Kiber Xəbərlər Jurnalı

vol. 6

birbank

Giriş

Hörmətli oxucular,

2025-ci ilin ikinci yarısına daxil olduğumuz halda, kiberhücumların sayı qlobal səviyyədə artmağa davam edir. Bu prosesdə süni intellekt mühüm rol oynayır. Jurnalımızda yeni illə birgə gələn ən vacib kibertəhlükəsizlik yeniliklərini və trendlərini sizə təqdim edirik.

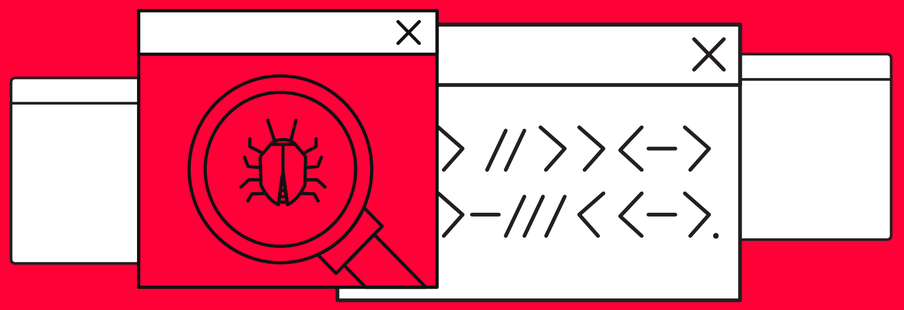
Kiber aləmdə təhlükələr sürətlə dəyişir, buna görə də ən yaxşı müdafiə üsulu daim xəbərdar və ayıq-sayıq olmaqdır.

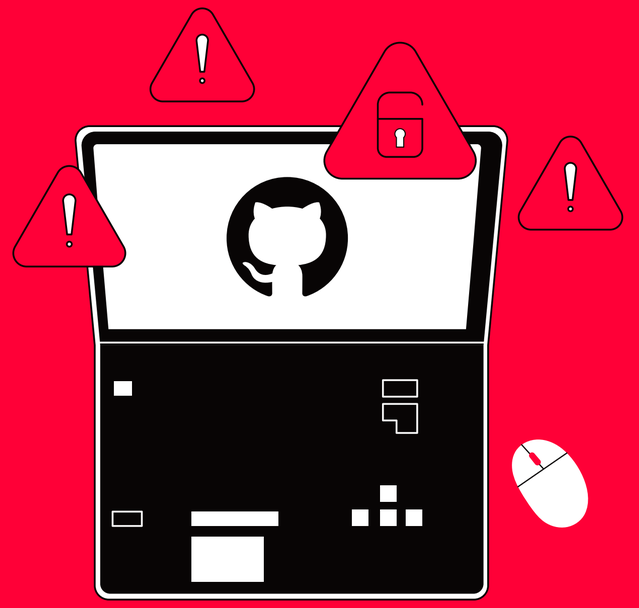
Elə isə gəlin 2025-ci ilin kibertəhlükəsizlik dinamikasına birlikdə nəzər salaq!

Microsoft, 1 milyondan çox cihaza təsir edən reklam kampaniyası barədə xəbərdarlıq edir

Microsoft son vaxtlar 2024-cü ilin dekabrında aşkarlanan və dünya üzrə 1 milyon cihazdan çoxuna təsir edən geniş yayılmış *malvertising kampaniyasının təfərrüatlarını açıqlayıb. Bu hücum, istifadəçilərin fərdi və həssas məlumatlarını oğurlamaq məqsədilə planlanmış bir hərəkət kimi görünür.

Microsoft tərəfindən Storm-0408 adı altında izlənilən bu kampaniya, phishing, malvertising və axtarış mühərriki manipulyasiyası kimi üsullardan istifadə edərək zərərli proqramlar yaymaqla tanınan bir qrupa aid edilir. Qrupun məqsədi, icazəsiz cihazlara giriş əldə etmək və dəyərli məlumatlar toplamaqdır.



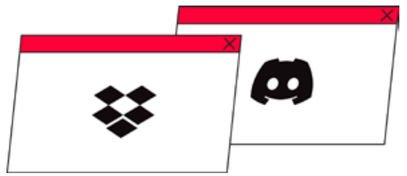


Kampaniya, zərərli reklamlar yerləşdirilən şübhəli yayım saytlarından başlayıb. Bu reklamlar istifadəçiləri aralıq bir sayta yönləndirir, oradan isə GitHub və digər platformalara keçərək zərərli proqramlar göndərilirdi.

