საქართველოს თავდაცვის სამინისტრო

სსიპ - კიბერუსაფრთხოების ბიურო

კიბერდაიჯესტი № 1

თბილისი 2018

სარჩევი

ევროპოლმა მავნე პროგრამა Luminosity link rat გაანეიტრალა

ბრიტანეთის კრიმინალთან ბრძოლის ეროვნული სააგენტოს და ევროპოლის კიბერდანაშაულთან ბრძოლის ცენტრის ერთობლივი წარმატებული მუშაობის შედეგად განეიტრალებულ იქნა მავნე პროგრამა Luminosity link rat. პროგრამის გამოყენებით შესაძლებელი იყო მსხვერპლის კომპიუტერზე არასანქცირებული კონტროლის მოპოვება. ოპერაციის მსვლელობისას, რომელშიც მონაწილეობდნენ აშშ-ს, ავსტრალიის და ევროპის სხვადასხვა ქვეყნის სამართალდამცავი უწყებების წარმომადგენლები, დაკავებული იქნენ მავნე პროგრამის მომხმარებლები და გამავრცელებლები.

კიბერკრიმინალებმა მავნე პროგრამა 78 ქვეყანაში 8600 მომხმარებელზე გაყიდეს, მავნე პროგრამის ფასი 40 ევროს შეადგენდა.

სამართალდამცველების წარმატებული მუშაობის შედეგად დაზარალებულების პერსონალური ინფორმაცია (პაროლები, სურათები, ვიდეო, აუდიო) იდენტიფიცირებულია.

EUROPOL

5 თებერვალი 2018 წელი

ჩინეთი კრიპტოვალუტის უცხოური ბირჟების შეზღუდვას გეგმავს

ჩინეთის ცენტრალური ბანკის განცხადებით, ქვეყანაში აიკრძალება კრიპტოვალუტის ადგილობრივი და საერთაშორისო სავაჭრო ბირჟები. ექსპერტების განცხადებით, მიუხედავად იმისა, რომ მსგავსი გადაწყვეტილება ჩინეთს ადრეც ჰქონდა მიღებული, ახალი აკრძალვა უფრო ხისტი იქნება.

შეზღუდვის მიხედვით, ქვეყანაში კრიპტოვალუტის გადახდის სისტემებიც აიკრძალება. აღნიშნული განცხადების შემდგომ ჩინეთის უმსხვილესმა საძიებო სისტემა Baidu-მ და სოციალურმა ქსელმა Weibo-მ შეწყვიტეს კრიპტოვალუტასთან დაკავშირებული პროექტების რეკლამირება.

BUSINESS INSIDER

5 თებერვალი 2018 წელი

მავნე პროგრამა ADB.miner ჭკვიან გაჯეტებს კრიპტოვალუტის მოსაპოვებლად იყენებდა

კომპანია QiHo 360-ის ექსპერტებმა ვებ-სივრცეში მავნე პროგრამა ADB.miner აღმოაჩინეს, რომლის გამოყენებით შესაძლებელი იყო მონეროს ტიპის კრიპტოვალუტის არასანქცირებული მოპოვება. ბოტნეტი მირაის ბაზაზე აგებული მავნე პროგრამა საფრთხეს უქმნის Android-ის ოპერაციულ სისტემაზე მომუშავე ყველა მოწყობილობას.

კომპანიის განცხადებით ADB.miner-ის აქტივობის შედეგად უმეტესად ჩინეთსა და სამხრეთ კორეაში არსებული 7400 მოწყობილობა დაინფიცირდა.

PAYSPACE MAGAZINE 7 თებერვალი 2018 წელი

AnonPlus-ის ჰაქტივისტებმა ვებ სივრცეში 2653 იტალიელი პოლიტიკოსის პერსონალური მონაცემები გამოაქვეყნეს

ჰაქტივისტების მიერ გამოქვეყნებული ბაზა იტალიის დემოკრატიული პარტიის წევრების ელექტრონული ფოსტის მისამართებს, ტელეფონის ნომრებს და სხვა სახის სენსიტიურ ინფორმაციას შეიცავს. დაზარალებულებს შორის არიან ფლორენციის მერი დარიო ნარდელა და დემოკრატიული პარტიის ლიდერი მატეო რენცი.

