საქართველოს თავდაცვის სამინისტრო

სსიპ - კიბერუსაფრთხოების ბიურო

კიბერდაიჯესტი № 2

თბილისი 2018

სარჩევი

ირანელი კიბერჯაშუშების არსენალი გაფართოვდა

ინფორმაციული უსაფრთხოების კომპანია Symantec-ის მკვლევარების განცხადებით, ირანულმა ჰაკერულმა დაჯგუფება “Chafer” გააფართოვა დანაშაულებრივი საქმიანობის არეალი. ჰაკერებმა, აშშ-ს ეროვნული უსაფრთხოების სააგენტოს მიერ შექმნილი ექსპლოიტის EternalBlue-ს გამოყენებით, კიბერშეტევები განახორციელეს რამდენიმე ქვეყნის სხვადასხვა ორგანიზაციაზე. თავდასხმის ობიექტები ისრაელის, იორდანიის, საუდის არაბეთის და თურქეთის სატრანსპორტო და ტელე-საკომუნიკაციო კომპანიები გახდნენ. ასევე აღმოჩენილი იქნა ერთ-ერთ აფრიკულ ავიაკომპანიასა და ავიაბილეთების დაჯავშნის საერთაშორისო კომპანიაზე განხორციელებული კიბერშეტევის კვალი. ჰაკერების ძირითად მიზანს სადაზვერვო ინფორმაციის მოპოვება წარმოადგენდა.

1 მარტი, 2018 წელი

რუსმა ჰაკერებმა გერმანიის სამთავრობო ქსელში შეაღწიეს

გერმანიის სპეცსამსახურებმა ქვეყნის თავდაცვის სამინისტროსა და საგარეო საქმეთა სამინისტროს ქსელში მავნე პროგრამული უზრუნველყოფა აღმოაჩინეს.

გავრცელებული ინფორმაციის თანახმად, ჰაკერებმა შეძლეს კონფიდენციალური დოკუმენტების მითვისება. ინციდენტის გამოძიებას გერმანიის ინფორმაციული უსაფრთხოების ფედერალური სამსახური (BSI) აწარმოებს.

გერმანიის მთავრობის წინააღმდეგ მასშტაბური კიბერშეტევის განხორციელებაში ეჭვმიტანილია რუსეთის სპეცსამსახურების კონტროლქვეშ მოქმედი ჰაკერული დაჯგუფება APT28.

1 მარტი 2018 წელი

აშშ-ს ეროვნული უსაფრთხოების სააგენტოს ხელმძღვანელი არ გამორიცხავს რუსეთის ჩარევას კონგრესის შუალედური არჩევნების პროცესში

აშშ-ს ეროვნული უსაფრთხოების სააგენტოსა და კიბერსარდლობის ხელმძღვანელმა, ადმირალმა მაიკლ როჯერსმა, სენატის შეიარაღებული ძალების საკითხების კომიტეტის

წინაშე გამოსვლისას განაცხადა, რომ მათ არ გააჩნიათ სათანადო უფლებამოსილება რათა წინ აღუდგნენ რუსეთის შესაძლო ჩარევას 2018 წლის 6 ნოემბრისთვის დანიშნული კონგრესის შუალედური არჩევნების პროცესში.

მისი თქმით, გატარებული ღონისძიებები საკმარისი არაა, ხოლო პრეზიდენტმა დ. ტრამპმა მას არ მიანიჭა ჰაკერული ოპერაციების აღსაკვეთად აუცილებელი პრევენციული დარტყმების განხორციელების უფლებამოსილება.

SecurityLab.ru by Positive Technologies The Washington Post 28 თებერვალი, 2018 წელი

საფრანგეთის პოლიციამ კიბერდანაშაულებრივი დაჯგუფება გაანეიტრალა

საფრანგეთის პოლიციამ ევროპოლთან ერთად განხორციელებული ოპერაციის შედეგად 2016 წლიდან მოქმედი კიბერდანაშაულებრივი დაჯგუფება გაანეიტრალა. სამართალდამცავების ინფორმაციით, დამნაშავეების მიერ მიყენებულმა ზარალმა 4.6 მილიონი ევრო შეადგინა.

