ქართული ინტერნეტ სივრცის უსაფრთხოების ანგარიში 2020

cyberhouse

შინაარსი

წინასიტყვაობა

როდესაც ვსაუბრობთ ქართულ ინტერნეტ სივრცის უსაფრთხოებაზე, ვსაუბრობთ დაუცველობაზე, რეგულაციების საჭიროებაზე, სისუსტეზე. ჩვენ არ გვიკვირს, როდესაც ფართომასშტაბიანი შეტევა ხდება საქართველოში. მეტიც, ველოდით და ველით კიდეც.

თუმცა უსაფრთხოების კონკრეტულ პრობლემებზე ცოდნა გაფანტულია. გვსმენია, რომ ზოგი ორგანიზაცია სერვერებზე უსაფრთხოების განახლებებს არ აყენებს. ყური მოგვიკრავს, რომ უახლეს კრიტიკულ სისუსტეს, რომელსაც აქტიურად იყენებენ უცხოეთის სპეცსამსახურები, ქართულ ინტერნეტში სათანადო ყურადღება არ ექცევა.

სწორედ ამ გაფანტული მონაცემების თავმოყრა ვცადეთ ამ ანგარიშით. ვეცადეთ ერთიანად გვეჩვენებინა რა მასშტაბის პრობლემასა და რისკებთან შეიძლება გვქონდეს საქმე.

რაც მთავარია, მონაცემები მხოლოდ ღია წყაროებითა და ღია კოდის ხელსაწყოებით მოვაგროვეთ.

ამას ხაზს ვუსვამთ იმიტომ, რომ გავიაზროთ - ამ ინფორმაციის მოგროვება ნებისმიერ ადამიანს შეუძლია, დაწყებული ე.წ. script kiddie-ებით, დამთავრებული ორგანიზებული ჯგუფებით და სპეცსამსახურებით. პრობლემები ზედაპირზეა. დროა დავიწყოთ მათი მოგვარება.

ვხვდებით, რომ საკითხების მხოლოდ ნაწილს შევეხეთ. რეპორტს 2021-შიც გავაკეთებთ. გვსურს ბევრად უკეთესი გამოვიდეს. ველით ფიდბექს. მივიღებთ კრიტიკას.

მიხეილ ბასილაია

კიბერჰაუსის თანა-დამფუძნებელი

შეჯამება და მეთოდოლოგია

თანამედროვე სამყაროში სულ უფრო მეტი ორგანიზაცია მიისწრაფის ციფრული ტრანსფორმაციისკენ, რომელიც დადებით ზეგავლენასთან ერთად, უფრო დიდ და კომპლექსურ გამოწვევებთან გამკლავებას მოიაზრებს. რაც უფრო ვითარდება სამყარო ტექნოლოგიური თვალსაზრისით, მით უფრო დახვეწილია თავდამსხმელების მიერ სისტემების გატეხვისა და მონაცემთა მოპოვების მიდგომები. გადავწყვიტეთ ჩაგვეტარებინა კვლევა იმისათვის, რომ უფრო თვალსაჩინო ყოფილიყო საქართველოს ინტერნეტ სივრცის ვითარება კიბერ უსაფრთხოების კუთხით.

მოცემულ კვლევაში თავმოყრილია ქართულ ინტერნეტ სივრცეში არსებული სერვერებისა და ვებ-გვერდების სტატისტიკური მონაცემები და გაანალიზებულია რეალურად არსებული თუ პოტენციური სისუსტეები და მათი გავლენა ქართულ კიბერსივრცეზე.

კვლევისთვის მოპოვებული ინფორმაცია მოიცავს მხოლოდ საჯაროდ ხელმისაწვდომ მონაცემებს

რეპორტი უფრო მეტად ინფორმირებულს გაგხდით ისეთი საკითხების შესახებ, როგორიცაა SSL/TLS სერტიფიკატები და მათი სისუსტეები, DNS, NTP სერვერები, მეილ სერვერები და ასევე გაგაცნობთ ქართული ვებ-გვერდების სტატისტიკურ მონაცემებს სხვადასხვა თემატიკის მიხედვით (ვებ სერვერები, პროგრამირების ენები, ვებ ფრეიმვორკები და ა.შ.).

კვლევისთვის მოპოვებული ინფორმაცია მოიცავს მხოლოდ საჯაროდ ხელმისაწვდომ მონაცემებს, რაც ნიშნავს იმას, რომ რესურსები ნებისმიერი დაინტერესებული პირისთვის ხელმისაწვდომია. ინფორმაციის შეგროვება განხორციელდა მხოლოდ ღია, ე.წ. open source ხელსაწყოების გამოყენებით. კვლევაში გამოვიყენეთ შემდეგი ღია კოდის ხელსაწყოები: testssl.sh, Masscan, Shodan, Wappalyzer.

ჩვენი გუნდის მიერ ჩატარებული კვლევა გამყარებულია საერთაშორისოდ აღიარებული წყაროებით და მაგალითებად მოყვანილია ოფიციალურად დადასტურებული სისუსტეები. რეპორტში მოყვანილი 2018 წლების მონაცემები მოპოვებულია ზვიად კიკვიძის მიერ და ღიად ხელმისაწვდომია github-ზე.

იმედი გვაქვს, კიბერჰაუსის მიერ ჩატარებული კვლევა დადებით ზეგავლენას მოახდენს ქვეყანაში ინფორმაციული უსაფრთხოების კუთხით არსებულ ვითარებაზე.

რეპორში მოყვანილი გვაქვს NVD-ის (National Vulnerability Database) სისუსტეების კრიტიკულობის შეფასების ქულათა სისტემა (CVSS v3.0), რომელიც მოცემული ცხრილში და რეპორტში სისუსტეების კრიტიკულობა სწორედ ამ შკალის მიხედვით იქნება აღწერილი.

