Awareness and Employment Impact Analysis in Cyber Security

G.A. Abdiyeva-Aliyeva

Institute of Control Systems of Azerbaijan National Academy of Sciences/Bakhtiyar Vahabzadeh street, 68, Baku, Azerbaijan

For correspondence:
Abdiyeva-Aliyeva Gunay / e-mail: gunay.abdiyeva@isi.az

Abstract

The recent cyber wars and their consequences in the world, the available statistical data, lay the foundation for regular awareness raising in the field of cyber security. At the same time, in order to prevent incidents that occur, it should be one of the priority issues for specialists to simulate work impact analysis scenarios. The article gives is to explore the importance of raising awareness of cyber security threats and attacks, as well as the current challenges and solutions.

Keywords: UEBA, Dar Vidar, Trickbot, Nit Ramnit, CVE, xHelper.

DOI 10.52171/2076-0515_2023_15_02_74_83

Received *18.05.2022*
Revised *19.06.2023*
Accepted *21.06.2023*

For citation:
Abdiyeva-Aliyeva G.A.
[Awareness and employment impact analysis in cyber security]
Herald of the Azerbaijan Engineering Academy, 2023, vol. 15, no. 2, pp. 74-83 *(in Azerbaijani)*

Kiber təhlükəsizlikdə məlumatlılıq və işə təsir analizi

G.Ə. Əbdiyeva-Əliyeva

Azərbaycan Milli Elmlər Akademkiyasının İdarəetmə Sistemləri İnstitutu (Bəxtiyar Vahabzadə küçəsi, 68, Bakı, Azərbaycan)

Yazışma üçün:
Əbdiyeva-Əliyeva Günay / e-mail: gunay.abdiyeva@isi.az

Xülasə

Son dövrdə dünyada baş verən kibermüharibələr və onların nəticələri, mövcud statistik məlumatlar kibertəhlükəsizlik sahəsində mütəmadi məlumatlılığın artırılmasına zəmin yaradır. Eyni zamanda, baş verən insidentlərin qarşısının alınması məqsədilə mütəxəssislərin işə təsir analizi ssenariləri üzərində simmulyasiya etməsi prioritet məsələlərdən biri olmalıdır. Məqalədə, kibertəhlükəsizlik təhdidləri və hücumlarına qarşı məlumatlılığın artırılmasının əhəmiyyəti, eyni zamanda mövcud problemlər və onların həlli yolları göstərilmişdir.

Açar sözlər: UEBA, Dar Vidar, Trickbot, Nit Ramnit, CVE, xHelper.

DOI 10.52171/2076-0515_2023_15_02_74_83

УДК 004.056

Осведомленность и анализ воздействия на занятость в области кибербезопасности

Г.А. Абдиева-Алиева

Институт Систем Управления Национальной Академии Наук Азербайджана (ул. Бахтияр Вагабзаде, 68, Баку, Азербайджан)

Для переписки:
Абдиева-Алиева Гюнай / e-mail: gunay.abdiyeva@isi.az

Аннотация

Недавние кибервойны и их последствия в мире, доступные статистические данные закладывают основу для регулярного повышения осведомленности в области кибербезопасности. В то же время для предотвращения возникновения инцидентов одним из приоритетных вопросов для специалистов должно быть моделирование сценариев анализа воздействия на работу. Показана важность повышения осведомленности об угрозах и атаках кибербезопасности, а также о текущих проблемах и решениях.

Ключевые слова: UEBA, Dar Vidar, Trickbot, Nit Ramnit, CVE, xHelper.

Giriş

İnsanlar kiber təhlükəsizlik və işə təsir analizi haqqında düşündükdə, bir şirkətin təhlükəsizlik cəhətdən pisniyyətli şəxslər tərəfindən nəzarəti və idarəetməni öz səlahiyyətlərinə keçirmə riskinin qiymətləndirilməsi kimi qəbul edirlər. İşin davamlılığı üçün qarşıya qoyulan məqsəd olduqda, risklər də dəyişir.

Xüsusilə nəzərə alınacaq məqamlar aşağıda təqdim olunmuşdur: Sertifikatlaşdırılmış İnformasiya Sistemləri Auditorlarının (CISA) mövcudluğu; İşçi heyətin uzaq məsafədən qoşulmalar üçün simsiz təhlükəsizliyi; Virtual Gizli Şəbəkələrin (VPN) istifadəsi; Şifrələmə proseslərinin tətbiqi; Çoxfaktorlu identifikasiya ilə aplikasiya istifadəçilərin girişini idarə etmək; İstifadəçi və aktiv davranışın monitorinqi (UEBA); Ən az imtiyaz prinsipinə əsasən istifadəçi girişinin məhdudlaşdırılması [1].