დაჯგუფების წევრები ახორციელებდნენ მსხვერპლი კორპორაციის ხანგრძლივ შესწავლას და არეგისტრირებდნენ კორპორატიული დომეინის მსგავს დომეინს (მაგ. example.com-ის მაგივრად exampie.com) საიდანაც ორგანიზაციის თანამშრომლები იღებდნენ ფიშინგურ კორესპონდენციას. ორგანიზაციის გენერალური დირექტორის სახელით გაგზავნილ წერილში, დამნაშავეები სთხოვდნენ თანამშრომლებს თანხის სასწრაფოდ გადარიცხვას. ჰაკერების გათვლით თანამშრომლები შეეცდებოდნენ უმოკლეს ვადაში შეესრულებინათ წერილში მითითებული დავალება, მიუხედავად იმისა, რომ აღნიშნული ეწინააღმდეგება კორპორატიულ წესებსა და პოლიტიკას.

ფრანგი სამართალდამცავების განცხადებით, საუბარია სულ მცირე 24 შეტევაზე, რომელმაც კორპორაციას 4.6 მილიონი ევროს ზარალი მიაყენა.

დამნაშავეთა განეიტრალებაში მონაწილეობა მიიღეს ბელგიის, რუმინეთის, ისრაელის და შვეიცარიის გამომძიებლებმა და ექსპერტებმა. გამოძიების ინფორმაციით დაკავებულია 7 პიროვნება, ხოლო დაჯგუფების ლიდერები იმალებიან ისრაელის ტერიტორიაზე.

threatpost EUROPOL 2 მარტი, 2018 წელი

მაღალტექნოლოგიური ტროიანი Android მოწყობილობებს უტევს

კომპანია Symantec-ის სპეციალისტებმა აღმოაჩინეს მავნე პროგრამული უზრუნველყოფა, რომელიც უტევს Android მოწყობილობებს (ტელეფონებს, პლანშეტებს) და ითვისებს მფლობელების სარეგისტრაციო მონაცემებს.

მავნე პროგრამა Fakeapp ვრცელდება დაინფიცირებული აპლიკაციების მეშვეობით, რომლებიც ხელმისაწვდომია GooglePlay-ის ალტერნატიულ ინგლისურენოვან სავაჭრო პლატფორმებზე. მოწყობილობაში მოხვედრის შემდეგ მავნე პროგრამა ხსნის Facebook-ის ყალბ სარეგისტრაციო ფანჯარას და იღებს მფლობელის პირად მონაცემებს. მიღებულ ინფორმაციას პროგრამა ავტომატურად უგზავნის დამნაშავეებს და ახდენს სოციალურ ქსელში ავტორიზაციას.

აღნიშნული მავნე პროგრამული უზრუნველყოფის ქცევა არ არის დამახასიათებელი ასეთი ტიპის ვირუსებისთვის, რადგანაც მიღებული ინფორმაცია ამ ეტაპზე არ გამოიყენება ფინანსური მანიპულაციებისთვის და სპამის გავრცელებისთვის, არამედ მიმდინარეობს მხოლოდ ანგარიშის მფლობელის მონაცემების - ძებნის ისტორიის, კონტაქტების სიის, მეგობრებისა და ნათესავების შესახებ ინფორმაციის და სხვა შეგროვება.

სპეციალისტების აზრით, სავარაუდოდ დამნაშავეები შემდგომი შეტევების განსახორციელებლად ქმნიან მონაცემთა ბაზას.

threatpost BLEEPINGCOMPUTER

6 მარტი, 2018 წელი

იაფფასიან ჩინურ სმარტფონებში აღმოჩენილია წინასწარ ჩაშენებული მავნე პროგრამული უზრუნველყოფა

კომპანია Dr.Web-ის სპეციალისტებმა 42 დასახელების იაფფასიან სმარტფონში აღმოაჩინეს წინასწარ ჩაშენებული Android ტროიანი სახელწოდებით Triada, რომელიც აზიანებს და ცვლის სისტემურ პროცესებს და განკუთვნილია ფინანსური ინფორმაციის მითვისებისთვის. მავნე პროგრამის წაშლა შესაძლებელია მხოლოდ ოპერაციული სისტემის გადაყენების გზით.

კომპანიის სპეციალისტებმა მავნე პროგრამა აღმოაჩინეს ნაკლებად ცნობილი ჩინური წარმოების ახალ იაფფასიან მოწყობილობებში - Leagoo, Doogee, Vertex, Advan, Cherry Mobile, STF.

ექსპერტების ვარაუდით დაინფიცირების წყაროს წარმოადგენს ქ. შანხაიში არსებული პროგრამული უზრუნველყოფის მწარმოებელი კომპანია.

