SAJBER BILTEN

CIRT.ME

01/2024

Top vijesti

Lucifer bot mreža cilja Apache servere

Novi malware STRELASTEALER krade e-mail kredencijale

Hakovan „AnyDesk“

Proizvođač softvera za udaljeni pristup AnyDesk je otkrio da je pretrpio sajber napad koji je doveo do kompromitovanja proizvodnih sistema.

Njemačka kompanija je saopštila da incident, koji je otkrila nakon bezbjednosne revizije, nije napad ransomvera i da je obavijestila nadležne organe.

Europol upozorava: onlajn prodavnice zaražene tzv. kradljivcima kreditnih kartica

LUCIFER BOT MREŽA CILJA APACHE SERVERE

Detektovan je povratak Lucifer bot mreže, sa primjetnim preusmjerenjem ka Apache Hadoop i Apache Druid tehnologijama.

Ovaj sofisticirani zlonamjerni softver kombinuje kripto rudarenje i DDoS napade. Preko 3,000 napada identifikovano je u posljednjem mjesecu, naglašavajući hitnost u rješavanju ranjivosti i zaštiti Apache servera. Napadači koriste poznate ranjivosti u Apache platformama kao što su Hadoop i Druid. Važno je proaktivno upravljati zakrpama i koristiti rješenja za detekciju i odgovor u stvarnom vremenu kako biste spriječili potencijalne napade.

Preporučujemo sprovođenje revizija konfiguracija Apache servera, ažuriranje zakrpi i korišćenje bezbjednosnih mjera kako biste spriječili potencijalne napade. Povećana svijest i upotreba open-source biblioteka su ključne zaštite protiv zlonamjernih napada kao što su Lucifer bot mreže.

EUROPOL UPOZORAVA: ONLAJN PRODAVNICE ZARAŽENE TZV. KRADLJIVCIMA KREDITNIH KARTICA

Europol je obavijestio preko 400 web sajtova da su njihove onlajn prodavnice hakovane zlonamjernim skriptama koje kradu podatke sa debitne i kreditne kartice od kupaca.

Skimeri su mali isječci JavaScript koda koji se dodaju na stranice za plaćanje ili se učitavaju sa udaljenog resursa da bi se izbjeglo otkrivanje. Oni su dizajnirani da presretnu i ukradu brojeve platnih kartica, datume isteka, verifikacione brojeve, imena i adrese za isporuku, a zatim otpreme informacije na servere napadača.

Ovi napadi mogu ostati neotkriveni nedjeljama ili čak mjesecima, a u zavisnosti od popularnosti probijenih platformi za e-trgovinu. Ova akcija dolazi u kritičnom trenutku kada aktivnost onlajn kupovine raste tokom praznične sezone.

Korišćenje digitalnih metoda plaćanja ili jednokratnih privatnih kartica može pomoći da se minimizira vjerovatnoća krađe podataka o platnoj kartici.

KAKO ZAŠTITITI GOOGLE NALOG OD HAKERA?

CloudSEK, kompanija za sajber bezbjednost, otkrila je bezbjednosni propust preko kojeg hakeri mogu da uđu u Google naloge.

Hakerski softver koristi kolačiće da bi omogućio pristup privatnim informacijama. Hakeri su pronašli način da dođu do kolačića, zaobilazeći dvofaktorsku autentifikaciju i prijavljivanje na korisničke naloge bez lozinki.
Korisnicima se savjetuje da preduzmu bezbjednosne korake kako bi uklonili potencijalni malver:

- Idite na Google nalog i odaberite „Bezbjednost".
- Kliknite na „Poboljšano bezbjedno pregledavanje za vaš nalog" .
- Odaberite „Upravljajte poboljšanim bezbjednim pregledavanjem".
- Uključite ili isključite „Poboljšano bezbjedno pregledanje."

PROCURILO VIŠE OD 70 MILIONA KORISNIČKIH NALOGA - PROVJERITE DA LI STE NA LISTI

Stručnjak za bezbjednost Troy Hunt otkrio je masovni napad u kojem je došlo do curenja korisničkih podataka a među zahvaćenim platformama su Facebook, Roblox, eBay i Yahoo.

Podaci postoje već četiri mjeseca na crnom tržištu koje se bavi trgovinom ukradenih kredencijala.

Napad *credentials stuffing* se odnosi na metodu u kojoj napadač koristi procurele korisničke podatke sa jedne platforme i pokušava da se uloguje ili pristupi drugim platformama koristeći te iste podatke. Ovo naglašava potrebu da korisnici koriste jače i jedinstvene lozinke kako bi smanjili potencijalne posljedice.
Provjerite da li ste pogođeni curenjem podataka:

- Posjetite web stranicu https://haveibeenpwned.com/
- Unesite email adresu u polje za pretragu i kliknite na "Pwned?"
- Stranica će prikazati rezultate pretrage i obavijestiti vas da li se vaša email adresa nalazi u bazi kompromitovanih adresa.

