmətlərində deyil, həm də rəqəmsallaşdırma prosesinin getdiyi və qabaqcıl informasiya texnologiyaları ilə məşğul olduqları bütün müəssisələrdə tələb olunur.

Aşağıda kibertəhlükəsizliyə dair ümumi məlumatlar veriləcək, bu da öz növbəsində İnformasiya texnologiyaları sahəsindən hətta tamamilə kənar bir adamda belə minimal təsəvvürü oyadacaq.

Kiber təhlükə.

Kiber təhlükə - siyasi, sosial və ya digər məqsədlərə çatmaq üçün virtual məkana qanunsuz giriş və ya zərərli müdaxilə təhlükəsidir.

Kiber təhlükə, məlumatları ehtiva edən, fiziki və ya virtual bir cihazın materiallarını saxlayan bir kompüterin məlumat sahəsini təsir edə bilər. Hücum ümumiyyətlə istifadəçinin şəxsi məlumatlarının saxlanması, işlənməsi və ötürülməsi üçün xüsusi hazırlanmış bir saxlama mühitinə təsir edir.

Kiber təhdidlər hakerlərdən, serverləri sındırmaq və onlardan qanunsuz yolla məlumat əldə etmək qabiliyyətli insanlardan gəlir. Hacker kompüter proqramlarının incəliklərini başa düşən yüksək ixtisaslı mütəxəssisdir. Tarixən bu söz indi çox vaxt "kompüterə müdaxilə edən" mənasında istifadə olunur.

Ümumiyyətlə, kiber hücumlar qlobal maliyyə sistemi üçün bir nömrəli təhlükədir. Təhlükələrinə görə, kiber hücumlar 2008-ci ildə qlobal maliyyə böhranına səbəb olan kredit və

likvidlik risklərini də hətta üstələyirlər. Bu barədə bir çox İKT mütəxəssisləri məlumat verir.

Məsələn, CBS-də ABŞ Federal Ehtiyat Sisteminin İdarə Heyətinin sədri Jerome Powell daha ətraflı bunu izah edir: "Deyərdim ki, hazırda ən çox izlədiyimiz risklər kiber risklərdir. Buna görə kiber məkan hadisələrindən narahat olmalısınız. Bu, Fed (ABŞ Federal Ehtiyat Sistemi - red.) və buna böyük sərmayə qoyan bütün böyük özəl maliyyə şirkətləri daxil olmaqla bütün böyük özəl müəssisələr daxil olmaqla bir çox dövlət idarəsi tərəfindən çox yaxından izlənilən bir şeydir. Və deyərdim ki, bu, qlobal maliyyə böhranı kimi görünən deyil, real bir riskdir" dedi.

Federal Rezerv Sisteminin rəhbərinin izah etdiyi kimi hadisələrin inkişafı üçün ən pis ssenarilərdən biri, hakerlərin böyük bir ödəmə sistemini söndürməyi bacardıqları bir vəziyyət ola bilər ki, bu da bir maliyyə qurumundan digərinə pul axınına mane olacaq. Powell, maliyyə sisteminin sektorlarını və hətta bütün təbəqələrini bağlaya biləcəyini söylədi.

Powell hökumətlərin və özəl müəssisələrin bu cür təhdidlərdən getdikcə daha çox ehtiyatlandığını qeyd etdi: "Bu kimi şeylərdən qorunmaq üçün çox vaxt, səy və pul sərf edirik. Halhazırda bütün böyük qurumlara qarşı kiberhücumlar gündəlik həyata keçirilir. Və hökumət bunun üzərində işləyir. Bütün özəl sektor şirkətləri kimi. Bu təhdidlərlə mübarizə aparmaq çox səy tələb edir. Bu, dünyadakı təhlükə mənzərəsinin böyük bir hissəsidir "dedi.

İnsanlar niyə kiberhücumlar edirlər?

Təcavüzkarlar korporativ sistemlərdəki zəifliklərdən istifadə etməyə çalışırlar ki, bu da kibercinayətlərin illik artımına səbəb olur. Tez-tez hakerlər fidyə (girov) tələb edirlər: kiber hücumların 53%-i 500.000 dollar və ya daha çox zərərlə nəticələndi.

Kiberhücumlarda gizli məqsədlər də ola bilər. Hakerlərin sistemləri və məlumatları məhv etmək üçün bəzi cəhdləri "hacktivism"in özünəməxsus təzahürləridir.

Botnet nədir?

Botnet - viruslar kimi zərərli proqram təminatlarına yoluxmuş cihazlar şəbəkəsidir. Hackerlər, hücumların miqyasını artırmaq üçün sahiblərini bilmədən bir botnet'i tək bir qrup olaraq idarə edə bilərlər. Botnetlər tez-tez DDoS (Distributed Denial of Service) hücumları nəticəsində sistemlərə dözülməz bir yük yaratmaq üçün istifadə olunur.

Fişinq

Fişinq - etibarlı bir alıcıya göndərilmiş kimi görünən saxta mesajların ümumiyyətlə e-poçt yolu ilə paylanmasıdır. Bu fəaliyyətin məqsədi kredit kartları və ya hesablar kimi məxfi məlumatları oğurlamaq və ya zərər çəkmiş şəxsin kompüterinə zərərli proqram yükləməkdir. Fişinq getdikcə daha çox yayılmış bir kiber təhdiddir.

Vasitəçi hücumu

Ortadakı adam hücumları (MitM), yəni "Man in the middle", hakerlər iki tərəfin qarşılıqlı

təsirinə sızdıqda meydana gəlir. Trafikə giriş əldə edərək hakerlər məlumatları süzə və oğurlaya bilərlər.

Vasitəçi hücumlarını həyata keçirməyin iki ümumi yolu:

1. Təminatsız bir ümumi Wi-Fi şəbəkəsində hakerlər ziyarətçinin cihazı ilə şəbəkə arasındakı ərazini idarə edə bilərlər. Bunu bilmədən ziyarətçi bütün məlumatları haker vasitəsi ilə ötürəcəkdir.
2. Zərərli proqram cihaza sızdıqda, haker qurbanın bütün məlumatlarını təhlil etmək üçün tətbiqetmələr qura bilər.

