საქართველოს თავდაცვის სამინისტრო

სსიპ - კიბერუსაფრთხოების ბიურო

კიბერდაიჯესტი № 2

თბილისი 2019

სარჩევი

დრონებმა შეიძლება ეროვნულ უსაფრთხოებას შეუქმნას საფრთხე

ბრიტანეთი დრონების გამოყენების კატეგორიული წინააღმდეგია, ვინაიდან ის ეროვნულ უსაფრთხოებას რისკის ქვეშ აყენებს და კიბერუსაფრთხოების ექსპერტებს მათგან წარმოშობილი საფრთხის შემცირება მართებთ.

უკანასკნელი შემაშფოთებელი ფაქტები ლონდონის 2 აეროპორტის მახლობლად მფრინავ დრონებთან იყო დაკავშირებული. გეთვიქის აეროპორტში იანვრის ბოლოს დრონების ფრენამ სრული ქაოსი გამოიწვია, რის შედეგადაც 800 ფრენა გაუქმდა და შეზღუდვები 120 000 მგზავრს შეეხო. ამგვარი პრობლემა ასევე იყო ჰითროუს აეროპორტში იანვრის დასაწყისში.

დრონებთან დაკავშირებული საყურადღებო საკითხს წარმოადგენს ის, რომ დრონი შესაძლოა გაიტაცონ ჰაკერებმა და მიგვიყვანონ ისეთ შედეგებამდე, როგორიც ზემოთ აღიწერა. მათ შორის აღნიშნულ შემთხვევაშიც, არსებობს ეჭვი, რომ დრონები გატაცებული იყო ჰაკერების მიერ და სწორედ მათ ჰქონდათ მოწყობილობაზე კონტროლი. ამგვარი შემთხვევების თავიდან აცილების მიზნით უნდა არსებობდეს საკმარისად დაცული ავთენტიფიკაციის მექანიზმები.

ანალიტიკურმა ინსტიტუტმა Parliament Street გამოკითხა 2000 ადამიანი და შეადგინა ანგარიში Drone 4 U. გამოკითხულთა 75% მიიჩნევს, რომ დრონი ეროვნული უსაფრთხოების საფრთხეა. 38% მიიჩნევს, რომ დრონები საერთოდ უნდა აიკრძალოს, ხოლო 83% მიიჩნევს, რომ უნდა არსებობდეს ლიცენზირების სავალდებულო სისტემა. ამავე რაოდენობის ხალხის აზრით, ბრიტანეთმა ფეხი ვერ აუწყო დრონების ტექნოლოგიის განვითარებას და ისინი თვლიან, რომ კიბერუსაფრთხოების ექსპერტებმა მეტად უნდა მიაქციონ ყურადღება ამგვარ სერიოზულ ინციდენტებს და დახმარება აღმოუჩინონ სახელმწიფოსა და საზოგადოებას.

დიდი ბრიტანეთის ტრანსპორტის მინისტრმა კრის გეილინგმა განაცხადა, რომ დრონის სარგებლობის წესების გამკაცრების შესახებ. კერძოდ, უპილიტო მფრინავი მოწყობილობების მფლობელები ვალდებულნი არიან დაარეგისტრირონ ისინი. აეროპორტის გარშემო საფრენად აკრძალული ზონა გაიზარდა 1-დან 5 კილომეტრამდე. მინისტრის განცხადებით, პოლიციას ექნება უფლება დააჯარიმოს ან დააკავოს სამართალდამრღვევები.

infosecurity GROUP TCH

24 იანვარი, 2019 წელი

iOs ოპერაციულ სისტემაზე მომუშავე აპლიკაციაში Whatsapp გაჩნდა ბიომეტრიული ავთენტიფიკაციის მხარდაჭერა

აპლიკაციის ახალი განახლების წყალობით, უსაფრთხოების ნორმები ბიომეტრიული მონაცემებით ავთენტიფიკაციის შესაძლებლობით გაძლიერდა. მომხმარებლებს შეუძლიათ დაბლოკონ აპლიკაცია, რის შედეგადაც მისი გახსნის თითოეულ მცდელობაზე, მოეთხოვებათ გაიარონ სახის (Face ID) ან თითის ანაბეჭდით (Touch ID) ავტორიზაცია.

ახალი ფუნქცია დამატებულია აპლიკაციის ვერსიაში WhatsApp 2.19.20. აღსანიშნავია, რომ კონკრეტული მიმოწერის ბლოკირება არ ხდება, რასაც უსაფრთხოების სპეციალისტები მიმოწერის კონფიდენციალურობის დაცვის კიდევ უფრო მაღალი ხარისხით უზრუნველყოფით ხსნიან.

ფუნქციის გააქტიურების შემდეგ მომხმარებლები კვლავ შეძლებენ სმარტფონის დაბლოკილ მდგომარეობაში უახლესი შეტყობინებების დანახვას, თუმცა მიმოწერის გასახსნელად, აუცილებელია ბიომეტრიული ავთენტიფიკაცია.

