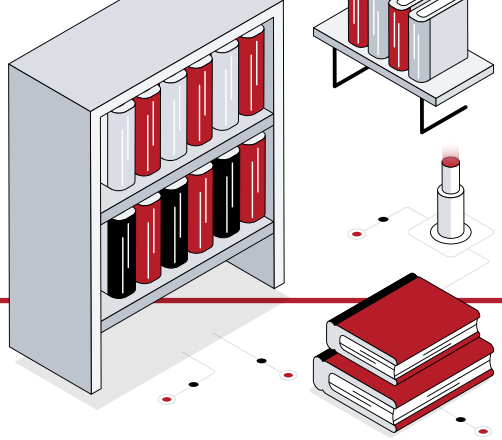
SAY 2

KİBER XƏBƏRLƏR JURNALI

Kapital Bank

2024

Mündəricat



Cisco AnyConnect VPN vasitəsilə məsafədən iş infrastrukturuna hücumu

Son zamanlarda kiberhücumlar daha çox məsafədən işlə əlaqəli sistemlərə yönəlib.

Kibercinayətkarlar Cisco AnyConnect VPN proqram təminatını təqlid edərək zərərli fayllar yayırlar. İşçilər bu VPN proqram təminatı yüklədikdə, zərərli proqram sistemə daxil olur və hədəfin kompüterindəki faylları şifrələyir. Şirkətlərdən bu şifrəni açmaq üçün müəyyən məbləğdə pul (fidyə) tələb edilir. Adətən ödənişlər kriptovalyutalar vasitəsilə tələb olunur, belə ki, kibercinayətkarlatın kimliyini gizlətmək daha asan olur.

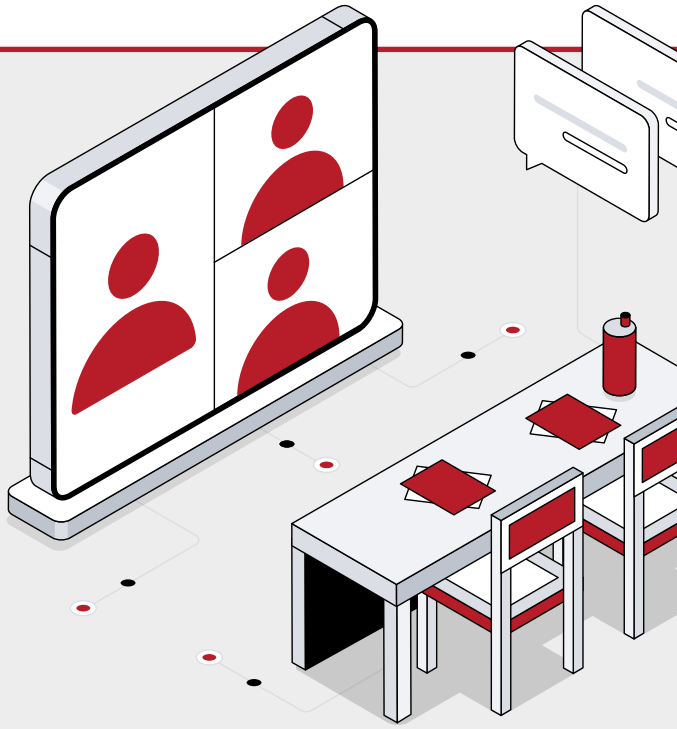
Bu tip hücumlar son dövrlərdə kəskin şəkildə artmışdır, çünki COVID-19 pandemiyası ilə əlaqədar sonralar uzaqdan işləmə modelləri geniş yayılmağa başlamışdır.

Necə həll edildi?

Şirkətlərə bu cür hücumların qarşısını almaq üçün, VPN proqramlarını müntəzəm olaraq yeniləmək, yalnız rəsmi və bilinən mənbələrdən proqram təminatlarını yükləmək, çox faktorlu autentifikasiya tətbiq etmək və istifadəçilərin sosial mühəndislik və onun növləri barədə ayıq-sayıqlığı artırmaq tövsiyə olunur.

