DOI: https://doi.org/10.36719/2663-4619/100/292-298

Hüseyn Abdullayev
Azərbaycan Dövlət İqtisad Universiteti
magistrant
huseyn-abdullayev@unec.edu.az

"RANSOMWARE" HÜCUMLARI KONTEKSTİNDƏ YOLUXMADAN SONRAKI BƏRPA STRATEGİYALARI

Xülasə

Araşdırmada məqsəd ən çox yayılmış kiberhücum olan "ransomware" (fidyə proqramı) hücumundan qorunma yollarını göstərmək və əsasən yoluxmadan sonra məlumatların bərpası prosesini detaylı şəkildə nümayiş etdirməkdir.

Məqalə sürətlə təkamül edən və inkişaf edən "ransomware" hücumları, onların tarixi, təkamülü, mutasiya və inkişaf edib kompleks hal alması haqqında məlumat verməklə yanaşı eyni zamanda real həyatda baş vermir bəzi hücumlardan, bu hücumların nəticələrindən və qurbanların bu hücumlarla necə mübarizə apardığından da bəhs edir. "Ransomware" proqramlarının işləmə prinsipindən, fidyənin necə ödənilməsindən və hansı yollarla qurbana fidyəni ödəməyə məcbur qoyduğu haqda məlumat verilir. Məqalə boyunca deşifrələmə proqramları, yedəkləmənin önəmi və nüsxələrin bərpası texnologiyaları, bərpa prosesinin mərhələləri, danışıqlar və etik mülahizələr, davranış analizi, DLP kimi müxtəlif "ransomware" hücumlarından qorunma yolları və yoluxmadan sonrakı bərpa prosesindən bəhs edilir.

Bundan əlavə məqalədə şirkətlərin və təşkilatların "ransomware" hücumlarına qarşı nə dərəcədə hazır olduğunu araşdırılır və bu 4 səviyyəli şkalada dəyərləndirilir.

Açar sözlər: *ransomware, yedəkləmə prosesi, deşifrə proqramları, etik mülahizələr, ehtiyat nüsxələri, kiberhücum*

Huseyn Abdullayev
Azerbaijan State Economic University
master student
huseyn-abdullayev@unec.edu.az

Post-infection recovery strategies in the context of ransomware attacks

Abstract

The purpose of the research is to show ways to protect against the most common cyber-attack, ransomware, and mainly to demonstrate in detail the process of data recovery after infection.

The article provides information about the rapidly mutation and evolving ransomware attacks, their history, progress and development and complexity, while also discussing some attacks from real life, the consequences of these attacks, and how victims combat these attacks. Information is given on the principle of operation of ransomware programs, how the ransom is paid, and in what ways they force the victim to pay the ransom. The article covers decryption software, the importance of backups and recovery technologies, steps in the recovery process, negotiation and ethical considerations, behavioral analysis, ways to protect against various ransomware attacks such as DLP, and the post-infection recovery process.

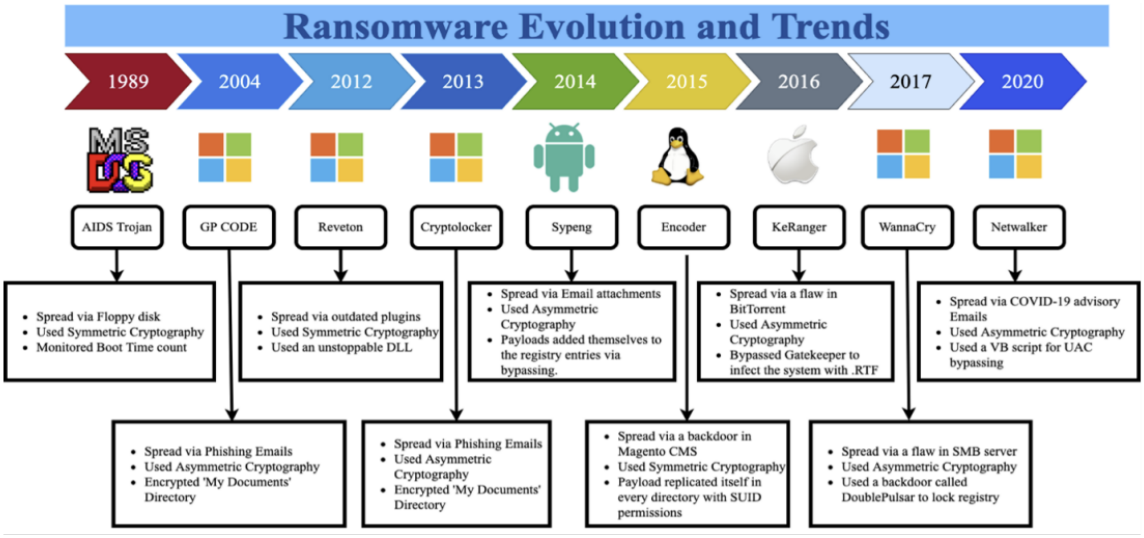
In addition, the article examines the extent to which companies and organizations are prepared against ransomware attacks and evaluates it on a 4-level scale.