დაინფიცირებული სმარტფონების მიწოდება ხორციელდება რუსეთში, პოლონეთში, ჩეხეთში, სერბეთში, ყაზახეთში, ინდონეზიასა და მექსიკაში.

threatpost 6 მარტი, 2018 წელი

რუსეთის უშიშროების ფედერალურმა სამსახურმა კრიტიკული ინფორმაციული ინფრასტრუქტურის ობიექტებზე განხორციელებული კიბერშეტევის შეტყობინების წესი შეიმუშავა

რუსეთის ფედერალური უშიშროების სამსახურმა მოამზადა ბრძანების პროექტი, კრიტიკული ინფრასტრუქტურის ობიექტებზე განხორციელებული კიბერშეტევის შეტყობინების წესის შესახებ.

პროექტის თანახმად, კომპიუტერული ინციდენტის შემთხვევაში კრიტიკული ინფორმაციული ინფრასტრუქტურის ობიექტები ვალდებულნი არიან აღნიშნულის შესახებ, ნებისმიერი გზით, დაუყოვნებლივ შეატყობინონ კომპიუტერული ინციდენტების ეროვნულ საკოორდინაციო ცენტრს. იმ შემთხვევაში თუ ინციდენტი შეეხო საბანკო და ფინანსური სფეროს ობიექტებს, აუცილებელია რუსეთის ეროვნული ბანკის ინფორმირებაც.

დოკუმენტი ავალდებულებს კრიტიკული ინფორმაციული ინფრასტრუქტურის ობიექტებს, შეიმუშაონ კომპიუტერულ ინციდენტებზე რეაგირების გეგმა, მიიღონ კიბერშეტევების შედეგების განეიტრალებისთვის საჭირო ზომები და სულ მცირე წელიწადში ერთხელ ჩაატარონ შესაბამისი წვრთნები.

SecurityLab.ru by Positive Technologies 12 მარტი, 2018 წელი

ჩინელმა ჰაკერებმა 5 მილიონი Android მოწყობილობისგან შემდგარი ბოტნეტი შექმნეს

ჩინელმა კიბერდამნაშავეებმა მავნე პროგრამულ უზრუნველყოფა „RottenSys“ ბოტნეტის შესაქმნელად გამოიყენეს, რომელიც ამ დროისთვის 5 მილიონი Android მოწყობილობისგან შედგება.

დღეისათვის „RottenSys“ ძირითადად დაინფიცირებული მოწყობილობის ეკრანზე სარეკლამო ხასიათის მასალების ასახვისთვის გამოიყენება, თუმცა სპეციალისტების

განცხადებით, ბოტნეტი კიბერდამნაშავეებს გაცილებით ფართო შესაძლებლობებს აძლევს. აღნიშნულ ბოტნეტს შეუძლია მოწყობილობაზე დამატებითი აპლიკაციების ფარულად ინსტალირება და სამომხმარებლო ინტერფეისის ავტომატიზაცია.

ამ ეტაპზე მავნე პროგრამა აქტუალურია ჩინურ ბაზარზე და ვრცელდება დაინფიცირებული ჩინური აპლიკაციების მეშვეობით. ბოტნეტის უდიდეს ნაწილს დღეისათვის Huawei-ის მოწყობილობები შეადგენენ (1 მილიონზე მეტი).

SecurityLab.ru by Positive Technologies CHECK POINT RESEARCH

15 მარტი, 2018 წელი

სოციალური ქსელი Twitter კრიპტოვალუტის რეკლამირების აკრძალვას აპირებს

სოციალური ქსელი Twitter კრიპტოვალუტისა და სხვა ციფრული ვალუტის სარეკლამო ბანერების განთავსების აკრძალვას გეგმავს. გავრცელებული ინფორმაციით, აკრძალვა შეეხება კრიპტოვალუტით ვაჭრობასთან დაკავშირებულ ყველა სახის სარეკლამო მასალას, მათ შორის კრიპტოსავალუტო ბირჟებსაც.

ICTONLINE sky news

19 მარტი, 2018 წელი

რუსეთის საპრეზიდენტო არჩევნების მსვლელობისას კიბერშეტევები განხორციელდა

რუსეთის ცენტრალური საარჩევნო კომისიის თავმჯდომარის ელა პანფილოვას განცხადებით, 2018 წლის 18 მარტს ღამის 2 საათიდან 5 საათამდე მიმდინარეობდა DDoS შეტევა კომისიის ვებ-გვერდზე, რომლის მიზანსაც პორტალის მწყობრიდან გამოყვანა წარმოადგენდა. შეტევისას გამოყენებული იქნა 15 ქვეყნის IP მისამართები.

