საქართველოს თავდაცვის სამინისტრო

სსიპ - კიბერუსაფრთხოების ბიურო

კიბერდაიჯესტი № 3

თბილისი 2019

სარჩევი

კიბერშეტევების ახალი ტალღა პოს-ტერმინალებზე

უსაფრთხოების საკითხებზე მომუშავე კომპანია Morphisec იუწყება კიბერშეტევების ახალი ტალღის შესახებ, რომელიც საბანკო ბარათების მონაცემების მოპარვის მიზნით პოს-ტერმინალებზე ხორციელდება მთელი მსოფლიოს მასშტაბით. კიბერკრიმინალების მსხვერპლნი ინდოეთში, იაპონიაში და აშშ-ში მოქმედი ფინანსური, სადაზღვევო, სამედიცინო და სხვა კომპანიები გახდნენ.

გამოცემის ინფორმაციით, ჯერ-ჯერობით არ არსებობის საკმარისი ფაქტები იმისთვის, რომ კიბერშეტევები ერთ კონკრეტულ დაჯგუფებას მიეწეროს. გარდა ამისა, მავნე პროგრამული უზრუნველყოფა რომელიც პოს-ტერმინალებზე იტვირთებოდა, განსხვავდება ერთმანეთისგან. პროგრამული უზრუნველყოფა Cobalt Strike ჩასატვირთად ზოგიერთ მათგანში გამოყენებული იყო ინსტრუმენტი FrameworkPOS, ზოგიერთში PowerShell/WMI. აღნიშნული პროგრამა კიბერკრიმინალს საშუალებას აძლევს მოიპოვოს დაზიანებულ სისტემაზე კონტროლი და შეაღწიოს ქსელის სისტემებში. მისი დახმარებით შესაძლებელია მსხვერპლის ინფორმაციის მოპარვა და სხვადასხვა მავნე ოპერაციების განხორციელება.

SecurityLab.ru by Positive Technologies MORPHISEC Moving Target Defense

4 მარტი, 2019 წელი

Huawei ბრიუსელში კიბერუსაფრთხოების ცენტრს ხსნის

ამერიკის შეერთებული შტატების მთავრობის ბრალდების საპასუხოდ, რის თანახმადაც Huawei საფრთხეს უქმნის ეროვნულ უსაფრთხოებას, ჩინურმა ტელეკომუნიკაციების გიგანტმა გადაწყვიტა გახსნას კიბერუსაფრთხოების გამჭვირვალობის ცენტრი ბელგიის დედაქალაქ ბრიუსელში.

კომპანიის წარმომადგენლის კენ ჰუს განცხადებით, ნდობა დაფუძნებული უნდა იყოს ფაქტებზე, ფაქტები კი უნდა ექვემდებარებოდეს გადამოწმებას, რისი საერთო სტანდარტებიც წინასწარ უნდა იყოს შემუშავებული. მისი აზრით, კიბერუსაფრთხოების გამჭვირვალობის ცენტრის შექმნა არის დღევანდელ ციფრულ ერაში ნდობის მოპოვების ეფექტური მოდელი.

ცენტრს სამი მთავარი ფუნქცია ექნება. უპირველეს ყოვლისა, მასში იქნება დემონსტრირებული Huawei-ს პროდუქტების შექმნის კომპლექსური პროცესები ინფორმაციული უსაფრთხოების კუთხით. მეორე ფუნქცია მდგომარეობს დაინტერესებულ პირებსა და კომპანიას შორის თანამშრომლობის გამარტივებაში, რაც საშუალებად იძლევა მარტივად მოხდეს ინფორმაციული უსაფრთხოების უზრუნველყოფა. ხოლო მესამე ფუნქცია იქნება პლატფორმის როლის მორგება, რათა მოხდეს პროდუქტის ტესტირება და უსაფრთხოების საკითხების გადამოწმება.

კომპანიის განცხადებით, კიბერუსაფრთხოების გამჭვირვალობის ცენტრის გახსნა ბრიუსელში სხვადასხვა მთავრობებს და ევროპელ პარტნიორებს დაუდასტურებს, რომ მონაცემების დაცვა Huawei-ს ერთ-ერთი ძირითადი პრიორიტეტია.