Keywords: *ransomware, recovery process, decryption tools, ethical considerations, backups, cyber-attack*

Giriş

Dünya üzərində 14 ölkənin 1200-dən çox şirkətləri ilə keçirilən sorğuya əsasən, keçdiyimiz ildə həmən şirkətlərinin 87 faizi "ransomware" hücumuna məruz qalıb və bu şirkətlərin 77 faizi tələb olunan fidyəni ödəmişdir (1). Bu, hər il kibercinayətkarlıq nəticəsində itirilən milyardlarla dollar deməkdir. "Ransomware" hücumlarının qarşısını ala bilən və ya məlumatlarını hücumlardan qoruya bilən şirkətlər özlərini kifayət qədər çox olan bərpa xərclərindən xilas edə, bizneslərinin davamlılığının pozulma riskini azalda və reputasiyalarını qoruya bilərlər. “Ransomware” hücumlarından qorunma tədbirlərini öncədən həyata keçirmək çox vacibdir. Hücum baş verdikdən sonra, etibarlı qorunma tədbirləri yoxdursa, məlumatları xilas etmək qeyri-mümkün hala gələ bilir. Ona görə ki, “ransomware” getdikcə təkminləşir və yüksək sürət və dəqiqliklə şəbəkələrə nüfuz edə bilir və hətta bəzən əlavə edilmiş ehtiyyat nüsxələri də tapa bilir.

“Ransomware” (Fidyə proqramı) nədir? “Ransomware” faylları şifrələmək və ya istifadəçilərin sistemlərini kilitləmək üçün nəzərdə tutulmuş bir növ zərərli proqramdır. Bu proqram fidyə ödənilənə qədər məlumatlarını effektiv şəkildə özündə girov saxlayır. Bir dəfə yoluxmuş qurbanlar çox vaxt çətin seçim qarşısında qalırlar: ya kibercinayətkarın tələb etdiyi fidyəni ödəmək, ya da öz dəyərli məlumatlarının itirilməsini qəbul etmək. “Ransomware” hücumlarının təsiriləri çox böyük ola bilir, adətən maliyyə itkiləri, reputasiyanın zədələnməsi və təsirə məruz qalan təşkilatlar üçün davam edən əməliyyatların pozulması ilə nəticələnir. Kiçik bizneslərdən tutmuş iri müəssisələrə qədər hər bir qurum - səhiyyə, maliyyə, təhsil və hökumət daxil olmaqla, bu hücumun qurbanı ola bilər. Bundan əlavə, ransomware proqramlarının gün keçdikcə daha da inkişaf etməsi kibertəhlükəsizlik mütəxəssislərinin onları aşkarlaması və təsirlərinin azaldılmasını getdikcə çətinləşdirib. Müasir ransomware tətbiqləri mürəkkəb şifrələmə alqoritmlərindən istifadə edir, ənənəvi təhlükəsizlik metodlarından yayınır və hədəf mühitlərə sızmaq və daha çox cihaza yayılmaq üçün proqram təminatı və şəbəkə infrastrukturlarının zəifliklərdən istifadə edir.