აღსანიშნავია, რომ კვალის დაფარვის მიზნით ჰაქტივისტებმა გერმანული IP მისამართი გამოიყენეს.

AnonPlus-ის ჰაქტივისების განცხადებით ისინი არ თანამშრომლობენ დაჯგუფება Anonymous-თან და არ არიან დაკავშირებული რომელიმე პოლიტიკურ პარტიასთან.

SecurityLab.ru by Positive Technologies THE TIMES 8 თებერვალი 2018 წელი

აშშ-ს სპეცსამსახურები თაღლითობის მსხვერპლნი გახდნენ

რამდენიმე თვიანი საიდუმლო მოლაპარაკებების შედეგად აშშ-ს სპეცსამსახურების თანამშრომლები ბერლინში რუსი ჰაკერის კვალზე გავიდნენ, რომელიც მათ 1 მილიონი დოლარის სანაცვლოდ, 2016 წელს ეროვნული უსაფრთხოების სააგენტოზე განხორციელებული კიბერშეტევის შედეგად მოპარული ე.წ. კიბერ-იარაღის დაბრუნებასა და დ.ტრამპის მაკომპრომეტირებელი მასალების გადაცემას დაპირდა.

მოთხოვნილი თანხის ნაწილის (100 ათასი დოლარი) გადახდის მიუხედავად სპეცსამსახურის წარმომადგენლებმა დაპირებული მასალები ვერ მიიღეს, რის შემდეგაც აღნიშნულ პიროვნებასთან თანამშრომლობა შეწყვიტეს.

The New York Times SecurityLab.ru by Positive Technologies 9 თებერვალი 2018 წელი

სამხრეთ კორეაში მიმდინარე ზამთრის ოლიმპიადის გახსნისას სერვერებზე კიბერშეტევა განხორციელდა

9 თებერვალს განხორციელებული კიბერშეტევის შედეგად ზამთრის ოლიმპიადის ოფიციალური ვებ-გვერდი 12 საათის განმავლობაში მიუწვდომელი იყო, შეუძლებელი გახდა ელექტრონულად ბილეთების შეძენა, ოლიმპიურ სტადიონზე გაითიშა Wifi, ხოლო მთავარ პრეს-ცენტრში ტელევიზია და ინტერნეტი.

ინფორმაციული უსაფრთხოების ექსპერტების ვარაუდით, შესაძლოა კიბერშეტევა რუსეთმა განახორციელა, ოლიმპიური კომიტეტის მიერ თამაშებზე რუსეთის ნაკრების არ დაშვების გამო.

CSO SecurityLab.ru 12 თებერვალი 2018 წელი

ჰაკერებმა კრიპტოვალუტის მოპოვების მიზნით დიდი ბრიტანეთის 4000-ზე მეტი სამთავრობო ვებ-გვერდი გატეხეს

კრიპტოვალუტის უკანონო მოპოვების მიზნით ჰაკერებმა დიდი ბრიტანეთის სამთავრობო ვებ-გვერდები გატეხეს და საიტების ვიზიტორების მოწყობილობების სიმძლავრეს არასანქცირებულად იყენებდნენ. გავრცელებული ინფორმაციით კიბერკრიმინალებმა სულ 4 000-ზე მეტი სამთავრობო ვებგვერდი დააინფიცირეს. ოფიციალური პირების განცხადებით, პრობლემის მოსაგვარებლად მუშაობა აქტიურად მიმდინარეობს.

ZDNet 12 თებერვალი 2018 წელი

გერმანიის სასამართლომ Facebook-ი დამნაშავედ სცნო

მომხმარებელთა უფლებების დაცვის ორგანიზაციის (Der Verbraucherzentrale Bundesverband, vzbv) განცხადებით, სოციალურ ქსელ Facebook-ში არსებული პერსონალური მონაცემების დამუშავების პარამეტრები არღვევს გერმანიის კანონმდებლობას, რის გამოც მათ სასამართლოში შესაბამისი სარჩელი შეიტანეს.

სასამართლოს გადაწყვეტილებით სოციალურ ქსელს დაეკისრა პასუხისმგებლობა პერსონალური ინფორმაციის დამუშავებისას გერმანიაში დადგენილ სტანდარტებთან შეუსაბამობის გამო.