იმ შემთხვევაში, თუკი სმარტფონის სენსორები წყობიდან გამოვა, აპლიკაციის განსაბლოკად საჭირო იქნება შესაძლებელი სმარტფონის „iPhone“ პაროლის გამოყენება.

SecurityLab.ru by Positive Technologies BIOMETRIC UPDATE.COM

4 თებერვალი, 2019 წელი

Android ოპერაციულ სისტემაზე მომუშავე სმარტფონის გატეხვა მსხვერპლის მიერ გრაფიკული გამოსახულების გახსნითაა შესაძლებელი

Android ოპერაციული სისტემის მომხმარებლებს ყურადღების გამოჩენა მართებთ, ვინაიდან ინტერნეტიდან გადმოწერილი ან შეტყობინებით მიღებული გრაფიკული გამოსახულებების გახსნის შემთხვევაში, ისინი შეიძლება სმარტფონის გატეხვის საშიშროების წინაშე აღმოჩნდნენ.

საფრთხის მიზეზად ექსპერტები3 ახლად აღმოჩენილ უზუსტობას ასახელებენ, რომელიც Android სისტემის 7.0 Nougat ვერსიიდან 9.0 Pie ვერსიამდე გვხვდება. Google ამ დრომდე არ ასაჯაროებს ინფორმაციას აღნიშნულთან დაკავშირებით, თუმცა სისტემის განახლებებში აღნიშნულია მეხსიერების ბუფერის გადავსების გამოსწორების და სხვადასხვა პრობლემების შესახებ, რომელიც PNG ფოტოსურათების დამუშავების კომპონენტებთანაა დაკავშირებული.

სისუსტის ბოროტად გამოსაყენებლად კიბერდამნაშავისთვის საკმარისია მსხვერპლს მოტყუებით გაახსნევინოს მავნე PNG ფორმატის ფოტოსურათი, რომლის გარჩევაც უსაფრთხო გამოსახულებისგან, ერთი შეხედვით, შეუძლებელია.

მიმდინარე წლის თებერვალში დაგეგმილ განახლებებში ვხვდებით აღნიშნული სისუსტეების აღმოფხვრის ფაქტებს, თუმცა იქიდან გამომდინარე, რომ Android-მოწყობილობის ყველა მწარმოებელი არ გამოსცემს განახლებებს ყოველთვიურად, უცნობია, თუ როდის მიაღწევს უსაფრთხოების გაძლიერებული ნორმები საბოლოო მომხმარებლამდე.

SecurityLab.ru by Positive Technologies The Hacker News 7 თებერვალი, 2019 წელი

მსხვილი ავიაკომპანიები მგზავრებს მონაცემებს გაჟონვის რისკის ქვეშ აყენებენ

კომპანიის Wandera სპეციალისტების განცხადებით, ბილეთების გაყიდვის და ონლაინ რეგისტრაციის ელექტრონული სისტემები, რომლებიც გამოიყენება ისეთი მსხვილი ავიაკომპანიების მიერ, როგორიცაა Air France, KLM, Vueling, Southwest, Jetstar, Thomas Cook Airlines, Air Europa და Transavia, შეიცავენ სისუსტეს, რომლის გამოყენებითაც კიბერკრიმინალებს შეუძლიათ მიიღონ წვდომა მგზავრების პერსონალ მონაცემებზე, შეცვალონ მათი ადგილები ავიალაინერის ბორტზე და შეცვალონ მონაცემები ჩასხდომის ბარათებზე.

პრობლემის არსი რეისზე რეგისტრაციის ბმულის ელექტრონულ ფოსტაზე დაგზავნის დროს შიფრაციის არარსებობაში მდგომარეობს. შიფრაციის არარსებობის გამოყენებით, ბოროტმოქმედებს შეუძლიათ დაუკავშირდნენ იმავე Wi-Fi ქსელს, რასაც მომხმარებელი და გადაქაჩონ მოთხოვნა ბმულზე, რითაც ისინი მიიღებენ წვდომას მსხვერპლის რეგისტრაციის გვერდზე, სადაც განთავსებულია სხვადასხვა პერსონალური ინფორმაცია, დაწყებული მისამართებითა და პასპორტის ნომრებით, დამთავრებული ფრენის დეტალებით.

მიუხედავად იმისა, რომ სპეციალისტებმა ავიაკომპანიებს სისუსტის შესახებ რამდენიმე კვირის წინ შეატყობინეს და ავიაგადამზიდავების წარმომადგენლებმა განაცხადეს, რომ მოახდინეს სწრაფი რეაგირება, ექსპერტების განცხადებით, პრობლემა ამ დრომდე აღმოუფხვრელია.