Hücum həm fərdi istifadəçiləri, həm də bizneslərı hədəf alaraq geniş miqyaslı bir təhlükə yaratmışdı.

Kampaniya, zərərli reklamlar yerləşdirilən şübhəli yayım saytlarından başlayıb. Bu reklamlar istifadəçiləri aralıq bir sayta yönləndirir, oradan isə GitHub və digər platformalara keçərək zərərli proqramlar göndərilirdi.

Hücum həm fərdi istifadəçiləri, həm də bizneslərı hədəf alaraq geniş miqyaslı bir təhlükə yaratmışdı.



Hücum bir neçə mərhələdə həyata keçirilir:

Mərhələ 1:
Onlayn Platforma

Mərhələ 2:
Zərərli reklam proqramı (adware)

Mərhələ 3:
Zərərli vebsayt

Mərhələ 4:
Yoluxan istifadəçi

Bu kampaniya malvertising risklərini və kibercinayətkarların taktikalarının inkişafını vurğulayır, həm fərdi istifadəçilər, həm də bizneslər üçün təhlükəsizlik tədbirlərini gücləndirmək və diqqətli olmaq üçün bir xatırlatmadır.

**Malvertising - zərərli proqramları yaymaq məqsədilə reklamlar vasitəsilə həyata keçirilən hücumdur.*

https://thehackernews.com/2025/03/microsoft-warns-of-malvertising.html

Microsoft Fevral 2025 Təhlükəsizlik Yeniləmələri: **Kritik Zəifliklər Aradan Qaldırıldı**

Microsoft
Patch Tuesday

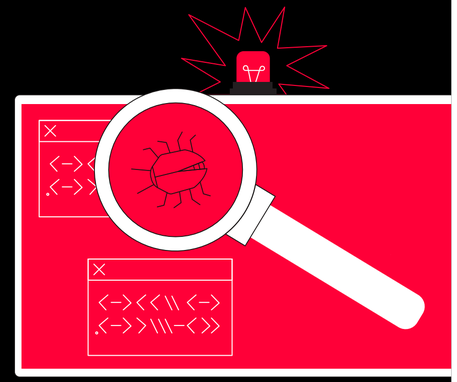
Microsoft, fevral ayında 63 təhlükəsizlik boşluğunu aradan qaldırdığını bildirdi. Bu yeniləmə əvvəlki ayın böyük təhlükəsizlik yeniləmələrinə nisbətən kiçik olsa da, belə görünür ki, vacib təhlükəsizlik məsələləri hələ də mövcuddur.

Xüsusilə diqqət çəkən iki ciddi zəiflik artıq aktiv şəkildə mövcud olmağa davam edir. Yəni, kibercinayətkarlar bu boşluqlardan istifadə edərək sistemlərə hücum edə bilərlər.

Ən kritik hesab edilən 2 (iki) zəiflik aşağıdakılardır:

- Kibercinayətkarlara faylları silmək imkanı verir. Məlumatların sızması ehtimalı olmasa da, kritik faylların silinməsi xidmətin əlçatmaz olmasına səbəb ola bilər.

- Hücumçulara sistem səviyyəsində tam imtiyaz əldə etməyə imkan yaradır. Bu, onların bütün sistem üzərində tam nəzarət əldə etmələrinə səbəb ola bilər.



Microsoft
Active Directory

Active Directory (AD)

Digər bir boşluq Active Directory (AD) ilə bağlıdır. AD, şirkətlərin istifadəçi və cihazlarını idarə etdiyi əsas sistemdir. Kibercinayətkarlar, LDAP protokolundakı zəiflikdən istifadə edərək bu sistemə müdaxilə edə bilərlər.

Bu nə deməkdir?

- Uzaqdan zərərli kod icra edə bilərlər, yəni sistemlərə icazəsiz müdaxilə edə bilərlər.
- İcazələrini artıraraq daha çox səlahiyyət əldə edə bilərlər, yəni adi istifadəçidən administrator səviyyəsinə yüksələ bilərlər.
- Şirkət şəbəkəsində yayılıb daha çox sistemə təsir edə bilərlər.

Niyə vacibdir?

Çünki Active Directory şirkətin şəbəkəsində istifadəçi girişlərini və icazələrini idarə edən əsas sistemdir. Bu sistemə hücum etmək o deməkdir ki, hücumçular şirkətin bütün məlumatlarına giriş əldə edə bilərlər.