THE VERGE 12 თებერვალი 2018 წელი

უკრაინაში სახელმწიფო უნივერსიტეტის თანამშრომელი სამსახურში კრიპტოვალუტის უკანონო მოპოვების გამო დააკავეს

უკრაინის კიბერპოლიციის განცხადებით, ქალაქ ლუცკის სახელმწიფო უნივერსიტეტის თანამშრომელმა უმაღლესი სასწავლებლის რამდენიმე ოთახი კრიპტოვალუტის არასანქცირებული მოპოვებისათვის საჭირო მოწყობილობებით აღჭურვა. კერძოდ, ელექტროენერგიასა და ინტერნეტზე თანხის დაზოგვის მიზნით მძლავრი ვიდეოდაფები საკუთარ სამსახურში განათავსა. გარდა აღნიშნულისა, კიბერკრიმინალი რეალიზაციის მიზნით პერსონალური მონაცემების მითვისებით იყო დაკავებული.

SecurityLab.ru by Positive Technologies

12 თებერვალი 2018 წელი

რუსეთის ფედერაციის ცენტრალური ბანკი ფინანსური ორგანიზაციების კიბერუსაფრთხოების ცენტრს ქმნის

რუსეთის ცენტრალური ბანკის თავმჯდომარის მოადგილემ, დიმიტრი სკობელკინმა ურალის კიბერუსაფრთხოების ფორუმზე განაცხადა, რომ ცენტრალური ბანკი ინფორმაციული უსაფრთხოების დეპარტამენტის შექმნაზე მუშაობს. კიბერუსაფრთხოების კუთხით ფინანსური და საკრედიტო სფეროს მდგრადობის უზრუნველყოფის მიზნით დეპარტამენტს ცენტრის სტატუსი მიენიჭება. კიბერშეტევების პრევენციის გარდა, ორგანიზაციის მიზანი კომპიუტერული შეტევების აღმოჩენისა და შედეგების ლიკვიდაციის სახელმწიფო სისტემასთან(ГосСОПКА) მონაცემების გაცვლა იქნება.

რუსეთის ცენტრალურ ბანკს, ГосСОПКА-სთვის ინფორმაციის მიწოდებას კრიტიკული ინფრასტრუქტურის შესახებ კანონი ავალდებულებს.

SecurityLab.ru by Positive Technologies

13 თებერვალი 2018

რუსეთის თავდაცვის სამინისტრო სამხედრო მოსამსახურეებს სოციალური ქსელის გამოყენებისგან თავის შეკავებას ურჩევს

რუსეთის თავდაცვის სამინისტროს რეკომენდაციების თანახმად, არ არის მიზანშეწონილი სამხედრო მოსამსახურეების მიერ საკუთარი და თანამშრომლების შესახებ პერსონალური ინფორმაციის, საქმიანობის სფეროს, გეოლოკაციის, ვიდეო-ფოტო მასალების და სხვა სენსიტიური ინფორმაციის სოციალურ ქსელში გამოქვეყნება. რეკომენდაციები სამხედრო მოსამსახურეთა ოჯახის წევრების მიმართ სხვადასხვა ინფორმაციული უსაფრთხოების რჩევებსაც ითვალისწინებს. გარდა ამისა თავდაცვის სამინისტრო პერსონალს მოუწოდებს, არ გამოიყენონ მარტივი პაროლები და უსაფრთხოების მიზნით მუდმივად განაახლონ აპლიკაციები.

აღნიშნული პაკეტი 2017 წლის ბოლოს შემუშავდა და ამ ეტაპზე სარეკომენდაციო ხასიათს ატარებს, თუმცა, უახლოეს მომავალში შესაძლოა იგი სავალდებულო გახდეს, რადგანაც თავდაცვის უწყებამ უკვე შეიმუშავა საკანონმდებლო ცვლილებების პროექტი.

