საქართველოს თავდაცვის სამინისტრო

სსიპ - კიბერუსაფრთხოების ბიურო

კიბერდაიჯესტი № 1

თბილისი 2019

სარჩევი

გერმანიაში ასობით პოლიტიკოსის პერსონალურ მონაცემთა გაჟონვა მოხდა

კიბერშეტევის შედეგად ასობით გერმანელი პოლიტიკოსის, მათ შორის კანცლერი ანგელა მერკელის პერსონალური მონაცემები და დოკუმენტები ღია ქსელში მოხვდა.

ინციდენტის შედეგად ხელმისაწვდომი გახდა საკრედიტო ბარათების მონაცემები, ტელეფონის ნომრები, მისამართები, პირადი და შიდა პარტიული დოკუმენტები. ამასთანავე, ყველა პარტიის წარმომადგენლის ბუნდესტაგისა და ევროპარლამენტის დეპუტატების ჩატების შინაარსი. აღნიშნულის გარდა გამოქვეყნებული იქნა მთელი რიგი ჟურნალისტებისა და საზოგადო მოღვაწეების პირადი მონაცემები.

გერმანიის მთავრობის წარმომადგენლის განცხადებით, გერმანიის კანცლერის გამოქვეყნებულ დოკუმენტებში კონფიდენციალური და საიდუმლო მასალები არ აღმოჩდა. მისი თქმით გამოძიებას აწარმოებენ ინფორმაციული ტექნოლოგიების სფეროში უსაფრთხოების (BSI), კონსტიტუციის დაცვისა და სისხლის სამართლის საქმეების ფედერალური უწყებები.

გავრცელებული ინფორმაციით, დაკავებულია დანაშაულში ეჭვმიტანილი ქალაქ ესენში მცხოვრები გიმნაზიის 20 წლის სტუდენტი.

Made for minds. ZDNet

4 იანვარი, 2019 წელი

აშშ-მ ქვეყნის ენერგოსისტემაზე განხორციელებულ კიბერშეტევებში ეჭვი რუსეთის ფედერაციაზე მიიტანა

აშშ-ს შიდა უსაფრთხოების სამინისტროს 2016-2017 წლებში ქვეყნის ენერგოსისტემაზე განხორციელებულ მასშტაბურ კიბერშეტევებში ეჭვი რუსულ კიბერკრიმინალურ დაჯგუფებებზე მიიტანა. გამოცემის The Wall Street Journal ინფორმაციით, აღნიშნული მიზნების მისაღწევად ბოროტმოქმედებმა ამერიკის 24 შტატის, დიდი ბრიტანეთისა და კანადის ასობით კონტრაქტორ კომპანიაზე მიიტანეს იერიში. მსხვერპლ კომპანიებს მიეკუთვნებოდა All-Ways Excavating USA, Carlson Testing და Commercial Contractors.

ამერიკის შიდა უსაფრთხოების სამინისტროს კიბერუსაფრთხოების დეპარტამენტის უფროსის განცხადებით, კიბერშეტევების პირველი ნიშნები აღინიშნებოდა 2016 წელს, ხოლო რუსი კიბერდამნაშავეების კვალზე გამოყენებული ინსტრუმენტები, ტაქტიკა და ხელწერა მიუთითებს.

აღნიშნულ ბრალდებას რუსეთის ფედერაციის მაღალჩინოსნები გამუდმებით უარყოფენ. პრეზიდენტების ვლადიმერ პუტინისა და დონალდ ტრამპის შეხვედრაზე, რუსეთის ფედერაციის პრეზიდენტმა კიბერუსაფრთხოების გაერთიანებული ჯგუფის მუშაობის ფარგლებში თანამშრომლობაზე მზადყოფნა გამოთქვა.

SecurityLab.ru by Positive Technologies REUTERS

11 იანვარი, 2019 წელი

პოლონეთმა შესაძლოა Huawei-ს პროდუქციის გამოყენება აკრძალოს

პოლონეთში ჯაშუშობის ბრალდებით Huawei-ს წარმომადგენელის დაკავების შემდეგ ქვეყანამ მოუწოდა ნატოს და ევროკავშირს განიხილონ ამ კომპანიის პროდუქციის ბაზრიდან განდევნის საკითხი. კიბერუსაფრთხოების საკითხების კურატორმა კაროლ ოკონსკიმ განაცხადა, რომ პოლონეთი განიხილავს სახელმწიფო ორგანოების მიერ Huawei-ს პროდუქტების გამოყენების აკრძალვის საკითხს.