კრიტიკულობა	ქულების დიაპაზონი
დაბალი	0.1 – 3.9
საშუალო	4 – 6.9
მაღალი	7 – 8.9
კრიტიკული	9.0 – 10.0

SSL/TLS სისუსტეების სტატისტიკა

SSL/TLS პროტოკოლი გამოიყენება მონაცემთა კონფიდენციალურობისა და მთლიანობის დასაცავად და ასევე შეუძლია კომუნიკაციის მხარეების აუთენთიფიკაცია. SSL/TLS სერტიფიკატები ერთმანეთთან აკავშირებენ კრიპტოგრაფიულ გასაღებსა და დომეინის სახელს, და არიან ციფრულად ხელმოწერილები სანდო მესამე მხარის (სასერტიფიკატო ორგანო / Certification Authority/CA) მიერ. SSL პროტოკოლი ჩაანაცვლა TLS პროტოკოლმა, თუმცა SSL და TLS ხშირად სინონიმური მნიშვნელობით იხმარება.

71%-ს

დასკანირებული სერვერების გააჩნია 1 სისუსტე მაინც

SSL-ზე სკანირება ჩატარდა მასიური სკანირების ხელსაწყო masscan-ით. 443-ე პორტზე დასკანერებული ქართული IP დიაპაზონების შემოწმების შედეგად გამოვლინდა 7644 სერვერი, რომლებიც, თავის მხრივ, დასკანირდა SSL/TLS სისუსტეებზე. სისუსტეების სკანირებისთვის გამოვიყენეთ ხელსაწყო testssl.sh.

7644 გამოვლენილი სერვერიდან ხელსაწყოს საშუალებით განხორციელდა 5473 სერვერის სკანირება. გაანალიზებული სერვერები შეგვიძლია დავყოთ ხუთ სკანირებულ ტიპად:

1. მოწყვლადი,
2. პოტენციურად მოწყვლადი,
3. პოტენციურად არამოწყვლადი,
4. არამოწყვლადი,
5. სკანირება შეუძლებელია.

56%

სერვერების ამ ნაწილს გააჩნია მაღალი კრიტიკულობის სისუსტე(ები)

გრაფიკზე წარმოდგენილია პირველი სამი ტიპის მონაცემები ერთად, იმისთვის, რომ უფრო თვალსაჩინო ყოფილიყო დაუცველობის მაჩვენებელი. სისუსტეებიდან რაოდენობრივად ყველაზე მეტი არის Lucky13, ხოლო ყველაზე ნაკლები - Heartbleed და Ticketbleed. თითოეული სისუსტე აღწერილია ცალ-ცალკე და მოცემულია მათი კრიტიკულობის მაჩვენებლები.

ამასთან, testssl-ით სკანირებისას, აღნიშნული სისუსტეების ნაწილი გამოვლინდა პოტენციურად მოწყვლადი ან პოტენციურად არამოწყვლადი ტიპის სახით. გამომდინარე იქიდან, რომ სკანერის ოფიციალურ სახელმძვანელოში ტერმინები დაზუსტებული არ არის, სისუსტის პოტენციური გამოვლინება მივაკუთვნეთ მოწყვლად ვარიანტს.