Eyni zamanda, məlumatların ehtiyat nüsxəsini alaraq ransomware hücumlarının zərərlərindən az da olsa yayınmağa kömək edə bilər.

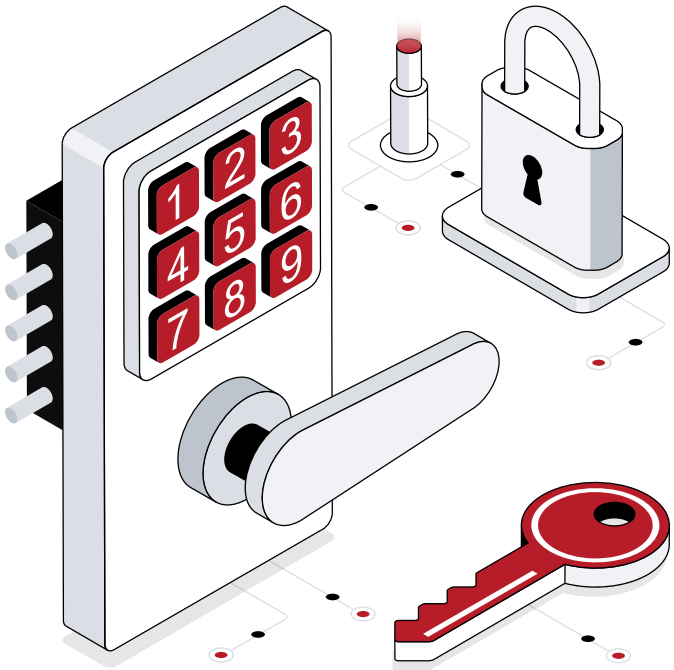
Zoom platformasında Sıfır-Gün zəifliyi: **şirkətlərin casusluq qurbanı olmasına səbəb oldu**



Zoom, xüsusilə pandemiya dövründə, ən çox istifadə edilən video-konfrans platformalarından birinə çevrildi. Lakin bu populyarlıq kibercinayətkarların diqqətindən kənarda qalmadı.

Yeni aşkarlanan sıfır-gün zəifliyi Zoom konfranslarına icazəsiz daxil olmağa imkan verirdi və bir sıra şirkətlərin məxfi məlumatları bu yolla oğurlanmasını mümkün edirdi. Bu hücum zamanı kibercinayətkarlar konfranslara birbaşa qoşularaq məlumatları sızdırmaqla yanaşı, iştirakçıların kompüterlərinə də zərərli proqramlar quraşdıra biliblər.

Bu problemi necə aradan qaldırmaq olardı?

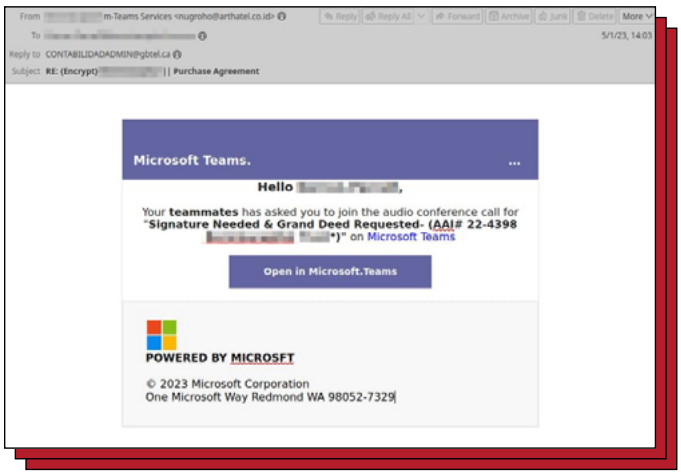


Zoom təhlükəsizlik yenilənmələrini (patch) yayımlayıb bu boşluğu aradan qaldırmasına baxmayaraq, mütəxəssislər şirkətlərə təhlükəsiz video-konfranslar üçün şifrə ilə qorunan otaqlar yaratmağı, iştirakçıların giriş hüquqlarını ciddi şəkildə nəzarət etməyi və iclaslarda yalnız şifrəli kommunikasiya vasitələrindən istifadə etməyi məsləhət görür. Təhlükəsizlik tədbirləri görməyən şirkətlər isə ciddi məlumat sızmaları və itkilərlə üzləşə bilərlər.

