საქართველოს თავდაცვის სამინისტრო

სსიპ - კიბერუსაფრთხოების ბიურო

კიბერდაიჯესტი № 4

თბილისი 2019

სარჩევი

ბოროტმოქმედებმა ASUS-ის განახლებებში ბექდორის ჩატვირთვა შეძლეს

„კასპერსკის ლაბორატორიის“ სპეციალისტები იუწყებიან, რომ დაჯგუფებამ „ShadowHammer“, Asus Live Update-ში(რომელიც BIOS-ის, UEFI-ს და პროგრამული უზრუნველყოფის განახლებების მიწოდებაზეა პასუხისმგებელი) ბექდორის ჩატვირთვა შეძლო. კომპანიის მონაცემებით, აღნიშნული ინციდენტის მსხვერპლი შესაძლოა 2 მილიონამდე მომხმარებელი გამხდარიყო.

მიუხედავად იმისა, რომ უცნობია, რამდენმა მომხმარებელმა ჩამოტვირთა Asus Live Update ჩაშენებული ბექდორით, კასპერსკის ლაბორატორიის ინფორმაციით, 57 000 მომხმარებელმა ის ნამდვილად დააინსტალირა საკუთარ კომპიუტერში.

არსებული ინფორმაციით, კიბერკრიმინალებისთვის მნიშვნელოვანი იყო კონკრეტული 600 MAC მისამართი. თუკი შესაბამისი მოწყობილობის მისამართი აღნიშნულ სიაში არ იყო, ამ შემთხვევაში, მოწყობილობაზე მავნე ზემოქმედება არ განხორციელდებოდა. სწორედ ამიტომ, ეს კიბერშეტევა დიდი ხნის განმავლობაში იყო შეუმჩნეველი.

2019 წლის 26 მარტს კომპანიამ ASUS გამოუშვა განახლება, რომელიც არის მოდიფიცირებული და მომხმარებლებს დაიცავს კიბერშეტევისგან.

SecurityLab.ru by Positive Technologies MOTHERBOARD

25 მარტი, 2019 წელი

ბენზინგასამართი სადგურები კვლავ წარმოადგენს კიბერკრიმინალების სამიზნეს

პარიზსა და მის შემოგარენში ბენზინგასამართი სადგურების ქსელი “Total” კიბერკრიმინალების მსხვერპლი გახდა და 120 000 ლიტრზე მეტი საწვავის ზარალი განიცადა.

გავრცელებული ინფორმაციის თანახმად, ინტერნეტით ნაყიდი სპეციალური მოწყობილობის საშუალებით, კრიმინალებმა შეძლეს საწვავის ტუმბოების განბლოკვა, რომელზეც დაყენებული იყო პირველად PIN კოდი - 0000, ხოლო შემდეგ შეცვალეს საწვავის ფასი და მოხსნეს საწვავის გაშვების შეზღუდვა.

თაღლითები მოქმედებდნენ 2-3 კაციანი ჯგუფებით, რომელიც სადგურზე მიდიოდა 2 ავტომობილით. პირველი გუნდი ახდენდა მოწყობილობების განბლოკვას, ხოლო მეორე ავსებდა უზარმაზარ რეზერვუარს, რომელიც განთავსებული იყო ავტომობილებში. თითოეულ რეზერვუარს ისინი ავსებდნენ 2000-3000 ლიტრი საწვავით, რომელსაც მოგვიანებით სოციალურ ქსელში ყიდიდნენ სტანდარტულზე დაბალ ფასად. ამგვარი გზით დაჯგუფება დაეუფლა 150 000 ევროს.

სქემა მას შემდეგ გაიშიფრა, როდესაც 2018 წლის აპრილში დაჯგუფების 1 წევრი დააკავეს, ხოლო 1 წლის შემდეგ, 2019 წელს, დანარჩენი 5.

აღსანიშნავია, რომ ცოტა ხნის წინ აშშ-ს ქალაქ დეტროიტში, ორმა უცნობმა პირმა მიითვისა 2300 ლიტრი ბენზინი, სპეციალურ მოწყობილობაზე წვდომის მოპოვების საშუალებით.