HUAWEI FORTUNE

5 მარტი, 2019 წელი

ირანელმა ჰაკერებმა ბოლო 2 წლის განმავლობაში 200-ზე მეტ კომპანიაზე მიიტანეს იერიში

კომპანია Microsoft-ის მკვლევარების ანგარიშის მიხედვით, ირანელმა ჰაკერებმა გასული 2 წლის განმავლობაში სხვადასხვა ქვეყნის 200-ზე მეტ კომპანიაზე განახორციელეს კიბერშეტევა. კიბერკრიმინალების მიზანს სენსიტიური ინფორმაციის მოპარვა და წაშლა წარმოადგენდა.

თავდასხმის ობიექტები ძირითადად ნავთობმომპოვებელი კომპანიები, ასევე გერმანიის, საუდის არაბეთის, დიდი ბრიტანეთის, ინდოეთისა და აშშ-ის საერთაშორისო კომპანიები გახდნენ. კორპორაცია „მაიკროსოფტის“ ანგარიშის თანახმად, ბოლო ორი წლის განმავლობაში ირანელი ჰაკერების თავდასხმის შედეგად მიყენებული ზარალი ასობით მილიონ დოლარს შეადგენს.

დოკუმენტის თანახმად, ბოლო ორ წელიწადში განხორციელებული ჰაკერული თავდასხმები სავარაუდოდ, ირანის ხელისუფლებასთან იყო დაკავშირებული.

„მაიკროსოფტის“ სპეციალისტების განმარტებით, ჰაკერული თავდასხმების უკან კიბერდამნაშავეების ჯგუფი „ჰოლმიუმი“ დგას. მიუხედავად იმისა, რომ დაზარალებულ კომპანიებს შორის ამერიკულ და ევროპულ ორგანიზაციებს ვხვდებით, კიბერუსაფრთხოების მკვლევარების აზრით, შეტევები გამიზნული იყო ძირითადად შუა აღმოსავლეთზე. თუმცა აღსანიშნავია ისიც, რომ ირანი ზრდის კიბერშესაძლებლობებს აშშ-სა და ირანს შორის არსებული დაძაბული ვითარების გამო.

DW MarketWatch

6 მარტი, 2019 წელი

შვეიცარიის საარჩევნო სისტემაში აღმოჩენილ სისუსტეს არჩევნების შედეგებზე გავლენის მოხდენა შეუძლია

ინფორმაციული უსაფრთხოების მკვლევართა ჯგუფმა შვეიცარიის ელექტრონული ხმის მიცემის სისტემაში მოწყვლადობა აღმოაჩინა, რომელსაც შეეძლო არჩევნების დროს ლეგიტიმური ხმების ყალბით შეცვლა.

ექსპერტების სარა ჯემი ლუისის, ოლივიე პერეირასა და ვანესა ტიგეს მიერ გამოქვეყნებული დოკუმენტის მიხედვით, ერთ-ერთი მოწყვლადობა აღმოჩენილ იქნა კრიპტოგრაფიულ სისტემაში რომელიც ახდენს ხმების ნამდვილობის დადასტურებას. ექსპერტების აზრით, გამოყენებული ალგორითმი არასანდოა და ხმების ფალსიფიკაციის საშუალებას იძლევა.

სისტემის დეველოპერების კერძოდ Swis Post-ისა და ესპანური კომპანიის Scytl-ის განცხადებით, მოწყვლადობა გამოსწორებულია. ექსპერტების განცხადებით, ელექტრონული საარჩევნო სისტემების დანერგვის შემდეგ, მათ არაერთხელ გააფრთხილეს ხელისუფლება მოსალოდნელი საფრთხის შესახებ.

2019 წლის თებერვალში, შვეიცარიის მთავრობამ ელექტრონული ხმის მიცემის სისტემაში გამოვლენილი ხარვეზების აღმოჩენისთვის ჯილდო დააწესა. საზოგადოებრივი ტესტირების დაწყებიდან ერთი კვირის შემდეგ ექსპერტები ტექნიკურ დოკუმენტაციასა და გამავალ კოდთან დაკავშირებულ პრობლემებს წააწყდნენ.