ქვეყნის მთავრობამ შესაძლოა გაამკაცროს კანონმდებლობა და შეზღუდოს ნებისმიერი კომპანიის მიერ წარმოებული იმ პროდუქციის ხელმისაწვდომობა, რომელიც საფრთხეს უქმნის ქვეყანის უსაფრთხოებას.

Huawei-ს წარმომადგენლობამ განაცხადა, რომ მათ დაკავებული თანამშრომელი გაათავისუფლეს და მის უკანონო ქმედებებს არანაირი კავშირი არ აქვს კომპანიის საქმიანობასთან.

პოლონეთის შინაგან საქმეთა მინისტრმა მოუწოდა ევროკავშირს და ნატო-ს შეიმუშაონ ერთობლივი პოზიცია კომპანია Huawei-ს ბაზარზე ყოფნასთან დაკავშირებით.

აღსანიშნავია, რომ ჩეხეთმა, ავსტრალიამ, იაპონიამ, ახალმა ზელანდიამ, ბელგიამ, ამერიკის შეერთებულმა შტატებმა და ზოგიერთმა სხვა სახელმწიფომ, უკვე შეზღუდეს ან სრულებით აკრძალეს Huawei- ს ხელმისაწვდომობა მათ ბაზრებზე.

SecurityLab.ru by Positive Technologies sky news

14 იანვარი, 2019 წელი

ბანკომატების ქსელზე დაშვების მოსაპოვებლად Skype-ში განხორციელებული ერთი ზარი გახდა საკმარისი

სკაიპში განხორციელებული ერთი ზარისა და თანამშრომლის მიერ დაშვებული შეცდომის გამოყენებით, ჩრდილოეთ კორეის ჰაკერულმა დაჯგუფებამ მოახერხა კომპანია Redbanc-ის კომპიუტერულ ქსელში შეღწევა. კომპანია ჩილეში მოქმედი ყველა ბანკის ბანკომატების ინფრასტრუქტურის მომსახურეობას უზრუნველყოფს.

თავდასხმა სავარაუდოდ განხორციელდა პრო-სამთავრობო დაჯგუფების Lazarus Group (იგივე Hidden Cobra)-ს მიერ, რომელიც ცნობილია მთელ მსოფლიოში ბანკებზე, ფინანსურ ინსტიტუტებსა და კრიპტოსავალუტო ბირჟებზე თავდასხმებით. კომპანია Redbanc-მა აღიარა კიბერშეტევის ფაქტი, მაგრამ ინციდენტის შესახებ დეტალები არ გაასაჯაროვა.

გამომცემლობა TrendTic-მა ჩაატარა საკუთარი გამოძიება და თავდასხმის დეტალების მოპოვებაც შეძლო. გამოძიების თანახმად თავდასხმა Redbanc-ის ერთ-ერთი თანამშრომლის დახმარებით გახდა შესაძლებელი, იგი გამოეხმაურა LinkedIn-ის დეველოპერის ვაკანსიას, რომელიც სინამდვილეში ჰაკერული დაჯგუფების Lazarus Grop-ის განთავსებული იყო. Skype-თ გასაუბრების დროს აპლიკანტს სთხოვეს PDF ფაილის ჩამოტვირთვა და დაარწმუნეს რომ ეს ფაილი წარმოადგენდა სტანდარტული განაცხადის ფორმას. ინფორმაციული უსაფრთხოების კომპანია Flashpoint-ის სპეციალისტების ანალიზის თანახმად, სინამდვილეში, მათ ამ ფაილის დახმარებით ჩანერგეს მავნე პროგრამული უზრუნველყოფა PowerRatankba malware რომელიც პირდაპირ კავშირშია Lazarus Grop-ის შემდგომ თავდასხმებთან.

მავნე პროგრამული უზრუნველყოფის მეშვეობით მათ Redbanc- ის თანამშრომლის კომპიუტერში არსებული ინფორმაცია მოიპოვეს, რომლსაც გზავნიდნენ დისტანციურ სერვერზე. მონაცემები მოიცავდა ინფორმაციას აპარატურის, ოპერაციული სისტემის, მიმდინარე პროცესების შესახებ და ა.შ. მოპოვებული ინფორმაციის საფუძველზე კიბერდამნაშავეები იღებდნენ გადაწყვეტილებას დამატებით სხვა მავნე პროგრამული უზრუნველყოფის ჩატვირთვის თაობაზე.