Microsoft Teams hesabları fişinq hücumları ilə hədəf alındı: **daxili məlumatların oğurlanması**

Microsoft Teams geniş şəkildə istifadə edilən əməkdaşlıq və ünsiyyət platformasıdır. Bu platforma vasitəsilə hücumlar adətən fişinq e-poçtları və ya saxta veb giriş səhifələri ilə həyata keçirilir.

Kibercinayətkar istifadəçilərə Microsoft Teams-ə daxil olmaq üçün təcili yeniləmə və ya sistemlə bağlı xəbərdarlıq göndərirlər və qurbanları saxta giriş səhifələrinə yönləndirirlər. Burada onların giriş məlumatları oğurlanır və bundan sonra kibercinayətkarlar şirkət daxili məlumatlara giriş əldə edir.



Hədəf götürülən şirkətlər Microsoft Teams-də saxlanılan həssas sənədləri, layihə məlumatlarını və məxfi yazışmaları itirə bilərlər. Hücumlar nəticəsində əməliyyatlar pozulur, şirkətlərin nüfuzuna xələr gəlir. Microsoft təhlükəsizlik mütəxəssisləri çox faktorlu autentifikasiyanın (MFA) istifadəsini tövsiyə edirlər və fişinq hücumlarını tanımaq üçün işçilərə təlimlər keçilməsinin vacibliyini vurğulayırlar. Belə ki, təhlükəsiz kommunikasiya üçün alternativ yolların da nəzərdən keçirilməsi çox vacibdir.

Google Workspace troyan hücumu: **Google Docs əlavələri vasitəsilə casusluq**

Google Workspace, bir çox müəssisələr üçün məhsuldarlıq və əməkdaşlıq vasitəsi kimi geniş istifadə edilir. Lakin bu yaxınlarda aşkar edilmiş troyan virusu vasitəsilə platformada yeni bir təhlükə meydana çıxdı.

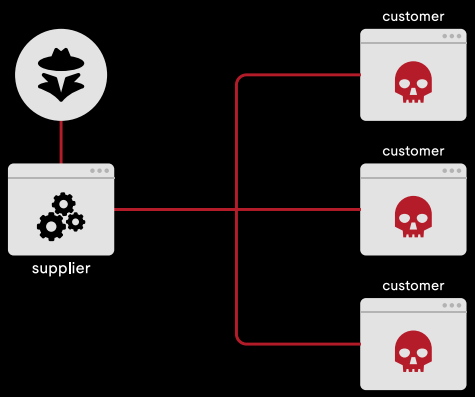
Zərərli proqram özünü Google Docs əlavələri kimi təqdim edir və istifadəçilər bu əlavələri quraşdırdıqda zərərli fəaliyyətlərə başlayır. Troyan virusu hədəfin sisteminə tam nəzarət imkanı verir və şəxsi məlumatlar, fayllar oğurlanır. Kibercinayətkarlar istifadəçilərin fəaliyyətini izləyir, həssas məlumatları toplayır və sistemlərə arxa qapılar (backdoor) yerləşdirirlər.

Hücum zamanı böyük miqdarda məlumat oğurlana və ya silinə bilər. Google bu hücuma cavab olaraq təhlükəsizlik yenilikləri yayımlayıb, lakin ekspertlər təşkilatlara yalnız təsdiqlənmiş əlavələrdən istifadə etməyi, həssas sənədlərin saxlanılmasını məhdudlaşdırmağı və təhlükəsizlik konfiqurasiyalarını gücləndirməyi tövsiyə edirlər.

Şirkətlərin əlavə təhlükəsizlik monitorinqi ilə sistemlərini qorumaq üçün daim nəzarət etməsi vacibdir.