Şəkil 1: "Ransomware"proqramlarının inkişafı (2)

Ransomware proqramlarına örnək olaraq ən sadə versiyada , ekranda fidyə tələb edən pop up çıxardan "Scareware" və daha inkişaf etmiş, istifadəçinin cihazını və hətta bütün şəbəkəni tamamilə kilitləyə və şifrələyə bilən “WannaCry”, “Netwalker” kimi hücumların adını çəkə bilərik. Bu artan təhlükələrə cavab olaraq, “ransomware” hücumları ilə mübarizə və onların təsirini yumşaltmaq üçün innovativ və effektiv strategiyalara ehtiyac var. Antivirus proqramı və şəbəkə “firewall”ları kimi ənənəvi təhlükəsizlik tədbirlərindən əlavə, şirkətlər kibertəhlükəsizliyə ciddi yanaşmalı, ehtiyyat nüsxələrinin yaradılması və bu nüsxələri geri qaytarma mexanizmlərinin tətbiqi, hadisələrə cavab planının qurulması kimi metodları icra etməlidir. Bu məqalədə isə hücum baş verdikdən sonra ediləbiləcək həll yollarından əsas üç üsula diqqət yetirəcəyik.

Deşifrələmə alətləri. "Ransomware" hücumlarının qurbanlarına kömək etmək üçün kibertəhlükəsizlik tədqiqatçıları və təşkilatlar tərəfindən bir neçə deşifrələmə alətləri hazırlanmışdır. Məsələn, "WannaKey" və "WannaKiwi" kimi alətlər "WannaCry" ransomware tərəfindən təsirlənmiş faylların şifrəsini açmaq üçün, "CryptoLocker" şifrə açma aləti isə "CryptoLocker ransomware" tərəfindən şifrələnmiş faylların şifrəsini açmaq üçün hazırlanmışdır (4). Buna baxmayaraq, deşifrə proqramlarına tamamilə güvənmək düzgün deyil. Bu alətlərinin ən böyük problemi uyğunluq problemidir. Bu proqramlar sadəcə spesfik bir növ "ransomware"in şifrələdiyi faylları deşifrə etməyə yarayır. Həmən "ransomware"in yeni versiyalarında və yaxud başqa növ şifrələmə alqoritmlərini deşifrə etmək üçün başqa alət istifadə olunmalı və ya istifadə olunmuş şifrələmə alqoritminə uyğun yeni bir alət hazırlanmalıdır (5). Bundan əlavə başqa bir məhdudiyyət olaraq deşifrə açarlarının əlçatmazlığını göstərmək olar. Adətən deşifrə alətlərinin iş prinsipi müxtəlif üsullarla əldə edilən və ya hal hazırda bilinən şifrə açma açarlarının (decrytion key) mövcudluğuna əsaslanır. Əyər bu açar məlum deyilsə və ya əlçatan deyilsə onda mövcud alətlərdən istifadə edərək şifrələnmiş məlumatları bərpa etmək mümkün olmayacaq.

Fidyə proqramları inkişaf etdikcə və daha mürəkkəb şifrələmə üsullarını mənimsədikcə, mövcud deşifrələmə vasitələrinin effektivliyi zamanla azala bilər. Kibercinayətkarlar şifrənin açılması cəhdlərinin qarşısını almaq üçün davamlı olaraq yeniliklər edir və bu, deşifrə alətlərinin inkişaf edən "ransomware" təhdidləri ilə ayaqlaşmasını çətinləşdirir.

Yedəkləmə və Bərpa Texnikaları. Şirkərlər, "ransomware" hücumu zamanı potensial məlumat itkisini minimuma endirmək üçün, kritik məlumatların tez-tez yedəklənməsini təmin etməlidir (6). Avtomatlaşdırılmış yedəkləmələr, bu prosesini sadələşdirməyə və davamlılığı təmin etməyə kömək edə bilər. Ehtiyat nüsxələrin onlayn mühit ilə yanaşı oflayn və ya şəbəkədən təcrid olunmuş mühitdə də saxlanması "ransomware" proqramının ehtiyat nüsxə fayllarına daxil olmasının və şifrələməsinin qarşısını ala bilər. Oflayn ehtiyat nüsxələri "ransomware" hücumlarına qarşı əlavə qorunma qatını təmin edir və məlumat itkisi riskini azaldır (7).