SecurityLab.ru by Positive Technologies MOTHERBOARD

12 მარტი, 2019 წელი

აშშ-ს სამხედრო საზღვაო ძალები მოწინააღმდეგეების მუდმივი კიბერშეტევის ქვეშ იმყოფებიან

აშშ-ის სამხედრო საზღვაო ძალები ჩინეთის ფლოტის ინტერესებში მოქმედი ჰაკერების "კიბერბლოკადის“ ქვეშ იმყოფებიან. კიბერჯაშუშები რეგულარულად ესხმიან თავს ამერიკის სამხედრო საზღვაო ძალებს, სამხედრო კონტრაქტორებს და იმ უნივერისტეტებს რომლებიც საზღვაო ძალებთან თანამშრომლობენ. ეს დასკვნა ამერიკის სამხედრო საზღვაო ძალების ექსპერტთა მიერ ჩატარებული შიდა აუდიტის საფუძველზე დაიდო.

აშშ-ს სამხედრო საზღვაო ძალების ხელმძღვანელმა რიჩარდ სპენსერმა აღნიშნა, რომ საზღვაო ძალებიდან საიდუმლო ინფორმაციის მოპარვის მცდელობები სულ უფრო ინტენსიური ხდება. "ჩვენ უნდა ვიმოქმედოთ აქტიურად რათა გავიგოთ თავდასხმების ხასიათი და ხელი შევუშალოთ მნიშვნელოვანი სამხედრო ინფორმაციის გაჟონვას", - განაცხადა სპენსერმა.

ანგარიშის თანახმად აშშ-ის საზღვაო ძალების კიბერუსაფრთხოება სერიოზული საფრთხის ქვეშ დგას. ფლოტი არაერთი მოწინააღმდეგე ქვეყნის მხრიდან განიცდის კიბერშეტევებს და მთელი ძალებით ცდილობს მათთან გამკლავებას.

SecurityLab.ru by Positive Technologies Hacker News 13 მარტი, 2019 წელი

Android სისტემის ანტივირუსების 60% არაეფექტური აღმოჩნდა

გამოცემა AV-Comparatives კვლევის შედეგად დადგინდა, რომ ანდროიდის ოპერაციულ სისტემის 250 ანტივირუსიდან (Google Play Store-შია ხელმისაწვდომი) მხოლოდ 80-ს შეუძლია სარგებელი მოუტანოს მომხმარებელს.

მკვლევარების ინფორმაციით, 10-დან საშუალოდ მხოლოდ 1-მა ანტივირუსმა შეძლო მობილური ტელეფონის 2000 მავნე პროგრამისგან დაცვა.

მკვლევარები ასევე აღნიშნავენ, რომ აპლიკაციების განახლებები პირდაპირ არასოდეს მიგვანიშნებს იმაზე, რომ ისინი ამიერიდან შეძლებენ მოწყობილობის სათანადო დაცვას.

რეკომენდაციის სახით დადგინდა, რომ მომხმარებლებმა უნდა გამოიყენონ ყველაზე ცნობადი, გადამოწმებული, მაღალი რეპუტაციის მქონე აპლიკაციები.

SecurityLab.ru by Positive Technologies MYBROADBAND 13 მარტი, 2019 წელი

ჭკვიანი ავტომობილების 10%-ზე იერიშის მიტანამ შესაძლოა ნიუ-იორკის ბლოკირება გამოიწვიოს

სმარტ-ავტომობილების არსებობა დიდი ხანია ფანტასტიკის ჟანრს აღარ განეკუთვნება. მოძრაობის ოპტიმიზაციისთვის ასეთი ავტომობილები ერთმანეთთან ამყარებენ კომუნიკაციას და გააჩნიათ ავტოპილოტის ფუნქცია.

ჯორჯიას შტატის ტექნოლოგიური ინსტიტუტის მკვლევარებმა შეიმუშავეს ამ ტიპის ავტომობილებზე ჰაკერული შეტევის შედეგად განვითარებული მოვლენების რამდენიმე ვარიანტი. კვლევის შედეგად დადგინდა, რომ სმარტ-ავტომობილების 10%-ზე იერიშის მიტანით მანჰეტენის 4000 ქუჩა სრულიად დაიბლოკება, ხოლო 20%-ის ბლოკირებით, მანჰეტენი სრულიად პარალიზებული გახდება, რაც თავის მხრივ სრულ ქაოსს გამოიწვევს ისეთ მეგაპოლისში, როგორიცაა ნიუ-იორკი.