Təchizat zənciri hücumu **SaaS platformasında kütləvi məlumat sızmasına səbəb oldu**

SaaS (Software-as-a-Service) platformaları bir çox şirkətlərin əsas xidmətlərindən birinə çevrilib, lakin onların təhlükəsizliyi ilə bağlı ciddi problemlər ortaya çıxır. Yaxın zamanda SaaS platformalarından birində təchizat zənciri hücumu baş vermişdir. Kibercinayətkarlar, bu platformanın xidmətlərini alan üçüncü tərəflərin istifadəsində olan kitabxanalara zərərli kod yerləşdirmişdilər. Bu kod vasitəsilə platformaya giriş əldə edən kibercinayətkarlar, minlərlə istifadəçinin hesablarını və şəxsi məlumatlarını oğurlayıblar.

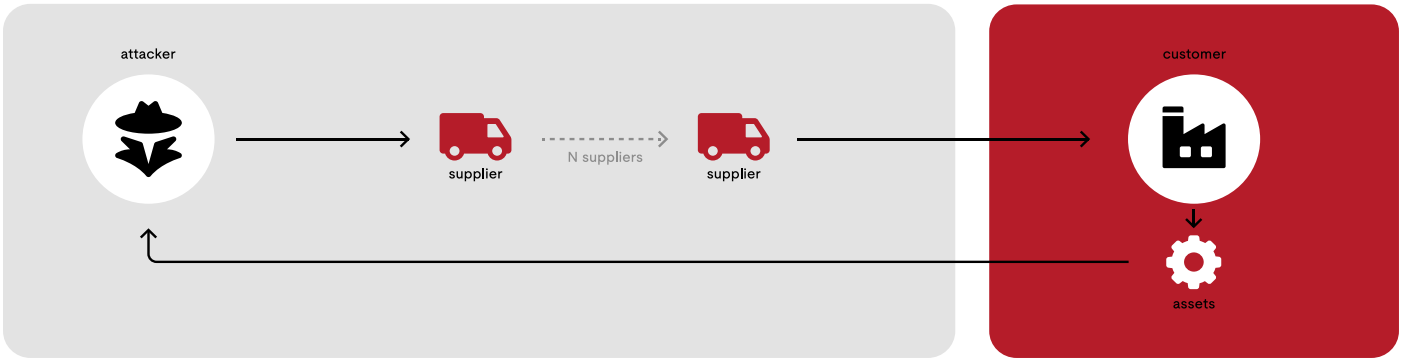


Bu hücum nəticəsində, xüsusilə maliyyə və səhiyyə sektorundakı məlumatlar təhlükə altında idi. Təchizat zənciri hücumları mürəkkəbdir, çünki onlar birbaşa platformanın özündən deyil, üçüncü tərəf resurslarından gəlir və platformaların təhlükəsizlik sistemləri bəzən bu cür hücumları aşkar etməkdə çətinlik çəkə bilərlər.

Ekspertlər, şirkətlərin üçüncü tərəf təminatçıları ilə işgüzar münasibətlərini daha diqqətlə nəzərdən keçirməli və təhlükəsizlik auditi aparmalı olduqlarını vurğulayırlar. Təchizat zəncirindəki zəifliklərin tapılması və aradan qaldırılması şirkətlərin məlumatlarını qorumaq üçün çox vacibdir.

SUPPLIER ATTACK

CUSTOMER APT ATTACK



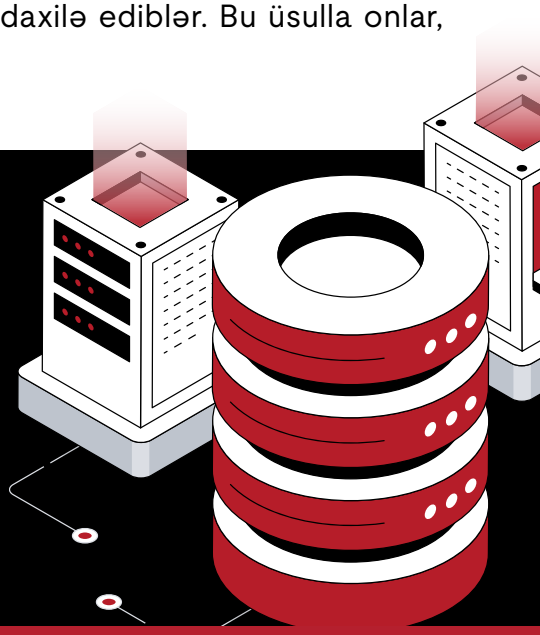
Microsoft Exchange Server-də **yeni zəiflik aşkar olundu**