Bərpa prosedurunda isə ilkin olaraq yoluxmuş sistem və ya sistemlərin identifikasiyası durur. "Ransomware" infeksiyası aşkar edildikdə, təşkilatlar şəbəkə daxilində daha da yayılmasının qarşısını almaq üçün yoluxmuş sistemləri dərhal müəyyən etməli və təcrid etməlidir. Şəbəkə monitorinqi alətlərindən və son nöqtənin aşkarlanması və cavablandırılması (Endpoint Detection and Response (EDR)) kimi həllərdən istifadə "ransomware" hücumunun müəyyən edilməsinə kömək edə bilər. Yoluxmuş mühit aşkar edilib şəbəkədən təcrid olunandan sonra növbəti mərhələ yedəkləmələrdən məlumatların bərpasıdır. Tətbiq olunan yedəkləmə növündən asılı olaraq, administratorlar təsirə məruz qalmış sistemlərdə məlumatları bərpa etmək üçün ehtiyat idarəetmə konsollarından və ya bərpa proqramından istifadə edə bilərlər. Məlumatların bərpası başa çatdıqdan sonra təşkilatlar bütün kritik faylların uğurla bərpa olunmasını təmin etmək üçün bərpa edilmiş məlumatların bütövlüyünü və tamlığını yoxlamalıdırlar. Məlumatların bütövlüyünün yoxlanılması və təsdiqləmə prosedurlarının həyata keçirilməsi bərpa edilmiş məlumatlarda hər hansı uyğunsuzluq və ya səhvləri müəyyən etməyə kömək edə bilər.

Daha təkminləşmiş həll yolu olaraq avtomatlaşdırılmış yedəkləmə mexanizmlərinin tətbiqi ehtiyat məlumatların bütövlüyünü və etibarlılığını təmin etməyə kömək edə bilər. Müntəzəm yoxlama vasitəsi ilə ehtiyat nüsxə fayllarının uyğunluğunu yoxlaya, hər hansı pozulma və ya məlumat itkisini aşkarlaya və məlumatların bərpası prosesinə təsir edə biləcək potensial problemlər barədə administratorlara xəbərdar edə bilər (Curtis Preston, 2006: 37-38).

Danışıqlar Taktikası və Etik Mülahizələr. Bu cür hücumlara məruz qalan şirkətlər adətən fidyə ödəməsi, danışıqlar aparmaq və etik mülahizələrlə bağlı çətin qərarlarla üzləşirlər. "Ransomware" danışıqları həssas və çətin bir prosesdir, kibercinayətkarlar qurbanları fidyə tələblərini ödəməyə məcbur etmək üçün müxtəlif taktikalardan istifadə edirlər. Danışıqlar adətən şifrlənmiş mesajlaşma platformaları və ya qaranlıq veb (Dark web) forumları kimi anonim kanallar vasitəsilə baş verir ki, burada kibercinayətkarlar anonimliyi qorumaq üçün kriptovalyutalarla ödəniş tələb edirlər. Taktikalara təcili ödəniş üçün endirimlər təklif etmək, şifrəni açmaq qabiliyyətinə dair sübut təqdim etmək və ya tələblər yerinə yetirilmədiyi təqdirdə həssas məlumatları yaymaqla

hədələmək daxil ola bilər(9). Bu cür danışıqlara, hakerlərin qaranlıq veb portal vasitəsilə şirkətlə əlaqə saxladığı "Colonial Pipeline ransomware" hücumunu misal gətirmək olar, hansı ki, bu hücumda 4.4 milyon dollar məbləğində fidyə ödəməsi tələb olunur (10). Eynilə, yüksək nüfuzlu təşkilatları hədəf alması ilə tanınan REvil ransomware qrupu, qurbanları böyük məbləğdə pul ödəməyə məcbur etmək üçün tez-tez aqressiv danışıqlar taktikasından istifadə edir. Nümunədə də göründüyü kimi kibercinayətkarlar qurbana vaxt limiti qoyur və məlumatlarının silinməsi ilə hədələyir (Şəkil 2).