SecurityLab.ru by Positive Technologies ZDNet

28 მარტი, 2019 წელი

ირანელი კიბერჯაშუშები აშშ-სა და საუდის არაბეთის კომპანიებს ესხმიან თავს

ბოლო 3 წელიწადია ირანის მთავრობის მიერ დაფინანსებული კიბერჯაშუშური დაჯგუფება Elfin (ასევე ცნობილი როგორც APT33), აქტიურად ესხმის თავს აშშ-სა და საუდის არაბეთის ორგანიზაციებს.

კომპანიის Symantec სპეციალისტების ინფორმაციის თანახმად, დაჯგუფების მსხვერპლი სხვადასხვა სფეროს წარმომადგენლები გახდნენ. დაჯგუფება დაინტერესებულია სამთავრობო სექტორით, საგამოძიებო ორგანოებით, საკონსულტაციო კომპანიებით, საფინანსო და სატელეკომუნიკაციო დაწესებულებებით.

ამ პერიოდში დაჯგუფების მსხვერპლი 18 ამერიკული ორგანიზაცია გახდა. ბოლო შეტევა განხორციელდა ამა წლის თებერვალში. მათ სცადეს გამოეყენებინათ არქივატორის WinRAR სისუსტე, რომელიც ფაილებისა და სხვადასხვა კოდების ჩატვირთვის საშუალებას იძლეოდა.

შეტევის ინსტრუმენტად უმეტესად გამოიყენება ფიშინგ-წერილები. ამასთანავე, დაჯგუფება იყენებს სხვადასხვა ბექდორს, რომელიც მოიპოვებს წვდომას ფაილებზე. შეტევის ინსტრუმენტების დიდი ნაწილი შემუშავებულია თავად დაჯგუფების მიერ, ხოლო ნაწილი ნაყიდია შავ ბაზარზე, მათ შორის ტროიანები: Remcos, DarkComet, Quasar RAT და ა.შ.

კომპანია Symantec განცხადებით, აღნიშნული დაჯგუფების მიერ განხორციელებული შეტევების ხასიათიდან გამომდინარე, შესაძლოა დაჯგუფება მოქმედებს ცნობილ Shamoon-თან ერთად, რომელიც 2018 წლის დეკემბერში ენერგო-სექტორს დაესხა თავს.

SecurityLab.ru by Positive Technologies SECURITY WEEK

28 მარტი, 2019 წელი

უკრაინის სამართალდამცავმა ორგანოებმა საარჩევნო სისტემაში შეღწევის მცდელობები დააფიქსირეს

უკრაინის შინაგან საქმეთა მინისტრის არსენ ავაკოვის განცხადებით, ქვეყნის სამართალდამცავმა ორგანოებმა ცენტრალური საარჩევნო კომისიის სისტემაში შეღწევის მცდელობა დააფიქსირეს. მისი თქმით, შინაგან საქმეთა სამინისტრო არსებულ სიტუაციას აკვირდება და განსაკუთრებულად აქტიურ მონიტორინგს ახორციელებს. სამინისტრომ რუსეთში და კიევში დარეგისტრირებული რამდენიმე IP მისამართიდან ცენტრალურ საარჩევნო სისტემაში შეღწევის მცდელობები აღმოაჩინა.

მინისტრის განცხადებით, არ არსებობს არავითარი საფუძველი იმისა, რომ უკრაინის საარჩევნო სისტემა დისკრედიტირებული იქნეს.

RT НА РУССКОМ International News

1 აპრილი, 2019 წელი

ირანი დიდი ბრიტანეთის სტრუქტურებს დაესხა თავს

დიდმა ბრიტანეთმა ირანი ეროვნული ინფრასტრუქტურის საკვანძო ელემენტებზე(ძირითადად ბანკებზე) განხორციელებულ კიბერშეტევაში დაადანაშაულა. შეტევები სხვადასხვა უწყებებზე 2018 წლის დეკემბერში, ხოლო ბრიტანეთის პარლამენტზე 2017 წელს განხორციელდა და დღემდე საკითხის კვლევა მიმდინარეობდა.