SecurityLab.ru by Positive Technologies wandera 7 თებერვალი, 2019 წელი

ავსტრალიის პარლამენტი კიბერშეტევის მსხვერპლი გახდა

ავსტრალიის სპეცსამსახურები იძიებენ ქვეყნის პარლამენტის კომპიუტერულ ქსელზე თავდასხმის ფაქტს. პარლამენტის წარმომადგენლების განცადებით, ამ დრომდე ვერ მოხერხდა მონაცემების გაჟონვის მტკიცებულებების აღმოჩენა.

Australian Signals Directorate ინფორმაციით, რომელიც ამჟამად ქსელის დაცვისა და ინციდენტების მავნე ზემოქმედების მინიმიზაციაზე მუშაობს, მათ შეძლეს კიბერშეტევაზე დროული რეაგირება. უსაფრთხოების ნორმებიდან გამომდინარე, სპეციალისტებმა კომპიუტერულ სისტემებზე შეცვალეს უსაფრთხოების პაროლები.

ავსტრალიის პარლამენტის წარმომადგენლებმა გაავრცელეს ინფორმაცია, რომლის თანახმადაც მათ ამ დროისთვის არ აქვთ უტყუარი მტკიცებულებები იმისა, რომ შეტევის მცდელობა მიზნად ისახავდა პოლიტიკურ პროცესებზე უარყოფითი გავლენის მოხდენას.

პრემიერ მინისტრ სკოტ მორისონის განცხადების თანახმად, ქვეყანაში მოღვაწე კიბერუსაფრთხოების ექსპერტებისგან მიღებულ ინფორმაციაზე დაყრდნობით, შეიძლება ითქვას, რომ კიბერშეტევის უკან კონკრეტული ქვეყანა შეიძლება იდგეს. მისი თქმით, ეჭვი აქვთ მხოლოდ რამდენიმე ქვეყანაზე, მაგრამ არ არიან დარწმუნებულები, რომ ისინი საჯაროდ შეძლებენ ვარაუდის გამოთქმას იმის შესახებ, თუ კონკრეტულად რომელ სახელმწიფოს მოიაზრებენ თავდამსხმელად.

SecurityLab.ru by Positive Technologies ABC

8 თებერვალი, 2019 წელი

კიბერკრიმინალებს რომლებმაც რუსეთის ბანკებიდან 1 მილიარდი რუბლი მოიპარეს განაჩენი გამოუტანეს

თორმეტ კიბერკრიმინალს, რომლებმაც ბანკებიდან დაახლოებით 1 მილიარდი რუბლი მოიპარეს, განაჩენი უკვე გამოუტანეს. მოსკოვის მეშჩანსკის სასამართლოს გადაწყვეტილებით, დანაშაულის სიმძიმიდან გამომდინარე, ბრალდებულები სასჯელს მკაცრი რეჟიმის კოლონიებში მოიხდიან.

დამნაშავეებს ბრალი ედებოდათ კრიმინალური დაჯგუფების შექმნასა და მასში მონაწილეობაში, ინფორმაციული ტექნოლოგიების სფეროში თაღლითობასა და განსაკუთრებით დიდი ოდენობით თანხების მიტაცებაში ედებოდათ.

გამოძიების ინფორმაციით, 2014 წლიდან მოქმედი დაჯგუფების წევრები ცვლიდნენ ლეგალურ პროგრამულ უზრუნველყოფას, რის შედეგადაც ბანკების კლიენტების ანგარიშებიდან ხდებოდა თანხების მითვისება, ხოლო კლიენტთა ანგარიშზე ბალანსის აღდგენა ბანკების ხარჯზე ხდებოდა.

ბრალდების თანახმად, კრიმინალური დაჯგუფება შედგებოდა სამი ცალკეული ჯგუფისგან. დაჯგუფების წევრები ერთმანეთს უსაფრთხოების მიზნებიდან გამომდინარე არ უკავშირდებოდნენ. ოპერაციების შესასრულებლად მოსკოვში სპეციალურად ნაქირავებ ბინაში განთავსებული იყო ყველა საჭირო ტექნიკა და ხდებოდა საჭირო ინფორმაციის გაცვლა.

TADVISER ZDNet

8 თებერვალი, 2019 წელი

ირანს ისრაელის სარაკეტო თავდასხმის გამაფრთხილებელ სისტემაზე(EWS) კიბერშეტევის მცდელობა ჰქონდა

დაახლოებით ერთი წლის წინ ირანს ისრაელის სარაკეტო თავდასხმის გამაფრთხილებელ სისტემაზე (EWS) კიბერშეტევის მცდელობა ჰქონდა. ამის შესახებ ისრაელის არმიის კიბერთავდაცვის დანაყოფის მეთაურმა ნოამ შაარმა განაცხადა.