İstifadəçi giriş proqramının idarə edilməsi. Təşkilat, istifadəçi girişini idarə etməkdə gecikirsə, artıq buna diqqət yetirməyin vaxtıdır. VPN istifadəçilərinin şəbəkə üzərində saytlara giriş-çıxışını nəzarətə almaq mümkündür. Lakin şəbəkə üzərində apardıqları bütün əməliyyatlara fiziki olaraq nəzarət etmək çətindir. Həddən artıq verilmiş səlahiyyətlə işçilər məlumatları səhvən təhlükə altına ata bilərlər.

İstifadəçi girişinin idarə edilməsi baxımından aşağıdakılardan məlumatlı olmaq vacibdir: İstifadəçilərin rol anlayışları; Şifrə siyasəti; İT ekosistemində müxtəlif şəbəkələrə, tətbiqlərə və bulud xidmətlərinə girişin məhdudlaşdırılması; Giriş siyasətinə daxilolma vaxtı və coğrafi yer kimi kontekstlərin daxil edilməsi; Məsafədən qoşulmalar zamanı super istifadəçilərə girişin məhdudlaşdırılması [2]; UEBA-nın Təhlükəsizlik Planına daxil edilməsi.

İstifadəçinin Fərdi Davranışının Təhlili (UEBA). Aktiv olaraq fəaliyyət göstərən bütün şirkətlər təhdid və hücumlara məruz qalırlar. Bu təhdidlər və hücumlar iki hissəyə bölünür: daxili və xarici. Hakerlər tez-tez mənfəət əldə etmək üçün qurumlarda fərdi, eyni zamanda maliyyə məlumatlarına diqqət yetirirlər.

Təhdidlərin qarşısını almaq üçün atılacaq addımlar. Bu tip hücumların olma ehtimalının proqnozlaşdırılmasına ehtiyac var. Hazırda istifadəçi davranışını izləmək və təhlil etmək üçün həll yolları lazımdır. Bu sistem, istifadəçinin davranışı haqqında ümumi məlumat toplamağa köməklik edir. Bu məlumatlar, normal və ya şübhəli davranışları aşkar edir, eyni zamanda, əldə edilən məlumatlarla ətrafdakı təhlükəni asanlıqla müəyyənləşdirir və lazımi qabaqlayıcı tədbirləri vaxtında alır.

UEBA sistemi daxili təhdidləri, hədəfli hücumları, maliyyə saxtakarlığını aşkar etmək üçün istifadə olunur. UEBA həlləri insanın davranışları, cihazları, tətbiqləri, serverləri, məlumatları və ya bütün qurumların IP adresinə nəzər salaraq bütün potensial təhdid edilən anormal halları aşkar etməyə imkan verən maşın öyrənmə alqoritmləri və statistik təhlillər tətbiq edir. UEBA sistemi adətən fərq edilməyəcək sui-istifadənin və zərərli davranışın aşkarlanmasını təmin edir.

UEBA bütün istifadəçiləri və prosesləri izləyir və bu hadisələri özündə cəmləyir [3].

UEBA-nın işləmə mexanizmi. İstənilən istifadəçinin məlumatlarını oğurlamaq asan ola bilər. Ancaq şəbəkədə o insan kimi davranmaq daha çətindir. Bu səbəbdən, pisniyyətli haker fərqli bir şəkildə hərəkət edərkən UEBA həyəcan verəcəkdir.

UEBA proqram təminatı, yeni tətbiqetmələrin (aplikasiya) başlanması, şəbəkədəki

fəaliyyətlər və fayl çıxışı kimi istifadəçi hərəkətlərinə diqqət yetirir. Faylın nə vaxt əldə edildiyini, kimin daxil olduğunu və hansı fəaliyyətdə olduğunu yoxlayır. Texnologiya, şübhəli davranış nümunələri götürərək pisniyyətli hakeri tanımağa kömək edir. Hücumu dayandırmaq üçün heç bir tədbir görməz, əvəzində hücumu aşkar edər və təhdidin vurduğu ziyanı minimuma endirər.