აღსანიშნავია, რომ ჭკვიანი ავტომობილების ავტოპილოტები ერთმანეთთან კავშირს ქსელების საშუალებით ამყარებენ. კვლევამ გამოკვეთა, რომ აღნიშნული ქსელები არ არის საკმარისად უსაფრთხო და შესაძლოა ბოროტმოქმედებმა შეძლონ მასში შეღწევა.

კვლევის შედეგად გაიცა სარეკომენდაციო დასკვნა, რომლის თანახმადაც ქალაქებმა უნდა გამოიყენონ ავტომობილების დაკავშირების რამდენიმე ალტერნატიული ქსელი, რათა ერთი ან რამდენიმე ავტომობილის, ან ქსელის დაზიანებამ არ გამოიწვიოს სრული ქაოსი, რაც არამარტო ქუჩების ბლოკირებას, არამედ ავტომობილებისა და მგზავრების ფიზიკურ უსაფრთხოებასაც შეუქმნის საფრთხეს.

SecurityLab.ru by Positive Technologies Hacker News

14 მარტი, 2019 წელი

არქივატორის WinRAR სისუსტეს კრიმინალები აქტიურად იყენებენ

თებერვლის თვეში WinRar-ში, რომელიც ერთ-ერთი ყველაზე პოპულარული და სანდო არქივატორია, აღმოჩნდა სისუსტე, რომელიც კრიმინალს საშუალებას აძლევს, ფაილების გადაწერა მოხდეს მისთვის სასურველ ფოლდერში, და არა იმაში, რომელსაც მომხმარებელი ირჩევს. სისუსტე დაკავშირებულია ბიბლიოთეკა UNACEV2.DLL-თან, რომელიც გამოიყენება ACE ფაილების დეკომპრესირებისთვის.

ამ მავნე კამპანიის ფარგლებში კიბერკრიმინალებმა გაავრცელეს არიანა გრანდეს ალბომის ყალბი ვერსია, რომელიც მხოლოდ 11-მა ანტივირუსმა ჩათვალა მავნე კოდის შემცველად. დაინფიცირებული rar არქივი, რამდენიმე .mp3 ფაილით შეიცავს მავნე პროგრამული უზრუნველყოფას, რომელიც ავტომატურად გადადის ავტომატურ გაშვებაზე და ოპერაციული სისტემის ჩართვისთანავე იტვირთება.

მიუხედავად იმისა, რომ დეველოპერებმა გამოსცეს WinRAR-ის ახალი ვერსია, წინა ვერსიების უზუსტობა კვლავ გამოიყენება თავდამსხმელების მიერ, ვინაიდან ყველა მომხმარებელს პროგრამული უზრუნველყოფა ჯერ კიდევ არ განუახლებია.

აღნიშნულიდან გამომდინარე, აუცილებელია WinRAR პროგრამული უზრუნველყოფის უახლესი ვერსიის ინსტალაცია WinRAR (5.70 beta 1) და მომხმარებლებმა არ უნდა გახსნან უცნობი წყაროდან მიღებული ფაილები.

SecurityLab.ru by Positive Technologies ars TECHNICA

15 მარტი, 2019 წელი

პაკისტანის სამთავრობო ვებ-გვერდი დაინფიცირებულია

უცნობმა პირებმა პაკისტანის მთავრობის ვებ-გვერდი გატეხეს და keylogger-თა და სხვა მავნე პროგრამული უზრუნველყოფით დააინფიცირეს. ჰაკერების მიზანს იმ მოქალაქეთა პირადი მონაცემების მითვისება წარმოადგენს, რომლებიც ამოწმებენ საკუთარ განაცხადს პაკისტანის მოქალაქეობის მინიჭების თაობაზე. კომპანია Trustwave-ის სპეციალისტებმა პაკისტანის შინაგან საქმეთა სამინისტროს საიმიგრაციო და საპასპორტო დირექტორატის ვებ-გვერდზე აღმოაჩინეს ე.წ. Scanbox, რომელიც ტელემეტრიის მონაცემების უჩვეულო ფუნქციონირებაში გამოიხატებოდა.

Keylogger-ი აგროვებდა მომხმარებელთა ისეთ ინფორმაციას როგორიცაა IP მისამართები, მონაცემები კომპიუტერში ინსტალირებული პროგრამების შესახებ და სხვა.