ჯამში გაანალიზდა

7644

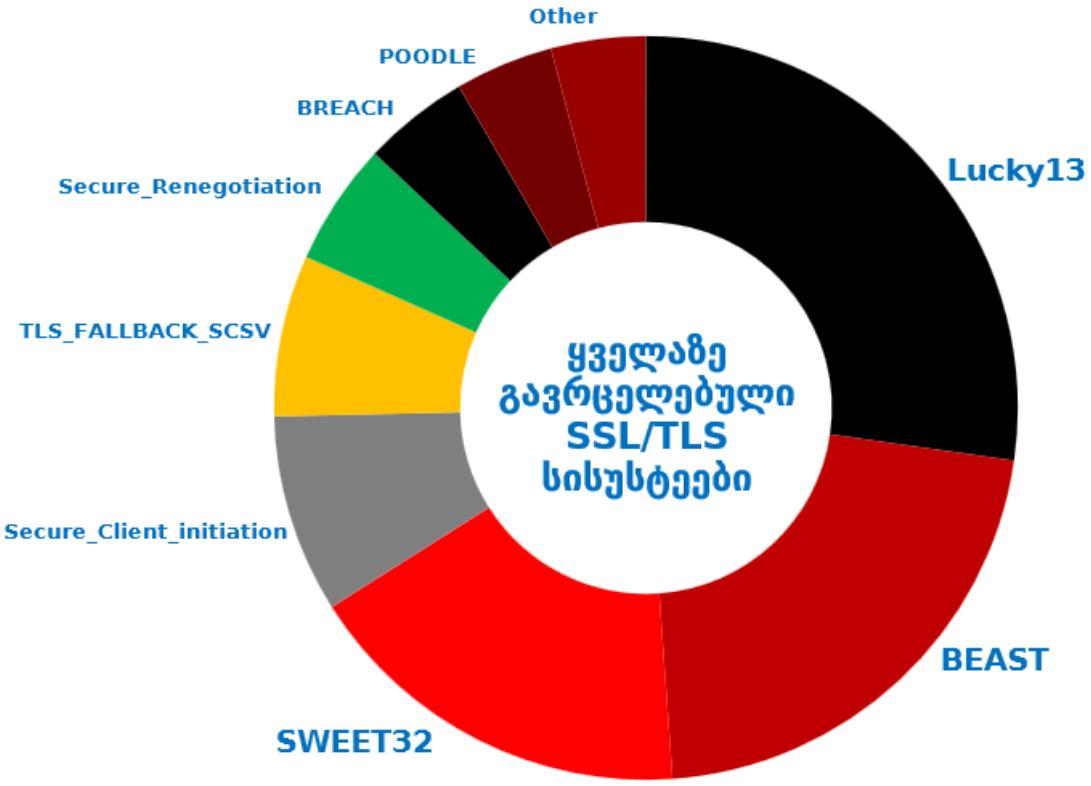
სერვერი

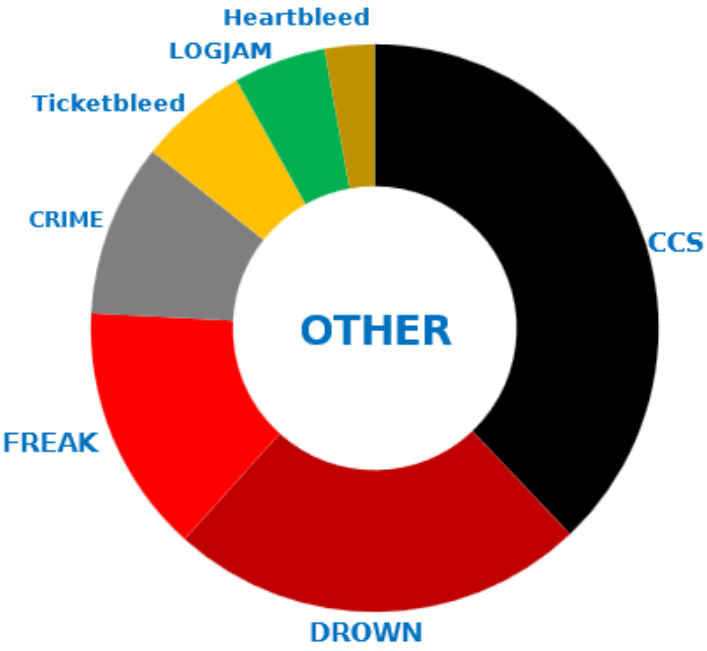
სისუსტე დაფიქსირდა

5473

სერვერზე

სისუსტე	CVE ID	CVSS ქულა	კრიტიკულობა	რაოდენობა
Ticketbleed	CVE-2016-9244	7.5	High	**46**
SWEET32	CVE-2016-2183	7.5	High	**3089**
Heartbleed	CVE-2014-0160	7.5	High	**21**
CCS	CVE-2014-0224	7.4	High	**281**
DROWN	CVE-2016-0800	5.9	Medium	**176**
BEAST	CVE-2011-3389	4.3	Medium	**3889**
FREAK	CVE-2015-0204	4.3	Medium	**105**
LOGJAM	CVE-2015-4000	3.7	Low	**39**
POODLE	CVE-2014-3566	3.4	Low	**769**
LUCKY13	CVE-2013-0169	2.6	Low	**4909**
CRIME	CVE-2012-4929	2.6	Low	**73**


Other
POODLE
BREACH
Secure_Renegotiation
TLS_FALLBACK_SCSV
Secure_Client_initiation
SWEET32
BEAST
Lucky13
ყველაზე გავრცელებული SSL/TLS სისუსტეები


Heartbleed
LOGJAM
Ticketbleed
CRIME
FREAK
DROWN
CCS
OTHER

BEAST

CVE-2011-3389 4.3 Medium

Beast (**B**rowser **E**xploit **A**gainst **S**SL/**T**LS) შეტევის დროს ხდება Cipher Block Chaining (CBC) შიფრაციის მოდელის სისუსტის ექსპლუატაცია SSL/TLS კავშირის „გასატეხად“. გრაფიკის მიხედვით, სკანირებისას გამოვლენილია 3889 Beast სისუსტე. აღსანიშნავია, რომ ამ სისუსტემ შეიძლება გამოიწვიოს ე.წ. MITM შეტევები SSL-ის წინააღმდეგ, რაც საშუალებას მისცემს ჰაკერებს მოახდინონ დეშიფრაცია და მიიღონ ავტორიზაციის token-ები, რითაც შეძლებენ წვდომა ჰქონდეთ ვებ აპლიკაციასა და მომხმარებელს შორის გაცვლილ ინფორმაციაზე.

BREACH

Browser **R**econnaissance & **E**xfiltration via **A**daptive **C**ompression of **H**ypertext შეტევა CRIME-ის მსგავსია (და ასევე Low (დაბალი) კრიტიკულობისაა), თუმცა მისგან განსხვავებით, ამ დროს თავდასხმა ხორციელდება HTTP პასუხზე და TLS-ის დონეზე კომპრესია არ ხდება. ეს სისუსტე 833 სერვერზე გვხვდება.

CCS

CVE-2014-0224 7.4 High

CCS სისუსტე საშუალებას აძლევს არაავტორიზებულ პირებს ხელში ჩაიგდონ დაშიფრული მონაცემები და მოახდინონ მათი დეშიფრაცია. CCS სისუსტე გამოსაყენებლად შედარებით მარტივია. კვლევის მიხედვით, გამოვლინდა 195 მოწყვლადი CCS სისუსტის მქონე სერვერი.

CRIME

CVE-2012-49292.6 Low

CRIME (**C**ompression **R**atio **I**nfo-leak **M**ade **E**asy) წარმოადგენს უსაფრთხოების ექსპლოიტს ვებ cookie-ების წინააღმდეგ. სისუსტე ეხება ისეთ HTTPS კავშირებს, რომლებშიც გამოყენებულია მონაცემთა კომპრესია. მოცემული სისუსტე ეხება TLS 1.2 პროტოკოლს ან მის ადრეულ ვერსიებს. შეტევა MITM თავდამსხმელებს საშუალებას აძლევს მოიპოვონ დაუშიფრავი HTTP ჰედერები. Crime სისუსტის რაოდენობა, როგორც გრაფიკზე ხედავთ, 73-ის ტოლია. წინა წლებში სისუსტეს უფრო ხშირი გამოვლინება ჰქონდა, წლევანდელ მონაცემებში რაოდენობა შემცირებულია.

Drown

CVE-2016-0800 5.9 Medium

Drown შეტევა საშუალებას აძლევს თავდამსხმელებს, დაარღვიონ შიფრაცია და წაიკითხონ ან მოიპარონ სენსიტიური ინფორმაცია, მათ შორის, პაროლები, საკრედიტო ბარათის ნომრები, ფინანსური მონაცემები. შეტევა ხორციელდება SSLv2 და TLS პროტოკოლებზე. სკანირების შედეგად გამოვლინდა 176 Drown სისუსტე. 2018 წელთან შედარებით სისუსტის რაოდენობა შემცირებულია.