EWS ისრაელის სამხედრო ინფრასტრუქტურის ერთ-ერთი ყველაზე მგრძნობიარე ელემენტია. მასთან წვდომის მქონე პირს შეუძლია ჩართოს განგაშის სირენა ან სულაც გამორთოს სიგნალი რომელიც საავიაციო თავდასხმის შესახებ იუწყება.

შაარის თქმით, მისმა დანაყოფმა შეძლო კიბერშეტევის წარმატებით მოგერიება რითაც თავიდან აიცილა შესაძლო კატასტროფული შედეგები. ინციდენტის აღკვეთა შესაძლებელი გახდა ირანის ისლამური რევოლუციის გუშაგთა კორპუსის დაქვემდებარებაში მყოფი ჰაკერული დაჯგუფების აქტივობაზე უწყვეტი მონიტორინგის შედეგად.

EWS- ის გარდა, ირანელი ჰაკერები ისრაელში სხვა კომპიუტერული სისტემების გატეხვასაც ცდილობდნენ. შაარის თქმით, ირანი მუდმივად თავს ესხმის ისრაელის სამხედრო და სამოქალაქო სისტემებს. საერთო ჯამში, კიბერუსაფრთხოების დანაყოფმა დაახლოებით 130 კიბერშეტევა მოიგერია, რომელთა უმეტესობა ირანიდან განხორციელდა.

SecurityLab.ru by Positive Technologies BREAKINGISRAELNEWS Latest News Biblical Perspective

10 თებერვალი, 2019 წელი

რუსეთი გეგმავს გლობალურ ინტერნეტს გაეთიშოს

რუსეთი გეგმავს რომ მცირე დროით გლობალურ ინტერნეტ ქსელს გაეთიშოს, რომელიც კიბერთავდაცვითი პოტენციალის შემოწმებისთვის იქნება გამიზნული.

BBC ინფორმაციით, ტესტირების დროს მონაცემების გაცვლა მხოლოდ ქვეყნის შიგნით მოხდება და საერთაშორისო, გლობალურ ქსელთან კავშირი არ იარსებებს.

აღნიშნულთან დაკავშირებით რუსეთის პარლამენტში კანონპროექტი "ციფრული ეკონომიკის ეროვნული პროგრამა" წინა წლის დეკემბერში დარეგისტრირდა. კანონპროექტში ნახსენებია, რომ რუსეთი შეიმუშავებს ქსელის მისამართის საკუთარ ვერსიას, ცნობილს როგორც DNS, რისი საშუალებითაც ის მუშაობას გააგრძელებს იმ შემთხვევაშიც, თუ მას საერთაშორისო ქსელიდან ჩახსნიან.

რუსეთის მთავრობას სურს, რომ შიდა ქსელის მონაცემებმა გაიარონ სპეციალური შემოწმების წერტილები. აღნიშნული შემთხვევა ძალიან ჰგავს ჩინეთის ცენზურის სისტემას, რომელიც ბლოკავს შესაბამის აკრძალულ მონაცემთა გაცვლას.

ინტერნეტ-სერვისის პროვაიდერების განცხადებით, ეს ტესტი სერიოზულ პრობლემებს წარმოქმნის, ვინაიდან რუსეთის მთავრობა ავალდებულებს მათ შეცვალონ საკუთარი ინფრასტრუქტურა.

BBC ВЕДОМОСТИ

11 თებერვალი, 2019 წელი

ფრანგი ჟურნალისტები წლობით ანონიმურად დასცინოდნენ ქალ კოლეგებს ფეისბუქ ქსელის გამოყენებით

BBC ინფორმაციით, რამდენიმე ფრანგი ჟურნალისტი და რედაქტორი გაათავისუფლეს სამსახურიდან ინტერნეტ-ჯგუფში „Ligue du LOL“ თანამშრომლების (ძირითადად ქალბატონების) დაცინვის გამო.

ათობით ქალბატონმა უკვე დაადასტურა, რომ ისინი ხდებოდნენ ჯგუფის წევრების მხრიდან დაცინვის მსხვერპლნი. თავდამსხმელები ამზადებდნენ კოლაჟებს პორნოგრაფიული ხასიათის სურათებისა და მსხვერპლის ფოტოების გამოყენებით.

ანონიმური ჯგუფის საქმიანობა ამხილა გაზეთმა Libération და სტატიაში დაიწერა 2 კონკრეტული თანამშრომლის სახელი და გვარი, რომელიც ჯგუფში იყო გაწევრიანებული. მათ შორის ერთ-ერთი იყო ფრილანსერი (შტატგარეშე მომუშავე ჟურნალისტი) ვინსენტ გლადი, რომელმაც ჯგუფი (Ligue du LOL) გახსნა 2009 წელს.

ინფორმაციული ტექნოლოგიების მინისტრმა მუნირ მახჟუბმა განაცხადა, რომ ჯგუფის წევრებს თავი ყოვლისშემძლენი ეგონათ, თუმცა მათი უკანონო ქმედების შედეგები რეალურ ცხოვრებაში აისახა.