Şəkil 2:Yoluxmuş cihazda görünən kilitlənmiş ekran təsviri

Fidyə ödəmək qərarı təşkilatlar üçün əhəmiyyətli etik dilemmalar yaradır. Fidyənin ödənilməsi şifrələnmiş məlumatların bərpası ilə nəticələnə bilər, amma , cinayət fəaliyyətini maliyyələşdirir və gələcək hücumları stimullaşdıra bilər. Bundan əlavə, fidyə ödəmək nəticəsində yarana biləcək potensial mənəvi təhlükə ilə bağlı narahatlıqlar da var, çünki bu, kibercinayətkarları digər qurbanlara qarşı "ransomware" hücumlarını davam etdirməyə təşviq edə bilər. "JBS ransomware" hücumu kimi hadisələr fidyə ödəməsi qərarlarının etik mürəkkəbliyini vurğulayır. Sözü gecən hücum eyni rus təşkilatı olan "Revil" tərəfindən "Colonial Pipeline" hücumundan sonra baş verir və bu dəfə 11 milyon dollar dəyərində fidyə tələb olunur. Şübhəsiz ki "JBS" hücumunun baş verməsində daha əvvəlki 4.4 milyon dollarlıq mənfəətin rolu böyükdür. Nəticədə amerikalı ət istehsal edən bu nəhəng şirkət daha çox ziyana uğramamaq üçün 11 milyon dollarlıq fidyəni ödəməyə qərar verir (11)."Ransomware" hücumlarının artan təhlükəsinə cavab olaraq, danışıqlar və təsirlərin azaldılması üçün alternativ yanaşmalar ortaya çıxdı. Hüquq-mühafizə orqanlarının müdaxiləsi ransomware hücumlarının araşdırılması və mühakimə olunmasında mühüm rol oynayır. Hökumət və sənaye hissədarlarının birgə səyləri nəticəsində, "ransomware" əməliyyatlarını pozmaq və qlobal miqyasda kibertəhlükəsizlik müdafiəsini gücləndirmək üçün təsirli tövsiyələr və strategiyalar hazırlamaq məqsədi daşıyan Ransomware İşçi Qrupu (Ransomware Task Force (RTF)) kimi qruplarının formalaşıb (12). Dövlət-özəl tərəfdaşlığı həm də "ransomware" təhlükələrinin kollektiv şəkildə həlli ilə mübarizədə mühüm rol oynayır. Kibertəhlükəsizlik və İnfrastruktur Təhlükəsizliyi Agentliyi (Cybersecurity and Infrastructure Security Agency (CISA)) kimi təşkilatlar texniki yardım göstərmək və "ransomware" hücumlarına qarşı kibertəhlükəsizliyin dayanıqlığını artırmaq üçün özəl sektor şirkətləri ilə əməkdaşlıq edir (13).

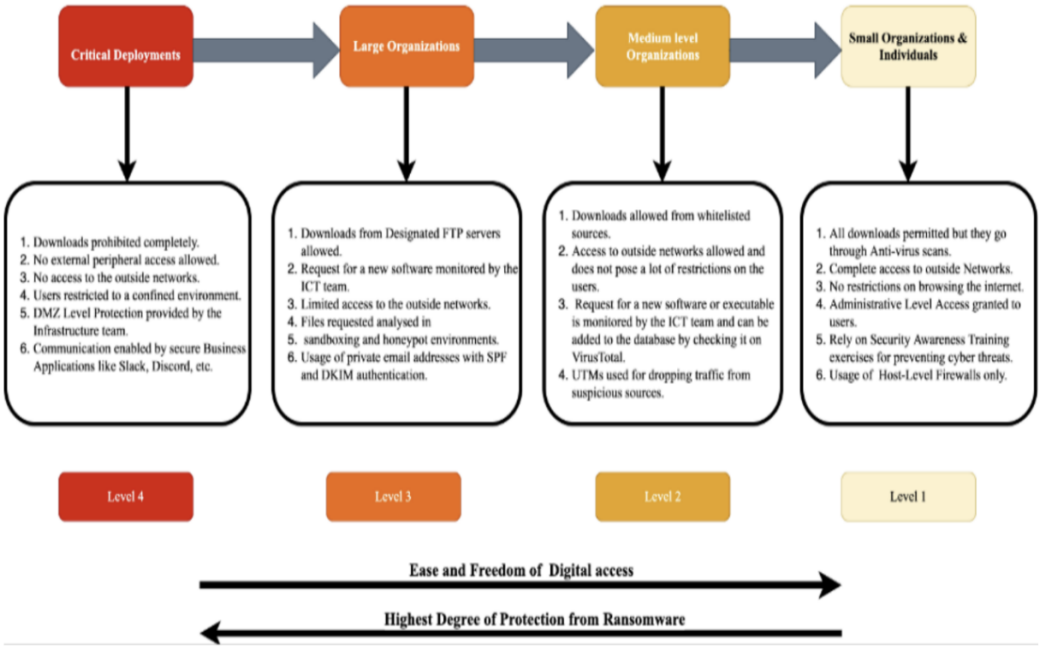
Nəticə olaraq, "ransomware" danışıqlarının dinamikasını başa düşmək, etik mülahizələri nəzərə almaq və əməkdaşlıq strategiyalarını araşdırmaqla təşkilatlar fidyə proqramı təhdidlərinə effektiv cavab verə və onların qurbanlara və cəmiyyətə təsirini azalda bilər.