TLS_FALLBACK_SCSV

TLS Signaling Cipher Suite Value (SCSV) არის მახასიათებელი, რომელიც იცავს პროტოკოლს ე.წ. downgrade შეტევებისგან. სერვერზე ეს ფუნქცია თუ არ არის ჩართული, MITM თავდამსხმელმა შესაძლოა კლიენტი ყველაზე სუსტ (და მოწყვლად) პროტოკოლზე გადაიყვანოს. თავდამსხმელს შეეძლება კომუნიკაციის დროს გადაცემული ინფორმაციის როგორც წაკითხვა, ასევე, შეცვლა. სკანირების შედეგად გამოვლინდა **tls_fallback_scsv** ტიპის 371 სისუსტე.

FREAK

CVE-2015-0204 4.3 MEDIUM

Freak შეტევა საშუალებას აძლევს თავდამსხმელს აიძულოს HTTPS კავშირის მხარეები გამოიყენონ სუსტი კრიპტოგრაფია და მათი ექსპლუატაციით ხელში ჩაიგდოს კონფიდენციალური ინფორმაცია ან შეცვალოს კომუნიკაციის შინაარსი. სერვერები, რომლებიც იყენებენ RSA Export Cipher Suites-ს (მაგ. TLS_RSA_EXPORT_WITH_DES40_CBC_SHA) იმყოფებიან რისკის ქვეშ. 105 სერვერს გააჩნია FREAK სისუსტე.

Heartbleed

CVE-2014-0160 7.5 High

Heartbleed არის ცნობილი და სერიოზული უსაფრთხოების ბაგი OpenSSL-ის კრიპტოგრაფიულ ბიბლიოთეკაში. ამ სისუსტის საშუალებით თავდამსხმელს შეუძლია სისუსტის მქონე სერვერის RAM-დან მიიღოს მონაცემები, რომელშიც მოცემულია სხვადასხვა HTTPS კავშირების ინფორმაცია, მათ შორის დახურული გასაღებებიც. ცხადია ამ ინფორმაციით, თავდამსხმელი შეძლებს სხვისი HTTPS კომუნიკაციის გაშიფრვას. აღსანიშნავია Heartbleed სისუსტის მარტივი ექსპლუტაცია (ავტომატური ხელსაწყობეიც არსებობს). ქართულ კიბერ სივრცეში ამ სისუსტის მქონე 21 სერვერი არსებობს.

LOGJAM

CVE-2015-4000 3.7 Low

Diffie–Hellman key exchange არის კრიპტოგრაფიული ალგორითმი, რომელიც საშუალებას აძლევს მხარეებს გაცვალონ შიფრაციის დახურული გასაღებები უსაფრთხოდ. DH Key Exchange უამრავ პროტოკოლში გამოიყენება, მაგალითად SSH, IPSec, SMTPS, HTTPS. . . Logjam შეტევა TLS პროტოკოლის წინააღმდეგ საშუალებას აძლევს MITM თავდამსხმელებს ჩამოაქვეითონ მოწყვლადი TLS კავშირები სუსტ ალგორითმებამდე, შემდეგ კი „გატეხონ“ ეს კავშირი და წაიკითხონ კონფიდენციალური ინფორმაცია ან შეცვალონ კომუნიკაციის შინაარსი. სკანერმა გამოავლინა Logjam სისუსტის მქონე 39 სერვერი.

LUCKY13

CVE-2013-0169 2.6 Low

შეტევის ეს ტიპი ხორციელდება CBC შიფრაციის მოდელისა და MAC-then-Encrypt სქემის წინააღმდეგ. TLS MAC მოიცავს ჰედერის ინფორმაციის 13 ბაიტს, სწორედ ამიტომ ჰქვია ამ სისუსტეს Lucky 13. Testssl-ით სკანირების დროს გამოვლინდა 0 მოწყვლადი და 7740 პოტენციურად მოწყვლადი lucky13 სისუსტე.

POODLE

CVE-2014-3566 3.4 Low

Poodle (**P**adding **O**racle **O**n **D**owngraded **L**egacy **E**ncryption) წარმოადგენს MITM ექსპლოიტს. ეს სისუსტე გააჩნია SSL 3.0 ვერსიას, რომელიც იყენებს CBC შიფრაციას. კვლევის შედეგად გამოვლინდა 769 (სერვერების 10%-ზე მეტი) Poodle სისუსტე.

Secure Client-Initiated Renegotiation

წარმოადგენს ფუნქციას, რომელიც საშუალებას აძლევს კლიენტს გადააკეთოს დაშიფვრის პარამეტრები SSL/TLS კავშირისთვის TCP-ს გამოყენებით. შეტევის ეს ტიპი მნიშვნელოვანია იმით, რომ იგი DoS-ის საფრთხის შემცველია. გამოვლენილია 1409 მოწყვლადი (სერვერების 20%)სერვერი.

Secure Renegotiation

შეტევის დროს არაავტორიზებულ მხარეს სერვერთან კავშირის დამყარების შემდეგ საშუალება აქვს დაშიფრულ პაკეტებში დეტალები შეცვალოს. გამოვლინდა 960 სისუსტის მქონე სერვერი (2018 წელს იყო 811).

SWEET32

CVE-2016-2183 7.5 High

Sweet32 Birthday Attack 64-ბიტიან ბლოკურ შიფრების CBC რეჟიმის სისუსტეა. სკანირების შედეგად გამოვლინდა 3089 Sweet32 სისუსტე. გასულ წლებთან შედარებით მონაცემები შემცირებულია, თუმცა უმნიშვნელოდ.