Redbanc-ის მაგალითი ნათლად აჩვენებს, რომ მხოლოდ ერთი თანამშრომლის დაუდევრობაც საკმარისია მთელი კორპორატიული ქსელის კომპრომიტირებისთვის.

SecurityLab.ru by Positive Technologies ZDNet

16 იანვარი, 2019 წელი

ავიაბილეთების ჯავშნის სისტემა ამადეუსის ხარვეზი მგზავრებს საფრთხის ქვეშ აყენებს

ავიაბილეთების დაჯავშნის ცნობილ სისტემა Amadeus-ში არსებული სისუსტე ბოროტმოქმედებს საშუალებას აძლევს ცვლილებები შეიტანონ მომხმარებლების

მონაცემებში. უსაფრთხოების გაძლიერებისკენ მიმართული სისტემური განახლება არასაკმარისად ეფექტური აღმოჩნდა.

აღნიშნული სისუსტის შესახებ გამოცემა Safety Detective გვამცნობს. სისუსტე მდგომარეობს მომხმარებლის სპეციალური რეგისტრაციის ჩანაწერის (PNR) გამოცნობის სიმარტივეში. როგორც გამოცემა Noam Rotem იუწყება, არასაკმარისი დაცულობის გამო, ბოტების გამოყენებით კიბერკრიმინალებს შეუძლიათ მრავალჯერ სცადონ მომხმარებლის გვერდზე შესვლა, ვიდრე სწორ PNR კოდს არ მიაგნებენ, ხოლო აღნიშნულით უკვე შესაძლებელი ხდება ბონუს-მაილების სხვა მომხმარებლის ანგარიშზე გადატანა, საკონტაქტო ინფორმაციის რედაქტირება და ჯავშნის სრულიად გაუქმება.

სისტემა Amadeus-ის ინჟინრების განცხადებით, უზუსტობა უკვე აღმოფხვრილია, რასაც ზემოხსენებული გამოცემები არ ეთანხმებიან და თვლიან, რომ მგზავრები კვლავ საფრთხის ქვეშ იმყოფებიან.

SecurityLab.ru by Positive Technologies TC

16 იანვარი, 2019 წელი

თადარიგში მყოფ რუს სამხედროებს სოციალური ქსელების გამოყენება 5 წლამდე ვადით აეკრძალებათ

კანონში სამხედრო მოსამსახურეების სტატუსის შესახებ დაგეგმილია ცვლილებების შეტანა, რომლებიც თადარიგში გადასულ სამხედრო მოსამსახურეებს სოციალური ქსელებით სარგებლობას 5 წლით აუკრძალავენ.

რუსეთის ხელისუფლება აუცილებლად მიიჩნევს სოციალური ქსელების გამოყენების აკრძალვას სამხედრო სამსახურიდან დათხოვილ პირებზე, რათა არ მოხდეს საიდუმლო ინფორმაციის გაჟონვა. გასული წლის შემოდგომაზე რუსეთის დუმაში შევიდა კანონპროექტი სამხედრო პერსონალის სტატუსის შესახებ კანონში ცვლილებების შეტანის თაობაზე. კერძოდ, სამხედრო პირებს უნდა აკრძალვოდათ სოციალური ქსელების გამოყენება. ნოემბერში დეპუტატებმა პირველი მოსმენით მიიღეს კანონპროექტი, სანამ დოკუმენტი მზადდება მეორე მოსმენისთვის, თავდაცვის სამინისტროს შეუძლია აკრძალვა გაავრცელოს სამხედრო სამსახურიდან დათხოვილ პირებზეც.

პროექტის პირველი ვერსიით, აკრძალვა არ ეხებოდათ რეზერვისტებს, თუმცა ინფორმაციის უსაფრთხოების საკითხების სპეციფიკიდან გამომდინარე, სამინისტრომ გადაწყვიტა აკრძალვა რეზერვისტებზეც გაევრცელებინა. დოკუმენტის მიღების შემთხვევაში კანონი გავრცელდება არა მხოლოდ ოფიცრებზე, არამედ ჯარისკაცებზე, სერჟანტებზე, მედპერსონალსა და მეზღვაურებზეც. კანონის დარღვევის შემთხვევაში პირს წაეყენება

ადმინისტრაციული ან სისხლის სამართლებრივი სასჯელი (დანაშაულის სიმძიმის მიხედვით).