Scanbox-ი დიდი ხანია ცნობილია - FireEye ექსპერტებისთვის, რომელთაც ის APT ჯგუფების არსენალს მიაკუთვნეს. იგი გამოყენებულ იქნა ჩინური კიბერშჯაშუშური დაჯგუფების APT 10 მიერ ოპერაცია TradeSecret-ის კამპანიის დროს, რომელიც აშშ საგარეო ვაჭრობის ეროვნული საბჭოს წევრების წინააღმდეგ იყო მიმართული.

მკვლევარებმა კომპრომეტირებული რესურსის ადმინისტრაციას შეატყობინეს პრობლემის შესახებ, მაგრამ პასუხი არ მიუღიათ, ხოლო საიტი ამ დრომდე ინფიცირებულია.

SecurityLab.ru by Positive Technologies BLEEPINGCOMPUTER

15 მარტი, 2019 წელი

ჩრდილოეთ კორეა ეჭვმიტანილია ჩინელ ჩინოვნიკებზე კიბერშეტევის განხორციელებაში

ჩინეთის სახელმწიფო უწყებებზე კიბერშეტევა გამომძალველი მავნე პროგრამული უზრუნველყოფა Gandcrab-ის გამოყენებით განხორციელდა.

ხელისუფლების მიერ გავრცელებული პრეს-რელიზის თანახმად მავნე პროგრამა ელექტრონული ფოსტის მეშვეობით გავრცელდა.

ელექტრონულ წერილებს თანდართული ჰქონდა არქივი, რომელიც მავნე პროგრამულ უზრუნველყოფა Gandcrab 5.2-ის საინსტალაციო ვერსიას შეიცავდა. სისტემაში გაშვების შემდეგ პროგრამა იწყებს მყარ დისკზე მონაცემების დაშიფვრას და სთავაზობს მსხვერპლს „დაცული“ ბრაუზერი Tor-ის ინსტალაციას, საიდანაც მომხმარებელი უნდა გადავიდეს ვებ-გვერდზე და გადაიხადოს გამოსასყიდი კრიპტოვალუტაში.

თავდასხმები მიმდინარე წლის 11 მარტს დაიწყო. კამპანიის მასშტაბები ჯერჯერობით დადგენილი არაა. ასევე უცნობია თავდასხმის ორგანიზატორთა ვინაობა. ზოგიერთ

მინიშნებაზე დაყრდნობით, მიიჩნევენ, რომ კიბერშეტევა შესაძლოა ჩრდილოეთ კორეის კიბერდანაშაულებრივი დაჯგუფების ორგანიზებული იყოს.

SecurityLab.ru by Positive Technologies Bitcoin.com

15 მარტი, 2019 წელი

კიბერთაღლითები ახალ ზელანდიაში ტერორისტული თავდასხმისა და ეთიოპიაში თვითმფრინავის ჩამოვარდნის ნიუსებს, ვირუსების გასავრცელებლად იყენებენ

სპამერები ცდილობენ ისარგებლონ გარკვეული მოვლენების ირგვლივ ატეხილი აჟიოტაჟით და მიიქციონ ინტერნეტ მომხმარებელთა ყურადღება. ბოლო რამდენიმე დღის განმავლობაში მსოფლიოში ერთ-ერთი ყველაზე განხილვადი მოვლენა ახალ ზელანდიაში ტერორისტული თავდასხმა და ეთიოპიაში Boeing 737 Max თვითმფრინავის ჩამოვარდნაა. კიბერთაღლითებმა ისარგებლეს მომენტით და წამოიწყეს ახალი ზიანის მომტანი კამპანია.

360 Threat Intelligence Center-ის ექსპერტების ინფორმაციის თანახმად, ბოროტმოქმედები მავნე პროგრამული უზრუნველყოფის გასავრცელებლად, ეთიოპიაში მომხდარ ავიაკატასტროფას იყენებენ. სპამი სავარაუდოდ გატეხილი ელექტრონული ფოსტიდან @IsgecPresses (info@isgec.com) იგზავნება და მონიშნულია ჰაშთეგით ბოინგ (#Boeing). როგორც წესი სტატიის თემა ბოინგის ჩამოვარდნაა.

დაინფიცირებული წერილები შენიღბულია, როგორც კერძო ანალიტიკოსის პრესრელიზი, რომელიც თითქოს ფლობს ინფორმაციას მომავალი კატასტროფების შესახებ და შეიცავს ავიაკომპანიების ჩამონათვალს, რომელთა თვითმფრინავებს უახლოეს მომავალში იგივე ბედი ეწევათ.