კიბერკრიმინალებმა შეძლეს დაუფლებოდნენ ათასობით თანამშრომლის პერსონალურ ინფორმაციას, მათ შორის ბრიტანეთის საფოსტო უწყების დირექტორის ელ-ფოსტასა და ტელეფონის ნომერს. Sky News-ის ინფორმაციით, კრიმინალების ხელში აღმოჩნდა 10 204 ჩანაწერი თანამშრომელთა შესახებ.

კალიფორნიელი ანალიტიკოსების ინფორმაციით, აღნიშნული შეტევების, ასევე პარლამენტზე შეტევის უკან დგას ირანის „ისლამური რევოლუციის გუშაგთა კორპუსი“. აღნიშნული დაჯგუფება ასევე იყო ეჭვმიტანილი ისრაელის სარაკეტო თავდასხმის საწინააღმდეგო სისტემაზე იერიშის მიტანაში.

SecurityLab.ru by Positive Technologies silicon

3 აპრილი, 2019 წელი

კიბერკრიმინალებმა მსხვილ ფარმაცევტულ კომპანია “Bayer”-ს შეუტიეს

გერმანული ფარმაცევტული კომპანია Bayer აცხადებს, რომ მის კომპიუტერულ სისტემებზე კრიმინალებმა იერიში მიიტანეს. Reuters-ის ინფორმაციით, კომპანიის ქსელში რამდენიმე თვეა აღმოაჩინეს მავნე პროგრამული უზრუნველყოფა, რომელიც ჩატვირთული იყო დაჯგუფების „Winnti“ მიერ და პროგრამის განეიტრალებამდე სპეციალისტები მასზე ფარულ დაკვირვებას აწარმოებდნენ.

მხოლოდ 2019 წელს დაჯგუფება Winnti-ს მიერ ჩანერგილი მავნე პროგრამული უზრუნველყოფა კიდევ 3 გერმანული კომპანიის ქსელში აღმოაჩინეს. აღნიშნული დაჯგუფება, რომელიც დაკავშირებულია ჩინეთთან, ასევე ცნობილია როგორც Axiom და APT17. ხშირ შემთხვევაში Winnti-ს ინფრასტრუქტურისა და მეთოდების გამოყენება დაიწყეს ჩინეთის მთავრობასთან დაკავშირებულმა სხვა დაჯგუფებებმაც, მათ შორის BARIUM, Wicked Panda, GREF და PassCV.

ზოგიერთი ექსპერტის აზრით, აღნიშნულ დაჯგუფებებს შესაძლოა კავშირი ჰქონდეთ ASUS-ის კომპიუტერებში ბექდორის ჩატვირთვის საქმესთან.

SecurityLab.ru by Positive Technologies REUTERS

4 აპრილი, 2019 წელი

კიბერკრიმინალები ახერხებენ D-Link-ის მარშრუტიზატორების ტრაფიკის მავნე საიტებზე გადამისამართებას

ბოლო 3 თვეა დაუდგენელ კიბერკრიმინალურ დაჯგუფებას იერიში მიაქვს სახლის როუტერებზე (ძირითადად D-Link-ის მოდელების), ცვლის DNS-სერვერის პარამეტრებს და ახდენს მავნე ვებ-გვერდებზე ტრაფიკის გადამისამართებას. აღნიშნულისთვის ბოროტმოქმედები იყენებენ როუტერის პროგრამული უზრუნველყოფის სისუსტეს.

Bad Packets სპეციალისტების ინფორმაციით, მსხვერპლ მოდელებს განეკუთვნება D-Link DSL-2640B, D-Link DSL-2740R, D-Link DSL-2780B, D-Link DSL-526B, ARG-W4 ADSL, DSLink 260E, ასევე Secutech-ის და TOTOLINK-ის როუტერები.