17 იანვარი, 2019 წელი

სამხრეთ კორეის თავდაცვის შესყიდვების სააგენტო კიბერთავდასხმის მსხვერპლი გახდა

სამხრეთ კორეის თავდაცვის შესყიდვების სააგენტოს კომპიუტერული ქსელი (ეროვნული უშიშროების სამინისტროს სტრუქტურა) დაუდგენელმა პირებმა გატეხეს და ახალი თაობის ავიაგამანადგურებლების შეიარაღების შესყიდვასთან დაკავშირებული დოკუმენტაცია მოიპარეს.

არსებული ინფორმაციის თანახმად, თავდამსხმელებმა ქსელში აპლიკაციის "Data Storage Prevention Solution“ მეშვეობით შეაღწიეს. აპლიკაცია ყველა სამთავრობო კომპიუტერში იყო დაინსტალირებული, რათა აღეკვეთათ კონფიდენციალური დოკუმენტაციის ჩამოტვირთვა და ინტერნეტთან დაკავშირებულ კომპიუტერებზე შენახვა.

თავდამსხმელებმა სერვერზე მოიპოვეს ადმინისტრატორის დაშვება და შეძლეს 30 კომპიუტერში შეღწევა და მათგან სულ მცირე 10-დან ინფორმაციის მოპოვება.

აქტივობა პირველად 2018 წლის ოქტომბრის ბოლოს დაფიქსირდა, მაგრამ სამხრეთ კორეის ხელისუფლებამ ინციდენტის შესახებ ინფორმაცია მხოლოდ ახლახან გაავრცელა. კიბერთავდასხმის ორგანიზატორის ვინაობა გასაიდუმლოებულია. მიმდინარეობს ინციდენტის გამოძიება.

17 იანვარი, 2019 წელი

აშშ-ს ერთ-ერთი უმსხვილესი სატელეფონო მომსახურების კომპანია მომხმარებელთა პერსონალურ მონაცემებს ღია ბაზაში ინახავდა

კალიფორნიაში დაფუძნებული კომპანია VOIPO, რომელიც VoIP სატელეფონო მომსახურებას უზრუნველყოფს, ღია დომენში ინახავდა ათობით გიგაბაიტ მომხმარებელთა მონაცემებს. მილიონობით ზარების ჩანაწერები, SMS და MMS შეტყობინებები ინახებოდა

ElasticSearch-ის დაუცველ მონაცემთა ბაზაში და ნებისმიერი მსურველისთვის იყო ხელმისაწვდომი.

VOIPO ამერიკის შეერთებულ შტატებში VoIP სერვისის ერთ ერთი ყველაზე დიდი პროვაიდერია. კომპანია CloudFlare ის წარმომადგენელმა ღია მონაცემთა ბაზა გასულ კვირას საძიებო სისტემა Shodan-ის მეშვეობით აღმოაჩინა. მკვლევარმა VOIPO- ს ხელმძღვანელობას არსებული ვითარების შესახებ 8 იანვარს შეატყობინა და მონაცემთა ბაზა რომელიც მომხმარებელთა ინფორმაციას ოთხი წლის განმავლობაში ასაჯაროებდა, იმავე დღეს დაიბლოკა.

მონაცემთა ბაზა შეიცავდა 6.7 მილიონ ჩანაწერს ზარებზე, რომლებიც განხორციელდა 2017 წლის ივლისიდან, 6 მილიონ SMS და MMS შეტყობინებას რომელიც იგზავნებოდა 2015 წლის დეკემბრიდან და სხვა. ჩანაწერები ასახავდა ინფორმაციას ზარის ხანგრძლივობისა და აბონენტთა შესახებ. მონაცემთა ბაზაში ასევე შედიოდა SMS და MMS შეტყობინებების სრული შინაარსი.

მკვლევარის აზრით, თუ VOIPO არ იყენებდა ფაიარვოლს /ან კორპორატიული VPN-ს, შეიძლება, წარმოების სისტემა ჩამოიშალოს

მკვლევარის გზავნილის საპასუხოდ, VOIPO- ის წარმომადგენლებმა განაცხადეს, რომ მონაცემები განთავსებული იყო „Development" სერვერზე, რომელიც შემთხვევით მოხვდა ღია დომეინში, თუმცა კომპანიამ მონაცემების გაჟონვის ფაქტის სინამდვილე დაადასტურა.