Kiber təhlükəsizlik və gizlilik perspektivləri baxımından bir çox qurumda bu tip yoxlamaların bəzi formaları yerində ola bilər. Bununla birlikdə daha uzaq məsafədə işləyənlərlə yoxlamaların əlçatanlığı ən az imtiyaz prinsipinə görə uyğun şəkildə hüdudlanıb-hüdudlanmadığını təyin etmək lazımdır. Məsələn, uzunmüddətli işləyənlər qurum daxilindən ayrılarkən (və ya işdən çıxarkən) keçmiş səlahiyyətlərə sahib ola bilərlər. Bu, bütün səlahiyyət haqlarını nəzərdən keçirməyə və lazımsız sistem imtiyazlarının aradan qaldırılmasına dair göstəricidir. Qurumlar bunun ən yaxşı qabaqlayıcı tədbir olduğunu bilmələrinə baxmayaraq, çox insan bunu mütəmadi olaraq nəzərdən keçirmirlər. Başqa bir çətinlik də idarəetmə panelinə tətbiq olunan qoşulmaları gözdən keçirmək ola bilər. Bir çox qurum işçiləri yerli korporativ Wi-Fi şəbəkəsindən kritik əhəmiyyətə sahib proqramları əldə etməkdən uzaq tutmağa çalışarkən adətən bu siyasətlər həyata keçirilən müddətdə əksik icra olunur. Virusun yayıldığı müddətdə uzaq məsafədən xidmət göstərənlər bu müddət ərzində karantinə alınmaya bilər, bu da bütün xarici qoşulmaları nəzarət saxlamağın əhəmiyyətini göstərir. Sonda isə fərdi məlumatların ələ keçirilməsi daha da böyük diqqət çəkən məqamlardan birdir. İşçilərin uzaqdan qoşulduqları Wi-Fi təhlükəsiz deyilsə qurumdaxili sistemlər SQL və saytlararası komanda hücumları (XSS) üçün daha böyük bir risk daşıyır. Bütün bunlar uzaq məsafədən qoşulan bir işçinin qurumdaxili bütün İT sistemlərini və ekosistemi məlumatlarının hər növ risklə üz-üzə qalması diqqət mərkəzində olmasının vacibliyini göstərir.

Tamamlanmayan məlumatların təhlükəsizliyinin təmin etmək üçün strategiyanın işlənməsi. Uzaq məsafədən fəaliyətdə istifadə olunan proqram təminatını xüsusilə nəzərdən keçirmək gizlilik və təhlükəsizlik risklərini azaltmaq üçün görüləcək ilkin tədbirlərdəndir.

İşin davamlılığı planını (BCP) hazırlayarkən aşağıdakılara nəzər yetirmək lazımdır: qorunması lazım olan həssas məlumat növləri; həssas olmayan məlumatları özündə saxlayan, ötürən və cəmləyən ünvanlar; e-poçt və məlumatların yüksək keyfiyyətli şifrələməsi; bulud xidmətləri "link ilə paylaşmaq" parametrləri; veb-sayt məlumatlarının idarəedilməsi; birbaşa mesajlaşma tətbiqi proqram məlumatlarının idarəedilməsi.

Uzaq məsafədən fəaliyyət göstərən işçi ilə iş yerində işləyən işçi arasında adətən birbaşa mesajlaşma və e-poçt fəaliyyəti nəzərdən qaçan iki əsas risk mənbəyidir. İki fərqli mühitdə işləyən işçi arasında sürətli şəkildə sual-cavab mexanizmi ilə iş fəaliyyəti keyfiyyətli formada davam etsə də, bu tip fəaliyyət uzaq məsafədən işləyənlər üçün fərqli effekt verəcəkdir. Birbaşa mesajlaşma və e-poçt tətbiqi proqramlarının yenilənməsi zamanı saxlanılan, ötürülən və daxil olan məlumatlara necə təsir edəcəyini nəzərdən keçirmək lazımdır.

Çoxlu sayda istifadəçinin uzaq məsafədən işləməsini nəzərə alaraq, işin davamlılığı və uzaqdan planlaşdırıması üçün aşağıdakı addımların yerinə yetirilməsi lazımdır: işçi cihazları üçün təhlükəsizlik yeniləmələrini tətbiq etmək; video-konfrans proqramlarını yeniləmək; əlavə işçi qüvvəsi tələb edən müraciətlərə baxmaq.

E-poçtlarda və mesajlarda olan məlumatları izləməkdən əlavə, qurumlar bu tətbiqi proqramların nə qədər tez-tez yenilənmələrini də nəzərə almalıdırlar. Bir mesajlaşma platforması işə başlamazdan əvvəl yüksək riskli bir tətbiq proqramı hesab edilməsə də, işçilər ofisdən kənarda olduqda kritik bir tətbiq halına gələ bilər.

Bununla yanaşı, təşkilatlara video-konfrans tətbiqetmələrini izləmək imkanı verilməlidir. Uzaqdan işləyənlər WebEx, Skype və ya Google Hangouts, Teams, Zoom kimi texnologiyalardan istifadə etdikləri üçün bu tətbiqlərin təhlükəsizliyi kibertəhlükəsizlik riskini azaltmaq üçün zəruri hala gəlir.

