ყოველკვირეული დაიჯესტი კიბერუსაფრთხოებასა და ინფორმაციულ ტექნოლოგიებში

1-13 აგვისტო, 2023

CRC კიბერმედეგობის ცენტრი
CYBER RESILIENCE CENTER

პრორუსულად განწყობილი ჰაკერების ჯგუფი კიბერშეტევის სამიზნედ ამჯერად იტალიურ ბანკებს იღებს

პირველ აგვისტოს, იტალიის კიბერუსაფრთხოების ეროვნულმა სააგენტომ, განაცხადა, რომ რამდენიმე მსხვილ იტალიურ ბანკზე მიზანმიმართული ჰაკერული თავდასხმა განხორციელდა. პრორუსულად განწყობილმა ჰაკერულმა ჯგუფმა "NoName057(16)" დაიწყო DDoS ტიპის თავდასხმები იტალიის სულ მცირე ხუთ ბანკზე, რომელთა შორის არიან - Intesa Sanpaolo, Monte dei Paschi di Siena, BPER Banca, FinecoBank და Banca Popolare di Sondrio. თავდასხმებმა დროებით შეაფერხა ბანკების ვებსაიტები, რის შედეგადად მომხმარებლებს საბანკო სერვისებზე წვდომა შეეზღუდათ. ACN-მა, იტალიის კიბერუსაფრთხოების ეროვნულმა სააგენტომ, "NoName057(16)" დამნაშავედ ცნო და აღნიშნა, რომ კონკრეტული დაჯგუფება ხშირადაა შემჩნეული უკრაინასთან მოკავშირე ევროპული ქვეყნების ფინანსურ ინსტიტუტებსა და ინფრასტრუქტურაზე თავდასხმებში.

01.08.2023

ჩინეთი აძლიერებს რეგულაციებს AI ტექნოლოგიების მიმართ

პირველ აგვისტოს, ჩინეთმა გაავრცელა ინფორმაცია სამომავლო აკრძალვებისა და რეგულაციების შესახებ, რომელებიც კონკრეტულად AI ტექნოლოგიებსა და მოდელებს შეეხება. ჩინეთმა აკრძალა ChatGPT-ის გამოყენება და შეაფერხა წვდომა მისი გამოყენების ყველა საშუალებაზე. უახლესი ცნობის მიხედვით, ბანის დადების საფრთხე ყველა იმ აპლიკაციასა და პროგრამას ემუქრება, რომელიც რაიმე კავშირში მაინც არის AI ტექნოლოგიასთან. ჩინეთი მსგავს ნაბიჯს ისეთი მიზეზებით ასაბუთებს, როგორებიცაა - მასობრივ უმუშევრობაზე ხელოვნური ინტელექტის პოტენციური გავლენა, ხელოვნური ინტელექტის უარყოფითი გავლენა საზოგადოებაზე და ა.შ. საზოგადოების აზრით, ეს ნაბიჯი შეიძლება დაკავშირებული იყოს ჩინეთსა და აშშ-ის შორის მიმდინარე სავაჭრო ომთან, სადაც ჩინეთი ცდილობს სათანადო კონკურენცია გაუწიოს ამერიკას.

01.08.2023

Microsoft–ის განცხადებით, 40-ზე მეტი გლობალური ორგანიზაცია ფიშინგის მსხვერპლი გახდა

რუსულმა ჰაკერულმა დაჯგუფებამ, ცნობილი, როგორც "Midnight Blizzard" და/ან "APT29", რუსეთის მთავრობასთან თანამშრომლობით, დაიწყო მიზანმიმართული სოციალური ინჟინერიის შეტევა დაახლოებით 40 გლობალურ ორგანიზაციაზე. "Midnight Blizzard" დაფიქსირებულია ბევრ სამთავრობო და არასამთავრობო ორგანიზაციების, IT სერვისების, ტექნოლოგიების, წარმოებისა და მედიის სექტორებზე თავდასხმის არაერთ პრეცენდენტში. თავდამსხმელებმა ამჯერად Microsoft Teams-ის ჩათებში თავი ტექნიკური მხარდაჭერის აგენტებად გაასაღეს, რათა მოეტყუებინათ მომხმარებლები პერსონალური

მონაცემების მოპარვის მიზნით. ჰაკერები ყალბი დომენებისა და ანგარიშების შექმნაში მომხმარებლებს მრავალფაქტორული ავთენტიფიკაციის (MFA) დადასტურებას სთხოვდნენ და მსგავსი მეთოდის მეშვეობით ახორციელებდნენ კიბერ თავდასხმებს.

03.08.2023

აშშ-ის ჯანდაცვის კომპანიაზე, „Synergy“, კიბერშეტევის შედეგად, 58 000 პაციენტის პირადი ჩანაწერი გამოქვეყნდა

„Synergy“-ზე განხორციელებული კიბერშეტევის შედეგად, ათასობით პაციენტის შესახებ ჯანმრთელობის ჩანაწერი და პირადი ინფორმაცია გამჟღავნდა. დარღვევა დეკემბერში დაფიქსირდა, მაგრამ კომპანიამ ინციდენტი მეინის გენერალურ პროკურატურას 31 ივლისს გადასცა. მიუხედავად იმისა, რომ მეინის მხოლოდ ოთხი მცხოვრები დაზარალდა, მსხვერპლთა საერთო რაოდენობამ აშშ-ში 58 000-ს მიაღწია. გამჟღავნებული მონაცემები მოიცავდა სახელებს, დაბადების თარიღებს, დაზღვევის დეტალებს, სოციალური დაცვის ნომრებს, სამედიცინო ისტორიასა და ფინანსურ ინფორმაციას. „Synergy“ დაზარელებულთათვის ერთწლიან უფასო საკრედიტო მონიტორინგს უზრუნველყოფს.