SecurityLab.ru by Positive Technologies avast blog

17 იანვარი, 2019 წელი

კრიპტოჯეკინგის მავნე პროგრამული უზრუნველყოფა სამიზნე სერვერებიდან შლის უსაფრთხოების ღრუბლოვან პროგრამებს

კრიპტოჯეკინგის (კრიპტოვალუტის ფარული მითვისების საშუალება) მავნე პროგრამულ უზრუნველყოფას შეუძლია წაშალოს უსაფრთხოების სერვისები, რომელიც განთავსებულია ლინუქსის სერვერზე ჩამონტაჟებულ ღრუბლოვან საცავებში.

კომპანია Palo Alto Networks' Unit 42 მკვლევართა ჯგუფის განცხადებით, მავნე პროგრამული უზრუნველყოფის გავრცელება ხდება ჩინურენოვანი კიბერდანაშაულებრივი ჯგუფის „Rocke" მიერ, რომლის სპეციალიზაციასაც დაინფიცირებული კომპიუტერების მეშვეობით კრიპტოვალიუტა Monero-ს მოპოვება წარმოადგენს.

მავნე პროგრამული უზრუნველყოფის წინა ვერსიებისგან განსხვავებით, რომლებსაც ღრუბლოვანი უსაფრთხოების სერვისების დროებით გათიშვა შეეძლოთ, ახალ ვერსიას უკვე აქვს საშუალება, სრულიად წაშალოს დამცავი პროგრამული უზრუნველყოფა. სავარაუდოა,

რომ აღნიშნული მავნე პროგრამული უზრუნველყოფა ამ დროისთვის პირველია, რომელსაც აქვს უნიკალური შესაძლებლობა, წაშალოს ღრუბლოვან საცავში განთავსებული უსაფრთხოების უზრუნველყოფის საშუალებები.

18 იანვარი, 2019 წელი

დასავლეთ აფრიკის 5 ქვეყნის ბანკები კიბერშეტევის მსხვერპლნი გახდნენ

ინფორმაციული უსაფრთხოების კომპანია Symantec-ის სპეციალისტებმა 2018 წელს გამოავლინეს, რომ დასავლეთ აფრიკის ქვეყნების (კამერუნი, DR კონგო, ეკვატორული გვინეა, განა და კოტ დ'ივუარი) ბანკებსა და საფინანსო ინსტიტუტებზე ოთხი სხვადასხვა სახის კიბერშეტევა განხორციელდა.

დამნაშავეებმა PowerShell, PsExec-ი, Windows RDP, და UltraVNC-ის პროგრამული უზრუნველყოფა გამოიყენეს, რომელთაც ზოგიერთი კომპანია და სისტემური ადმინისტრატორები დისტანციური სისტემებთან დაკავშირებისა და მართვისთვის იყენებენ.

ბოლო ორი წლის განმავლობაში, რუსული და ჩრდილოეთ კორეული ჰაკერული დაჯგუფებები არაერთხელ დაესხნენ ბანკებსა და ფინანსურ ინსტიტუტებს სამხრეთ-აღმოსავლეთ აზიაში, აღმოსავლეთ ევროპასა და სამხრეთ ამერიკაში.

როგორც ექსპერტები აღნიშნავენ, დასავლეთ ევროპის ან ჩრდილოეთ ამერიკის ბანკებთან შედარებით, დასავლეთ აფრიკის თითქმის ყველა ფინანსურ ინსტიტუტში ცუდად კონფიგურირებული ქსელებია, რადგან ორგანიზაციები არ დებენ ინვესტიციას ინფორმაციული ტექნოლოგიების ინფრასტრუქტურასა და კიბერუსაფრთხოებაში, რაც თავდამსხმელებს უადვილებს საქმეს და ისინი ახერხებენ ხანგრძლივი პერიოდის განმავლობაში მიჩქმალონ თავდასხმა.

21 იანვარი, 2019 წელი

GDPR ნორმების დარღვევის გამო Google 50 მილიონით დაჯარიმდა

საფრანგეთის ინფორმაციული ტექნოლოგიებისა და ადამიანის უფლებათა ეროვნულმა კომისიამ (CNIL) კომპანია გუგლს მონაცემთა დაცვის წესების დარღვევისა და

მომხმარებელთა პირადი ინფორმაციის გამოყენებისთვის 50 მილიონი ევროს ჯარიმა დააკისრა. სამინისტროს ცნობით, ეს პირველი შემთხვევაა, როდესაც CNIL პერსონალური მონაცემების დაცვის შესახებ ევროკავშირის კანონით გათვალისწინებულ მაქსიმალურ ჯარიმას იყენებს.