2024-cü ilin fevralında Microsoft Exchange Server-də kritik bir zəiflik (CVE-2024-21410) aşkar edilib. Bu zəiflik kibercinayətkarlar tərəfindən fəal şəkildə istismar olunub. Kibercinayətkar istifadəçilərin Net-NTLMv2 “hash relay” edərək, onlarla eyni imtiyazları əldə ediblər. NTLM (NT LAN Manager), Microsoft-un şəbəkə mühitlərində istifadə etdiyi bir kimlik doğrulama protokoludur. İstifadəçilərin məlumatlarını şifrələyərək serverə göndərir.

"Relay" isə kibercinayətkarların bir sistemdəki kimlik doğrulama məlumatlarını (hash-ləri) digər sistemə yönləndirməsi deməkdir. Xüsusilə, kibercinayətkarlar Outlook kimi NTLM müştərilərindən istifadə edərək bu hash-ləri oğurlayıb və Exchange Server-ə müdaxilə ediblər. Bu üsulla onlar, qurbanların adından müxtəlif əməliyyatlar həyata keçiriblər.

Zəifliyin nəticələri

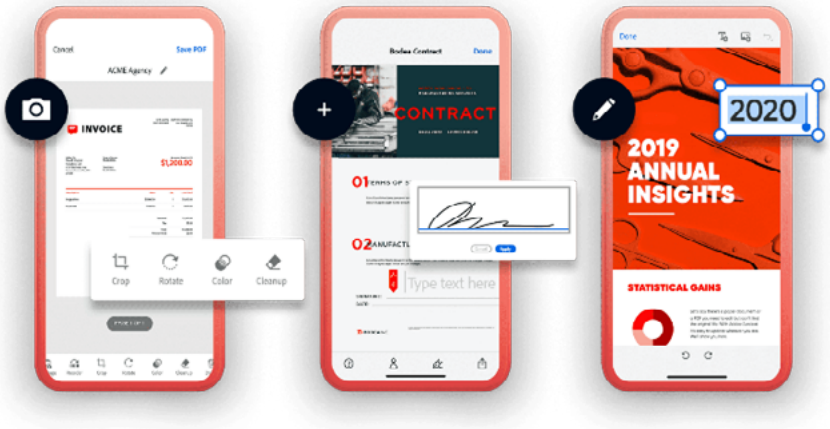
Bu istismar nəticəsində kibercinayətkarlar şirkətlərin elektron poçt sistemlərindəki məlumatlara qanunsuz giriş əldə ediblər. Onlar həmçinin məxfi yazışmaları və kritik məlumatları oğurlayıblar. Bu da şirkətlər üçün böyük həcmdə məlumat itkisinə səbəb olub.



Problemin həlli üçün atılan addımlar

Microsoft bu zəifliyi aşkar etdikdən sonra Exchange Server 2019 üçün “Cumulative Update 14” (CU14) adlı təhlükəsizlik yeniləməsini yayımlandı. Bu yenilənmə əlavə müdafiə yaradaraq gələcək hücumların qarşısını almağa kömək edir. Microsoft, bütün istifadəçilərə bu yeniləməni təcili şəkildə tətbiq etməyi tövsiyə edib. Yeniləmə tətbiq olunduqdan sonra zəiflik aradan qaldırılıb.

Adobe Acrobat Reader-da zəiflik aşkar olundu: **İstifadəçilərin məlumatları təhlükədə!**



Son dövrlərdə Adobe Acrobat Reader-da ciddi bir zəiflik aşkar edilib. Bu zəiflik CVE-2024-41896 kodu ilə tanınır və “use after free” adlanır. Kibercinayətkar bu boşluqdan istifadə edərək, məsafədən daxil olaraq zərərli kodu hədəf cihazlarda işə sala bilirdi.