Fişinq hücumları və əks tədbirlər. Bir linki klikləməyi və ya bir əlavə açmağı tələb edən bir e-poçt və ya qısa mesaj alsanız, özünüzə bu sualı verin: "Şirkətdə hesabım var və ya mənimlə əlaqə quran şəxsi tanıyırammı?" Cavab "Xeyr" olarsa, bu bir fırıldaqçı ola bilər. İşi dayandırın və fişinq fırıldaqçılığını axtarmaq üçün təlimatları nəzərdən keçirin. Daha sonra fişinqə dair şübhə olarsa, mesajı bildirin və həmin mesaji silin. Cavab "Bəli" olarsa, bildiyiniz bir telefon nömrəsi və ya veb saytdan istifadə edərək şirkətlə əlaqə saxlayın. Cihazınıza e-poçtdakı mətn mesajı deyil, əlavələr və bağlantılar (linkə keçid) zərərli proqram təminatını quraşdıra bilər.

Zərərli proqram - cihaza bulaşarsa, müxtəlif növ zərərli dəyişikliklər görməyə davam etməyimiz ehtimal olunur. Bəziləri uzaqdan məsafədən fəaliyyət göstərmək üçün müxtəlif növ proqramlar təklif edən, iş elanı veb saytlarına yönlənən istifadəçiləri hədəfləmiş və s. kimi proqramları təqlid edər.

Məsələnin həlli

Yuxarıda qeyd olunan məsələlərin həlli olaraq daxil olan zərəli keçidlər və ya əlavələrə dair məlumatlı olmaqla yanaşı kiber təhlükəsizlik vasitələrindən də istifadə oluna bilər.

Gəlir cinayətinə çevrilmə. İşsizliyin artması, bəzi insanlara, maliyyə qurumlarına qarşı kiberhücumlar zamanı bankomatlardan oğurlanmış pul vəsaitlərini çıxaran nağd pullar kimi cinayətkar qruplar üçün işləmək kimi yüksək maaşlı, yüksək riskli iş axtarmağa səbəb ola bilər.

İşçiləri və sistemləri qorumaq. İşçinin uzaq məsafədən İT idarəetmə sistemləri qurma qabiliyyətinin, həm təhlükəsiz, həm də effektiv olmasına baxmayaraq, boşluqların və problemlərin yaranacağı qaçılmazdır. Müsbət hal olardı ki, təşkilatlar, öncədən fövqəladə vəziyyətə uyğun olaraq məsafədən fəaliyyət ilə bağlı tədbirlər planını (DRP) hazırlamış olsun. Burada qarşımıza əsas İT avadanlıqları və proqram təminatının mövcudluğu və digər problemlər çıxır.

Təşkilatların şəbəkə sərhədləri və buna görə hücum səthi əvvəlkinə nisbətən daha böyükdür. Artıq təşkilatlarda bir çox məlumatlar öz hüdudlarından kənarda əldə oluna bildiyinə görə bu məlumatlara yönəlmiş hücumların riski yüksək səviyyədədir. Bu məqamda işçilər, xüsusilə sosial mühəndislik hücumlarına və oxşar fırıldaqçılıqlara qarşı daha həssas olmalıdır [4].

Ev şəbəkəsi. İstifadəçinin ev şəraitində bant genişliyi yüksək olan xəttdən istifadə etməsi, zəif Wi-Fi təhlükəsizliyi, sızılabilən paylaşma nöqtələri və başqa köhnə protokollardan istifadə edərək bu tip korporativ şəbəkələrə qoşularaq məlumatlardan istifadə etməsi də əlavə olaraq bu məlumatları riskə atmış olur. Bu səbəbdən də tövsiyyə olunan köhnə metod LAN üzərindən sabit şəbəkə ilə VPN istifadə edərək korporativ şəbəkəyə qoşulmaqdan ibarətdir.

Firewall, VPN və təhlükəsizlik siyasəti. Şəxsiyyət və Giriş İdarəetməsi (IAM) kimi etibarlı bir əlaqə də vacibdir. Əlbəttə ki, bütün işçilər yalnız VPN ilə əlaqə qurmalıdırlar. Ancaq bunun mümkün olmayacağı vəziyyətləri də planlaşdırmaq lazımdır. Məsələn, problemin pik həddi olaraq, zədələnmiş və ya sıradan çıxmış aparat təminatını düşünmək olar. Bu zaman, bir çox təşkilat işçiləri uzaq məsafədən fəaliyyət üçün öz cihazlarından istifadə etmək zərurəti ilə üzləşirlər. Qurumların Mobil Cihaz İdarəetmə (MDM) siyasətindən və həssas istifadəçi, virtual maşın və digər texnologiyaların mövcudluğundan asılı olaraq, bu proqramlar həm üstünlük, həm də riskləri meydana çıxarır. İstismar müddətini bitirmiş, nasaz və lisenziyasız proqram və aparat təminatı təhlükəsizliyi təmin etmək əvəzinə işi daha da mürəkkəbləşdirir.