ექსპერტებმა თავდასხმების 3 ტალღა აღმოაჩინეს - 2018 წლის დეკემბერში, 2019 წლის იანვარში და 2019 წლის მარტის ბოლოს.

სპეციალისტების რეკომენდაციით, როუტერების მფლობელებმა უნდა განაახლონ პროგრამული უზრუნველყოფა და შეამოწმონ DNS-ის პარამეტრები მონაცემების ცვლილებაზე.

SecurityLab.ru by Positive Technologies HACKER NEWS

5 აპრილი, 2019 წელი

სოციალურ ქსელში Facebook კიბერდანაშაულებრივი ბაზარი აღმოაჩინეს

Cisco Talos-ის ექსპერტებმა სოციალურ ქსელში Facebook აღმოაჩინეს კიბერდანაშაულებრივი დაჯგუფება, რომელიც წარმოდგენილი იყო 74 ჯგუფითა და 385 ათასი წევრით. ჯგუფების უმეტესობის სახელწოდება თავად ამჟღავნებდა მათ მიზანს, როგორებიცაა: „Spam Professional“, „Spammer & Hacker Professional“, „Buy Cvv On THIS SHOP PAYMENT BY BTC», «Facebook hack (Phishing)“ და ა შ.

ჯგუფის წევრები ყიდიან, ყიდულობენ და ცვლიან ყველაფერ იმას, რაც კიბერდანაშაულებრივ საქმიანობასთანაა დაკავშირებული, მათ შორის მოპარულ მონაცემებს, ფიშინგ-ინსტრუმენტებს, საბანკო ბარათების მონაცემებს და გაყალბებულ პირადობის დამადასტურებელ მოწმობებს. ამასთანავე, სპამერები ყიდიან ელექტრონული ფოსტის მისამართების სიებს, ხოლო ფინანსური მაქინაციებით დაკავებული პირები მომხმარებლებს სთავაზობენ დიდი ოდენობით ფულადი თანხის მოპოვებას.

ამგვარი ჯგუფების მოძებნა სოციალურ ქსელში რთული არ იყო. თავდაპირველად მკვლევრები ცდილობდნენ ჯგუფების დახურვას შესაბამისი ფორმის შევსების საშუალებით, თუმცა აღნიშნული მცდელობა არ აღმოჩნდა წარმატებული და საჭირო გახდა კომპანიასთან პირდაპირ დაკავშირება. შედეგად, ჯგუფების დიდი ნაწილი დაიხურა, ხოლო ნაწილი კვლავ აქტიურია. საყურადღებოა ისიც, რომ ახალი ჯგუფების შექმნა განუწყვეტლივ ხდება.

SecurityLab.ru by Positive Technologies cisco TALOS

8 აპრილი, 2019 წელი

კიბერთავდასხმის გამო ტაილანდში ჰოიას ქარხანამ მუშაობა სამი დღით შეწყვიტა

გავრცელებული ინფორმაციით, ოპტიკური აღჭურვილობის მწარმოებელი იაპონური კომპანია HOYA კიბერთავდასხმის გამო იძულებული გახდა ტაილანდში არსებული საწარმოს მუშაობა სამი დღით შეეჩერებინა.

ბოროტმოქმედებმა შეძლეს მონაცემების მითვისებისთვის და კრიპტოვალუტის მაინინგისთვის განკუთვნილი მავნე პროგრამული უზრუნველყოფით ასობით კომპიუტერის დაინფიცირება. ინციდენტმა მოიცვა ტაილანდში არსებული სერვერები და იაპონიაში HOYA-ს შტაბ-ბინაში ქსელებთან დაკავშირებული კომპიუტერები, რის გამოც კომპანიის თანამშრომლებს არ შეეძლოთ ინვოისების გაცემა. კომპანიის წარმომადგენელთა განცხადებით, მათ შეძლეს კრპტომაინერის მუშაობის დაბლოკვა, თუმცა კიბერშეტევის შედეგად წარმოების მოცულობა 40%-ით შემცირდა. მათი განცხადებით, ინფორმაციის გაჟონვის ფაქტი გამოვლენილი არ იქნა, ხოლო კონკრეტულად რომელი კრპტოვალუტის მაინინგს ახორციელებდნენ დამნაშავეები არ საჯაროვდება.

