CIRT.ME

04/2024

SAJBER BILTEN

TOP VIJESTI

CrowdStrike ažuriranje izazvalo probleme širom svijeta

361 milion e-mailova i lozinki na prodaju na Telegramu

Nova prijetnja za Android: Malver koji krade OTP kodove iz SMS poruka

CrowdStrike ažuriranje izazvalo probleme u kritičnoj infrastrukturi širom svijeta

Nedavno su hiljade Windows računara širom svijeta, uključujući banke, avio-kompanije, TV stanice i supermarkete, pogođene problemom zbog ažuriranja softvera CrowdStrike Falcon. Ova greška uzrokuje čuveni Plavi ekran smrti (Blue Screen Of Death) čime se računarima i sistemima onemogućava rad.

CrowdStrike je objavio instrukcije i preporučeno rješenje za oporavak:

- Pokrenuti Windows u sigurnom režimu ili Windows Recovery Environment.
- Ukucati putanju do direktorijuma C:\Windows\System32\drivers\CrowdStrike.
- Pronaći i obrisati datoteku "C-00000291*.sys".
- Ponovo pokrenuti računar u normalnom režimu.

Hakovani domeni korisnika Squarespace-a

SQUARESPACE

Nepoznati napadači kompromitovali su više domena registrovanih kod Squarespace-a. Napadači su iskoristili ranjivosti u procesu migracije, stekli neovlašćen pristup Squarespace nalozima i preuzeli kontrolu nad DNS zapisima. Ovo im je omogućilo preusmjeravanje saobraćaja i presrijetanje elektronske pošte.
Preporuke za korisnike:

- Omogućite dvofaktorsku autentifikaciju (2FA).
- Uklonite nepotrebne naloge.
- Onemogućite pristup preprodavaca na Google Workspace.
- Provjerite i ispravite DNS zapise.
- Izbrišite nepotrebne administratore.
- Razmotrite prebacivanje domena.

Indikatori kompromitacije:

- IP adresa: 185[.]196[.]9[.]29
- MX zapisi: mx[.]zoho[.]eu, mx2[.]zoho[.]eu, mx3[.]zoho[.]eu

Microsoft ponovo doživio pad: Globalni problemi u pristupu ključnih servisa

NMicrosoft se suočava sa značajnim izazovima jer su njihovi ključni servisi, Azure i Microsoft 365, pretrpjeli ozbiljan prekid rada.
Microsoft je izjavio da radi na što bržem rješavanju situacije i da će pružiti dodatne informacije čim budu dostupne.

Ukoliko imate problema sa povezivanjem na Azure usluge, preporučujemo:

- Pratite zvaničnu Azure stranicu za najnovija ažuriranja o prekidu.
- Redovno provjeravajte Microsoft Azure internet stranicu i društvene mreže.
- Ako i dalje imate probleme kontaktirajte Microsoft podršku za pomoć.

361 milion e-mailova i lozinki na prodaju na Telegramu

Set podataka veličine 122 GB koji sadrži 2 milijarde redova podataka raspoređenih u 1.700 fajlova, nudi se za samo 500 dolara putem ekskluzivnog Telegram kanala.
Ovaj malver koristi napredne tehnike za ekstrakciju osetljivih podataka uključujući keylogging, sakupljanje podataka iz memorije, pa čak i zaobilaženje autentifikacije u nekim slučajevima.

Među kompromitovanim nalozima su:

- Gmail
- Amazon
- Facebook
- Spotify
- Netflix
- PayPal
- Instagram
- Twitter
- LastPass
- Adobe
- Twitch
- Coinbase

Stručnjaci za sajber bezbjednost preporučuju hitne mjere:

- Promijenite lozinke za sve online naloge.
- Omogućite dvofaktorsku autentifikaciju.
- Koristite jedinstvene, snažne lozinke.
- Pažljivo pratite naloge kako bi spriječili neovlašćeni pristup i detektovali sumnjive aktivnosti.
- Budite oprezni prema potencijalnim fišing napadima.

Nova prijetnja za Android: Malver koji krade OTP kodove iz SMS poruka

Zimperium upozorava na malver koji inficira Android uređaje i krade OTP kodove za više od 600 servisa a do sad je otkriven u 113 zemalja.
Malver se širi putem lažnih oglasa ili preko Telegram botova koji komuniciraju sa žrtvama.
Žrtve se preusmjeravaju na stranice koje izgledaju kao Google Play prodavnica a potom instaliraju aplikaciju koja traži dozvolu za čitanje SMS poruka, što omogućava malveru da pristupi osjetljivim informacijama.
Malver šalje preuzete SMS poruke na „fastsms.su“, sajt koji nudi virtuelne brojeve za anonimizaciju i autentifikaciju.
Preuzimajte aplikacije samo sa Google Play prodavnice, budite oprezni sa dozvolama i provjerite da li je Play Protect uključen na pametnom uređaju.

Ažuriranja za Windows Server dovode do prekida u Remote Desktop vezama

Microsoft je potvrdio da sigurnosna ažuriranja koja su objavljena u julu uzrokuju prekide u Remote Desktop vezama u organizacijama gdje se koristi zastarjeli protokol. Ovaj problem se može javljati svakih 30 minuta pri čemu se gube sesije prijavljivanja i korisnici će morati ponovo da se povežu sa serverom. Administratori mogu pratiti ovo kao problem sa završetkom rada TSGateway servisa, što se dokumentuje kao događaj 1000 u sistemskom logu.