SSL ვერსიების სტატისტიკა

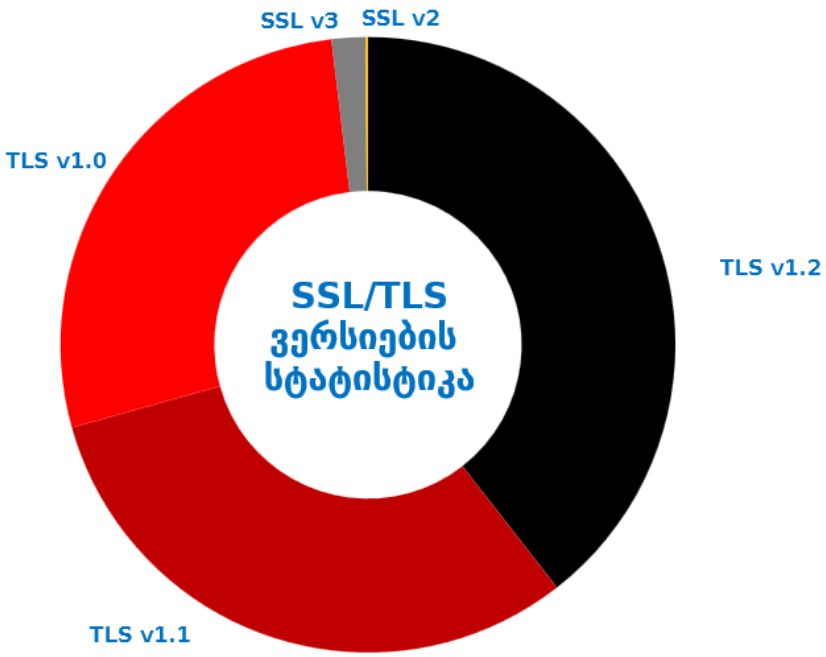
გამომდინარე იქიდან, რომ ღიად ხელმისაწვდომი ქართული ვებ-გვერდების თავმოყრა ყველაზე უკეთ Top.ge-დან შეიძლებოდა, გადავწყვიტეთ ვერსიების სკანირებისას კვლევაში სწორედ ამ საიტზე რეგისტრირებული ვებ-გვერდები გაგვეანალიზებინა.

2020 წლის მონაცემებით, Top.ge-ზე რეგისტრირებული ვებ-გვერდების სკანირებისას მივიღეთ შემდეგი სტატისტიკა: 7687 საიტი იყენებს TLSv1.2 ვერსიას, დანარჩენ ვერსიებზე ნაკლები რაოდენობით, თუმცა მაინც აქტიურად, გამოყენებულია SSL-ის ძველი ვერსიები, რაც მკვეთრად ზრდის დაუცველობის რისკებს. ვებ-გვერდების TLSv1.3 ვერსიაზე სკანირება არ განხორციელებულა.

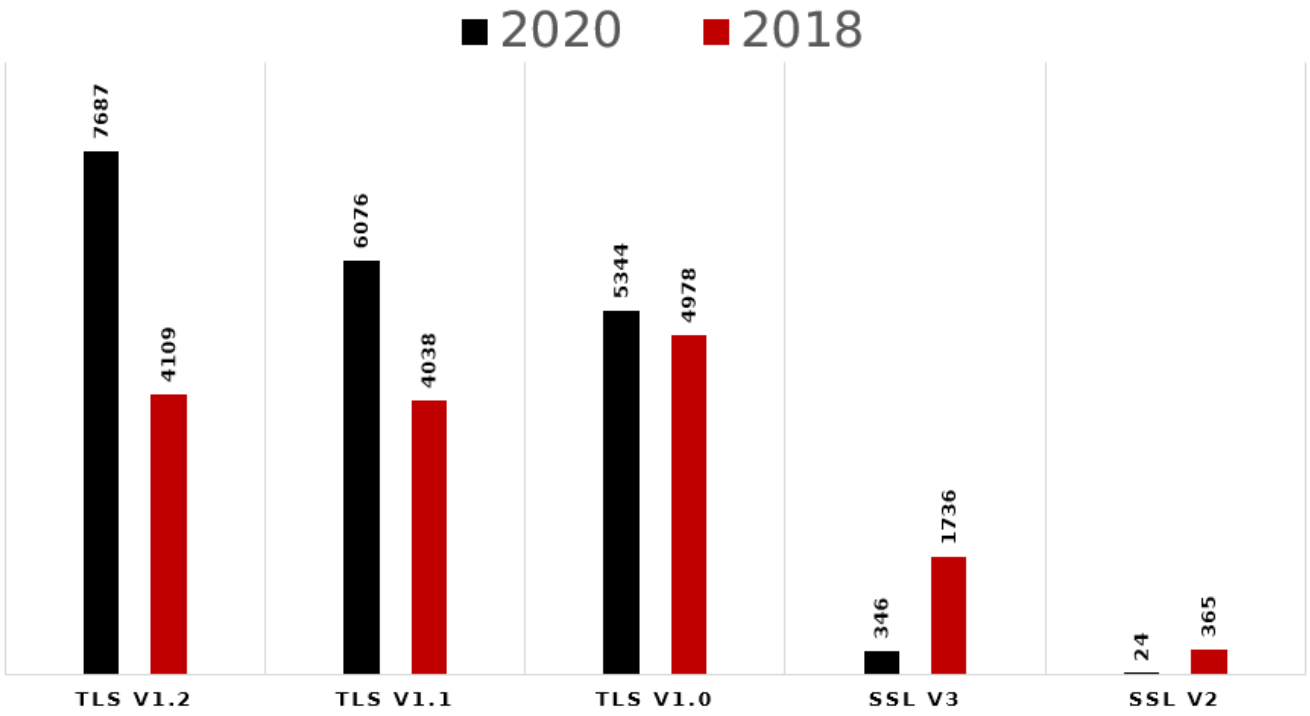
ვებ გვერდების ნაწილი ისევ იყენებს SSL/TLS პროტოკოლის იმ ვერსიებს, რომლებიც ადვილად მოწყვლადია და სენსიტიურ ინფორმაციას რისკის ქვეშ აყენებს

ზემოთ აღწერილი სისუსტეები უმეტესობა SSL v2-სა და SSL v3-ს აქვთ. პროტოკოლის ეს ვერსიები ამოღებულია ხმარებიდან და მათი გამოყენება სერიოზულ რისკებს წარმოშობს.

საუკეთესო პრაქტიკას აღარ შეესაბამება არც TLS v1.0-სა და TLS v1.1-ის გამოყენება.