SecurityLab.ru by Positive Technologies BLEEPINGCOMPUTER

9 აპრილი, 2019 წელი

ეკვადორის პროკურატურამ შესაძლოა ჯულიან ასანჟთან დაკავშირებულ ორ რუს ჰაკერს ქვეყნის დატოვება აუკრძალოს

ეკვადორის მთავრობამ ორგანიზაცია "WikiLeaks" და "რუსი ჰაკერები" ქვეყანაში ძალაუფლების დესტაბილიზაციის მცდელობაში დაადანაშაულა. ხელისუფლებამ WikiLeaks-ის დამფუძნებელ ჯულიან ასანჟს მოქალაქეობა ჩამოართვა.

ამჟამად არ საჯაროვდება, რუსი ჰაკერების ვინაობა. ეკვადორის შინაგან საქმეთა მინისტრის მარია პაულა რომოს განცხადებით, ხელისუფლება არ ფლობს ახალ ინფორმაციას ვიკილიქსსა და ჯულიან ასანჟთან დაკავშირებულ რუს ჰაკერებზე, თუმცა მისთვის ცნობილია რომ ისინი ჯერ კიდევ ეკვადორში იმყოფებიან.

SecurityLab.ru by Positive Technologies HACKER NEWS

13 აპრილი, 2019 წელი

ინტერნეტში ათასობით ამერიკელი პოლიციელისა და გამოძიების ფედერალური ბიუროს თანამშრომელთა პირადი ინფორმაცია გამოქვეყნდა

აშშ-ს გამოძიების ფედერალურ ბიუროსთან დაკავშირებულ რამდენიმე ვებ-გვერდი, ერთ-ერთმა კიბერდანაშაულებრივმა დაჯგუფებამ გატეხა და არსებული ინფორმაცი ინტერნეტში განათავსა. ხელმისაწვდომი გახდა ათასობით პოლიციელისა და ფედერალური აგენტის პერსონალური ინფორმაციის შემცველი ათეულობით ფაილი.

არსებული ინფორმაციით კომპრომეტირებული იქნა გამოძიების ფედერალური ბიუროს აკადემიასთან(კუანტიკო) დაკავშირებული ასოციაციის რესურსები.

თავდამსხმელებმა მონაცემთა გარკვეული ნაწილი თავიანთ ვებ-გვერდზე განათავსეს. (უსაფრთხოების მიზნებიდან გამომდინარე ვებ მისამართი არ საჯაროვდება).

ჟურნალისტებმა შეძლეს ერთ-ერთ თავდამსხმელთან დაკავშირება, რომელმაც მათ განუცხადა რომ დაჯგუფებამ უკვე 1 000-ზე მეტ ვებ-გვერდი გატეხა, ახლა მიმდინარეობს მონაცემების დამუშავება და იგეგმება ამ მონაცემების გაყიდვა.

ჰაკერებთან კონტაქტზე გასულმა ჟურნალისტმა განაცხადა, რომ დაჯგუფება სულ ცოტა ათი წევრისგან შედგება, ხოლო მათი მთავარი მიზანი გამოცდილების მიღება და რაც შეიძლება მეტი ფულის შოვნაა.

SecurityLab.ru by Positive Technologies TC

15 აპრილი, 2019 წელი

ერთ წელიწადში ავსტრიამ შესაძლოა ინტერნეტში ანონიმურობა აკრძალოს

2020 წლიდან, ავსტრიის მთავრობა მოქალაქეებს დაავალდებულებს ინტერნეტ პლატფორმებზე რეგისტრაციისას რეალური ვინაობა დააფიქსირონ. ახალი კანონპროექტის თანახმად, რომელიც სავარაუდოდ 2019 წლის შემოდგომიდან შევა ძალაში, ისეთი მაშტაბური პლატფორმები, როგორიცაა Facebook, Twitter და Instagram ვალდებულნი იქნებიან შეინახონ მომხმარებელთა რეალური მონაცემები, რათა უკანონო ქმედებების განხორციელების შემთხვევაში შესაძლებელი გახდეს მათი კანონის შესაბამისად დასჯა.