BBC афишаDaily

12 თებერვალი, 2019 წელი

გარკვეული ტიპის USB კაბელი დისტანციურად იღებს და მიჰყვება ჰაკერის მითითებებს

უსაფრთხოების ექსპერტმა მაიკ გროვერმა შექმნა მავნე USB კაბელი სახელწოდებით O-MG, ჩაშენებული უკაბელო ქსელის დაფით, რომელიც შესაძლებლობას იძლევა გადაიცეს ბრძანებები Wi-Fi ქსელის დახმარებით, თითქოს, ისინი შეყვანილია კომპიუტერის კლავიატურიდან.

გროვერი განმარტავს, რომ კაბელი აღიქმება ისე, როგორც კლავიატურა და მაუსი. დემონსტრაციისას მან აჩვენა, თუ როგორ შეიძლება MacBook პორტატულ კომპიუტერის მართვა აღნიშნული კაბელისა და სმარტფონის გამოყენებით, ასევე, კომპიუტერის მფლობელის ისეთი ინფორმაციის მიღება, როგორიცაა პაროლი. USB კაბელის გამოყენებით ბოროტმოქმედს თავდასხმა შეუძლია განახორციელოს Linux, Mac, Windows და iOs სისტემებზე, ასევე უკაბელო ქსელებზე.

გროვერი ამგვარი კაბელების გამოშვებას კვლავ გეგმავს. მკვლევარების ხელში მათი აღმოჩენა უსაფრთხოების გაუმჯობესებამდე მიგვიყვანს.

SecurityLab.ru by Positive Technologies GEEK.COM

12 თებერვალი, 2019 წელი

მოდერნიზებული ამერიკელი ჯავშანტრანსპორტიორები Stryker Dragoon ჰაკერების თავდასხმის სამიზნე გახდა

დაახლოვებით ერთი წლის წინ ევროპაში მოდერნიზებული ამერიკული ჯავშანტრანსპორტიორები Stryker Dragoon (ასევე ცნობილი, როგორც XM1296) გამოჩნდა.

როგორც გაირკვა აღნიშნული მოდელი კიბერშეტევებისგან დაცული არ აღმოჩნდა, კიბერდამნაშავეებმა მოახერხეს მისი რამდენიმე სისტემის ფუნქციონირების მოშლა. აშშ-ს სამხედრო ძალების ოპერაციების წარმოების განვითარებისა და შეფასების დირექტორატმა (Director, Operational Test and Evaluation, DOT&E) აღნიშნული დაადასტურა, თუმცა ანგარიშში არ არის ინფორმაცია კიბერშეტევის ზუსტი თარიღის, მისი ორგანიზატორების შესახებ. არ არის მითითებული კონკრეტულად რა სისტემები გახდა კიბერდამნაშავეების სამიზნე, მაგრამ საუბარია იმაზე, რომ მიზანში ამოღებული სისტემები უზრუნველყოფდა მონაცემთა მიმოცვლას, ნავიგაციას და კომუნიკაციას. ამ სისტემების მოშლა ან მათში არასწორი ინფორმაციის ჩაწერა ხელს შეუშლის როგორც სამხედრო ოპერაციების ჩატარებას ასევე წარმოშობს დამატებით რისკებს სამხედროებისთვის.

შესაძლებელია, რომ კიბერშეტევების სამიზნე იყო არა ჯავშანმანქანა, არამედ კომპიუტერული ქსელები რომლებიც საბორტო სისტემების ფუნქციონირებას უზრუნველყოფენ. DOT & E ანგარიშის თანახმად თავდასხმა განხორციელდა Stryker-ის მხოლოდ ერთ მოდელზე კერძოდ "dragoon"-ზე.

SecurityLab.ru by Positive Technologies THE DRIVE

13 თებერვალი, 2019 წელი

ინდოეთის ხელისუფლება Whatsapp-ისგან ითხოვს შესაძლებლობას გაეცნონ მომხმარებელთა მიმოწერას

კომპანია ფეისბუქი, რომელიც 2014 წლის ოქტომბრიდან ფლობს Whatsapp-ს, კვლავ აღმოჩნდა ინდოეთის ხელისუფლების ზეწოლის ქვეშ, მისგან ინდოეთი მომხმარებელთა მიმოწერებზე წვდომის მინიჭებას მოითხოვს.

ინდოეთის ელექტრონიკისა და ინფორმაციული ტექნოლოგიების მინისტრი მოთხოვნის საფუძვლად მესენჯერის კრიმინალური საქმიანობის დაგეგმვისთვის(მათ შორის ბავშვთა პორნოგრაფიის გავრცელებისთვის) გამოყენებას ასახელებს. შესაბამისად, კრიმინალების შეჩერების ერთადერთ საშუალებად სამართალდამცავი ორგანოებისთვის შეტყობინებებზე წვდომის მინიჭებას მიიჩნევს.