Zəng edənin şəxsiyyəti. Son zamanlar saxta zəng mərkəzləri tərəfindən gələn zənglərdə dələduzluq halları çoxalıb. Bu tip fövqəladə vəziyyətlərdə həmin fırıldaqçılar üçün yaranan ən uyğun şərait əhalinin stress vəziyyətində belə zənglərə həssas olmasından ibarətdir. Xüsusilə korporativ şəbəkəyə uzaq məsafədən qoşulma zamanı baş verən xətalarda və qoşulmanın mümkün olmaması ilə bağlı gələn zənglərdə qarşı tərəfin kimliyinin təyin olunması çox önəmlidir. Bu tip risklər narahatçılıqlara səbəb olur. Etibarlı rabitə kanallarında fəaliyyət uğursuz və ya nasaz olarsa, təhlükəsizlik işçilərinin nəzarəti altında olmayan kənar şəxslərdən dəstək almaq istifadəçilərə cəzbedici görünə bilər. Bu identifikasiya ilə bağlı ikinci məsələni ortaya çıxarır. Bu problemlərdən bəziləri hər iş stansiyasında (server) monitorinq, telemetriya və aşkaretmə vasitələrindən istifadə edərək problemin başlanğıc nöqtəsində bərpa edilə bilər. Ekspertiza və müdaxilə vasitələrinin yaradılması ilə uzaq məsafədən araşdırıla və lazım gəldikdə cihazları izolə etmək mümkündür.

Şifrəni dəyişdirməyin 3 səbəbi. Şifrələrin daha güclü şifrələrlə əvəz edilməsi üçün mükəmməl zamandır. Şifrələri ad, doğum tarixi, ev ünvanı, telefon nömrəsi və kredit kartı məlumatları kimi vacib şəxsi məlumatları gizlətmək üçün istifadə olunan seyfin açarı kimi təsəvvür etmək lazımdır. Cinayətkarlar fərdi məlumatları şəxsiyyət oğurluğu üçün istifadə edə bilərlər. Şifrə təhlükəsizliyi vacibdir, çünki profillərinizdəki fərdi məlumatlar şifrələrlə qorunur. Ancaq hər kəs şifrə təhlükəsizliyinə əhəmiyyət vermir. Təəccüblüdür ki, bir çox insanlar "admin", "123456", "qwerty" və s. kimi sadə şifrələrdən istifadə edir. Ayrıca, əksər insanlar parolları birdən çox hesabda təkrar istifadə edirlər. Sadə şifrələrdən istifadə etmək və onları təkrar istifadə etmək təhlükəsizlik üçün mənfi xarakter daşıyır. Şifrələri daha güclü formaya gətirmək üçün onu dəyişdirməyin 3 səbəbi aşağıda təqdim olunmuşdur:

1. Şifrələr onlayn yerləşdirilmiş fərdi məlumatlarınızın açarıdır. Bir e-poçt ünvanı və ya istifadəçi hesabınıza giriş üçün istifadə edildikdə, şifrə istifadəçi hesablarınızın açarıdır. O hesablarda heç bir surpriz yoxdur. Ancaq istifadəçi hesablarında çox vacib şəxsi məlumatların olduğunu düşünürdünüzmü? İnternetdəki bir çox xidmət, işləməsi üçün sizdən şəxsi məlumatları doldurmağınızı tələb edir. Əlbəttə ki, hər zaman yalan məlumat verə bilərsiniz. Ancaq məsələn, bir alış-veriş icrası zamanı düzgün məlumat verməlisiniz.

Bir pisniyyətli haker profilinizi əldə etmək üçün istifadə etdiyiniz e-poçt və şifrə kombinasiyalarını öyrənərsə, həmin profildəki bütün şəxsi məlumatlarınızı əldə edə bilər.

2. Şifrələrinizi yoxlayan tək siz deyilsiniz. Şifrənizi yəqin ki, heç kim bilmir. Ancaq istifadə etdiyiniz veb xidmətlərin verilənlər bazasında qeyd olunur. Antivirus və VPN kimi təhlükəsizlik tədbirləri ilə öz cihazınızdakı məlumatlarınızı qoruya bilərsiniz. Ancaq internet xidmətlərindəki istifadəçi hesabları sizin nəzarətinizdən kənarda qalır.

Qeydiyyatda olduğu servislərin sıradan çıxmasının qarşısını almaq üçün heç bir istifadəçinin edə biləcəyi tədbir yoxdur. Nə qədər diqqətli olmağınızdan asılı olmayaraq, istifadə etdiyiniz servis sıradan çıxdıqda məlumatlarınız təhlükə altında qalır. Hər zaman servislərdə sıradan çıxma riski vardır.

3. Təkrar istifadə olunmuş şifrələr digər profillərə təhlükə yarada bilər. Əksər insanlar şifrələri birdən çox profildə təkrar istifadə edirlər. Bir pisniyyətli haker hər hansı bir hesabda istifadə etdiyiniz şifrənizi əldə edərsə, çox güman ki, digər populyar xidmətlərdə də sınayacaq. Hakerlər tez-tez Amazon, eBay, Netflix kimi bank kartı məlumatları olan insanların profillərinə daxil olmağa çalışırlar.