SQL inyeksiyası

SQL (structured query language) inyeksiyası zərərli SQL-in SQL sorğularını işləyən bir serverə ötürülməsi və serverin ifşa etməyi planlaşdırmadığı məlumatları ifşa etməsidir. SQL kodunu vurmaq üçün bəzən həssas veb saytın axtarış sahəsinə zərərli kod daxil etmək kifayətdir.

DNS Tunelləşdirmə

DNS (Domain Name System) tunelləşdirmə, DNS protokolunun 53 nömrəli portda DNS olmayan trafiği ötürmək üçün istifadəsidir. Bu hücum HTTP və digər protokol trafikinin DNS vasitəsilə göndərilməsinə imkan verir. DNS tunelləşdirmə müxtəlif qanuni məqsədlər üçün istifadə edilə bilər. Bununla birlikdə, zərərli DNS tunel üçün VPN xidmətlərindən istifadə etmək mümkündür. Onların köməyi ilə, DNS trafiki adı altında, ümumiyyətlə bir İnternet kanalı ilə ötürülən məlumatları ötürə bilərsiniz. Təcavüzkar, DNS sorğularını istifadə edərək, təhrif olunmuş bir sistemdən məlumat çıxara və ətraf mühitə köçürə bilər. Bunlar, həm də hacker infrastrukturundan zədələnmiş idarəetmə sistemini güzəştli bir sistemə yönəltmək üçün istifadə edilə bilər.

Kriptoqrafiya (ümumi məlumat)

Kriptoqrafiya (qədim yunan dilindən hiddenρυπτός “gizli” + γράφω “yazıram”) məxfiliyi (məlumatı yad insanlar tərəfindən oxumağın mümkünsüzlüyü), məlumatların bütövlüyünü (məlumatdakı hiss olunmayan dəyişikliklərin mümkünsüzlüyünü), identifikasiyanı (doğrulamağı) təmin edən metodlar haqqında elmdir. bir obyektin müəllifliyinin və ya digər xüsusiyyətlərinin həqiqiliyi), şifrələmə (məlumatların kodlaşdırılması).

Başlanğıcda kriptoqrafiya məlumat şifrələmə metodlarını - gizli alqoritm və ya açar əsasında açıq (orijinal) mətnin şifrə mətninə çevrilməsini öyrənirdi. Ənənəvi kriptoqrafiya simmetrik kriptosistemlərin bir hissəsini təşkil edir ki, burada şifrə və şifrənin açılması eyni gizli açardan istifadə olunur.

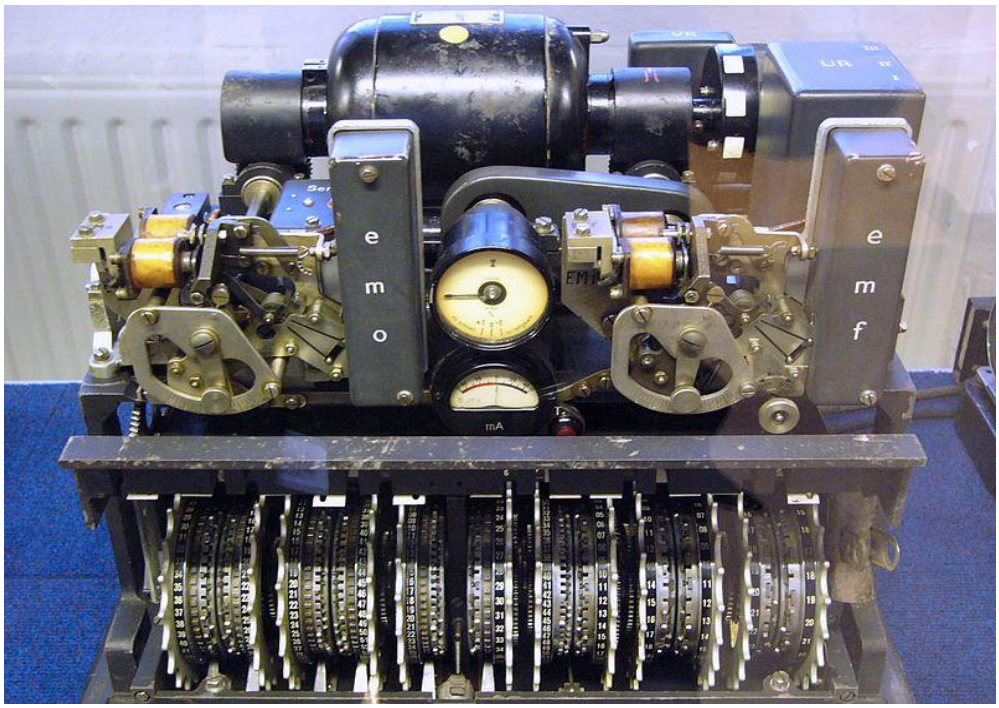
“Lorenz” alman kripto maşını, İkinci Dünya Müharibəsi dövründə ən gizli mesajları şifrələmək üçün istifadə edilmişdir

Bu bölməyə əlavə olaraq müasir kriptoqrafiya asimmetrik kriptosistemləri, elektron rəqəmsal imza (EDS) sistemləri, hash funksiyaları, açar idarəetmə, gizli məlumatların alınması, kvant kriptoqrafiyasını əhatə edir.

Kriptoqrafiya qanuni abunəçilərin aldatma, rüşvət və ya şantaj, açarların oğurlanması və təhlükəsiz məlumat ötürmə sistemlərində ortaya çıxan digər məlumat təhdidlərindən qorunmaq deyil.

Kriptoqrafiya ən qədim elmlərdən biridir, tarixi bir neçə min il əvvələ gedib çıxır.

Şifrə mətni, şifrə (qapalı) mətn - kriptosistemdən istifadə edildikdən sonra əldə edilən məlumatlar (ümumiyyətlə müəyyən bir açarla). Başqa bir ad: kriptoqram.



Şifrə, kriptosistem - düz mətnin şifrəli mətnə çevrilə bilən çevrilmələr ailəsi.

Şifrələmə - düz mətnin bir alqoritm və açara əsaslanan şifrəli mətn çevrilməsinin normal tətbiqi.

Şifrənin açılması şifrəli mətni düz mətnə kriptoqrafik olaraq çevirmək üçün tətbiq olunan normal prosesdir.