31.07.2023

EY-ის მიმართ განხორციელებულმა კიბერშეტევამ ამერიკის ბანკის 30 000-ზე მეტი მომხმარებელი დააზარალა

Ernst & Young (EY), მსოფლიოში პროფესიონალური სერვისების ერთ-ერთი უმსხვილესი ქსელი, იტყობინება მონაცემთა დარღვევის ინციდენტის შესახებ, რომელმაც ამერიკის ბანკის 30 000-ზე მეტი მომხმარებელი დააზარალა. „Cl0p“ ჯგუფმა საჯაროდ აღიარა, რომ ისინი იდგნენ მონაცემთა გარღვევისა და „MOVEit Transfer“-ის პროგრამული უზრუნველყოფის თავდასხმების უკან, რის შედეგად, კიბერ კრიმინალებმა მიიღეს წვდომა სენსიტიური ინფორმაციის ბაზაზე - ფინანსურ ანგარიშებზე და საკრედიტო ბარათების ნომრებზე. EY-ის განმარტების მიუხედავად იმის შესახებ, რომ მათ შიდა სისტემებზე კონკრეტულ თავდასხმას გავლენა არ მოუხდენია, ინციდენტმა მომხმარებლები ისეთი სენსიტიური ინფორმაციის გასაჯაროებით დააზარალა, როგორიცაა - პერსონალური მონაცემები, მათ შორის სახელები, მისამართები, სოციალური დაცვის ნომრები, სამთავრობო პირადობის მოწმობები და სხვა.

10.08.2023

ანდროიდის პროგრამების მწარმოებელი, „LetMeSpy“, კიბერშეტევის შედეგად წყვეტს ფუნქციონირებას

ანდროიდის ჯაშუშური პროგრამების მწარმოებელი, „LetMeSpy“, წყვეტს მუშაობას მას შემდეგ, რაც ჰაკერებმა სერვერებიდან მომხმარებლის სენსიტიური ინფორმაცია მოიპარეს. მათი განცხადებით, 31 აგვისტოს, ვებსაიტი „letmespy.com“ სამუდამოდ შეწყვეტს ფუნქციონირებას. განხორციელებული კიბერშეტევისას ჰაკერებმა შეაღწიეს კომპანიის სისტემაში და მოიპარეს მომხმარებლის მონაცემები, მათ შორის - ზარების ჟურნალი, SMS შეტყობინებები და ადგილმდებარეობის მონაცემები. ინციდენტის დროს, თავდამსხმელებმა ასევე წაშალეს კომპანიის სერვერები. „LetMeSpy“, რომელიც გათვლილია მშობლებისა და თანამშრომლების კონტროლისთვის, საშუალებას აძლევს მომხმარებლებს თვალყური ადევნონ ტექსტურ შეტყობინებებს, ზარების ჟურნალებსა და მდებარეობებს სამიზნე მოწყობილობებზე. კომპანიის თქმით, თავდასხმის შემდეგ მომხმარებლის ანგარიშებზე წვდომა დაუყოვნებლივ დაიბლოკა და დარჩენილი მონაცემები სექტემბრის ბოლოს წაიშლება.

07.08.2023

ინტერნეტ თაღლითობა, რომელმაც თვითმკვლელობა გამოიწვია

ოკეჩუკვუ ნვოფორს, 32 წლის მამაკაცს ბრუკლინიდან, ექვს წლამდე თავისუფლების აღკვეთა მიესაჯა საქმიანი ელ.ფოსტის თაღლითობით (BEC) მოპოვებული ფულის გათეთრებისთვის. თაღლითობის მეშვეობით, მან მსხვერპლს ერთი მილიონი დოლარი გამოძალა, რამაც დაზარალებული თვითმკვლელობამდე მიიყვანა. ნვოფორი და მისი თანამზრახველები FBI-იმ დააკავა, ხოლო სასამართლომ განაჩენი კი 7 აგვისტოს გამოიტანა.

09.08.2023

ფინეთისა და ნორვეგიის ხელისუფლებამ Yandex-სს მომხმარებელთა პირადი მონაცემების რუსეთისთვის გადაცემა აუკრძალეს

8 აგვისტოს, ფინეთისა და ნორვეგიის მარეგულირებლებმა, განაცხადეს, რომ ისინი უკრძალავენ რუსულ ტექნოლოგიურ ჯგუფებს - Yandex-სა (YNDX.O) და მის ნიდერლანდებში დაფუძნებულ პარტნიორ Ridetech International-ს რუსეთში Yandex-ის სამგზავრო აპლიკაციის გამოყენებით მომხმარებელთა პერსონალური მონაცემების რუსეთისთვის გადაცემა. Yandex-მა განაცხადა, რომ იგი შეესაბამება GDPR-ისა და ევროკავშირის კანონმდებლობას და რუსული რეგულაციები არ ვრცელდება მის საერთაშორისო სამგზავრო ბიზნესზე. აღსანიშნავია ის ფაქტიც, რომ ივნისში, მოსკოვის სასამართლომ, Yandex-სს 2 მილიონი რუბლი (20,810 აშშ დოლარი) დააკისრა იმის გამო, რომ მან განმეორებით უარი თქვა რუსეთის უშიშროების ფედერალური სამსახურისთვის, მომხმარებლთა შესახებ ინფორმაცია მიეწოდებინა.

08.08.2023