Daha dəqiq desək, AD zəifliyi təşkilatın məlumat təhlükəsizliyini pozmaq üçün çox ciddi təhlükə yarada bilər, lakin AD həmçinin məlumat saxlama sisteminin tam özü deyil. O, daha çox identifikasiya və idarəetmə funksiyasını yerinə yetirir. Məlumat saxlama konkret olaraq ayrıca serverlər və verilənlər bazası sistemləri tərəfindən idarə oluna bilər.

Bu yeniləmələr zamanı görülən təhlükəsizlik boşluqlarını aşağıdakı kimi klassifikasiya etmək olar:

- **25 Uzaqdan Kod İcra boşluğu (RCE)**
- **20 İmtiyazın Yüksəldilməsi boşluğu (EoP)**
- **9 Xidmətdən İmtina boşluğu boşluğu (DoS)**
- **5 *Spoofing boşluğu**
- **2 Təhlükəsizlik Xüsusiyyətlərini Atlatma zəifliyi**
- **1 Məlumatın Açıqlanması zəifliyi**
- **1 Dəyişiklik edə bilmə zəifliyi**

Nəticə olaraq, Microsoft-un fevral ayı yeniləməsi kritik zəifliklər aradan qaldırsa da, bu boşluqlar artıq aktiv şəkildə istifadə edilməsi təhlükə yaradır. Bu, şirkətlər üçün bir xəbərdarlıqdır ki, təhlükəsizlik yeniləmələrini gecikdirməməli və mümkün olan ən qısa zamanda sistemlərini qorumaq üçün tədbirlər görməlidirlər.

**Spoofing – kibertəhlükəsizlikdə kibercinayətkarın özünü etibarlı bir şəxs, sistem və ya qurğu kimi təqdim etməsi nəticəsində məlumat oğurlamaq, icazəsiz giriş əldə etmək və ya istifadəçiləri aldatmaq məqsədilə həyata keçirilən hücum növüdür.*

https://thehackernews.com/2025/02/microsofts-patch-tuesday-fixes-63-flaws.html

Bu zəifliklər kibercinayətkarların sistemlərə nəzarət etmələrinə, kritik məlumatları silmələrinə və təşkilatın şəbəkəsi daxilində yayılmalarına imkan yaradır. Microsoft və CISA (Amerikanın Kibertəhlükəsizlik və İnfrastruktur Təhlükəsizliyi Agentliyi), təşkilatları bu boşluqlara qarşı dərhal yeniləmə tətbiq etməyə çağırır.

Saxta iş təklifləri:
Lazarus qrupunun LinkedIn planı

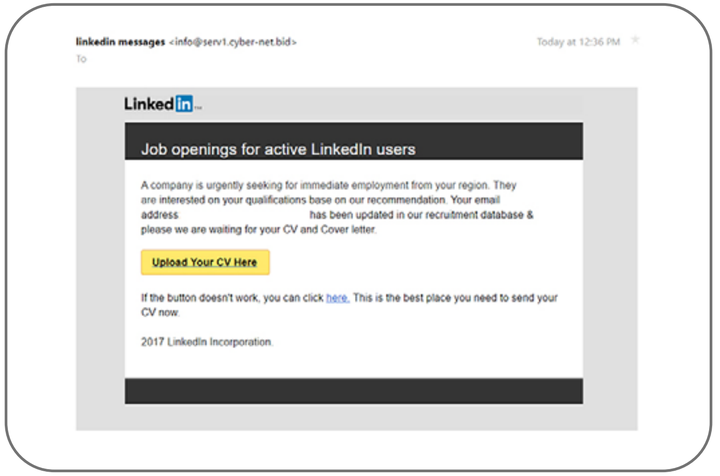
Kibercinayətkar qrupu, Lazarus son zamanlar LinkedIn platformasından istifadə edərək kiber casusluq fəaliyyətlərini artırıb. Bu yeni hücumun məqsədi maliyyə və turizm istiqamətində çalışan əməkdaşları hədəf almaqdır. Qrup, saxta iş təklifləri ilə insanları aldatmağa çalışır və bu yolla mobil cihazlarına zərərli proqramlar yükləyir.