Asimmetrik şifrə - iki açar şifrə, açıq açar şifrə - şifrələmə və şifrəni açmaq üçün iki düymədən istifadə edən şifrədir. Eyni zamanda, yalnız şifrələmə düyməsini bilməklə mesajın şifrəsini açmaq mümkün deyil və əksinə.

Kriptanaliz məlumatların məxfiliyi və bütövlüyünün pozulmasının riyazi metodlarını araşdıran bir elmdir.

Kriptanalizator kriptanaliz metodlarını yaradan və tətbiq edən bir elm adamıdır.

Kriptoqrafik hücum - kriptanalizatorun hücum edilən təhlükəsiz məlumat mübadiləsi sistemində sapmalara səbəb olma cəhdidir. Uğurlu bir kriptoqrafik hücuma hack və ya hücum deyilir.

Deşifrovka - məlum şifrələnmiş kriptoqrafik açarı bilmədən düz mətnin çıxarılması prosesidir. Şifrələmə termini ümumiyyətlə şifrəli mətnin kriptanaliz prosesi ilə əlaqədardır (kriptanalizin özü, ümumiyyətlə, şifrələnmiş açıq mesajla yanaşı, kriptosistemin analizindən də ibarət ola bilər).

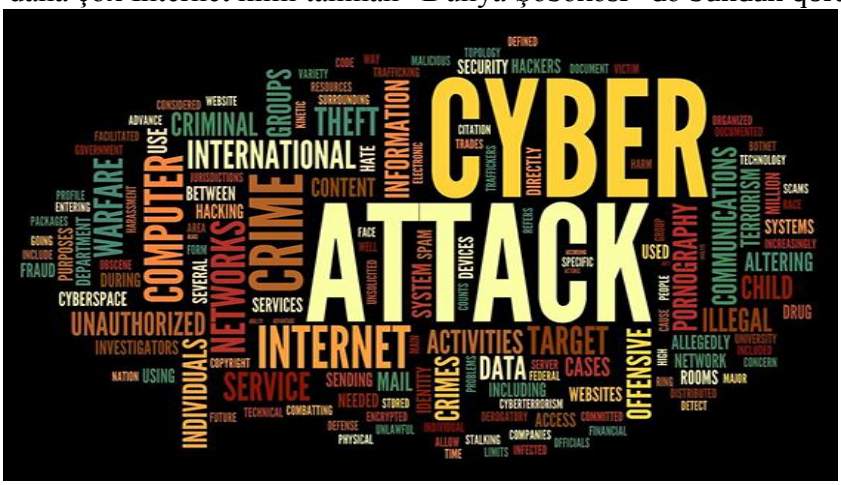
Hibrid kriptosistem ümumi açar kriptosisteminin üstünlüklərini simmetrik kriptosistemlərin performansı ilə birləşdirən şifrələmə sistemidir.

Elektron rəqəmsal imza və ya elektron imza - asimmetrik imitasiya (təhlükəsizlik açarı doğrulama düyməsindən fərqlidir). Başqa sözlə, imtahan edən şəxsin saxta edə bilməyəcəyi elə bir təqlid əlavəsidir.

Sosial şəbəkələr artıq təhlükəlidir.

İsrail alimləri yaxın gələcəkdə sosial şəbəkələrin istifadəçilərinin "şəxsiyyət itkisi" ilə təhdid olunduğuna inanırlar. Xüsusi bir proqramın köməyi ilə təcavüzkarlar İnternet istifadəçiləri haqqında bütün məlumatları toplayacaq və bunun əsasında cinayət törətmək üçün istifadə edilə bilən bir şəxsin virtual ikiqatını yaradacaqlar.

İnsan çox qəribə bir məxluqdur. Həmişə elmi və texnoloji tərəqqinin hər bir nailiyyətini cinayət törətmək üçün bir silah kimi istifadə etməyə çalışır. Təəssüf ki, əksər insanlar tərəfindən çox sevilən, daha çox İnternet kimi tanınan "Dünya Şəbəkəsi" də bundan qorunmur.



Bu ecazkar virtual rabitə vasitəsi lüks deyil, zərurət "əmtəəsinə" çevrilən kimi dərhal müxtəlif cinayətkarlar tərəfindən mənimsənildi. Üstəlik, əvvəlcə, virtual təhlükəsizlik sistemləri hələ o qədər mükəmməl olmadığında, hakerlər çox vaxt izlərini gizlətmirdilər. Daha sonra İnternet istifadəçiləri bu problemdən ciddi şəkildə narahat olduqda, cinayətkarlar daha hiyləgər fəndlərdən istifadə etməli, məsələn, başqasını təqlid etməli idilər. Bu texnikanın uzun müddət müvəffəq olması, təhlükəsizlik xidmətlərinin təcavüzkarın özünü anlaya bilməməsi, ancaq cinayətin törədildiyi kompüteri müəyyənləşdirmələri ilə əlaqədardır.

Ancaq son vaxtlar "şəbəkə nəzarəti" sistemləri getdikcə daha da təkmilləşdirilir və bir cinayətkarın başqasının ləqəbi altında gizlənməsi getdikcə çətinləşir. Bununla birlikdə, hakerlərin qısa müddətdə virtual hüquq mühafizə xidmətlərinə zərbə endirə biləcəyi ehtimalı var. Lakin, şəbəkə məkanının "pis dahiləri" bu dəfə nəyi ixtira edəcək?

Bu problemlə məşğul olan İsrail alimləri, "şəbəkə haker işçiləri"nin növbəti addımının insanların fərdi məlumatlarını sosial şəbəkələrdən oğurlayacaq və bunun əsasında "virtual ikiqatlıqlar" yaradan bir proqramın tərtibi ola biləcəyinə inanırlar. Belə bir cinayət şəxsiyyət oğurluğu kimi təsnif edilməlidir. Üstəlik, bu vəziyyətdə bir adam sadəcə əylənmək üçün deyil, onun əsasında yaradılan "surətin" İnternet vasitəsilə bəzi qanunsuz hərəkətlər etməyi planlaşdıran cinayətkarlar üçün qalxan rolunu oynaması üçün oğurlanır, m.ü.. bank hesabının oğurlanması.