გრაფიკზე წარმოდგენილია SSL ვერსიების სტატისტიკა 2018 და 2020 წლებში. უახლესი ვერსიების უფრო მასშტაბურად გამოყენების ტენდენციის მიუხედავად, რჩება ვებ-გვერდების საკმაოდ დიდი ნაწილი, რომელსაც კვლავ განუახლებელი აქვს SSL/TLS პროტოკოლის კონფიგურაცია და იყენებს პროტოკოლის იმ ვერსიებს, რომლებიც ადვილად მოწყვლადია და სენსიტიურ ინფორმაციას მაღალი რისკის ქვეშ აყენებს.



DNS

DNS-ის (Domain Name System) საშუალებით დომენური სახელები ითარგმნება IP მისამართებად. DNS წარმოადგენს იერარქიულ და დეცენტრალიზებულ სისტემას ინტერნეტთან დაკავშირებული მოწყობილობებისთვის.

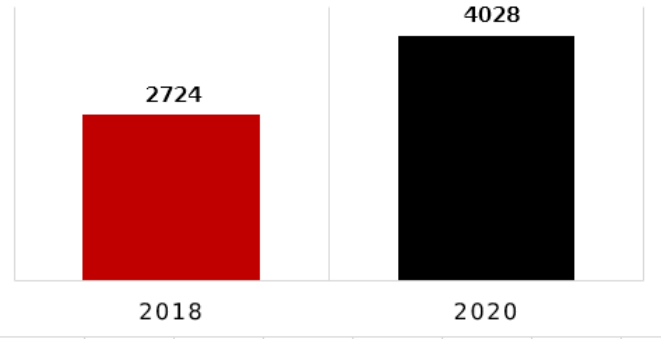
ქართულ კიბერ სივრცეში მივაკვლიეთ 8874 DNS სერვერს (უფრო ზუსტად, მოწყობილობას, რომელზეც გააქტიურებულია DNS – მაგალითად, შეიძლება იყოს ქსელური მარშრუტიზატორი). კვლევისას გამოვიყენეთ ინტერნეტთან დაკავშირებული მოწყობილობების საძიებო სისტემა Shodan, რომელიც ფასდაუდებელი ინსტრუმენტია დაუცველობის შესაფასებლად. სხვა დანარჩენი ხელსაწყოების მსგავსად, Shodan-იც ღია პროექტს წარმოადგენს და მისი გამოყენება ნებისმიერ ადამიანს შეუძლია.

დიაგრამაზე ნაჩვენებია სერვერების პროცენტული განაწილება ინტერნეტ სერვის პროვაიდერების მიხედვით. კვლევის შედეგად გამოვლენილ DNS სერვერებში Magticom Ltd ყველაზე დიდი მომწოდებელია (43.8%), მეორე ადგილზეა LTD CGC Co - 34.3%, მესამეზე კი JSC Silknet - 8.2%. დარჩენილი პროვაიდერები კიდევ უფრო ნაკლები სიხშირით გვხვდება.

Magticom	3128
CGC CO	2490
Silknet	595
Proservice	186
System Net	185
Global Erty	184
Caucasus Online	175
Cloud 9	171
Service	98
Serv.Ge	76
OTHER	1586

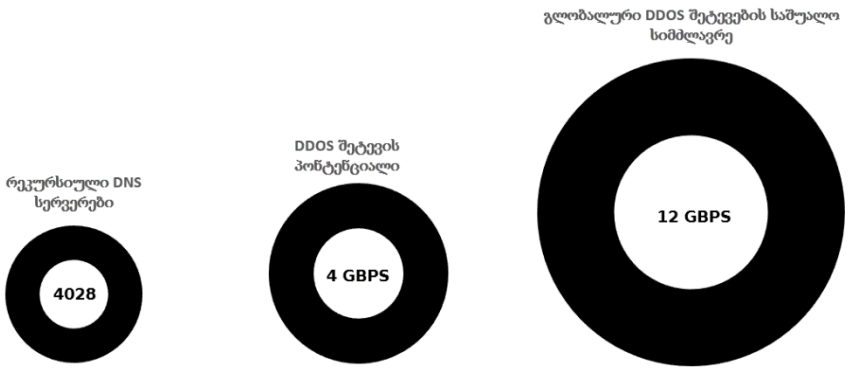
DNS სერვერებში გავაანალიზეთ რეკურსიულობა. ისეთი DNS სერვერი, რომელიც არა მხოლოდ სანდო ქსელიდან, არამედ ინტერნეტიდანაც იღებს DNS მოთხოვნებს და ჩართულია აქვს რეკურსიის ფუნქცია, შეიძლება გამოყენებულ იქნას DNS ამპლიკაციის შეტევაში. ასეთი სერვერების წინააღმდეგ შესაძლებელია DNS cache poisoning შეტევაც.

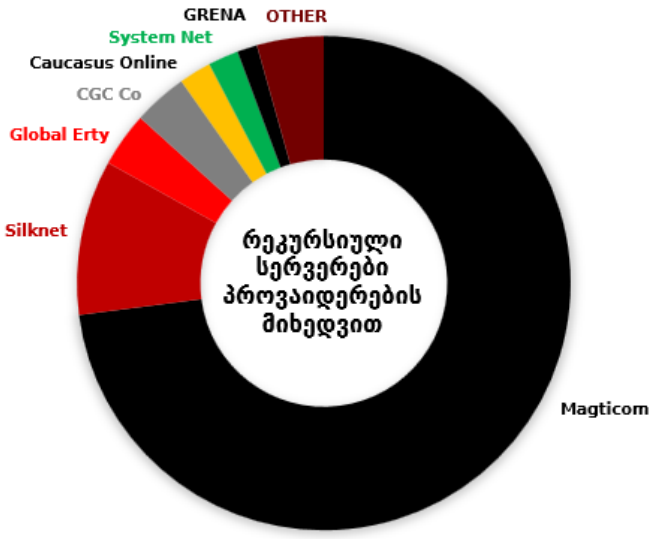
2018 წელთან შედარებით რეკურსიული DNS სერვერების რაოდენობა გაიზარდა