აშშ-ს შიდა უსაფრთხოების სამინისტრომ გააფრთხილა მომხმარებლები, ახალი ზელანდიის ტერიტორიაზე მომხდარი ტერაქტის სპამერების მიერ გამოყენების შესაძლებლობის თაობაზე.

SecurityLab.ru by Positive Technologies The State of Security NEWS. TRENDS. INSIGHTS.

18 მარტი, 2019 წელი

აშშ-ს პოლიტიკოსები Google-ს ჩინეთთან თანამშრომლობაში ადანაშაულებენ

აშშ-ს პრეზიდენტმა დონალდ ტრამპმა Twitter-ზე გამოაქვეყნა განცხადება სადაც კომპანია Google ჩინეთისა და მისი სამხედრო ძალების დახმარებაში ღიად დაადანაშაულა.

Google- მა საპასუხო განცხადება დაუყოვნებლივ გამოაქვეყნა რომელშიც იუწყება რომ ჩინურ სამხედრო ძალებთან არანაირი კავშირი არ აქვთ და რომ ისინი ყველა ასპექტში მათ შორის კიბერუსაფრთხოების, პერსონალისა და ჯანდაცვის სფეროში მხოლოდ აშშ-ს მთავრობასა და თავდაცვის სამინისტროს ინტერესებში მუშაობენ.

აშშ-ს შეიარაღებული ძალების გაერთიანებული შტაბის თავმჯდომარე ჯოზეფ დანფორდმა კონგრესში სიტყვით გამოსვლის დროს კომპანიას ანალოგიური ბრალდებები წაუყენა. მისი განცხადებით "სამუშაო, რომელსაც Google-ი ჩინეთში ახორციელებს, ირიბად (თუ შეიძლება ყოველივე ამას ირიბი ეწოდოს) ჩინური სამხედრო ძალებისთვის სარგებლის მომტანია".

SecurityLab.ru by Positive Technologies NEWS

18 მარტი, 2019 წელი

რუსული ჰაკერული დაჯგუფებები კიბერშეტევებს აძლიერებენ

FireEye-ს მკვლევარების ინფორმაციით, ევროპარლამენტის არჩევნების მოახლოებასთან ერთად კრემლთან კავშირის მქონე დაჯგუფებები ცდილობენ განახორციელონ ოპერაციები ევროპული მთავრობების, მედიისა და პოლიტიკური პარტიების წინააღმდეგ.

სავარაუდო თავდამსხმელად მიიჩნევა რუსეთის მთავრობასთან დაკავშირებული დაჯგუფება APT28, ანუ Fancy Bear, რომელიც ცდილობდა გავლენა მოეხდინა აშშ-ს საპრეზიდენტო არჩევნებზე 2016 წელს, ახორციელებდა კიბერშპიონაჟის კამპანიებს სხვადასხვა საელჩოებისა და ორგანიზაციების წინააღმდეგ.

მეორე დაჯგუფება, რომელიც ეჭვმიტანილია მავნე აქტივობებში, არის რუსეთის სამხედრო დაზვერვასთან (GRU) დაკავშირებული Sandworm Team.

როგორც ირკვევა, აღნიშნული ორი ჯგუფი, მუშაობს ერთობლივად და კიბერშპიონაჟის წარმოებისთვის იყენებს ფიშინგს.

ევროპული მთავრობის წარმომადგენლებმა მიიღეს ბმულის შემცველი წერილები, რომელიც თითქოსდა ამისამართებდა სამთავრობო ვებ-გვერდებზე, რეალურად კი, ეს იყო მავნე პროგრამული უზრუნველყოფის შემცველი ბმულები და მიზნად ისახავდა პირადი მონაცემების მითვისებას.

FireEye-ს კიბერშპიონაჟის ანალიზის უფროსი მენეჯერის აზრით, ეს დაჯგუფებები ცდილობენ მიიღონ ინფორმაცია, რათა მის საფუძველზე რუსეთმა უფრო გააზრებული პოლიტიკური გადაწყვეტილებები მიიღოს ან გაავრცელონ ინფორმაცია კონკრეტული პოლიტიკური პარტიის ან კანდიდატის დისკრედიტაციის მიზნით.