კანონპროექტის ძალაში შესვლის შემთხვევაში, მომხმარებლები ვეღარ შეძლებენ ინტერნეტში ანონიმური კომენტარების დატოვებას, რაც გაადვილებს კიბერბულინგთან ბრძოლას. კულტურისა და მასმედიის მინისტრის, გერნოტ ბლუმელის განცხადებით, კანონის მოქმედება გავრცელდება ყველა ინტერნეტ პლატფორმაზე, რომლის აუდიტორიაც მინიმუმ 100 ათას მომხმარებელს შეადგენს. ახალი კანონის შეუსრულებლობა გამოიწვევს ოპერატორების 500 000 ევროთი დაჯარიმებას.

SecurityLab.ru by Positive Technologies HACKER NEWS

16 აპრილი, 2019 წელი

ასანჟის დაკავების შემდეგ ეკვადორის სამთავრობო ვებგვერდებზე 40 მილიონი თავდასხმა განხორციელდა

ეკვადორის საკომუნიკაციო ტექნოლოგიების მინისტრის მოადგილემ პატრიციო რეალმა განაცხადა, რომ WikiLeaks- ის დამფუძნებლის ჯულიან ასანჟის დაკავების შემდეგ ქვეყნის სამთავრობო უწყებების ვებ-გვერდებზე 40 მილიონზე მეტი კიბერშეტევა განხორციელდა.

მისივე თქმით, თავდასხმები მსოფლიოს ყველა წერტილიდან ხდება, მათ შორის შეერთებული შტატებიდან, ბრაზილიიდან, გერმანიიდან, საფრანგეთიდან და რუმინეთიდან.

ეკვადორის პრეზიდენტის, ლენინ მორენოს განცხადებით, ვიკილიქსის დამფუძნებელი ცდილობდა დიპლომატიური მისია, ჯაშუშური მიზნების განსახორციელებლად გამოეყენებინა.

RT НА РУССКОМ engadget

16 აპრილი, 2019 წელი

ჰაკერებმა თავდასხმა Microsoft-ის მეშვეობით განახორციელეს

Microsoft- ის ელექტრონული ფოსტის მომხმარებლებმა მიიღეს წერილები, სადაც კომპანია მათ ახლად აღმოჩენილი ინციდენტის შესახებ ატყობინებდა.

Microsoft- ის მონაცემებით, 2019 წლის 1 იანვრიდან 28 მარტამდე, გარკვეულ პირთა ჯგუფს მომხმარებელთა ანგარიშებზე ჰქონდა წვდომა. კომპანია განცხადებით, რომ უცნობმა პირებმა მომხმარებელთა მონაცემები, კომპანიის ტექნიკური დახმარების ჯგუფის ერთ-ერთი თანამშრომლის ანგარიშის კომპრომეტირების შედეგად მოიპოვეს.

Microsoft- ის თავდაპირველი განცხადების თანახმად მომხმარებელთა პირადი მიმოწერის შინაარსი თავდამსხმელთათვის არ იყო ხელმისაწვდომი, თუმცა მალევე გაირკვა რომ მათი ეს განცხადება სიმართლეს არ შეესაბამებოდა. გამოცემა Vice Motherboard-ის ჟურნალისტებმა ანონიმურ წყაროსთან საუბრის შემდეგ განაცხადეს, რომ ჰაკერებს ხელი არა მარტო კორპორატიულ ანგარიშებზე არამედ მომხმარებელთა პირად Outlook, MSN და Hotmail-ზე მიუწვდებოდათ.