თუ ჩავთვლით, რომ ყველა რეკურსიული სერვერის გამოყენება შეიძლება DDoS ამპლიფიკაციის შეტევაში, მხოლოდ ქართული რესურსით 4GB წამში სიმძლავრის შეტევის მიღწევა შეიძლება

(თითოეულ მოწყობილობას 1 MBPS მოცულობა რომ ჰქონდეს)

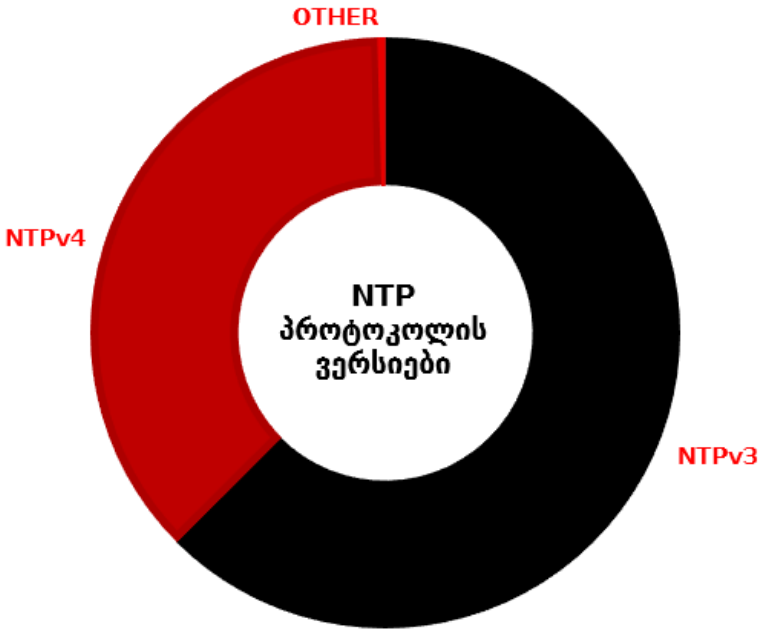




NTP

NTP არის ქსელის სტანდარტული პროტოკოლი დროის სინქრონიზაციისთვის. დროის სინქრონიზაცია მნიშვნელოვანია სერვერების გამართული მუშაობისა და ლოგირების ფუნქციონალისთვის. პროტოკოლში გათვალისწინებულია სხვადასხვა შესაძლებლობები, მათ შორის გამართული მუშაობის მონიტორინგის შესაძლებლობა.

ქართულ კიბერ სივრცეში NTP პროტოკოლს 13,535 სერვერი იყენებს. დიაგრამაზე ასახულია გამოყენებული NTP პროტოკოლის ვერსიების გადანაწილება Shodan-ის მონაცემების მიხედვით. როგორც ხედავთ, სერვერების უმრავლესობა (62.5%) NTP v3 ვერსიას იყენებს, 37.1% - NTP v4 ვერსიას. NTP v3 პროტოკოლის ძველი ვერსიაა, რომელიც უსაფრთხოების ბაგებს შეიცავს და გარკვეული კონფიგურაცია შეიძლება ექსპლუატაციის მაღალი რისკით გამოირჩეოდეს. თუმცა მე-3 ვერსიის გამოყენება ავტომატურად არ ნიშნავს სისუსტეების ქონას, არამედ დამოკიდებულია კონკრეტულ კონფიგურაციაზე.



Remote Code Execution (RCE) წარმოადგენს ზოგად ტერმინს შეტევის ტიპებისთვის. RCE შეტევა თავდამსხმელს საშუალებას აძლევს დისტანციურად გაუშვას მავნე კოდი და წვდომა მოიპოვოს მსხვერპლის კომპიუტერზე ან სერვერზე.

NTP v3-ის ერთ-ერთი სისუსტის გამოყენებით, 1 GB-იანი ქსელური ინტერფეისით თავდამსხმელს თეორიულად შეუძლია დააგენერიროს 200 GB ტრაფიკი

NTPv3-ის ყველაზე საშიში რისკია DDoS შეტევა monlist (MON_GETLIST)-ის გამოყენებით. როდესაც NTP სერვერი იღებს monlist ბრძანებას, ის აბრუნებს უახლესი აქტივების ჩამონათვალს, რომლებიც სერვერთან იყვნენ კონტაქტში. დაახლოებით 250 ბაიტიანმა monlist მოთხოვნამ, შესაძლოა სერვერს დააბრუნებინოს რამდენიმე კილობაიტის ინფორმაცია. ამ შემთხვევაში პასუხი 200-ჯერ და უფრო მეტჯერ დიდია მოთხოვნის ზომაზე. ამრიგად, 1 GB-იანი ქსელური ინტერფეისით თავდამსხმელს თეორიულად შეუძლია დააგენერიროს 200 GB ტრაფიკი. ეს დაუცველობა კლასიფიცირდება, როგორც CVE-2013-5211.

მხოლოდ DDoS შეტევა არ წარმოადგენს NTPv3 ვერსიის რისკს. შესაძლოა თავდამსხმელმა გამოიყენოს remote code execution სისუსტეები, რომლებიც ჰაკერს მისცემს დისტანციური წვდომის უფლებას სერვერზე ან სახლის როუტერზე ადმინისტრატორის/root პრივილეგიით.

NTP პროტოკოლის უახლესი ვერსიების უმრავლესობა დაუცველი არ არის, რადგან monlist ბრძანება სტანდარტულად გათიშულია. თუმცა, თუ ძველ ვერსიებთან თავსებადობა გააქტიურებულია, NTP daemon-ის ძველმა ვერსიებმა შესაძლოა monlist ბრძანება ავტომატურად გააააქტიურონ. ამრიგად, თუ ქსელში NTP სერვერები გაქვთ, განაახლეთ NTP უახლეს ვერსიამდე, ხოლო თუ განახლება შეუძლებელია, გათიშეთ monlist ბრძანება ან დარწმუნდით, რომ ყოველი მოთხოვნა ვალიდური წყაროებიდან მოდის.