Ancaq yaxın illərdə belə bir proqram yaratmaq mümkündürmü? Ben-Gurion Universitetinin (Negev) tədqiqatçılarının işi bəli olduğunu göstərdi. İsrail mütəxəssisləri bu yaxınlarda bu cür proqramın demo versiyasını nümayiş etdirdilər. Bu onlayn proqram, uzun müddətdir bir neçə spesifik İnternet istifadəçisinin davranışını, sosial əlaqələrini və asılılıqlarını izlədi və daha sonra maraqlandığı bütün məlumatları öz şəxsi səhifələrindəki göstərilən bölməyə göndərdi.

Tədqiqatçılar inanırlar ki, fırıldaqçılar istənilən an şəxsiyyət oğurluğunun əsas təhlükəsinin mənbəyi və dəyişdirilməsi çətin olan istifadəçi məlumatlarını oğurlamağa qadirdirlər. Məsələn, oğurlanmış bir kredit kartı nömrəsi və ya şifrə daha sonra başqa birinə dəyişdirilə bilərsə (köhnəsini blokladıqdan sonra), belə bir cinayət qurbanının adını, doğum ilini, pasport nömrəsini, həm də xarakterik vərdişlər və zövqlərin dəyişdirməsi çox çətin olacaq.

Bəzi amillər, məsələn, keçmişdəki faktlar və ya valideynlərin adları heç bir şey ilə əvəz edilə bilməz. Bu mümkünsüzdür. Ancaq virtual bir şəxsiyyət yaratmaq üçün, bir qayda olaraq, yalnız sosial şəbəkələrin istifadəçisinə yaxın insanların bildiyi məlumatlar daxil olmaqla hər hansı bir məlumat istifadə olunur. Üstəlik, virtual ikiqat nə qədər detallı və "canlı" olarsa, cinayətkarın arxasında gizlənməsi o qədər asan olar.

Ən acınacaqlısı budur ki, indi də orada "qeydiyyatdan keçən" hər bir istifadəçi ilə bağlı sosial şəbəkələrdə bir çox maraqlı şeyləri öyrənə bilərsiniz. Bu şəbəkələrdən ünsiyyət və virtual məkanda yaşamaq üçün istifadə edən insanlar tez-tez əlaqə saxladıqları şəxslərdən heç bir şey gizlətmirlər, ziyarətçilərdən hər hansı birinin bu cür şəxsi məlumatları axtaran bir müdaxilə çevrilə biləcəyini tamamilə bilmirlər. Belə çıxır ki, bir gün bu istifadəçilərin "virtual ikiqatlığı" tərəfindən törədilən bir cinayətdə ittiham olunurlarsa, təəssüf ki, baş verənlərdə özlərini, daha doğrusu həddindən artıq açıqlıqlarını (səmimiyyətini) günahlandırmalıdırlar.

İsrail alimləri tərəfindən hazırlanan proqram, hərəkətinin aşkarlanmasının çox çətin olması ilə də təhlükəlidir. Bütün müasir şəbəkə təhlükəsizliyi vasitələri hal-hazırda sosial şəbəkələr üzərindən göndərilən fayllarda gizlənə bilən bu zərərli agenti tanıya bilmir. Əlbəttə ki, gələcəkdə kompüter alimləri bununla mübarizə yollarını mütləq tapacaqlar (axı əvvəllər tutulmayan "Trojan"ları - başqalarının şifrələrini oğurlayan proqramları zərərsizləşdirmə yolları tapdılar). Ancaq o zamana qədər yüzlərlə "virtual şəxsiyyət" artıq qaçırılmış (qarət edilmiş) ola bilər.

Alimlər bu cür qaçıranların kütləvi inkişafının şəbəkə "qul ticarəti"nin yaranmasına səbəb ola biləcəyini - hakerlər tərəfindən oğurlanmış "virtual ikiqat"ların cinayətkar məqsədlər üçün istifadə etmək istəyənlərə satılmasına əsaslanan bir işin ortaya çıxmasına səbəb ola biləcəyini təxmin edirlər. Tədqiqatçıların hesablamalarına görə, yaxın gələcəkdə bu tip kölgə virtual işi spam və ya onlayn pornoqrafiyanın yayılmasından daha sərfəli ola bilər. Üstəlik, bu cür "virtual kölə tacirləri"ni izləmək və zərərsizləşdirmək çox çətin olacaq.

Yaxşı, "şəbəkə" kimliyinizin cinayətkarlar tərəfindən qaçırılmaması üçün nə etməlisiniz?

İnformasiya təhlükəsizliyi mütəxəssisləri sosial media istifadəçilərinin hesablarını mümkün qədər çox bağlamalarını tövsiyə edir və bu hesabı yalnız əlaqə siyahısında olanlara təqdim edirlər. Ancaq təsəvvür etdiyiniz kimi, bu cür təhlükəsizlik tədbirləri, dostlarınızın şəxsiyyətinin "virtual surətini" istifadə edərək əlaqə siyahısına düşə bilən kiber cinayətkarlara qarşı yüz faiz qorunmasını təmin etmir.

Göründüyü kimi, ünsiyyət qurmaq üçün bu şəbəkələrdən istifadə edən hər kəs həmsöhbətləri ilə daha az səmimi olmalı və səhifələrində tamamilə "açılmamalıdır". Yalnız belə ehtiyatla onları şəbəkə müdaxiləçiləri tərəfindən şəxsiyyət oğurluğundan xilas edə bilərsiniz.

Razılığa gəlin ki, özünüzü virtual ikiqatınızın "arxasında gizlənərək" başqasının törətdiyi bir cinayətə görə məsuliyyət daşımaqdansa, gizli bir şəxs kimi qurmağınız daha yaxşıdır ...

İnternet gözətçiləri sizi izləyir! Facebook-dan...

Amerikanın New Hampshire əyalətindəki müstəntiqlər, cinayətkarların ... qurbanların özlərinin kömək etdiyi görünməmiş bir sıra oğurluq hadisələrinin üstünü açıblar. Üç cinayətkardan ibarət mütəşəkkil bir qrup, yüz min dollardan çox pulla onlarla evi qarət etdi və başqasının əmlakını oğurladı.