Digər mübarizə üsulları. Kibertəhlükəsizliyin daim inkişaf edən mənzərəsində ransomware hücumlarına qarşı mübarizə şifrələmə alətləri, yedəkləmələr və danışıqlar taktikası kimi ənənəvi metodlardan kənara çıxan çoxşaxəli yanaşma tələb olunur. Bu strategiyalar yoluxmadan sonrakı bərpanın vacib komponentləri olsalar da, təşkilatlar ransomware təhdidlərinə qarşı davamlılığını artırmaq üçün bir neçə əlavə üsuldan da istifadə edə bilərlər. Belə üsullardan biri sistem bərpa nöqtələrinin (system restore points) istifadəsidir. Təsirə məruz qalmış sistemləri "ransomware" infeksiyası baş verməzdən əvvəlki vəziyyətinə qaytarmaqla təşkilatlar deşifrələmə alətlərinə və ya yedəkləmələrə ehtiyac duymadan faylları və sistem parametrlərini bərpa edə bilərlər. Bu, bərpa prosesini əhəmiyyətli dərəcədə sürətləndirə və "ransomware" hücumlarının biznes əməliyyatlarına təsirini minimuma endirə bilər. Məlumat itkisinin qarşısının alınması (data loss prevention (DLP)) tədbirlərinin istifadə olunması ransomware hücumlarının təsirini azaltmaq üçün bir başqa mühüm strategiyadır. DLP həlləri təşkilatlara həssas məlumatların "ransomware" tərəfindən əldə edilməsini, dəyişdirilməsini və ya şifrələnməsini müəyyən etməyə və qarşısını almağa imkan verir.

Buna misal olaraq Kaliforniya Universiteti, San Fransisko (UCSF) Tibb Mərkəzinə edilən "ransomware" hücumunu göstərmək olar, burada DLP proqramlarının tətbiqi konfidensial xəstə məlumatlarının şifrələnməsinin qarşısını almağa, hücumun xəstələrin qayğısına və məxfiliyə təsirini azaltmağa kömək etdi (14). Davranış analizi (Behavioral analysis) üsulları həmçinin "ransomware" infeksiyaları ilə əlaqəli şübhəli və ya zərərli fəaliyyətlərin müəyyən edilməsində və bloklanmasında mühüm rol oynaya bilər. İstifadəçi davranışını, fayla giriş modellərini və şəbəkə trafikini təhlil etməklə davranış təhlili həlləri "ransomware" fəaliyyətini göstərən anomaliyaları aşkarlaya və təşkilatlara təhlükəni azaltmaq üçün fəal tədbirlər görməyə imkan verə bilər.

Yoluxmuş sistemlərin təcrid edilməsi və saxlanması "ransomware" hücumu zamanı əlavə zərərin və məlumat itkisinin qarşısının alınması üçün vacib strategiyalardır. Şəbəkə mühitini seqmentləşdirmək və şəbəkə paylaşımlarını söndürməklə təşkilatlar yoluxmuş cihazları karantinə qoya və öz şəbəkələrində "ransomware" yayılmasının qarşısını ala bilər.

Ransomware hücumları ilə mübarizə, strategiya və texnikaların birləşməsindən istifadə edən hərtərəfli və proaktiv yanaşma tələb edir. Yuxarıda qeyd edilən üsulların bir neçəsini eyni anda tətbiq etməklə şirkətlər "ransomware" təhdidlərinə qarşı davamlılığını artıra və onların biznesə təsirini effektiv şəkildə azalda bilər. "Ransomware" hücumlarına qarşı həssaslıq dərəcəsinə və istifadə etdiyi qorunma taktikalarına əsasən şirkətlər 4 səviyyədə dəyərləndirilir (15).



Şəkil 3: 4 səviyyədə "ransomware" ilə mübarizə

4 cü səviyyə kritik infrastrukturlara aiddir və onların istifadəçilərini qapalı və şəbəkədən təcrid olunmuş mühit ilə məhdudlaşdırır. Bu üsul istifadəçilərin rəqəmsal azadlıqlarını alaraq "ransomware" hücumlardan qorunmağı hədəfləyir və sistem xarici heç bir təsirə məruz qalmadığı üçün hücumlara qarşı böyük qoruma yaradır.