Whatsapp-ის წარმომადგენლის კარლ ვუგის განცხადებით, მესენჯერში შეტყობინებების შიფრაცია ავტომატურად ხდება, რაც მომხმარებლებს აძლევს გარანტიას, რომ მესამე პირს ვერ ექნება წვდომა მიმოწერაზე. გამონაკლისის დაშვება, რასაც ინდოეთის ხელისუფლება მოითხოვს, დაარღვევდა მესენჯერის კონცეფციას, რაც მოითხოვს Whatsapp-ის არქიტექტურის შეცვლას და ასეთ შემთხვევაში მივიღებთ სულ სხვა პროდუქტს, რომელიც არ იქნება აღჭურვილი სრული კონფიდენციალურობით.

გარდა აღნიშნული მოთხოვნისა, ინდოეთის მთავრობა აპირებს საკანონმდებლო დონეზე დაავალდებულოს Facebook, Whatsapp, Twitter და Google ქსელიდან წაშალოს უკანონო შინაარსის შემცველი მასალა შესაბამისი მოთხოვნიდან 24 საათის განმავლობაში.

SecurityLab.ru by Positive Technologies

14 თებერვალი, 2019 წელი

Lenovo-ს ჭკვიანი საათი "Watch X" ინფორმაცია ჩინეთში განთავსებულ სერვერზე გზავნის

Lenovo- ს საათი „Watch X" კრიტიკის ქარცეცხლში მაღალი მოწყვლადობის გამო გაეხვა. აღნიშნული მოდელი საფრთხეს უქმნის მომხმარებელთა უსაფრთხოებასა და

კონფიდენციალობას. კომპანია Checkmarx- ის ექსპერტმა დევიდ სოპმა გამოავლინა რიგი ხარვეზები, რამაც შესაძლოა Lenovo Watch X- ის მომხმარებლების უსაფრთხოება რისკის ქვეშ დააყენოს.

1.საათი მომხმარებლის ადგილმდებარეობის შესახებ მონაცემებს გზავნიდა ჩინეთში არსებულ უცნობ სერვერზე უცნობი საკომუნიკაციო არხის მეშვეობით;

2.არსებული ხარვეზი მობილურ აპლიკაციასა და ვებ-სერვერს შორის ინფორმაციის მიმოცვლის გადაჭრის საშუალებას იძლევა;

3.ხარვეზი ჭკვიანი საათის მეპატრონის ანგარიშების გატეხვის შესაძლებლობას იძლევა;

4.ანგარიშის ვერიფიკაციისა და ნებართვების შემოწმების არარსებობის გამო, შესაძლებელია მომხმარებლის დაუკითხავად პაროლის შეცვლა. ნებისმიერს ვინც იცის მომხმარებლის ID შეუძლია შეცვალოს პაროლი და გატეხოს ანგარიში.

2018 წლის ოქტომბერში ჩეკმარქსმა აცნობა, Lenovo- ს საათებში არსებული ხარვეზების შესახებ. რამდენიმე კვირის შემდეგ კომპანიის წარმომადგენლებმა აღიარეს მოწყვლადობის არსებობა, ხოლო 2019 წლის იანვარში, Lenovo-მ პრობლემების აღმოფხვრის შესახებ განაცხადა.

SecurityLab.ru by Positive Technologies threatpost

14 თებერვალი, 2019 წელი

გერმანია ნატოს თავის კიბერშესაძლებლობებს გაუზიარებს

გერმანია შეუერთდა ნატო-ს იმ ქვეყნების რიგებს, რომლებიც კიბერდანაშაულთან ბრძოლასა და ელექტრონულ ომში დახმარების მიზნით, ალიანსს საკუთარ კიბერშესაძლებლობებს უზიარებენ.

ნატო სახმელეთო, საზღვაო და საჰაერო სივრცეებთან ერთად კიბერსივრცეს განიხილავს როგორც კონფლიქტის ზონას. აღნიშნული განპირობებულია კიბერშეტევების, ჰაკტივისტების და სახელმწიფოებისგან დაფინანსებული კიბერდამნაშავეთა რიცხვის ზრდით.

გერმანიის თავდაცვის მინისტრის ურსულა ფონ დერ ლეიენის განცხადებით, "მსგავსად იმისა, როგორც ნატო იყენებს ჩვენ სამხედრო-საჰაერო და სამხედრო-საზღვაო ძალებს, ასევე მას შეეძლება გამოიყენოს ჩვენი კიბერშესაძლებლობები ჩვენთან არსებული ეროვნული და სამართლებრივი ჩარჩოების გათვალისწინებით".

იმ ქვეყნებს შორის, რომლებიც მზად არიან ალიანსს დაახმარონ საკუთარი შეტევითი კიბერიარაღი არიან: ამერიკის შეერთებული შტატები, დიდი ბრიტანეთი,

დანია, ჰოლანდია და ესტონეთი. ნავარაუდევია, რომ კონტრშეტევის შესაძლებლობა დააფრთხობს პოტენციურ აგრესორს.

