ყოველკვირეული დაიჯესტი კიბერუსაფრთხოებასა და ინფორმაციულ ტექნოლოგიებში

26 აგვისტო - 9 სექტემბერი, 2023

CRC კიბერმედეგობის ცენტრი
CYBER RESILIENCE CENTER

პრორუსულმა ჰაქტივისტურმა ჯგუფმა, “NoName057(16)”, მიზანში პოლონეთის ფინანსური სექტორი და სამთავრობო ვებგვერდები ამოიღო

პრორუსულმა ჰაქტივისტურმა ჯგუფმა, “NoName057(16)”, დაიწყო მიზანმიმართული კამპანია პოლონეთის ფინანსური სექტორისა და სამთავრობო ვებსაიტების წინააღმდეგ. 28 აგვისტოს, დილის 10 საათზე, დაჯგუფებამ თავდასხმის შესახებ წინასწარ გამოაქვეყნა შეტყობინება დაშიფრული Telegram-ის არხზე, სადაც ნათქვამია, რომ ის განახორციელებდა DDoS ტიპის შეტევებს პოლონეთში არსებულ კრიტიკულ სექტორებზე. თავდასხმები თავდაპირველად დაიწყო ვარშავის საფონდო ბირჟაზე და შემდგომ გაფართოვდა პოლონეთის მთავარ კომერციულ ბანკებზე, რომელთა შორისაა - Bank Pekao, Raiffeisen Bank, Plus Bank, Credit Agricole Bank და BNP Paribas.

29.08.23

Topgolf Callaway Brands-ის გატეხვის შედეგად მილიონზე მეტი პირი დაზარალდა

ცნობილი ამერიკული სპორტული აღჭურვილობის მწარმოებელი კომპანიის, “Topgolf Callaway Brands”-ის თანახმად, 2023 წლის 1 აგვისტოს, თავიანთ სერვერზე სისტემური კიბერშეტევა დაფიქსირდა. მომხმარებლის პროფილები, მათ შორის - სახელები, მისამართები, ელ. ფოსტა, ტელეფონის ნომრები, შეკვეთების ისტორია, ანგარიშის პაროლები და სხვა სენსიტიური ინფორმაცია გასაჯაროვდა. მოგვიანებით, როგორც ცნობილი გახდა, ჯამში 1 114 954 პირის პირადი ინფორმაცია დაიჰაკა. კომპანია დაზარალებულ მომხმარებლებს პაროლების შეცვლისკენ მოუწოდებს.

30.08.23

ყირგიზეთის ხელისუფლებამ ბავშვთა ფსიქიკური ჯანმრთელობის დასაცავად TikTok-ის გამოყენება აკრძალა

ყირგიზეთი უერთდება იმ ქვეყნების გრძელ სიას, რომლებმაც აკრძალეს ჩინეთის საკუთრებაში არსებული აპლიკაცია “TikTok” და მიზეზად ახალგაზრდა თაობის მენტალური ჯანმრთელობის დაცვას ასახელებს. გადაწყვეტილება კულტურის,

ინფორმაციის, სპორტისა და ახალგაზრდობის სამინისტრომ 30 აგვისტოს გააჟღერა. აქვე, აღსანიშნავია, რომ შეერთებულ შტატებში, ავსტრიაში, ავსტრალიაში, ბელგიაში, კანადაში, ახალ ზელანდიაში, ნორვეგიაში, საფრანგეთსა და დიდ ბრიტანეთში “TikTok”-ზე წვდომა შეზღუდული აქვთ საჯარო სამსახურში მომუშავე პირებს ეროვნული უსაფრთხოებისი მიზეზის გამო, ვინაიდან არსებობს საფრთხე, რომ აპლიკაცია შესაძლოა ჩინეთის ხელისუფლებას მომხმარებელთა მონაცემებს უზიარებდეს.