"Əslində, İnternetdə cinayətlər törədildi, çünki onun köməyi ilə oğrular bir evə girməyin mümkün olduğunu bildilər və planlarını qurdular" - yerli polis nümayəndələrindən biri deyir.

Bütün qurbanlar dünyanın ən populyarlarından biri olan (təqribən 500 milyon istifadəçisi olan) Facebook-da qeydiyyatdan keçiblər. Bu yaxınlarda bu portalın rəhbərliyi yeni bir funksiya təqdim etdi: indi sistemdə bir mobil telefon nömrəsini qeydiyyatdan keçirmək istəyən hər kəs yerləşdiyi yer barədə qısa mətn mesajları göndərəcək. Məsələn, "evimin yanındakı idman salonunda", "meydandakı bir kafedə", "hava limanında Haitiyə uçuram, hər kəs həsəd aparır" və s.

Əlbəttə ki, bu seçim ən yaxşı niyyətlə yaradıldı. Güman edilirdi ki, "Places" bölməsi dostlarına əyləncələrini koordinasiya etməyə kömək edəcək - bu anda yaxınlarının harada olduğunu öyrənmək və buna görə gündəlik işlərini qurmaq. İndiyə qədər New Hampshire polisi, yeni bir funksiyanın portalının tətbiqi ilə bir sıra oğurluqlar arasında birbaşa əlaqənin olub-olmaması barədə rəsmi bir açıqlama almamışdır. Ancaq jurnalistlər artıq nəticə çıxarıblar: hər halda MSNBC kanalı birbaşa cinayətlərin sosial şəbəkələrdə törədildiyini iddia edir.

Yeni fürsəti təqdim edən Facebook meneceri Michael Sharon jurnalistlərə "yerinizi bütün dünyaya açıqlamaq deyil, dostlarınız və ailənizlə ünsiyyəti daha da yaxın və isti etmək" məqsədi daşıdığını söylədi. Ancaq portalın bir çox digər funksiyaları kimi, burada da hər şey öz planlarını kimə və necə izah edəcəyinə qərar verən istifadəçilərin iradəsinə qalır. Lakin, bir çox insan diqqəti unutdurur.

Bəzi insanlar "onlayn səmimiyyətlərinin" nəticələrini düşünmürlər. Bəlkə də portal administratorları "müştərilərini" üzləşdikləri təhlükə barədə xəbərdar etməlidirlər, ancaq əsas tədbirlərə əməl etməsəniz, vəziyyətin nə qədər ciddi ola biləcəyini özləri başa düşdükləri ehtimal olunur.

"Qeydiyyatdan keçərkən profillərinin parametrlərini düzəldərək, əksər istifadəçilər bir neçə opsiyaları tərk edərək bir sıra variantları atlayırlar. Kimsə daha sürətli qeydiyyatdan keçmək istəyir və sadəcə ayarların edilməsinə ehtiyac görmür. Kimsə bunu daha sonra etməyi gözləyir və sonra unudur. Ancaq insanların böyük əksəriyyəti sözdə dostlara giriş üçün səhifələri tamamilə açıqdır. Və burada "dostlar" siyahısından kimin həqiqətən bizim dostumuz deyə özümüzdən soruşmalıyıq, —" dedi.

Amerikalı İnternet mütəxəssislərinin izah etdiyi kimi, portalın moderatorlarını dolayı yolla oğrulara qarşı ittiham etmək belə tamamilə haqsız olardı. Məsələ burasındadır ki, "Places"

funksiyası olmasa da, bir çox istifadəçi şəxsi səhifələrindən istifadə edərək dostlarına indi olduqlarını və ya müəyyən bir zamanda olacağını söyləmək imkanı tapırlar. Məsələn, on minlərlə insan tətilə getmədən əvvəl bu sevincli hadisəni "statuslarında" əks etdirməyi lazım bilir. "Məni bir həftə axtarmayın, tropik cənnətdə olacağam" və ya "Vay, bu axşam Madonnanın konsertindəyəm" kimi coşğulu mesajlar qeyd edilir. Bu tipli səhifələr ictimaiyyətə açıq olarsa, profil sahibinə, yəni qeydiyyatdan keçmiş istifadəçilərə zərər vurula bilər.

Nyu-Hempşirdə 88 min əhalisi olan kiçik Nashua qəsəbəsindəki polis, üç təcavüzkarın Facebook da daxil olmaqla sosial şəbəkələrdə yer məlumatları (location) axtardığını söylədi. İki yerli yeniyetmə və Massaçusetsdən bir gənc hansı istifadəçilərin evdən uzaq olduğunu və yaxın bir neçə saat ərzində ora qayıtmaq istədiklərini təyin etmək üçün məlumat toplayırdılar. İnsanlara planları, məsələn Foursquare və Gowalla haqqında məlumat yerləşdirməyə imkan verən bir sıra İnternet xidmətləri var, lakin populyarlıqları daha azdır. Bir çox insan Twitterdə öz mikrobloqlarından istifadə edərək dostlarına hara gedəcəklərini söyləyirlər: "Artıq cinayətkarların sosial şəbəkələrdə qurban seçdiyini müəyyənləşdirə bildik" - yerli polis kapitanı Ronald Dickerson The Nashua Telegraph-a verdiyi müsahibədə dedi. – Hər halda bu sizin tətil və ya həftə sonu planlarınız barədə şəbəkədəki məlumatlardır. "Bu anda istintaqda 18 cinayət epizodu haqqında məlumat var, lakin daha çox qaçırılma (yəni qarət, abduction) ola biləcəyini istisna etmir. Şübhəlilər artıq tutulublar və tezliklə məhkəməyə veriləcəklər.

Bu arada, İnternet təhlükəsizliyi sahəsində mütəxəssislər insanları İnternetdə lazımsız şəxsi məlumatların yerləşdirilməsinə qarşı xəbərdar etməyə davam edirlər. Bu yaxınlarda, World Wide Web-in Amerika seqmentində tamamilə kobud istifadəçilərə həsr olunmuş bir sayt ortaya çıxdı - onlayn yerləşdirdikləri məlumatların təhlili və müvafiq nəticələrlə dolu bir portal. Söhbət təkcə sosial şəbəkələrdən deyil, həm də orijinal ad və soyadla qeydiyyatı tələb edən bütün veb mənbələrdən, telefon nömrəsi, ev ünvanı və digər koordinatlardan gedir.