Eyni şifrəni fərqli yerlərdə təkrar istifadə edirsinizsə, əhəmiyyətsiz görünən bir profil şifrəsinin əldə olunması ağır nəticələr verə bilər. Hər bir profildə unikal və güclü təsadüfi şifrələrdən istifadə olunarsa, hesabın ələ keçirilməsi zamanı digər bütün hesablar da deyil, yalnız həmin hesab zərər görər.

Unikal şifrə istifadə etmək, şifrənizi dəyişdirmək lazım olduğunda vaxta qənaət edir. Bir tələb yarandıqda hesabınızı qorumaq üçün şifrənizi dəyişdirməlisiniz. Unikal bir şifrə istifadə edərkən yalnız tələb olunan hesabda onu dəyişdirməlisiniz. Eyni şifrəni digər hesablarda istifadə etmisinizsə, bütün digər hesabların şifrəsini dəyişdirməlisiniz. Bütün şifrələrin dəyişdirilməsi çox vaxt tələb edir. Bu müddət ərzində hesablarınız ələ keçirilə bilər. Cinayətkarlar hər zaman ələ keçirdiyi şəxsi məlumatlardan yararlanmaq üçün onlardan mümkün qədər sürətli şəkildə istifadə etməyə çalışırlar. Bir hücumdan sonra zaman vacib faktordur.

Güclü şifrə ilə təhlükəsizlik tədbirləri. Birinci qayda eyni şifrəni başqa hesabda istifadə etməməkdir. Nə qədər təhlükəsiz şifrəniz olursa olsun, yalnız bir profildə istifadə edin.

Təhlükəsiz bir şifrə tapmaq çətindir. Uzu cümlələr, qeyri-müəyyən xarakter və say sətirlərindən istifadə edərək birini yarada bilərsiniz. Bir çox insan uşaqlarının və ya öz adlarını şifrə kimi istifadə edir. Bəzən bu məlumatlar sosial şəbəkədən gizlədilə bilər. Ən güclü şifrələr xatırlaya bilmədiyiniz şifrələrdir. Şifrə idarəetmə panelləri güclü təsadüfi şifrələrinizi yadda saxlamağa kömək edir. Bir şifrə idarəetmə paneli istifadə edərkən digərlərini görmək üçün yalnız bir şifrəni xatırlamaq lazımdır. Şifrə meneceri ilə şifrələrinizi unutmayacaqsınız.

Ən tanınmış zərərli proqramlar:

Emotet – Emotet inkişaf etmiş, öz-özünə yayıla bilən və modulyar bir troyandır. Emotet əslində bir bank sektoruna hədəflənmiş troyan idi, ancaq son zamanlar digər pisniyyətli kampaniyalarda distrubuter olaraq istifadə olundu. Təyin olunmaqdan yayınmaq üçün qalıcılıq və qaçırma texnikaları üçün çoxlu metodlar istifadə edir. Üstəlik mənfi xarakterli əlavələr və ya keçidlərin olduğu şəxsiyyət oğurluğu spam e-poçtları yolu ilə də yayıla bilir.

XMRig - Monero kriptovalyutasının mayninq (mining) prosesi üçün istifadə olunan və ilk dəfə 2017-ci ilin May ayında meydana çıxan açıq kodlu bir CPU mayninq proqramıdır.

Rick Trickbot - Trickbot, tez-tez yeni qabiliyyətlər, xüsusiyyətlər və paylama vek-

torları ilə yenilənən basqın bir bank sektoru Troyanıdır. Bu, Trickbotun çox məqsədli kampaniyaların bir hissəsi olaraq paylaşıla bilən elastik və özəlləşdiriləbilən bir mənfi xarakterli proqram olmasını təmin edir.

Agent Tesla - Agent Tesla, keylogger və şifrə gəmisi olaraq işləyən geniş bir RAT proqramıdır. Agent Tesla, qurbanın klaviatura daxiletmələrini, sistem panelini izləmə, toplama, ekran görüntüsünü alma və qurbanın brauzerlərdəki (Google Chrome, Mozilla Firefox ve Microsoft Outlook daxil) müxtəlif giriş-çıxış sistemlərinə aid şəxsi məlumatlarını ələ keçirmə qabiliyyətinə sahibdir.

Formbook - Formbook, müxtəlif brauzerlərdən şəxsi məlumatları ələ keçirən, ekran görüntülərini toplayan, klaviş basılmalarını izləyən və yadda saxlayan və faylları C&C sifarişlərinə görə yükləyib istifadə edə bilən bir vəsaitdir.

Nit Ramnit - Ramnit, bank sektoru üzrə FTP şifrələrini, aktiv hesab kukilərini və şəxsi məlumatları oğurlayan bir troyandır.