Novi malware STRELASTEALER krade email kredencijale

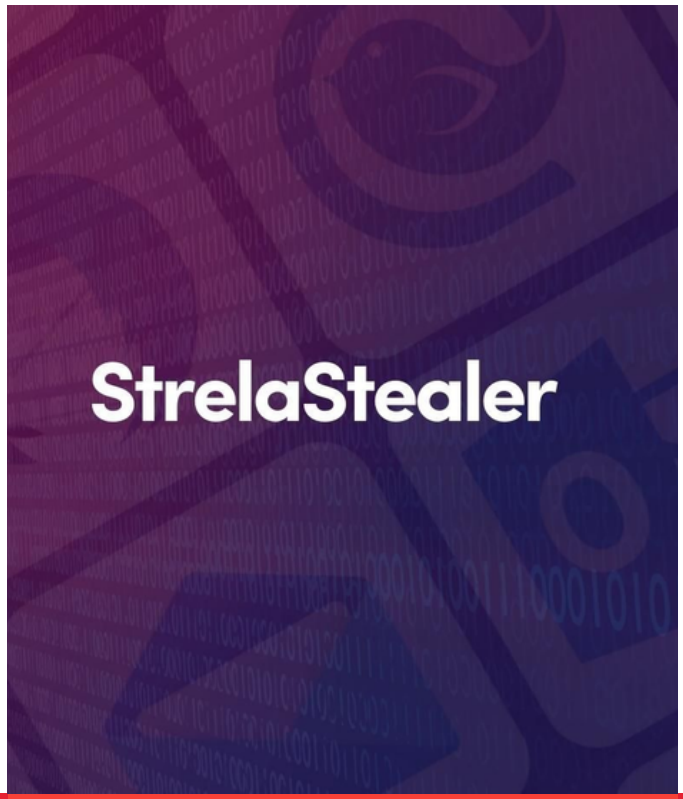
Nedavno otkriveni malver nazvan StrelaStealer postao je ozbiljna prijetnja za organizacije širom svijeta. Ovaj maliciozni softver, koji cilja poznate email klijente, izaziva ozbiljne bezbjednosne probleme kroz krađu log-in informacija za email naloge.

StrelaStealer je malware koji krade podatke za prijavljivanje na email naloge i šalje ih nazad na server napadača.

Kada je napad uspješno izvršen, napadač dobija pristup informacijama za prijavljivanje na email, koje zatim može koristiti za dalje napade.

Možete poboljšati zaštitu od zlonamjernog softvera kao što je Lumma Stealer slijedeći savjete:

- Izbjegavajte sumnjive internet stranice. Da biste provjerili je li web lokacija pouzdana, razmislite o korišćenju GridinSoft besplatnog online servisa za provjeru virusa.
- Budite oprezni sa linkovima, posebno u elektronskoj pošti, porukama na društvenim mrežama ili internet stranicama. Sajber kriminalci se često oslanjaju na ljudsku radoznalost za širenje zlonamjernog softvera.
- Koristite pouzdan anti-malver program i osigurajte da je uvijek ažuran.



Fišing napadi preko „Booking-a“

Kad je u pitanju sajt „Booking”, prevaranti obično putem elektronske pošte šalju zahtjev da se potvrdi rezervacija smještaja, ili da se, na primjer, uplati neka suma, iako je korisnik rezervisao apartman koji će platiti na licu mjesta.

Stručnjaci savjetuju građanima da obrate posebnu pažnju prilikom otvaranja SMS poruka i elektronske pošte od nepoznatih pošiljalaca kako bi se zaštitili od fišinga. To znači da provjere URL adresu internet stranice prije nego što unesu svoje podatke i provjere vjerodostojnosti izvora. Takođe, potrebno je da koriste različite lozinke za različite račune i da ih redovno ažuriraju.

Fišing kampanje koje ciljaju korisnike Viber-a

Ukoliko dođe do kompromitacije da biste deaktivirali pristup vašem Viber nalogu na drugim uređajima potrebno je da preduzmete sledeće aktivnosti:

- Otvorite Viber aplikaciju na svom mobilnom uređaju i izaberite opciju „Još” („More”)
- Izaberite opciju „Podešavanja” („Settings”) i stavku „Nalog” („Account”)
- Izaberite „Desktop i tablet” („Desktop and Tablets”) i provjerite koji sve uređaji imaju pristup vašem nalogu
- Ukoliko se na listi nalazi uređaj koji niste vi dodali deaktivirajte ga

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.