30.08.23

NSC-ის უნებლიე შეცდომა და 10 000-ზე მეტი დაზარალებული მომხარებელი

ეროვნული უსაფრთხოების საბჭომ (NSC), აშშ-ის არაკომერციულმა ორგანიზაციამ, უნებლიედ თავისი წევრების 10 000 ელ.ფოსტის მისამართი და პაროლი გამოაქვეყნა. დაზარალებულთა შორის აღმოჩნდა დაახლოებით 2 000 კომპანიისა და სამთავრობო უწყების თანამშრომელი. დაზარალებულ ორგანიზაციებს შორის არიან ისეთი მსხვილი კორპორაციები, როგორიცაა: Shell, BP, Exxon და Boeing, ასევე სამთავრობო უწყებები - იუსტიციის დეპარტამენტი (DoJ), FBI და NASA. ხარვეზი, რომელიც აღმოჩენილი იქნა Cybernews-ის კვლევითი ჯგუფის მიერ, საფრთხეს უქმნის არა მხოლოდ NSC-ის სისტემებს, არამედ იმ კომპანიებს, რომლებიც იყენებენ NSC სერვისებს, ვინაიდან გაჟონილი რწმუნებათა სიგელები შესაძლოა გამოყენებული ყოფილიყო კიბერთავდასხმებისთვის.

31.08.23

AI რუსეთის ჯაშუშები უკრაინაში Android მოწყობილობებზე თავდასხმისთვის ახალ მავნე პროგრამას იყენებენ

31 აგვისტოს, დიდი ბრიტანეთის ეროვნული კიბერუსაფრთხოების ცენტრმა (NCSC) და სხვა საერთაშორისო პარტნიორებმა უკრაინის უსაფრთხოების სააგენტოს მიერ აღმოჩენილი და აღწერილი მავნე კამპანიის ტექნიკური დეტალების შესახებ ანგარიში გამოაქვეყნეს. რეპორტი განიხილავს Android მოწყობილობებზე მომუშავე მავნე პროგრამის კამპანიას სახელწოდებით "Infamous Chisel" და მის კავშირს რუსეთის სამხედრო დაზვერვის სამსახურთან - GRU, რომელიც სამიზნედ უკრაინელი

სამხედროების მიერ გამოყენებად მოწყობილობებს იღებს. მავნე პროგრამა, რომელიც დაკავშირებულია “Sandworm”-ის საფრთხის აქტორთან, თავდამსხმელს საშუალებას აძლევას, არაავტორიზებული წვდომა მოიპოვოს კომპრომეტირებულ მოწყობილობებზე, რაც ავტომატურად უზრუნველყოფს მონაცემთა ქურდობას და ქსელის მონიტორინგს, შესაბამისად, კამპანია საფრთხეს უქმნის უკრაინის სამხედრო ინფორმაციის გავრცელებას.

31.08.23

ჩრდილოეთ კორეული დაჯგუფება “Lazarus Group” მავნე “VMConnect” კამპანიის სათავეში

“ReversingLabs”-ის ცნობით, “Lazarus Group”, ცნობილი როგორც ჩრდილოეთ კორეის აქტიური კიბერკრიმინალური დაჯგუფება, ამჯერად მიზნად “MacOS”, “Linux” და “Windows” სისტემებს იღებს. კამპანია, რომელიც ცნობილია როგორც “VMConnect”, მოიცავდა Python-ის მავნე პაკეტების გამოყენებას, რომლებიც განთავსებული იყო “PyPI” პროგრამული უზრუნველყოფის საცავში. “ReversingLabs”-ის მკვლევარებმა სწორედ რამდენიმე ათეული მსგავსი შემთხვევის აღმოჩენის შემდეგ შეძლეს კვალის Lazarus Group-ის Labyrinth Chollima ქვეჯგუფთან დაკავშირება. ეს ყოველივე ხაზს უსვამს პროგრამული უზრუნველყოფის მიწოდების ჯაჭვის შეტევების მუდმივ საფრთხეს და კიბერუსაფრთხოების გაუმჯობესებული ზომების საჭიროებას.