რუსეთის შინაგან საქმეთა მინისტრის პირველი მოადგილის განცხადებით, შესაბამისი სტრუქტურების დროული მოქმედების შედეგად შესაძლებელი გახდა შეტევის მოგერიება საარჩევნო პროცესზე ზიანის მიყენების გარეშე.

ოფიციალური პორტალის გარდა შეტევა მიმდინარეობდა საარჩევნო კომისიის საინფორმაციო ცენტრსა და საზოგადოებრივი პალატის პორტალზე.

threatpost

19 მარტი, 2018 წელი

მსხვილი Online ტურისტული სააგენტოდან მომხმარებელთა პირადმა მონაცემებმა გაჟონა

ამერიკული ტურისტული სააგენტო Expedia-ს შვილობილი კომპანია Orbitz მონაცემთა გაჟონვის მსხვერპლი გახდა. განხორციელებული კიბერშეტევის შედეგად დამნაშავეებმა 880 ათასი საბანკო ბარათის მონაცემი და მომხმარებელთა პერსონალური ინფორმაცია მიითვისეს.

ინციდენტის გამოძიების შედეგად დადგინდა, რომ ჰაკერებმა მოიპოვეს წვდომა 2016 წლის იანვრიდან 2017 წლის დეკემბრის ჩათვლით პერიოდში კლიენტების მიერ განხორციელებულ შესყიდვებთან დაკავშირებულ ინფორმაციაზე.

დამნაშავეებმა შეძლეს მიეთვისებინათ მონაცემები, რომლებიც შეიცავდა კლიენტთა სახელებს, ტელეფონის ნომრებს, ელექტრონულ მისამართებს და საგადახდო ანგარიშებს.

SecurityLab.ru by Positive Technologies REUTERS

20 მარტი, 2018 წელი

ევროპოლმა კიბერდამნაშავეთა მორიგი დაჯგუფება დააკავა

რუმინეთის და იტალიის პოლიციამ ევროპოლთან ერთად გამოაქვეყნა ანგარიში 2 წლიანი გამოძიების დასრულების შესახებ, რომლის შედეგადაც მასშტაბურ კიბერდანაშაულში ეჭვმიტანილი 20 პიროვნება დააკავეს.

სამართალდამცავების ინფორმაციით დამნაშავეებმა 2 მსხვილი საკრედიტო ორგანიზაციის ასეულობით საბანკო ანგარიშიდან 1 მილიონი ევროს მითვისება შეძლეს.

2018 წლის 28 მარტს რუმინეთსა და იტალიაში ჩატარებული საპოლიციო ოპერაციის შედეგად დააკავეს რუმინეთში 9 და იტალიაში 11 ეჭვმიტანილი.

ევროპოლის მიერ გავრცელებული ინფორმაციის თანახმად კიბერდამნაშავეები იყენებდნენ ფიშინგს, კერძოდ საგადასახადო ორგანოების სახელით აგზავნიდნენ ინდივიდუალურ წერილებს, რომელიც ახდენდა მსხვერპლის გადამისამართებას უწყების ოფიციალური ვებ-გვერდის მსგავს საიტზე. გახსნილ გვერდზე მომხმარებლის მიერ მონაცემების შეყვანის შემდგომ ხდებოდა თანხების გადარიცხვა დამნაშავეთა ანგარიშებზე.

ამ მომენტისთვის ინფორმაცია შემდგომი საგამოძიებო მოქმედებებისა და დამნაშავეთა მიმართ გამოყენებული სასჯელის ზომის შესახებ არ ვრცელდება.

threatpost EUROPOL

29 მარტი 2018 წელი

აშშ და დიდი ბრიტანეთი რუსეთს მასშტაბური კიბერჯაშუშური კამპანიის წარმოებაში ადანაშაულებენ

დიდი ბრიტანეთის ეროვნული კიბერუსაფრთხოების ცენტრის (NCSC), აშშ-ს გამოძიების ფედერალური ბიუროს და შიდა უსაფრთხოების დეპარტამენტის ერთობლივი განცხადების თანახმად, რუსეთის ხელისუფლების კონტროლქვეშ მოქმედმა ჰაკერებმა, კიბერჯაშუშური კამპანიის ფარგლებში, მსოფლიოს მასშტაბით დააინფიცირეს მილიონობით როუტერი.