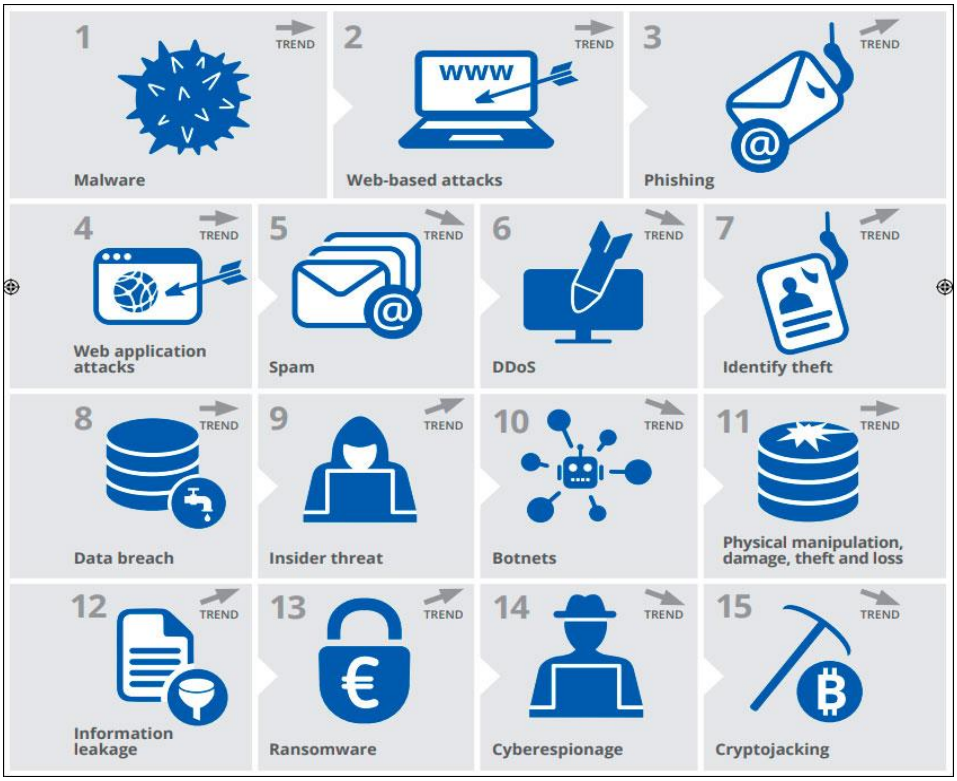
Belə bir saytın materialına əsasən bir qərib harada və nə vaxt olacağınızı müəyyən edə bilərsə, belə bir mənbədə qeydiyyatdan keçməmək daha yaxşıdır. Bu xəbərdarlıq ilk növbədə müəyyən tədbirlər, əyləncə, sənət (sərgilər cədvəli ilə və s.), idman və alış-verişə həsr olunmuş saytlara aiddir.

Müstəqil mütəxəssislərin fikrincə, Facebook istifadəçilərinin yüzdə 38-i və Twitter istifadəçilərinin yüzdə 33-ü tətillər və həftəsonları haqqında məlumatlarını mütəmadi olaraq internetdə yerləşdirirlər. Bu məlumatlar geniş insanlara təqdim olunduqca, soyğunçulara "müştəri" olma riski çox yüksəkdir.

Muzdlu haker sayında həyəcan verici artım - CloudSavvy IT
Qaranlıq hörümçək torunda gizlənmək

Haraya baxacağınızı bilirsinizsə, sizin üçün kiber cinayətlər törətmək müqabilində pulunuzu məmnuniyyətlə götürəcək muzdlu bir haker tapa bilərsiniz. Qaranlıq vebdə hakerlərin şübhəli xidmətlərini reklam etdikləri bir çox yer var. Bu hacker forumları və darknet bazarları illərdir mövcuddur. Onlar demək olar ki, yeni deyillər. Yenilik, hacker axtaran insanların özləri üçün çirkli işlərini görməsinə dair mesajların birdən-birə artmasıdır.

Darknet-ə çıxmaq o qədər də çətin deyil. Yalnız doğru vasitələrdən istifadə etməlisiniz. Qaranlıq ağ, darknets adlanan bir sıra örtük şəbəkələrindən ibarətdir. Ortaq internet infrastrukturu ilə işləyirlər, ancaq öz protokol dəstlərini və rele adı verilən marşrut qovluqlarını istifadə edirlər. Darknet veb ünvanlarında ".onion" və ".i2p" kimi qeyri-adi şəkilçilər var.



Darknets sizə iki supergüc (imkan) verir: anonimlik və görünməzlik. Qaranlıq veb protokollar şifrələnir, beləliklə internet trafikinizi heç kim görə bilməz və qaranlıq veb marşrut qovşaqları geriyə baxmaq və IP ünvanınızı müəyyənləşdirmək üçün başqa fəndlərdən istifadə edir.

Əksər şeylər kimi, darknet öz başına nə yaxşı, nə də pisdir. Cinayətkar olmayan bir çox darknet istifadəçisi də var. Repressiv rejimlərin müxalifləri onlardan dünya ilə əlaqə qurmaq üçün istifadə edirlər. Darknets qanuni səbəblərdən məlumat verənlər, aktivistlər və hətta hərbçilər tərəfindən istifadə olunur. Bir çox qəzet qaranlıq bir veb portal saxlayır, beləliklə anonim mənbələr məqalələr təqdim edərkən şəxsiyyətlərini qoruya bilər. Darknetin anonimliyi onu hər növ cinayətkarlar üçün belə cəlbedici bir cənnətə çevirir.

Görünməz İnternet Layihəsi (I2P), FreeNet və Tor Layihəsi ən məşhur qaranlıqlardan biridir. Tor qaranlıq şəbəkəsi cinayətkarlar üçün ən cəlbedici olduğunu sübut etdi.