01.09.23

კიბერშეტევა, რომელმაც მსოფლიოს მოწინავე ასტრონომიული ობსერვატორიების მუშაობა შეაჩერა

მსოფლიოს ორი ყველაზე მოწინავე ასტრონომიული ობსერვატორია, “Gemini North” ტელესკოპი ჰავაიში და “Gemini South” ტელესკოპი ჩილეში, იძულებული გახდა შეეჩერებინა ფუნქციონირება კიბერშეტევის გამო, რომელიც 1 აგვისტოს, დღის პირველ ნახევარში, იქნა იდენტიფიცირებული. აშშ-ის ნაციონალური ოპტიკურ-ინფრაწითელი ასტრონომიის კვლევითი ლაბორატორიის (NSF's NOIRLab) თანახმად, კიბერშეტევამ ასტრონომიული დაკვირვებების შეჩერება და კომპიუტერული სისტემების გათიშვა

გამოიწვია. თავდასხმა ასევე შეეხო მცირე ტელესკოპებს და გადადო სამეცნიერო კვლევა. “NOIRLab” აქტიურად იძიებს ინციდენტს კიბერექსპერტების დახმარებით.

01.09.23

დიდი ბრიტანეთის საარჩევნო კომისია ჩატარებული აუდიტის შედეგად კიბერუსაფრთხოების ტესტს ვერ აბარებს

გაერთიანებული სამეფოს საარჩევნო კომისიამ, რომელმაც აქამდე არსებული მონაცემთა დარღვევის შედეგად დაახლოებით 40 მილიონი ამომრჩევლის პერსონალური დეტალები გამოაშკარავა, კიბერუსაფრთხოების ძირითადი ტესტი, ცნობილი როგორც “Cyber Essentials” აუდიტი, ვერ გაიარა. თუმცა კომისია ირწმუნება, რომ აუდიტის ჩავარდნა არ არის დაკავშირებული კიბერშეტევასთან. კიბერუსაფრთხოების ექსპერტები შეშფოთებულნი არიან დარღვევით და წარუმატებლობით.

05.09.23

ამერიკა iMessage სმიშინგით კიბერკრიმინალური კამპანიის მსხვერპლი ხდება

ფართომასშტაბიანი “Smishing” (SMS ფიშინგის) კამპანია სამიზნედ ამჯერად აშშ-ს იღებს. კიბერდანაშაულებრივი ჯგუფი, ცნობილი როგორც "Smishing Triad", ახორციელებს პირადობის ქურდობასა და ფინანსურ თაღლითობას შემდეგი მეთოდის გამოყენებით: Apple iCloud-ის გატეხილი ანგარიშების გამოყენებით, ისინი iMessages-ის საშუალებით აგზავნიან ტექსტურ შეტყობინებებს პოტენციურ მსხვერპლებთან და თავს ასაღებენ პოპულარულ საფოსტო და/ან მიტანის სერვისებად. საბოლოოდ კი, ისინი მომხმარებლებს უგზავნიან ყალბი პაკეტის მიწოდების წარუმატებლობის შეტყობინებებს ბმულების სახით, რათა საკრედიტო ბარათის ინფორმაცია შეაგროვონ.

05.09.23

ჩრდილოეთ კორეული დაჯგუფება “Lazarus” ვირტუალური ფსონების საიტიდან 41 მილიონ დოლარს იპარავს

FBI-ის ინფორმაციით, “Lazarus”-მა, ჩრდილოეთ კორეის ერთ-ერთმა კიბერკრიმინალურმა დაჯგუფებამ, წარმატებით მოიპარა 41 მილიონი დოლარი კრიპტოვალუტაში, ეთერიუმის

ჩათვლით. კიბერქურდობა 4 სექტემბერს მოხდა, ხოლო FBI-იმ დანაშაული 6 სექტემბერს დაადასტურა. მიუხედავად იმისა, რომ FBI-იმ კიბერშეტევა “Lazarus” დაჯგუფებას არ მიაწერა, მან ხაზგასმით აღნიშნა ჩრდილოეთ კორეის მონაწილეობა რამდენიმე გახმაურებულ ვირტუალური ვალუტის ძარცვის დანაშაულში. მხოლოდ ამ წელს ჩრდილოეთ კორეასთან დაკავშირებულმა კიბერ კრიმინალებმა 200 მილიონ დოლარზე მეტი ვირტუალური ფონდი მოიპარეს.

06.09.23