Dar Vidar - Vidar, Windows əməliyyat sistemlərini hədəfləyən bir məlumat vasitəsidir. İlk dəfə 2018-ci ilin sonunda aşkar olundu. Müxtəlif brauzerlərdən və rəqəmsal pul kisələrindən şifrələri, bank kartı məlumatlarını və digər həssas məlumatları oğurlamaq üçün hazırlanmışdır. Vidar müxtəlif onlayn forumlarda satıldı və GandCrab fidyə proqramını ikinci yük olaraq yükləyən pisniyyətli proqram olaraq istifadə olundu.

Lokibot - Lokibot, təməl olaraq şəxsiyyət oğurluğu e-poçtları ilə yayılan bir Infostealer-dir və e-poçt şəxsi məlumatları kimi məlumatlardan əlavə CryptoCoin pul kisələrinə və FTP serverlərinə qarşı şifrələri oğurlamaq üçün istifadə olunur.

Hawkeye - əvvəlcə virus yoluxmuş Windows platformalarından istifadəçilərin şəxsi məlumatlarını oğurlamaq və bunları C&C serverinə təhvil vermək üçün hazırlanmış bir infostealer mənfi xarakterli proqramdır. Əvvəlki illərdə Hawkeye, e-poçt və veb brauzer şifrələri oğurlama və keyloggingin orginal işlərinə əlavə olaraq ekran görüntüsü alma, USB ilə yayılma və daha artığını edə bilmə qabiliyyəti əldə etdi. Hawkeye adətən MaaS (Xidmət olaraq ziyanlı proqram) olaraq satılmaqdadır.

H xHelper - xHelper, 2019-cu ilin mart ayından bu günə qədər görülən digər mənfi xarakterli proqramları yükləmək və görüntülü reklam yükləmək üçün istifadə olunan pisniyyətli proqramdır. Proqram özünü istifadəçidən gizlədə bilər və silindiyi təqdirdə özüözünü yenidən əməliyyat sisteminə quraşdıra bilər.

Ən çox istismar olunan təhlükəsizlik açıqları:

MVPower DVR uzaq məsafədən kod inyeksiyası - MVPower DVR cihazlarına uzaq məsafədən kod inyeksiya edilə bilən təhlükəsizlik açığıdır. Uzaq məsafə olan bir pisniyyətli haker, təsirlənəcək yönləndiricidə hazırlanmış bir istəklə istənilən kod inyeksiya etmək üçün bu zəiflikdən yararlana bilər.

Web Server Exposed Git bazası məlumat aşkarlanması - Git bazasında göstərilən bir məlumat sızdıran təhlükəsizlik açığıdır. Bu təhlükəsizlik açığını uğurla istismar edərək hesab məlumatlarının icazəsiz şəkildə ifşa edilməsi mümkündür.

PHP DIESCAN məlumatının açığı – Bir informasiyanın açığa çıxmasını təhlükəsizlik PHP səhifələri bildirdi. Uğurlu şəkildə istismar olunması, həssas məlumatların serverdən ifşa olunmasına yol aça bilər.

Dasan GPON routerlərində identifikasiyasını aşma (CVE-2018-10561) - Dasan GPON routerlərində giriş identifikasiyasını aş-

maq üçün istifadə olunan təhlükəsizlik açığıdır. Bu təhlükəsizlik açığının uğurlu şəkildə istismar edilməsi uzaq məsafədən hakerin həssas məlumatları əldə etməsinə və təsirə məruz qalmış sistemdə səlahiyyətsiz şəkildə idarəetmənin ələ alınmasına yol açır.

SS OpenSSL TLS DTLS ürək döyüntüsü məlumatlarının açığa çıxması (CVE-2014-0160; CVE-2014-0346)- OpenSSL-dəki məlumat sızıntısı təhlükəsizlik açığıdır. Təhlükəsizlik açığı TLS / DTLS paketləri istifadə olunarkən yaranan xətadan qaynaqlanır. Pisniyyətli haker qoşulu bir istifadəçinin və ya serverin yaddaşındakı məzmunları açığa çıxartmaq üçün bu təhlükəsizlik açığından faydalana bilir.

Ache Apache Struts2 məzmun tipli uzaq məsafədən kod yeritmə (CVE-2017-5638) - Jakarta çox hissəli incələyici istifadə edən Apache **Struts2**-da uzaq məsafədən kod yeritmə təhlükəsizlik açığıdır. Pisniyyətli haker, yükləmək istədiyiniz bir hissəsi olaraq etibarsız bir məzmun tipi göndərərək bu təhlükəsizlik açığından yararlana bilər. Uğurlu bir şəkildə istismar olunması, təsirlənən bir sistemdə təsadüfi kod inyeksiyasına səbəb ola bilər.