HELPNETSECURITY

16 აპრილი, 2019 წელი

ევროკავშირი აპირებს შექმნას ბიომეტრიულ მონაცემთა ბაზა, რომელშიც 350 მილიონზე მეტი ადამიანის მონაცემი იქნება შენახული

ევროპარლამენტმა ხმა მისცა ერთიანი მონაცემთა ბაზის შექმნას, რომელიც დაიკავშირებს სასაზღვრო კონტროლის, მიგრაციისა და სამართალდამცავ ორგანოებს. ახალი მონაცემთა ბაზა სახელწოდებით Common Identity Repository (CIR) შეინახავს როგორც ევროკავშირის წევრი, ასევე არაწევრი ქვეყნების მოქალაქეების ბიომეტრიულ მონაცემებს.

ნაგულისხმევია, რომ ბაზაში იქნება მოქალაქეთა სახელები, პასპორტის ნომრები, დაბადების თარიღი და ბიომეტრიული მონაცემები, როგორიცაა თითის ანაბეჭდები და სახის ასლები. წვდომა აღნიშნულ ბაზაზე ექნებათ სასაზღვრო და სამართალდამცავ ორგანოებს. პროექტის ეფექტურობა მდგომარეობს იმაში, რომ ორგანოების სამუშაო იქნება გამარტივებული და მათ არ მოუწევთ მონაცემების სხვადასხვა ბაზებში ცალ-ცალკე ძიება.

ევროპარლამენტის პრეს-რელიზის თანახმად, ახალ ბაზაში, ასევე, შევა შემდეგი სისტემები: შენგენის საინფორმაციო სისტემა, Eurodac, სავიზო საინფორმაციო სისტემა (VIS) და 3 ახალი სისტემა: მესამე ქვეყნების პირთა კრიმინალური დოსიეს ევროპული სისტემა (ECRIS-TCN), შესვლა/გამოსვლის სისტემა (EES) და შენგენის ზონაში შესვლის ავტორიზაციის ავტომატური სისტემა (ETIAS).

ევროპარლამენტის და ევროსაბჭოს ინფორმაციით, ბაზის შექმნისას გატარდება შესაბამისი ზომები მოქალაქეთა კონფიდენციალურობის დაცვისა და სამართალდამცავ უწყებათა მონაცემებზე წვდომის კონტროლის უზრუნველსაყოფად.

SecurityLab.ru by Positive Technologies POLITICO

22 აპრილი, 2019 წელი

რჩევები ფიშინგისგან თავის დასაცავად

ფიშინგ-თაღლითობა ინტერნეტის შექმნასთან ერთად გახდა აქტუალური და ნაკლებად სავარაუდოა, რომ ის მალე გაქრება. საბედნიეროდ, არსებობს სხვადასხვა საშუალებები, რომელთა გამოყენებითაც, მცირეა შანსი თავად გავხდეთ ინტერნეტ-თაღლითობის მსხვერპლი. გთავაზობთ რამდენიმე რჩევას, რომელიც დაგეხმარებათ ფიშინგისგან თავის დასაცავად:

1. კარგად დავფიქრდეთ ბმულზე გადასვლამდე

უცხო გამომგზავნისგან მიღებულ წერილში მოცემულ ბმულზე გადასვლა ერთობ სახიფათო შეიძლება აღმოჩნდეს. შესაძლოა, გახსნილი ვებ-გვერდი აბსოლუტურად იდენტური იყოს თქვენთვის ნაცნობი ვებ-გვერდისა და გთხოვდნენ თქვენი პირადი ინფორმაციის თუ პაროლების შეყვანას. მაშინ, როდესაც თქვენ გსურთ რომელიმე ნაცნობი

საიტის მონახულება, ნუ გადახვალთ მასზე ელ-ფოსტაში მითითებული ბმულიდან, არამედ თავად აკრიფეთ ვებ-ბრაუზერის სამისამართო ველში შესაბამისი ვებ-გვერდის მისამართი და მხოლოდ ასეთ შემთხვევაში შეიყვანეთ საკუთარ მონაცემები.