2018 წლის მაისის ბოლოს, ორგანიზაციებმა „None of your business" და "La Quadrature du Net", გუგლი აიძულებდა მომხმარებლებს ნებაყოფლობით გაეცათ თავიანთი პერსონალური ინფორმაცია.

გასული წლის სექტემბერში საფრანგეთის მარეგულირებელმა ორგანომ აღმოაჩინა, რომ მომხმარებლებს რომლებიც ახალი Android-ის სმარტფონით ცდილობენ Google ანგარიშის შექმნას, საჭირო ინფორმაციის მისაღებად ხუთი ან ექვსი ქმედების განხორციელება უწევთ და ფორმულირება ყოველთვის არ არის გასაგები. გარდა ამისა, Google ძალიან ბუნდოვნად განმარტავს, თუ როგორ აპირებს მომხმარებლის მონაცემების გამოყენებას და რა ხანგრძლივობით შეინახება პირადი მონაცემები მათ ბაზაში. მაშასადამე კომპანია არ იღებს მონაცემების დამუშავების შესახებ მომხმარებლების მკაფიო თანხმობას.

SecurityLab.ru by Positive Technologies THE VERGE

22 იანვარი, 2019 წელი

ჩინეთში მოვალეთა საძიებელი აპლიკაცია შექმნეს

ჩინეთში გამოჩნდა ახალი აპლიკაცია, რომელიც გამსესხებელს მისი მოვალის ადგილმდებარეობას უჩვენებს. ჩინური პრესის თანახმად აპლიკაცია სახელწოდებით „არაკეთილსინდისიერ მოვალეთა ბარათი" უკვე აქტიურად გამოიყენება ჰებეის პროვინციაში.

აღნიშნული აპლიკაცია არის მკაცრი სოციალური რეიტინგის სისტემა, რომელიც მიზნად ისახავს მოქალაქეთა სანდოობის განსაზღვრას. სისტემა საკრედიტო რეიტინგის შეფასების ერთ ერთი მეთოდია და 2020 წლისთვის მისი მოხმარება სავალდებულო გახდება.

ბარათის მიღება შესაძლებელია ჩინეთში ყველაზე პოპულარული საკომუნიკაციო სერვისით, WeChat-ით. აპლიკაცია მოვალის ზუსტ ადგილმდებარეობას განსაზღვრავს. ჯერჯერობით დაუდგენელია რა ოდენობის და ვისი ვალი უნდა ჰქონდეს პიროვნებას, რომ მოხვდეს არაკეთილსინდისიერ მოვალეთა ბარათზე და როგორ განსაზღვრავს აპლიკაცია მოვალის გადახდისუნარიანობას.

TNW SecurityLab.ru by Positive Technologies

23 იანვარი, 2019 წელი

ჩინეთის მთავრობამ საძიებო სისტემა Microsoft Bing-ი დაბლოკა

ჩინეთის მთავრობამ საძიებო სისტემა Microsoft Bing დაბლოკა. სახელმწიფო პროექტის „ოქროს ფაიარვოლის“ ფარგლებში, Facebook, Google, Yahoo, WhatsApp და Twitter-თან ერთად სისტემა ჩინეთში აკრძალული სერვისების ნუსხაშია შეყვანილი.

მომხმარებელთა საჩივრების შესვლის შემდეგ Microsoft-ის ექსპერტებმა ჩაატარეს გამოძიება და დაადასტურეს, რომ საძიებო სისტემა ჩინეთში ხელმისაწვდომი აღარ არის. მათი თქმით, კომპანია ახლა თავიანთ შემდგომ ქმედებებზე მსჯელობს.

Bing-ის დაბლოკვის გადაწყვეტილება მოულოდნელი იყო, რადგან Microsoft ზედმიწევნით იცავდა ჩინეთის მთავრობის მიერ დაწესებულ ყველა შეზღუდვას. Bing სიდიდით მეორე საძიებო სისტემაა Google-ის შემდეგ, რომელიც ჩინეთმა დაბლოკა.

როგორც "Financial Times" იტყობინება, Bing ჩინეთში მთავრობის განკარგულებით იქნა დაბლოკილი. დაბლოკვის მიზეზი კი ჯერ-ჯერობით უცნობია.

SecurityLab.ru by Positive Technologies CAPITAL BUSINESS

23 იანვარი, 2019 წელი