Privremena rješenja

Prvo rješenje zahtijeva zabranu konekcija preko pipe i porta \pipe\RpcProxy\3388 kroz RD Gateway.

Drugo rješenje zahtijeva izmjenu registarskog ključa RDGClientTransport pod Terminal Server Client odlaskom na HKCU\Software\Microsoft\Terminal Server Client\RDGClientTransport korišćenjem Windows Registry Editor-a. Zatim, pronađite 'DWORD' registarski ključ i postavite polje 'Value Data' na '0x0'.
Napravite rezervnu kopiju registra prije nego što uredite ovaj ključ kako biste osigurali jednostavan način za vraćanje u slučaju problema.

Sharepoint

Napad je tekao prema sledećem obrascu:

- Kampanja je počela fišing e-mailom sa linkom.
- Link je upućivao korisnike na PDF fajl smješten na SharePoint-u, koji je sadržao još jedan link.
- Nakon što su kliknuli na link, korisnici su bili upitani da riješe CAPTCHA.
- Na kraju, korisnici su preusmjereni na lažnu Microsoft login stranicu, gdje je zahtijevan unos korisničkog imena i lozinke.

Strela Stealer Distribuiran putem WebDAV-a

- Kampanja je počela BAT fajlom koji je pokrenuo PowerShell skriptu, aktivirajući net i rundll32 procese.
- Strela stealer je koristio net.exe da montira komandu i kontrolni (C2) server koji je sadržao 'davwwwroot' folder i prikupio 64-bit DLL fajl sa njega koristeći WebDAV.
- Otprilike hiljadu DLL fajlova sa Strela stealer-om pronađeno je na hxxp://45[.]9.74[.]32[:]8888.
- Tokom izvršenja, malver je koristio WordPad. C2 serveri za Strela su bili locirani na istoj lokaciji kao i payload.

DeerStealer Malver maskiran kao Google Authenticator

- Lanac infekcije je počeo sa lažnom internet stranicom, kopijom Google Authenticator-a.
- Nakon klika na “Download”, preuzeta bi bila lažna Google Authenticator datoteka sa Github-a. Datoteka je potpisana od strane Reedcode Ltd Certifikata sa serijskim brojem [5459 67FF 5732 8859 C677 4F85 3F6B 7F18].
- Kada se izvrši na sistemu, stealer započinje eksfiltraciju ukradenih podataka.

Eksfiltracija se vrši putem HTTP POST zahtjeva koji prenose PKZIP arhive koje sadrže ukradene korisničke podatke XOR-ovane sa ključem 0x0c. Ukradeni logovi se šalju na Telegram chat kreiran od strane naloga sa korisničkim imenom "fedor_emeliyanenko_bog." DeerStealer koristi enkripciju za API funkcijske nazive, obavlja API pozive kroz obavijanje i obfuskaciju svog koda.

Sigurnosni propust u VMware ESXi

Nedavno ispravljena sigurnosna greška koja utiče na VMware ESXi hipervizore aktivno je korišćena od strane ransomver grupa za instaliranje malvera za enkripciju fajlova.

Preporučene mjere za zaštitu:

- Instalirajte najnovije zakrpe za VMware ESXi
- Provjerite konfiguraciju vaših ESXi hostova i uvjerite se da se ne koriste AD grupe.
- Ažurirajte sigurnosne protokole uključujući 2FA i redovno praćenje bezbjednosnih događaja.

regreSSHion: Ranjivost daljinskog izvršavanja koda u OpenSSH serveru

Ova ranjivost može dovesti do kompromitacije gdje napadač može izvršavati proizvoljni kod, što rezultira potpunim preuzimanjem sistema, instalacijom malvera, manipulacijom podacima i kreiranjem backdoor-a za trajni pristup.

Preporučene mjere za zaštitu:

- Ažurirajte zakrpe za OpenSSH i dajte prioritet kontinuiranim procesima ažuriranja.
- Ograničite SSH pristup kroz mrežne kontrole kako biste minimizirali rizike napada.
- Podijelite mreže kako biste ograničili neovlašćeni pristup i pokrete unutar kritičnih okruženja i implementirajte sisteme za praćenje i upozoravanje na neobične aktivnosti koje ukazuju na pokušaje eksploatacije.

Ranjivost u Microsoft Office obrascima iskorišćena za fišing napade

Obrasci su dizajnirani da izgledaju legitimno, uz Microsoftove brendove i logotipe. Napadači su takođe koristili tehniku poznatu kao "OAuth phishing" kako bi dobili pristup korisničkom nalogu.

Preporučene mjere za zaštitu:

- Budite oprezni sa elektronskom poštom u kojoj se zahtijeva unos podataka poput korisničkog imena, lozinke i slično.
- Nikada ne unosite podatke na stranici koje ne posjeduju SSL sertifikat.
- Koristite dvofaktorsku autentifikaciju i redovno ažurirajte softver i operativni sistem.

CIRT (eng. Computer Incident Response Team) je u skladu sa Zakonom o tajnosti podataka i Zakonom o informacionoj bezbjednosti zadužen za odgovor na računarsko bezbjednosne incidente u sajber prostoru Crne Gore.

Osnovan je 2012. godine kao dio zajedničkog projekta Vlade Crne Gore i Međunarodne telekomunikacione unije (ITU).

Od svog početka do danas uspješno je riješio ili pomogao rješavanju velikog broja računarskih incidenata koji su imali nacionalni ili međunarodni karakter.