Hakerlərin axtarışımda

Tor brauzeri Tor darknet-ə keçməyə kömək edir. Bir Virtual Şəxsi Şəbəkə (VPN) ilə istifadə olunan əsl şəxsiyyətiniz mümkün qədər gizlədiləcəkdir. Beləliklə, siz qaranlıq şəbəkədəsiniz. İndi nə? Qaranlıq veb üçün Google-dan yaxşı bir şey yoxdur. İstədiyiniz yerdə axtarış edə bilməzsiniz. Ziyarət edəcəyiniz bazarın və ya saytın veb ünvanını bilməlisiniz.

Tor brauzerini, VPN-i və .onion saytlarını anlamaq vacibdir, bu cür brauzerlər müəyyən dərəcədə mülayim bir şəkildə internetə həssas (naşı) insanlar üçündür. Muzdlu hakerlərin mövcudluğu və təcrübələrini reklam etdikləri bir forum və ya bazar tapmaq da onlardan kənara çıxmamalıdır. Əsl çətinlik hansı mesajların fırıldaqçı olduğunu tapmaqdır.

Bir hackerin - ümumiyyətlə bu hackerdirsə - pulunuzu almayacağını və heç nə etməyəcəyini necə bilirsiniz? Və ya haradan bilirsiniz?

Bir hacker haradan bilir ki, onları hüquq-mühafizə tələsinə cəlb etməyə çalışmırsınız? Gecə keçid zolağının rəqəmsal ekvivalentində çətin anlaşmalar etmək problemidir. Etibar edə biləcəyiniz bir cinayətkar tapdığınızı necə bilirsiniz? Bu əsl təzaddır.

Ancaq hackinq xidmətlərini reklam edən yazıların çoxu fırıldaq olsa da, qalanları gerçəkdir. Darknet-də deponent xidmətləri mövcuddur. Əməliyyatlar üçün pulu hər iki tərəf də işlərinin qarşılıqlı məmnuniyyətlə tamamlandığından razı olana qədər saxlayırlar. Ancaq bəzi hacker yazılarının saxtakar olub-olmaması, hacker axtaran potensial müştərilərdən göndərilən yazı sayının artmasını izah etmir.

Alıcılar pulla ayrılırlar, bunu istəmirlər. Beləliklə, saxta olduqları halda heç bir şey qazanmayacaqlar. Hüquq mühafizə orqanları hakerləri aldatmaq üçün daha mürəkkəb strategiyalardan istifadə edir. Potensial bir alıcıya saxta reklam vermək çox böyük bir ümid bağlamaq üçün bir vasitədir.

Cinayətkarların kompromis anından əvvəlki fəaliyyəti iş həftəsi ərzində üç dəfə çoxdur, güzəştdən sonra trafik isə bu baxımdan daha az fərqlənir.

Bəzi təhdidlərin başqalarına nisbətən ümumi bir infrastrukturdan istifadə ehtimalı daha yüksəkdir. İstifadəçilər və müəssisələrin veb saytlarını yaratmağı asanlaşdıran veb platformalar, son illərdə kiber cinayətkarların diqqət mərkəzində saxladığı texnologiyaların nümunələridir.

Ransomware (soyğunçu proqramlar) yox olmayıb, daha çox hədəflənib və varlı istifadəçilərə yönəlib.

Təcavüzkarlar getdikcə kiberhücumları təmin etmək üçün hədəf sistemlərinə quraşdırılmış ikili məqsədli alətlərdən daha çox istifadə edirlər.

Təhlükəsiz rəqəmsal gələcək

Rəqəmsallaşma yayıldıqca kiber təhlükəsizlik mütəxəssislərinə tələb artacaq. Bu tendensiya xüsusilə Şərqi Avropa ölkələri üçün aktualdır: məlumata görə şirkətlərin% 80-dən çoxu rəqəmsal transformasiyanın başlanğıc mərhələsindədir, bu da inkişaf üçün böyük potensialın olduğu deməkdir.

Buna paralel olaraq, tələbələrin ixtisaslaşa biləcəyi informasiya təhlükəsizliyi sahələri də genişlənəcəkdir. Məsələn, Universitetlərdə ICB kiberpsixologiya, rəqəmsal istehsalın kiber

davamlılığı və nüfuz testləri sahəsində yeni təhsil proqramları açmağı planlaşdırır.

Ekspertlərin fikrincə, kibertəhlükəsizliyin İnstitutunun təhsil və elmi fəaliyyəti, birincisi, sənaye sistemlərinin kiber davamlılığı, rəqəmsal istehsal, nəqliyyat, məhsulların interneti, ağıllı ev, sonra isə kiberpsixologiya, şəxsi təhlükəsizlik istiqamətində inkişaf etməlidir. Rəqəmsal dünya, çünki rəqəmsallaşma fəal şəkildə sosial sahədə dəyişir. Rəqəmsal gələcək üçün bunlar çox tələb olunan ixtisaslardır.

Tədqiqatın əsas nəticələri

Araşdırmalar kiber cinayətkarların hər zaman imkanları maksimum dərəcədə artırmağa çalışdıqlarını göstərdi. Həftə içi və həftə sonları kiber öldürmə zənciri fazalarının veb süzgəcinin miqdarını iki mərhələ ilə müqayisə etdikdə, güzəştdən əvvəl aktivliyin iş həftəsi ərzində üç dəfə yüksək olduğu, bu baxımdan güzəştdən sonra trafikin az olduğu fərqləndirildi.

Bu, əsasən zəifliklərin axtarılması üçün kiminsə fişinq e-poçtundakı bir keçidi izləmək kimi bir hərəkətin tələb etməsi ilə bağlıdır. Bunun əksinə olaraq, aktiv addımlar üçün belə bir tələb yoxdur (command-and-control, C2), buna görə də bu cür fəaliyyət hər an müşahidə oluna bilər. Kiber cinayətkarlar bunu başa düşür və istifadəçilər ən çox İnternetdə olduqları iş həftəsi ərzində imkanlardan maksimum istifadə etməyə çalışırlar.

Müxtəlif təhdidlərin müəyyən bir infrastrukturdan istifadə dərəcəsi bir sıra vacib tendensiyalar barədə məlumat verir. Bəzi təhdidlər digərlərinə nisbətən vahid və ya ixtisaslaşmış infrastrukturlardan daha çox yek, yəni bir ümumi infrastrukturdan istifadə etmək ehtimalı daha yüksəkdir. Təhlükələrin demək olar ki, 60%-i ən azı bir ümumi domen daxilində həyata keçirilmişdir ki, bu da əksər botnetlərin artıq qurulmuş bir infrastrukturdan istifadə etdiyini göstərir.