Boşluğu kibertəhlükəsizlik mütəxəssisi Haifei Li tapıb. O, EXPMON adlı bir platforma yaradıb, hansı ki bu da yeni sıfır-gün boşluqlarını aşkar etməyə kömək edir. Bu platforma, müxtəlif faylların yüklənməsi zamanı boşluqları aşkarlayan bir platformadır. Mütəxəssis qeyd edir ki, artıq bu zəiflikdən istifadə etməyə başlanılıb, lakin hələlik bu zərərli PDF faylları yalnız hədəf cihazları sıradan çıxarmaq məqsədilə istifadə olunur. Bu da özlüyündə, boşluğun hələ tam geniş miqyas almadığını göstərir.

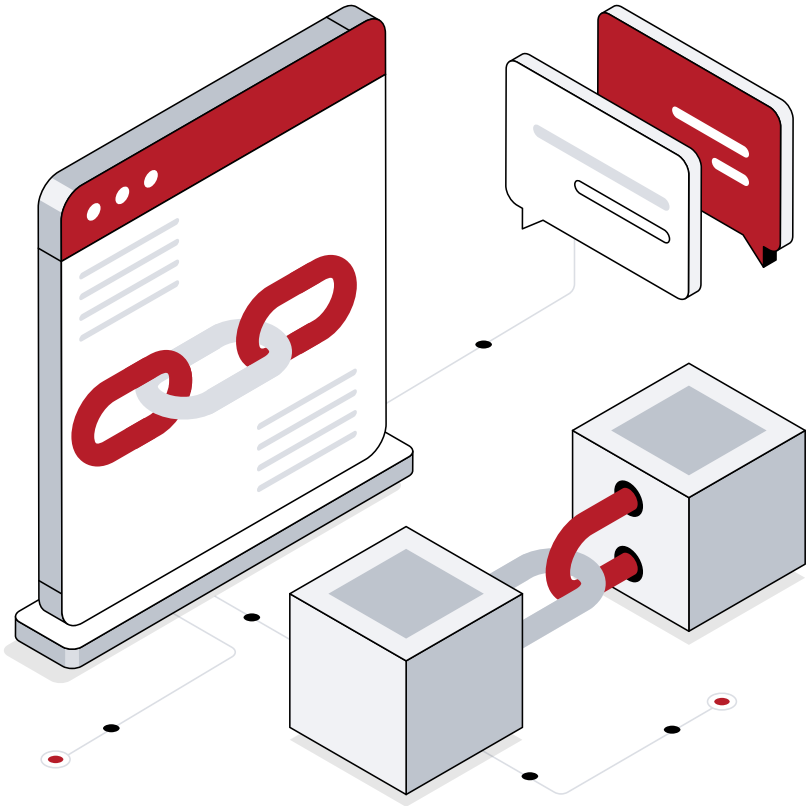
Boşluğun təsirləri

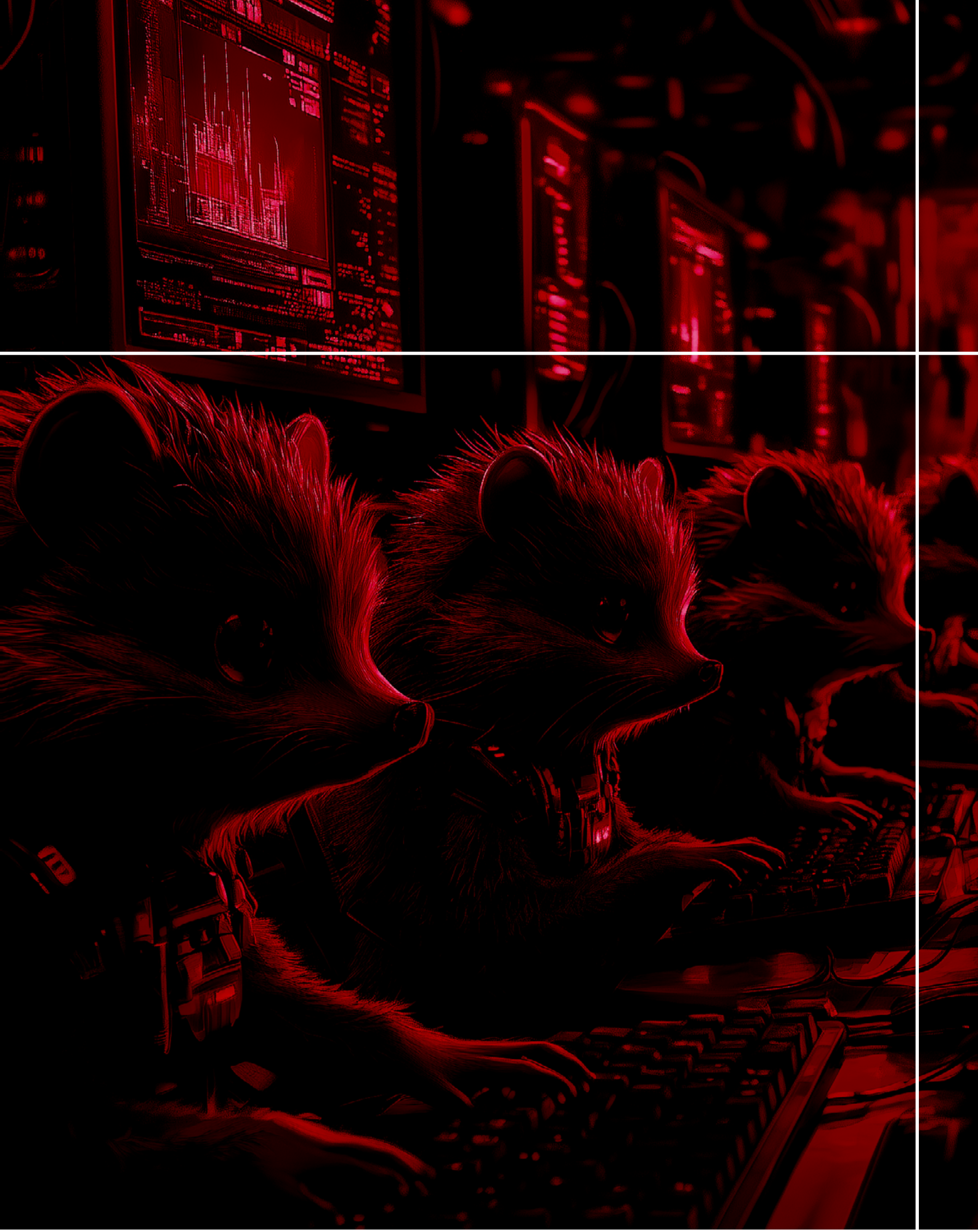
Bu boşluqdan istifadə edən kibercinayətkarlar, hədəf cihazları sıradan çıxara bilərlər, bu da istifadəçilərin məlumatlarına və sistemlərinə zərər verə bilər. Belə ki, kibercinayətkarlar bu boşluqdan istifadə edərək, sistemə daha ciddi təsir göstərə bilən zərərli proqramlar yerləşdirə bilərlər.

Adobe bu boşluğu aradan qaldırmaq üçün təhlükəsizlik yeniləmələri yayımlayıb. Şirkət bütün istifadəçilərə proqramlarını mütləq yeniləməli olduqlarını bildirib. Yeniləmələr, boşluqların aradan qaldırılmasına və potensial hücumların qarşısını almağa kömək edir.

Mənbələr

- www.truesec.com/hub/blog/akira-ransomware-and-exploitation-of-cisco-anyconnect-vulnerability-cve-2020-3259
- www.securityhq.com/blog/critical-zero-day-vulnerability-in-zoom/
- www.techtarget.com/searchsecurity/tip/Microsoft-Teams-phishing-attacks-and-how-to-prevent-them
- www.techradar.com/news/google-docs-is-being-weaponized-by-hackers
- www.adaptive-shield.com/academy/saas-attack-surface/
- www.securityweek.com/microsoft-warns-of-exploited-exchange-server-zero-day/
- www.techradar.com/pro/security/adobe-acrobat-reader-has-a-serious-security-flaw-so-patch-now





Kapital Bank