აღნიშნული კამპანიის შესახებ დეტალური ინფორმაცია ჯერ-ჯერობით არ არსებობს.

21 მარტი, 2019 წელი

Facebook ასობით მილიონი მომხმარებლის პაროლს დაუშიფრავად ინახავდა

სისტემაში გაპარული რამდენიმე შეცდომის გამო კომპანია Facebook-ში მილიონით მომხმარებლის პაროლი დაუშიფრავად იყო შენახული და მათზე წვდომა კომპანიის 20 000-ზე მეტ თანამშრომელს ჰქონდა. აღნიშნული პრობლემა ეხება Facebook-ის, Facebook Lite-ის და Instagram-ის მომხმარებლებს.

Facebook-ის პროგრამული უზრუნველყოფის ინჟინერმა სკოტ რენფრომ განაცხადა, რომ კომპანია არ არის მზად გაამჟღავნოს იმ თანამშრომელთა რაოდენობა, ვისაც შეიძლება ჰქონოდა წვდომა აღნიშნულ ინფორმაციაზე. ასევე, მისი განცხადებით, მომხმარებლები, რომელთა პაროლები თანამშრომლებისთვის ხელმისაწვდომი იყო, შეტყობინებას მიიღებენ, თუმცა პაროლის ცვლილება აუცილებელი არ იქნება.

გარდა ამისა, კომპანიის მიერ გავრცელებული ინფორმაციით, არსებული ინფორმაციის ბოროტად გამოყენების ფაქტი აქამდე არ გამოვლენილა.

21 მარტი, 2019 წელი

დაჯგუფება OceanLotus იყენებს Microsoft Office-ს სისუსტეს

APT-დაჯგუფება OceanLotus, ასევე ცნობილი, როგორც APT32, SeaLotus, APT-C-00 და Cobalt Kitty კიბერსივრცეში ახალი ექსპლოიტებით და მავნე არქივებით შეიარაღებული დაბრუნდა.

OceanLotus ცნობილია თავდასხმებით აზიის სხვადასხვა ორგანიზაციებზე თავდასხმებით. ESET-ის ანგარიშის მიხედვით, OceanLotus ახალ ტაქტიკას იყენებს, კერძოდ

Microsoft Office-ს სისუსტეს (CVE-2017-11882), რომელიც მარტივადაა ხელმისაწვდომია და მისი გამოყენება შესაძლებელია ფიშინგ შეტევებისთვის.

შეტევა იწყება მსხვერპლის მიერ მავნე დოკუმენტის ან შეტყობინების გახსნით, რომლის თემაც, ერთი შეხედვით, ისეა შერჩეული, რომ მომხმარებლისთვის საინტერესო იყოს. მავნე დოკუმენტის შიგნით კი მიმაგრებულია სატყუარა - ფოტო, დოკუმენტი, რომელსაც საკუთარი მიზნებისთვის იყენებენ თავდამსხმელები. მსხვერპლის მიერ ფაილის გახსნის შემდგომ აქტიურდება მაკროსები, სისტემაში იტვირთება ბექდორი, რომელიც აგროვებს ინფორმაციას.

ამავე კამპანიის ნაწილია მავნე პროგრამული უზრუნველყოფის შექმნა, რომლის დანიშნულებაც მსხვერპლის კომპიუტერიდან ყოველდღიურად ინფორმაციის შეგროვებაა.

გავრცელებული ინფორმაციით, აღნიშნული დაჯგუფება საკმაოდ აქტიურია და დღითიდღე ხვეწავს საკუთარ ტექნიკასა და ინსტრუმენტებს.

SecurityLab.ru by Positive Technologies Hacker News

22 მარტი, 2019 წელი

გამომძალველი პროგრამა LockerGoga- ს მსხვერპლი ორი ამერიკული კომპანია გახდა

მავნე პროგრამული უზრუნველყოფა LockerGoga, გამოყენებულ იქნა ალუმინის მსხვილ ნორვეგიულ მწარმოებელ Norsk Hydro- ზე განხორციელებულ თავდასხმაში. შეტევის შედეგად კომპანია იძულებული გახდა ერთი კვირით შეეჩერებინა ოპერაციები. ინციდენტის დროს ორი ამერიკული კომპანიაც დაზარალდა.