შეტევითი კიბეროპერაციების სამიზნე შესაძლოა გახდეს ინტერნეტთან დაკავშირებული ნებისმიერი ობიექტი - დაწყებული კომპიუტერიდან და სმარტფონებიდან დამთავრებული მოწყობილობებით რომლებიც აკონტროლებენ ელექტროსადგურებისა და სატრანსპორტო ქსელების საკვანძო მექანიზმებს.

SecurityLab.ru by Positive Technologies SECURITY WEEK

15 თებერვალი, 2019 წელი

ჰაკერები სოციალური ქსელების მეშვეობით ფიშინგის ახალ კამპანიას ეწევიან

მომხმარებლები, რომლებიც ზრუნავენ საკუთარი ანგარიშების უსაფრთხოებაზე სისტემაში შესვლისა და ავტორიზაციის წინ, ყურადღებას ამახვილებენ რამდენიმე ფაქტორზე, მაგალითად, რწმუნდებიან URL- ისა და HTTPS- ის სისწორეში ან იყენებენ ბრაუზერებს რომლებიც ფიშინგურ დომეინებს შიფრავენ. ცოტა ხნის წინ, ექსპერტებმა აღმოაჩინეს ახალი ფიშინგ კამპანია, რომელმაც შეიძლება შეცდომაში შეიყვანოს ყველაზე ფრთხილი მომხმარებელიც კი.

Facebook- ის ან სხვა სოციალური ქსელების მეშვეობით დარეგისტრირების პრაქტიკას ბევრი საიტი იყენებს რეგისტრაციის გასამარტივებლად. როგორც წესი, როდესაც თქვენ დააჭერთ ღილაკს "შესვლა Facebook- ზე", თქვენ ან გადაგამისამართებთ facebook.com ან გამოჩნდება pop-up ფანჯარა სადაც უნდა მიუთითოთ თქვენი Facebook ანგარიშის მონაცემები მხოლოდ ამ ნაბიჯების გავლის შემდეგ გექნებათ საშუალება მიიღოთ თქვენთვის სასურველი ინფორმაცია.

პაროლების მენეჯერის შემქმნელი კომპანია Myki- ის სპეციალისტის, Antoine Vincent Jebara- ის განცხადებით, თავდამსხმელები ბლოგებსა და სერვისებზე ავრცელებენ ბმულებს, ბმულზე გადასასვლელად მომხმარებელი თავის Facebook ანგარიშით რეგისტრირდება. მომხმარებლები ამას ძირითადად იმიტომ აკეთებენ რომ დაინტერესებულები არიან გარკვეული შემოთავაზებებით რომლის მიღებასაც (როგორც ვებ გვერდზე იუწყებიან) მხოლოდ ავტორიზაციის გავლის შემთხვევაში შეძლებენ.

მაგალითად ფასდაკლების ვაუჩერი ან უფასო ინტერნეტი და ასე შემდეგ. ამის გამო არაერთი მომხმარებელი წამოეგო სატყუარას, მათი პირადი ინფორმაცია კი ჩავარდა უცხო პირების ხელში. მავნე კამპანია დღემდე გრძელდება.

SecurityLab.ru by Positive Technologies ars TECHNICA

16 თებერვალი, 2019 წელი

Google Maps-მა ტაივანის საიდუმლო სამხედრო ბაზების ადგილმდებარეობა გამოააშკარავა

ტაივანის ხელისუფლება ცდილობს მიჩქმალოს სამხედრო ობიექტების უსაფრთხოებასთან დაკავშირებული სკანდალი, რომელიც Google maps-ზე ქვეყნის საიდუმლო სამხედრო ბაზების გამოჩენამ გამოიწვია. აპლიკაცია ოთხშაბათს, რუკაზე ტაივანის ოთხი ქალაქის რუკის დამატებით განახლდა. ესენია ტაიპეი, ახალი ტაიპეი, ტაიოუანი და ტაიშუანი

ადგილობრივი მედია იტყობინება, რომ გამოსახულებები ნათლად აჩვენებს საიდუმლო სამხედრო ბაზის ადგილმდებარეობას და ინფრასტრუქტურას (New Taipei) სადაც განლაგებულია საზენიტო-სარაკეტო კომპლექსები პატრიოტი(Patriot), მათ შორის გამშვები მოწყობილობის ტიპს და რაკეტების მოდელს.