Hücum, LinkedIn üzərindən, mərkəzləşdirilməmiş kriptovalyuta mübadiləsi layihələrində əməkdaşlıq təklif edən, diqqəti və marağı cəlb edən bir mesajla başlayır. Bu mesajda məsafədən, yarım-ştat vahidi ilə iş və yüksək maaş təklif edilirdi. Maraqlanan şəxslərdən CV və ya GitHub hesablarını göndərməsi istənilir. Bu, həm şəxsi məlumatları toplamaq, həm də qarşı tərəfi inandırmaq məqsədini daşıyır.

Bu cür hücumlar, istifadəçilərin fərdi məlumatlarını oğurlamaq və sistemlərini zədələmək məqsədini daşıyır. Bu səbəbdən, şübhəli iş təkliflərindən qaçınmaq və həmişə diqqətli olmaq vacibdir.

İlk əlaqəyə keçdikdən sonra, hədəf şəxslərə GitHub və ya Bitbucket üzərindən layihə göndərilir. Bu fayllar, kompüterlərə zərərli proqramlar yükləyən gizli kodları ehtiva edir. Bu proqram həm Windows, həm də macOS və və Linux sistemlərində işləyir. Əsas məqsəd, qurbanın brauzerindəki kriptovalyuta hesablarından məlumat oğurlamaqdır. Bu zərərli proqram, kompüterdə backdoor (arxa qapı) yaradır və kiber hücumçulara uzaqdan nəzarət etməyə şərait imkan verir.

https://socradar.io/lazarus-groups-cyber-espionage-involving-linkedin/



Yüzlərlə Saxta Reddit Saytı **Lumma Stealer Zərərli Proqramını Yayımlayır**

Kibercinayətkar, Reddit və WeTransfer kimi məşhur saytları təqlid edən 1,000-ə yaxın saxta veb səhifə yayımlayaraq, istifadəçiləri Lumma Stealer zərərli proqramını yükləməyə cəlb edirlər.

Bu saxta saytlar, Reddit brendindən sui-istifadə edərək müəyyən bir mövzu ilə əlaqədar saxta müzakirə başladır. Müzakirə başladan şəxs, xüsusi bir alət yükləmək üçün kömək istəyir, başqa biri isə WeTransfer-ə yükləyərək linki paylaşır, üçüncüsü isə təşəkkür edərək hər şeyi həqiqi göstərməyə çalışır.

Zərərsiz istifadəçilər bu linkə kliklədikdə, onları saxta WeTransfer səhifəsinə yönləndirir ki, burada "Yüklə" düyməsi Lumma Stealer zərərli proqramını yükləməyə səbəb olur.

Lumma Stealer Zərərli Proqramının Təhlükəsi

Lumma Stealer, kibercinayətkarlara satılır və onlar bu proqramı müxtəlif yollarla yayırlar, məsələn, GitHub, saxta veb saytlar və reklamlar vasitəsilə. Bu cür proqramlar, istifadəçilərin brauzerlərində saxlanılan parolları və hesabları ələ keçirmək üçün session token-lərini oğurlayır. Bu məlumatlar, şəbəkə hücumları və ya sosial mühəndislik vasitəsilə şirkətlərdən və fərdi şəxslərdən həssas məlumatlar əldə etmək üçün istifadə olunur.

https://www.bleepingcomputer.com/news/security/hundreds-of-fake-reddit-sites-push-lumma-stealer-malware/

Bütün bu saxta saytlar, təqlid etdikləri domen adı və ardınca təsadüfi nömrə və simvollar əlavə edərək, birbaşa baxışda etibarlı görünür.
Araşdırmalara əsasən bu sosial mühəndislikdə iştirak edən səhifələrin tam siyahısı paylaşılmışdır. Bu kampaniya çərçivəsində 529 saxta Reddit və 407 saxta WeTransfer saytı tapılıb.

Ransomware hücumu: Medusa qrupu qurbanlardan 15 milyon dollara qədər pul tələb edir

Medusa ransomware qrupu ilk dəfə 2023-cü ilin yanvarında ortaya çıxdığından bəri təxminən 400 hücumla əlaqələndirilib. 2023-2024-cü illər ərzində bu qrup üzrə insidentlər 42% artıb. Yalnız 2025-ci ilin ilk iki ayında qrupa aid 40-dan çox yeni hücum qeydə alınıb.

Medusa ikiqat şantaj modelindən istifadə edir: əvvəlcə qurbanların məlumatlarını oğurlayır, sonra isə sistemlərini şifrələyir. Bu taktika təşkilatlara təzyiqi artırır, çünki fidyə ödənilmədikdə oğurlanmış məlumatlar məlumat sızmalarını qeydə aldıqları qrupun saytında yayımlanır.