კომპანია Momentive-ის გენერალური დირექტორის ჯეკ ბოსის მიერ ხელმოწერილი დოკუმენტის თანახმად, ინციდენტმა "IT სისტემების გლობალური გათიშვა" გამოიწვია, შექმნილი ვითარებიდან გამომდინარე მათ დახმარებისთვის სპეციალური დანიშნულების დანაყოფ SWAT-ს მიმართეს.

გამოსასყიდის მოთხოვნის შინაარსმა დაადასტურა რომ თავდასხმა გამომძალველი პროგრამული უზრუნველყოფის LockerGoga-ს გამოყენებით განხორციელდა. თავდასხმის დღეს, ორივე კომპანიის Windows PC- ზე, ლურჯი ეკრანი გამოისახა და ყველა ფაილი დაიშიფრა.

ჯეკ ბოსის მიერ ხელმოწერილი დოკუმენტის თანახმად, დაინფიცირებულ სისტემებში არსებული ინფორმაცია სრულად განადგურდა ხოლო კომპანიამ ასობით ახალი კომპიუტერი შეუკვეთა.

SecurityLab.ru by Positive Technologies WIRED

24 მარტი, 2019 წელი

პაროლების უსაფრთხოება

გთავაზობთ რამდენიმე რჩევას, რომელიც დაგეხმარებათ შეარჩიოთ საიმედო პაროლი და თავი დაიცვათ კიბერშეტევებისგან:

1. სხვადასხვა ანგარიშებისთვის გამოიყენეთ განსხვავებული პაროლი:
განსაკუთრებული ყურადღება გამოიჩინეთ იმ პაროლების მიმართ, რომლებსაც ფინანსურ სერვისებში იყენებთ. ასეთი პაროლები სხვა ანგარიშებისთვის არავითარ შემთხვევაში არ უნდა გამოიყენოთ;

2. შეეცადეთ პაროლი არ შეიცავდეს პერსონალურ ინფორმაციას, როგორიცაა, მაგალითად:
    a. დაბადების თარიღი;
    b. თქვენი ოჯახის წევრების სახელი და გვარი;
    c. თქვენი სამუშაო ადგილი და სხვა.

3. პაროლი სასურველია შედგებოდეს მინიმუმ 8 სიმბოლოსგან და შეიცავდეს:
    a. ერთ ან ორ დიდ ასოს;
    b. რამდენიმე პატარა ასოს;
    c. ციფრებს;
    d. სიმბოლოებს.

რაც უფრო მეტი სხვადასხვა კომბინაციისაგან იქნება თქვენი პაროლი შემდგარი, მით უფრო დაცული იქნება ჰაკერებისგან.

4. ხშირად შეცვალეთ პაროლები. სასურველია პაროლი შეიცვალოს 2-3 თვეში ერთხელ მაინც;

5. არ გაანდოთ პაროლი მესამე, განსაკუთრებით კი უცხო პირებს;

6. დაუშვებელია პაროლის ფურცელზე დაწერა მისი შენახვის მიზნით, ასევე მისი განთავსება გამოსაჩენ ადგილას;

7. არსებობს სპეციალური საშუალებები, რომელიც უნიკალურ, ძნელად გამოსაცნობ პაროლებს აგენერირებს:
    a. https://www.lastpass.com/
    b. https://www.passwordbox.com/
    c. https://www.identitysafe.norton.com/

8. გთავაზობთ შეამოწმოთ თქვენი პაროლის სირთულე და ასევე დრო, რამდენ ხანშიც არის მისი გამოცნობა შესაძლებელი: https://howsecureismypassword.net

9. რაც არ უნდა ძლიერი პაროლით სარგებლობდეთ, მაინც გააქტიურეთ ორმაგი ავთენტიფიკაციის ფუნქცია.

„ორმაგი ავთენტიფიკაციის“ ფუნქცია მომხმარებელს საშუალებას აძლევს არასანქცირებული წვდომისგან დაიცვას საკუთარი ანგარიში. სერვისის გააქტიურების შემთხვევაში, ავტორიზაციისთვის აუცილებელი სახელის და პაროლის მოთხოვნას

ემატება SMS-ით მიღებული კოდიც. შედეგად, ბოროტმოქმედი მომხმარებლის პაროლის მოპოვების შემთხვევაშიც კი მავნე ქმედების განხორციელებას ვეღარ შეძლებს.