2. დარწმუნდით ვებ-გვერდის უსაფრთხოებაში

რომელიმე ვებ-გვერდზე ინფორმაციას შეყვანამდე, დააკვირდით, რომ ვებ-გვერდის მისამართი იწყება “https”-ით. ამასთანავე, აქვე უნდა ხედავდეთ ბოქლომის ნიშანს, რომელიც ადასტურებს ვებ-გვერდის უსაფრთხოების სერტიფიკატების არსებობას.

3. არასოდეს ჩამოტვირთოთ ფაილები საეჭვო ვებ-გვერდებიდან

საძიებო სისტემებშიც კი შეიძლება შევხვდეთ ისეთ გვერდებს, რომელიც გვამისამართებს ფიშინგ ვებ-გვერდებზე და გვთავაზობენ რაიმე პროდუქციას იაფ ფასად. ასეთი ვებ-გვერდები არსებობენ იმისთვის, რომ კიბერკრიმინალებმა მიიღონ თქვენი საკრედიტო ბარათის მონაცემები.

4. პერიოდულად განაახლეთ ვებ-ბრაუზერი

უსაფრთხოების განახლებები ვებ-ბრაუზერებისთვის პერიოდულად გამოდის. ისინი ებრძვიან სისუსტეებს, რომელიც არსებობდა წინა ვერსიებში და შესაძლოა გამოყენებული ყოფილიყო თაღლითების მიერ. დაუშვებელია განახლების შესახებ შეტყობინებების იგნორირება და აუცილებლად განაახლეთ პროგრამული უზრუნველყოფა ახალი განახლების გამოჩენისთანავე.

5. გამოიჩინეთ სიფრთხილე Pop-Up ფანჯრების მიმართ

როგორც წესი, ასეთი ფანჯრები სარეკლამო ხასიათისაა, თუმცა, არის შემთხვევები, როდესაც ის ფიშინგ-თაღლითობის მიზანს ემსახურება. პოპულარული ვებ-ბრაუზერების უმრავლესობა ბლოკავს ამგვარ ფანჯრებს. თუკი ამგვარი ფანჯარა მაინც გაიხსნა, აუცილებლად დახურეთ ის “X” ღილაკით ფანჯრის ზედა კუთხეში, და არა ფანჯარაშივე არსებული სხვადასხვა ღილაკებით, როგორიცაა “Cancel”, “Close” და სხვა.

6. არასოდეს გასცეთ პერსონალური ინფორმაცია

ის, რომ სენსიტიური პერსონალური და ფინანსური ინფორმაციის ინტერნეტით გაზიარება დაუშვებელია, ზოგადი წესია. არასოდეს გასცეთ თქვენი პირადი ინფორმაცია ელ-ფოსტის წერილით. აუცილებლად შეამოწმეთ წერილის ავთენტურობა შესაბამის ორგანიზაციაში ზარის განხორციელებით ან რაიმე სხვა საშუალებით.

7. გამოიყენეთ ანტივირუსული პროგრამული უზრუნველყოფა

აღნიშნული პროგრამული უზრუნველყოფის გამოყენების მიზეზი მრავალგვარია, თუმცა ერთ-ერთი მიზეზი ფიშინგ-თაღლითობისგან თავის დაცვაა. ის დაგიცავთ მავნე ფაილებისგან, ხოლო ოპერაციულ სისტემას დაზიანებისგან.

8. არ გახსნათ მიმაგრებული ფაილები

თუკი წერილის ავტორი თქვენთვის უცნობი პირი ან ორგანიზაციაა და წერილის შინაარსი არც თუ ისე ახლოს შეიძლება იყოს რეალობასთან, დაუშვებელია ნებისმიერი მიმაგრებული

ფაილის ჩამოტვირთვა. უბრალო ტექსტური დოკუმენტიც კი, როგორიცაა Microsoft Office Word-ის .doc(x) გაფართოების ფაილი, შესაძლოა შეიცავდეს მავნე პროგრამულ უზრუნველყოფას, რომელსაც დიდი ზიანის მიყენება შეუძლია თქვენთვის და თქვენი მოწყობილობისთვის.