3 cü səviyyə böyük şirkətlərə aiddir. Burada istifadəçilər sadəcə mərkəzi İnformasiya Texnologiyaları (İT) komandası tərəfindən təyin olunmuş Fayl Transfer Protokolu (FTP) serverlərindən faylları yükləyə bilirlər. Açıq internetdən tələb olunan bütün digər yükləmələr isə əvvəlcə şəbəkədən təcrid olunmuş mühitdə saxlanılr və zərərli proqramların aşkarlanması üçün həm statik, həm də dinamik olaraq təhlil edilir. Bundan əlavə, proqram yeniləmələri sadəcə mərkəzi İT komandası tərəfindən idarə oluna və yüklənə bilər və fərdi istifadəçilərin sistem səviyyəsində dəyişikliklər etmək üçün imtiyazları yoxdur.

2 ci səviyyə orta ölçülü müəssisələrə şamil edilir, istifadəçilərə açıq internetdən faylları endirməyə imkan verir, lakin zərərli proqramları aşkar etmək və şübhəli mənbələrdən trafiki azaltmaq üçün trafiki Vahid Təhdid İdarəetmə (Unified Threat Management (UTM)) cihazı yönləndirir və endirmələr bu cihaz üzərindən aparılır.

1 ci səviyyə lazımi İT infrastrukturuna və ya təhlükəsizlik siyasətinə malik olmayan kiçik təşkilatlara aiddir. Burada fərdi antivirus proqramına malik olmaqdan başqa, təhlükəsizlik siyasəti ilə bağlı çox şey yoxdur. Bu təşkilatlar "ransomware" hücumlarına qarşı çox həssasdırlar və istifadəçi məlumatlılığı və fərqindəliyi bu şirkətlərin "ransomware" hücumlarına qarşı ən təsirli strategiyalardır (15).

Nəticə

Nəticə olaraq bu yazıda günümüzün təhlükə mənzərəsində kibertəhlükəsizlikdən müdafiənin çoxşaxəli xarakterini vurğulayaraq, "ransomware" hücumlarından infeksiyadan sonrakı bərpa üçün bir sıra strategiya və üsulları araşdırdıq. "Ransomware" hücumları problemlər yaratmağa davam etsə də, fəal tədbirlər və birgə səylər daha möhkəm gələcəyə ümid verir. "Ransomware" müdafiəsinə hərtərəfli yanaşmanı mənimsəməklə və inkişaf edən təhdidlər haqqında məlumatlı olmaqla, biz "ransomware" tərəfindən törədilən riskləri effektiv şəkildə azalda və rəqəmsal infrastrukturumuzun bütövlüyünü qoruya bilərik.

Ədəbiyyat

1. https://www.veeam.com/analyst-reports/trends-report-ransomware_wpp.pdf
2. https://www.mdpi.com/2071-1050/14/1/8#
3. https://www.techrxiv.org/doi/full/10.36227/techrxiv.24596754.v1
4. https://ieeexplore.ieee.org/document/10099114
5. https://www.sciencedirect.com/science/article/abs/pii/S0167404821002935
6. https://www.sciencedirect.com/science/article/pii/S0268401223001056
7. https://www.veeam.com/blog/ransomware-recovery-what-you-need-to-know.html
8. Backup and Recovery: Inexpensive Backup Solutions for Open Systems (2006) By W. Curtis Preston
9. https://deliverypdf.ssrn.com/delivery.php?ID=485064027065077076091072100029114107009048072043057026110094113069119014009105069073038010111048053030011028107095093122072064121075061013081117013073006116071122111069065049116089024073089125011001092031090076121116123006029070072068103099012015103073&EXT=pdf&INDEX=TRUE
10. https://energyrights.info/sites/default/files/artifacts/media/pdf/the_colonial_pipeline_ransomware_hackers_had_a_secret_weapon_self-promoting_cybersecurity_firms_-_propublica.pdf
11. https://scholarship.shu.edu/cgi/viewcontent.cgi?article=2278&context=student_scholarship
12. https://www.in.gr/wp-content/uploads/2021/05/RTF.pdf
13. https://www.cisa.gov/

14. https://www.sanmateorcd.org/wp-content/uploads/2020/11/Grand-Jury-Report-Ransomware-letter-and-report-2020-10-7.pdf
15. https://www.mdpi.com/2071-1050/14/1/8

Göndərilib: 06.01.2024 Qəbul edilib: 02.03.2024