SecurityLab.ru by Positive Technologies

13 თებერვალი 2018

აშშ-ს ცენტრალური სადაზვერვო სააგენტო მოქალაქებს კომპანია Huawei-ის პროდუქციის გამოყენებისგან თავის შეკავებას ურჩევს

აშშ-ის ცენტრალური სადაზვერვო სააგენტოს (CIA), გამოძიების ფედერალური ბიუროს (FBI) და ეროვნული უსაფრთხოების სააგენტოს (NSA) მაღალჩინოსნებმა სენატში გამართულ მოსმენაზე განაცხადეს, რომ ჩინური მწარმოებლების მიერ დამზადებული სმარტფონები ქვეყნის უსაფრთხოებისთვის პოტენციურ რისკს წარმოადგენს. FBI-ის დირექტორის კრისტოფერ ვრეის განცხადებით, სმარტფონების საშუალებით ჩინეთს ამერიკის მოქალაქეთა თვალთვალი შეუძლია. საუბარია Huawei-ს, ZTE-სა და სხვა მწარმოებლების სმარტფონებზე. ვრეიმ სენატორ ტიმ კოტონის კითხვაზე განაცხადა, რომ ის არცერთ ამერიკულ კომპანიას თუ ფიზიკურ პირს არ ურჩევდა ამ მწარმოებლების მიერ დამზადებული სმარტფონების შეძენას.

The Register

14 თებერვალი 2018

დიდმა ბრიტანეთმა ოფიციალური რუსეთი მავნე პროგრამა NoTpetya-ს გავრცელებაში დაადანაშაულა

დიდი ბრიტანეთის თანამეგობრობისა და გაეროს საკითხებში სახელმწიფო მინისტრის ტარიკ მუჰამედის განცხადებით, რუსი სამხედროები 2017 წლის ივლისში აქტიურად იყვნენ ჩართულნი მავნე პროგრამა NoTpetya-ს გავრცელებაში. გარდა ამისა განცხადებაში საუბარია, რომ დიდი ბრიტანეთი აქტიურად მოქმედებს კიბერსაფრთხეების წინააღმდეგ, რაც ბრიტანეთის წინააღმდეგ კიბერშეტევების განხორციელების ნებისმიერი წყაროს ნეიტრალიზებას გულისხმობს.

The Register

15 თებერვალი 2018

FedEx-ის 119 000 მომხმარებლის მონაცემები Amazon-ის დაუცველ სერვერზე ინახებოდა

Kromtech Security Center-ის მკვლევარებმა ამაზონის S3 ტიპის დაუცველ სერვერზე აშშ-ს, მექსიკის, კანადის, ავსტრალიის, საუდის არაბეთის, იაპონიის, ჩინეთის და რამდენიმე ევროპული ქვეყნის FedEx-ის მომხმარებლების პერსონალური ინფორმაცია აღმოაჩინეს. მკვლევარების განცხადებით სერვერი Bonogo International-ს ეკუთვნოდა, რომელიც FedEx-ის

დაქვემდებარების ქვეშ ოპერირებს. მისი მთავარი ფუნქცია ლოგისტიკა და ვალუტის კონვერტაციაა.

GIZMODO 15 თებერვალი 2018

მიუნჰენის უსაფრთხოების 54-ე კონფერენციის ფარგლებში კიბერუსაფრთხოება ერთ-ერთ მთავარ გამოწვევად დასახელდა

გაეროს გენერალური მდივნის ანტონიუ გუტერეშის განცხადებით, კიბერუსაფრთხოება თანამედროვეობის ერთ-ერთ უმთავრეს გამოწვევას წარმოადგენს. მისი თქმით, სერიოზულ პრობლემებს აღნიშნული სფეროს რეგულაციის სამართლებრივი ბაზის არ ქონა იწვევს. კრიმინალები და ტერორისტული ორგანიზაციები მათი მიზნების მისაღწევად სულ უფრო ხშირად იყენებენ თანამედროვე ტექნოლოგიებს, ხოლო სახელმწიფოები ერთმანეთს კიბერსივრცეში მუდმივად უპირისპირდებიან. მდივანი იმედოვნებს, რომ სფეროს საერთაშორისო რეგულაციების შექმნის მიზნით დაიწყება აქტიური თანამშრომლობა კერძო და საჯარო სექტორს შორის.

კონფერენციის ფარგლებში საკუთარი აზრი გამოთქვა გერმანიის თავდაცვის მინისტრმაც, რომელმაც აღნიშნა, რომ ამ ათწლეულში კიბერუსაფრთხოების და ინფორმაციის დაცვის მექანიზმების სრულყოფას განსაკუთრებული ყურადღება მიექცევა.

Новости ООН SecurityLab.ru 16 თებერვალი 2018