LockBit və BlackCat kimi əsas Ransomware-as-a-Service (RaaS) qruplarının son fəaliyyətinin dayandırılması ilə Medusa kiber şantaj aləmində əsas oyunçu kimi ortaya çıxdı. RansomHub (həmçinin Greenbottle və Cyclops kimi tanınır), Play (Balloonfly) və Qilin (Agenda, Stinkbug, Water Galura) da daxil olmaqla digər ransomware qrupları da fəaliyyətlərini genişləndirdi.

Medusa-nın fidyə tələbləri 100,000 dollardan 15 milyon dollara qədər dəyişir. Qrup əsasən maliyyə qurumları, dövlət agentlikləri, qeyri-kommersiya təşkilatları və səhiyyə sektoru kimi böyük qurumları hədəf alır. Hücumlar adətən Microsoft Exchange Server kimi ictimaiyyətə açıq tətbiqlərdəki boşluqlardan istifadə edərək ilkin giriş əldə etməklə həyata keçirilir.

Əksər ransomware qrupları kimi, Medusa da maliyyə məqsədi güdür və heç bir ideoloji və ya siyasi yanaşma daşımır. Qrup müxtəlif sahələrdə yüksək dəyərə malik hədəflərdən pul qoparmağa fokuslanır.

https://www.linkedin.com/pulse/medusa-ransomware-hits-40-victims-2025-demands-100k15m-ransom-mafic/

https://thehackernews.com/2025/03/medusa-ransomware-hits-40-victims-in.html

16 Chrome uzantısı təhlükəyə məruz qaldı və **600.000-dən çox istifadəçi risk altında**

Bu yaxınlarda həyata keçirilən kiberhücum nəticəsində 16 Chrome uzantısı təhlükəyə məruz qalıb və 600,000-dən çox istifadəçinin fərdi məlumatları oğurlanma riski altındadır.

Hücumçular Chrome Web Store üçün uzantılar yaradan developerləri hədəf alan ağıllı fişinq sxemindən istifadə ediblər. Giriş əldə etdikdən sonra isə onlar həqiqi uzantılara zərərli kod yerləşdirərək istifadəçilərin kukilərini(cookie) və login tokenlərini oğurlayıblar.

cyberhaven

Dekabrın 27-də Cyberhaven şirkəti hücuma məruz qalan uzantılardan birinin onlara aid olduğunu açıqladı. Hücumçular bu uzantı vasitəsilə xarici serverlə əlaqə quraraq daha çox zərərli fayl yükləyib və istifadəçi məlumatlarını toplayıblar.

Hücumun təsviri:

Fişinq e-mailləri Google Chrome Web Store Developer Support-dan göndərilmiş kimi tərtib olunmuşdu. Onlar tərtibatçılara uzantılarının siyasət pozuntularına görə silinmə riski altında olduğunu bildirərək problemi həll etmək üçün bir linkə kliklәməyi təklif edirdilər. Bu link isə hücumçulara "Privacy Policy Extension" adlı zərərli tətbiqə giriş imkanı verən təhlükəli səhifəyə yönləndirirdi.

Mütəxəssislər xəbərdarlıq edir ki, adətən nəzərə alınmayan brauzer uzantıları həssas istifadəçi məlumatlarına geniş çıxış əldə edə bilər. ***"Bir çox təşkilat sistemlərində hansı uzantıların quraşdırıldığını bilmir və bu da onları belə hücumlara qarşı müdafiəsiz qoyur," –*** deyə LayerX Security-nin CEO-su Or Eshed bildirib.

Təhlükəsizliyinizi təmin etmək məqsədilə, istifadə etdiyiniz brauzer uzantılarını mütəmadi olaraq nəzərdən keçirməyinizi və artıq istifadə etmədiyiniz və ya tanımadığınız uzantıları silməyinizi tövsiyə edirik. Uzantıları yalnız etibarlı və rəsmi mənbələrdən quraşdırmağınız, həmçinin brauzer üzərindən hər hansı gözlənilməz pop-up mesajlarına və ya fəaliyyət göstərməyinizi tələb edən naməlum e-poçtlara qarşı diqqətli olmağınız vacibdir.

https://www.linkedin.com/pulse/16-chrome-extensions-hacked-exposing-over-600000-users-data-6urvc/

birbank

Hər hansı təklif və iradlarla bağlı bu e-mail adresi ilə əlaqə saxlayın: cyberjournal@kapitalbank.az