Google Maps-მა ასევე გამოააშკარავა ეროვნული უსაფრთხოების ბიუროსა და სამხედრო დაზვერვის ბიუროს დეტალური დაცვითი ინფრასტრუქტურა. ტაივანის თავდაცვის მინისტრის იენ ტეხ-ფას განცხადებით, სამინისტრომ Google-ს გამოსახულების დაფარვის თხოვნით ოფიციალური წერილი გაუგზავნა. მისი თქმით, სამხედრო ბაზების მდებარეობის გამოქვეყნება, სამხედრო ოპერაციების ჩატარებას ხელს ვერ შეუშლის, რადგან "მშვიდობიან პერიოდის დროს ბაზის თავდაცვითი ინფრასტრუქტურა განსხვავდება ომის დროს არსებული ინფრასტრუქტურისგან".

SecurityLab.ru by Positive Technologies MailOnline

18 თებერვალი, 2019 წელი

სმარტფონის უსაფრთხოება

სმარტფონის უსაფრთხოების უზრუნველყოფის აუცილებლობა დღითიდღე იზრდება. გთავაზობთ რამდენიმე რჩევას, რომელიც დაგეხმარებათ თქვენი მცირე მოწყობილობების დაცვაში.

1. გამოიყენეთ დაბლოკვის ფუნქცია (Screen Lock)

თანამდეროვე სმარტფონების დიდ ნაწილს აქვს დაბლოკვის სხვადასხვა ვარიანტები (თითის ანაბეჭდით, სახის ამოცნობით, პაროლით, PIN კოდით, გამოსახულებით და ა.შ.). სახისა და თითის ანაბეჭდით ავთენტიფიკაცია საუკეთესო ვარიანტად გვევლინება, თუმცა, თუკი პაროლზე შეაჩერებთ არჩევანს, გირჩევთ მისი შერჩევისას გამოიყენოთ როგორც ასოები, ასევე ციფრები და შექმნათ რთული კომბინაცია.

2. არ დაუკავშირდეთ უცნობ უკაბელო ქსელებს

უფასო უკაბელო ქსელები ხშირად ჰაკერების მიერ მოწყობილი მახეა. აქედან გამომდინარე, უფრთხილდით ასეთ ქსელებს. გარდა ამისა, ყოველთვის გათიშეთ უკაბელო ქსელთან კავშირი, როდესაც სმარტფონს აღნიშნული მიზნით არ იყენებთ. ამასთანავე, გათიშეთ უკაბელო ქსელთან ავტომატურად დაკავშირების ფუნქციაც.

3. გამოიჩინეთ სიფრთხილე გადმოწერილ ფაილებთან

აპლიკაციების გადმოტვირთვისას ავტომატურად ვდგებით ჩვენ სმარტფონში მავნე პროგრამული უზრუნველყოფის მოხვედრის საფრთხის წინაშე. გადაამოწმეთ ის მოთხოვნები, რომელსაც პროგრამული უზრუნველყოფა გიყენებთ ინსტალაციისას. თუკი რაიმე საეჭვოს ამჩნევთ, უმჯობესია, თავი შეიკავოთ ასეთი აპლიკაციის ჩამოტვირთვისგან.

4. ვებ-საიტების მონახულება

გამოიჩინეთ სიფრთხილე ვებ ბრაუზერში მუშაობისას, ვინაიდან ამ შემთხვევაში მარტივია დაეთანხმოთ ისეთ შეტყობინებებს, რომელსაც გახსნილი ფანჯრები (pop-up) გთავაზობენ. ამის შედეგად შესაძლოა ჩამოტვირთოთ მავნე პროგრამული უზრუნველყოფა, ან თქვენი პერსონალური ინფორმაცია ჰაკერებს გაუზიაროთ.

5. გათიშეთ გეოლოკაცია

სმარტფონების უმრავლესობაში ფოტოს გადაღებისას ავტომატურად ინახება ლოკაციის შესახებ ინფორმაცია, შესაბამისად, მაშინ, როდესაც თქვენ ფოტოებს სოციალურ ქსელზე ტვირთავთ, მესამე პირებს შეუძლიათ ნახონ, თუ კონკრეტულად სად იმყოფებოდით ფოტოს გადაღების მომენტში.

6. ჩატვირთეთ ანტივირუსი

სმარტფონის შესაძლებლობები პერსონალური კომპიუტერისას უტოლდება, შესაბამისად საფრთხეებიც იდენტურია. აქედან გამომდინარე, სმარტფონში ანტივირუსული პროგრამული უზრუნველყოფის არსებობა ძალზედ მნიშვნელოვანია.

სპამ წერილები, რომელსაც სმარტფონის საშუალებით ელ-ფოსტაზე ვხსნით, შესაძლოა შეიცავდეს ისეთ ჩანართებს, რომელიც საფრთხეს წარმოადგენს თქვენი მონაცემების უსაფრთხოებისთვის.

აქვე საყურადღებოა, რომ არსებობს ყალბი ანტივირუსული პროგრამული უზრუნველყოფა, რომელიც რეალურად თქვენს მოწყობილობაზე წვდომის მოსაპოვებლად ინსტალირდება, და არა თქვენს დასაცავად.