Bu, infrastrukturun zərərli kampaniyaların həyata keçirilməsində xüsusi rol oynadığını göstərir. Hansı təhdidlərin eyni infrastrukturdan istifadə etdiyini və hücum zəncirinin hansı nöqtələrində olduğunu anlamaq, təşkilatların gələcəkdə potensial inkişaf nöqtələrini və zərərli proqram və ya botnetlərdə dəyişiklikləri proqnozlaşdırmasına imkan verir.

Bir təşkilatın yalnız təhdidlərdən düzgün şəkildə müdafiə olunmağı deyil, həm də gələcək hücumları inkişaf etdirməyə və avtomatlaşdırmağa hazırlaşma qabiliyyətini artırmaq üçün bütün paylanmış şəbəkə daxilində mövcud olan təhlükəli kəşfiyyat vasitələrinə ehtiyac var. Əldə edilən bilik, meylləri müəyyənləşdirməyə, rəqəmsal bir hücum səthinə yönəlmiş müxtəlif metodların təkamülünü qiymətləndirməyə və kiber cinayətkarların məhz nəyə hədəfləndiyini əsas götürərək özü üçün kiber gigiyena prioritetlərini təyin etməyə kömək edəcəkdir.

Yalnız geniş miqyaslı, inteqrasiya olunmuş və avtomatlaşdırılmış platformaya əsaslanan struktur yaradılmalıdır, və bu struktur təhlükəsizliyə yanaşma ilə İnternetdəki məhsullardan tutmuş, nüvə və çox buludlu infrastrukturlara qədər bütün şəbəkə mühitiniz üçün sürətli və geniş bir qorumanı təmin edə bilər.

Məqalənin aktuallığı. İKT-nin həyata nüfuz etməsinin mövcud səviyyəsi ilə şəbəkə texnologiyaları, cihazlarda təhlükəsizliyin təmin edilməsi, İnternet təhlükəsizliyi, kriptoqrafiyaya, kriptovalyutaların öyrənilməsinə, "bulud" təhlükəsizliyinə, hər hansı bir "istifadəçinin" informasiya təhlükəsizliyinə diqqət yetirilir və məlumat mənbəyi kimi, proqramlaşdırma prosesində təhlükəsizlik nəzəriyyəsi və praktikası öyrənilməsi öz aktuallığı ilə secilir.

Məqalənin elmi yeniliyi. Yalnız geniş miqyaslı, inteqrasiya olunmuş və avtomatlaşdırılmış platformaya əsaslanan struktur yaradılmalıdır, və bu struktur təhlükəsizliyə yanaşma ilə İnternetdəki məhsullardan tutmuş, nüvə və çox buludlu infrastrukturlara qədər bütün şəbəkə mühitiniz üçün sürətli və geniş bir qorumanı təmin edə bilər.

Məqalənin praktik əhəmiyyəti və tətbiqi. Ekspertlərin fikrincə, kibertəhlükəsizliyin İnstitutunun təhsil və elmi fəaliyyəti, birincisi, sənaye sistemlərinin kiber davamlılığı, rəqəmsal istehsal, nəqliyyat, məhsulların interneti, ağıllı ev, sonra isə kiberpsixologiya, şəxsi təhlükəsizlik istiqamətində inkişaf etməlidir.

Ədəbiyyat

1.https://reports.beazley.com/2021/rr/index.html?utm_source=bing&utm_medium=cpc&utm_campaign=Beazley%20R%26R%20%7C%20Types%20Of%20Risk&utm_term=%2Bcyber%20%2Brisks&utm_content=Non-Branded%20-%20Cyber

2.https://www.channelfutures.com/strategy/what-do-hackers-want-anyway-a-look-at-different-cyberattack-goals

3.https://www.channelfutures.com/security/kaseya-ransomware-attack-sparks-scrutiny-of-msp-rsecurity-practices

4.https://www.pravda.ru/science/1054060-kragalichnosty/

5.https://www.rebellionresearch.com/cyber-attacks-examples

6.https://cpab.ru/trevozhnyj-rost-kolichestva-nanimaemyh-hakerov-cloudsavvy-it/

7.https://us-cert.cisa.gov/ics/content/cyber-threat-source-descriptions

8.https://www.mcafee.com/blogs/consumer/family-safety/7-types-of-hacker-motivations/

Э.Г. Гасанов, Б.Б. Азизов, З.Г. Бабазаде

Роль кибербезопасности в развитии информационных и коммуникационных технологий в Интернете

Резюме

Киберпреступное сообщество в своей деятельности учитывает общенациональные стратегии и методологии, а также технические особенности устройств и сетевых технологий, на которые направлены их атаки. Организациям следует пересмотреть свои стратегии, чтобы лучше защититься от кибер-рисков и научиться более эффективно управлять ими.

Один из первых важных шагов заключается в том, чтобы рассматривать кибер-безопасность как науку, и с максимальной щепетильностью отнестись к основе своей инфраструктуры, для чего, в свою очередь, необходимо обеспечить высокую скорость и сетевую связанность киберпространства для эффективной защиты.

Использование платформенного подхода к безопасности, микро и макро сегментации, технологий машинного обучения и автоматизации в качестве строительных блоков искусственного интеллекта, открывает огромные возможности для эффективного противодействия киберпреступникам.

E.G. Hasanov, B.B. Azizov, Z.H. Babazada

The role of cyber security in the development of information and communication technologies in the Internet

Summary

The cybercriminal community in its activities takes into account national strategies and methodologies, as well as the technical features of the devices and network technologies to which their attacks are directed. Organizations should rethink their strategies to better protect against cyber risks and learn how to better manage them.

One of the first important steps is to treat cyber security as a science and be as scrupulous about the core of your infrastructure, which, in turn, requires high speed and network connectivity of cyber space for effective protection.

The use of a platform-based approach to security, micro-and macro-segmentation, machine learning and automation technologies as building blocks of artificial intelligence opens up tremendous opportunities for effectively countering cybercriminals.

Redaksiyaya daxil olub: 08.09.2021