SQL İnyeksiyası (müxtəlif metodlar) – Bir proqramın daxilindəki kodların təhlükəsizlik açığından yararlanarkən, istifadəçi tərəfindən proqrama daxil olmuş bir SQL kod sorğusu inyeksiyası əlavətmə açığıdır.

HTTP üzərindən komanda inyeksiyası – HTTP təhlükəsizlik açığından bir komanda inyeksiyasını bildirilmişdir. Uzaq məsafədəki bir pisniyyətli haker, qurbana hədəflənmiş xüsusi hazırlanmış bir istək göndərərək bu problemdən yararlana bilər. Uğurlu bir şəkildə yararlanma pisniyyətli hakerin cihazda istənilən kodu işə salmasına səbəb olur.

WordPress portable-phpMyAdmin Əlavəli Kimlik Doğrulama Baypas (CVE-2012-5469) - WordPress portativ-phpMyAdmin Plugin-də autentifikasiya bypass həssaslığı mövcuddur. Bu həssaslığın müvəffəqiyyətlə istifadəsi uzaqdan hücum edənlərə həssas məlumatlar əldə etməyə və təsirlənmiş sistemə icazəsiz giriş əldə etməyə imkan verir.

D-Link DSL-2750B uzaq məsafədən komanda icrası - D-Link DSL-2750B routerlərində uzaq məsafədən kod icrasını həyata keçirəcək təhlükəsizlik açığı bildirilmişdir. Uğurlu bir şəkildə yararlanması, təhlükəsizlik açığı mövcud olan cihazda hədəfə niyyətə olaraq istənilən kodun icrasına səbəb ola bilər.

Ən tanınmış mənfi xarakterli mobil proqram alətləri:

xHelper – 2019-cu ilin mart ayından bu günə qədər və digər mənfi xarakterli proqramları yükləmək üçün, eyni zamanda görüntülü reklamlar yükləmək üçün istifadə olunan mənfi xarakterli proqramdır. Proqram özünü istifadəçidən gizlədə bilər və əgər silinərsə özüözünü sistemə yenidən yükləyə bilər.

Gerilla - Android troyanı, pisniyyətli fayllar yükləyə bilən birdən artıq qanuni proqram daxilində gizlədilmiş olaraq aşkar olunub. Gerilla, proqram hazırlayan mütəxəssislər üçün hiyləli reklam gəliri yaradır.

AndroidBauts - IMEI, IMSI, GPS ünvanını və digər cihaz məlumatlarını genişləndirən və üçüncü şəxs proqramların və qısayolların mobil cihazlara yüklənməsinə icazə verən Android istifadəçilərini hədəfləyən reklam proqramıdır [5].

Nəticə

Azərbaycan kiber orduya sahib dövlətlərin əhatəsindədir. Xüsusilə əksər dövlət və strateji əhəmiyyətli saytlarımızın serverlərinin xarici ölkələrdə yerləşməsi ciddi təhlükə mənbəyidir.

Bunları nəzərə alaraq, kibercinayətkarlıqla mübarizə sahəsində milli potensialın gücləndirilməsi və kiberhücumların işə təsiri analizinin aparılması vacib amillərdəndir.

Maraqlar münaqişəsi

Müəllif bu məqalədə araşdırılması tələb olunan maraqlar münaqişəsinin olmadığını qeyd edir.

REFERENCES

1. **Əbdiyeva-Əliyeva G.** Kibertəhlükəsizliyin əsasları. Dərs vəsaiti. ISBN: 978-9952-468-78-6. Bakı-2022. s.208 *(in Azerbaijani)*
2. **Özkaya E., Sarıca R., Durmaz Ş. Siber Güvenlik.** Saldırı ve Savunma Stratejileri. Ankara, 2019. S.564 *(in Turkish)*
3. **Əbdiyeva-Əliyeva G., Hematyar M., və Bakan S.** Süni intellekt metodlarından istifadə edərək kiberhücumların aşkarlanması və qarşısının alınması sisteminin inkişafı. Texnologiyada İnkişaf II Qlobal Konfrans (IEEE-GCAT), 2021, səh. 1-5 *(in Azerbaijani)*
4. **Əbdiyeva-Əliyeva G., Bakan S., Nəzərov. B.** Kibertəhlükəsizlik strategiyasının işlənməsinin Azərbaycan Respublikası üçün əhəmiyyəti. Azərbaycan və Türkiyə Universitetləri: təhsil, elm, texnologiya" I Beynəlxalq elmi-təcrübi konfransı, 2019, s.323-325 *(in Azerbaijani)*
5. **Əbdiyeva-Əliyeva G.** Binalarda baş verən yanğınların söndürülməsi və məhdudlaşdırılmasının kompüter modelləşdirilməsi. *Azərbaycan Mühəndislik Akademiyasının Xəbərləri*, Cild 9, 2018, №2, s. 83-90 *(in Azerbaijani)*