სპეცსამსახურების მონაცემებით ჰაკერების სამიზნეს წარმოადგენენ სამთავრობო დაწესებულებები, მსხვილი კომპანიები და კრიტიკული ინფრასტრუქტურის ობიექტები. რუსეთის ხელისუფლების მიერ დაფინანსებული ჰაკერები, დაგეგმილი კიბერშეტევების განხორციელების მიზნით, ცდილობენ დაეუფლონ საჭირო ინტერნეტ მოწყობილობებს.

გავრცელებულ ინფორმაციას გამოეხმაურა რუსეთის საელჩო დიდ ბრიტანეთში, რომლის პრეს-მდივნის განცხადებით, აღნიშნული წარმოადგენს ბოლო დროს რუსეთის წინააღმდეგ დიდი ბრიტანეთის მიერ წარმოებული საშიში რიტორიკის გაგრძელებას.

REUTERS ICTONLINE

17 აპრილი, 2018 წელი

რუსეთში მესენჯერ „Telegram"-თან ბრძოლის ფარგლებში 15 მილიონამდე IP მისამართი დაიბლოკა

რუსეთის მოსახლეობას მესენჯერ „Telegram"-ზე წვდომა მას შემდეგ დაებლოკა, რაც აპლიკაციის შემქმნელებმა ქვეყნის მთავრობას უარი განუცხადეს დაშიფრულ ინფორმაციასთან დაშვებაზე. მესენჯერთან ბრძოლის ფარგლებში დაიბლოკა 15 მილიონამდე Amazon-ისა და Google-ის IP მისამართი.

ტელეგრამის აღმასრულებელმა დირექტორმა პაველ დუროვმა განაცხადა, რომ მიუხედავად ინტერნეტ და მედია რეგულირების უწყების მოთხოვნისა, Apple, Google, Amazon და Microsoft არ ჩაერთნენ მათ წინააღმდეგ მიმართულ კამპანიაში.

ტელეგრამის მაგალითი რუსეთში არ წარმოადგენს შეზღუდვების დაწესების პირველ შემთხვევას. კერძოდ, აპლიკაცია „Zello"-ს ინტერნეტ-რეგულირების უწყებამ შეატყობინა, რომ ის აუცილებლად დაიბლოკებოდა, თუ მფლობელები საუბრის ჩაწერას და მთავრობისთვის გადაცემას არ უზრუნველყოფდნენ. ზეწოლის მიუხედავად, Zello-მ IP მისამართების უცხოურ სერვერზე გადამისამართება შეძლო და მისი დაბლოკვა ჯერ არ მომხდარა. აღანიშნავია რომ ამ აპლიკაციას 200 000 მომხმარებელი ჰყავს ქვეყანაში, მაშინ, როცა ტელეგრამს რუსეთსა და ახლო აღმოსავლეთში 200 მილიონზე მეტი.

შეზღუდვების მიუხედავად, მესენჯერის მომხმარებელთა რიცხვი მნიშვნელოვნად არ შემცირებულა, ვინაიდან აკრძალვებს გვერდის ავლა შესაძლებელია VPN-ის გამოყენებით. კომპანია Google-ისა და Amazon-ის წარმომადგენლები აღნიშნულზე კომენტარს ჯერ-ჯერობით არ აკეთებენ.

18 აპრილი, 2018 წელი

რუსეთში შესაძლოა Facebook დაიბლოკოს

რუსეთის კომუნიკაციების ზედამხედველმა უწყებამ (Роскомнадзор) შესაძლოა Facebook დაბლოკოს, თუკი სოციალური ქსელი არ დააკმაყოფილებს ქვეყნის კანონმდებლობის მოთხოვნებს და არ განახორციელებს რუსეთის მოქალაქეების მონაცემთა ბაზების განთავსებას რუსეთის ტერიტორიაზე.

უწყების განცხადებით, 2018 წლის ბოლომდე კომპანია „Facebook"-ი საფუძვლიანად შემოწმდება. შემოწმების პროცესში უწყება აპირებს მომხმარებელთა ბაზის გამოთხოვას, გარკვეული კონტენტის ამოშლას და რიგი შეზღუდვების დაწესებას. მოთხოვნების შეუსრულებლობის შემთხვევაში, სოციალური ქსელი შესაძლოა დაიბლოკოს.

18 აპრილი, 2018 წელი