მეილ სერვერები

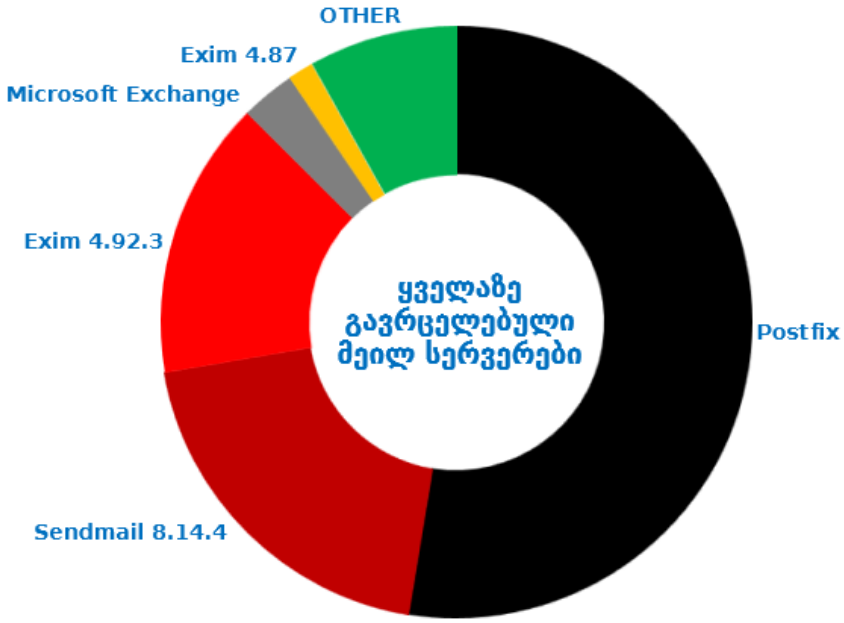
82

მეილ სერვერების სულ მცირე ამ რაოდენობას გააჩნია მაღალი კრიტიკულობის (CVSS >7.5) სისუსტე

მეილ სერვერი წარმოადგენს ელექტრონული ფოსტის მიმღებ და გამგზავნ საშუალებას. ყველაზე მნიშვნელოვანი საფოსტო პროტოკოლებია SMTP, POP3, IMAP4.

SMTP (Simple Mail Transfer Protocol) პროტოკოლის ფუნქციაა ელ-ფოსტის გაგზავნა. POP და IMAP პროტოკოლები მომხმარებელს საშუალებას აძლევს მიიღოს მეილები სერვერიდან კლიენტურ აპლიკაციაში. ერთ-ერთი განსხვავება ამ 2 პროტოკოლს შორის ის არის, რომ POP (Post Office Protocol) ჩამოტვირთავს მეილს სერვერიდან და სერვერზე არ ტოვებს, IMAP (Internet Message Access Protocol) კი სერვერიდან მეილს კლიენტურ აპლიკაციაში აკოპირებს. ამ პროტოკოლების ბოლო ვერსიებია POP3 და IMAP4.

არსებობს უამრავი საფრთხე, რომელიც შესაძლოა მეილ-სერვერებს დაემუქროს, ესენია: მონაცემებზე არაავტორიზებული წვდომა, მონაცემთა გაჟონვა, სპამი, მავნე პროგრამები, DoS და DDoS შეტევები და ა.შ. თითოეული პროტოკოლის შემთხვევაში ნაპოვნია კრიტიკული სისუსტეები, რომლებიც სერიოზულ საფრთხეს უქმნის მომხმარებლებს, და შესაძლოა მნიშვნელოვანი ფინანსური თუ ინფორმაციული ზარალი მიაყენოს ბიზნესს.



Shodan-ის საშუალებით მაილ-სერვერების კვლევისას გაანალიზდა 1894 სერვერი. სტატისტიკური მონაცემების მიხედვით, შემდეგი რეზულტატი მივიღეთ გამოყენებული მეილ სერვერების შესახებ: Postfix smtpd - 52.6%, Sendmail 8.14.4 - 19.7%, Exim smtpd 4.92.3 - 15.2%.

Exim-ის მეილ სერვერებში ნაპოვნია მრავალი კრიტიკული დაუცველობა, რომლებიც თავდამსხმელებს საშუალებას აძლევს მოიპოვონ დისტანციური წვდომა და განახორციელონ მავნე მოქმედებები. მაგალითად, CVE-2019-16928, CVE-2019-15846 და CVE-2019-10149. Exim ბაგები საშიშია Heap-based Buffer Overflow და Remote Code Execution შეტევებით. აქვე აღსანიშნავია, რომ Exim smtpd 4.92.3 ვერსიაში კრიტიკული სისუსტეები გასწორებულია.

SMB

SMB (Server Message Block) წარმოადგენს კომპიუტერებს შორის ფაილების გასაზიარებელ პროტოკოლს.

Shodan-ის გამოყენებით გავაანალიზეთ 583 სერვერი, რომლებიც იყენებდნენ SMBv1 და SMBv2 ვერსიებს. სერვერების 81.8% SMBv1 ვერსიაზე მოდის, ხოლო ამავე ვერსიის გაუაქტიურებელ ვარიანტზე - 6.7%. გააქტიურებულ SMBv2 ვერსიაზე - 11.1%, გაუაქტიურებელზე კი - 0.3%.

477

სწორედ ამდენ სერვერზეა გააქტიურებული SMBv1, რომელსაც კრიტიკული სისუსტეები აქვს

მოძველებულ SMB ვერსიებს აქვთ უამრავი კრიტიკული სისუსტე. დისტანციურ თავდამსხმელს Microsoft SMBv1 ვერსიაზე შესატევად მაღალი და კრიტიკული სისუსტეების ფართო არჩევანი აქვს: CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, CVE-2017-0276. ეს მხოლოდ არაავტორიზებული წვდომის მოსაპოვებელი სისუსტეები იყო. ამათ ემატება DoS შეტევების სისუსტეები: CVE-2017-0269, CVE-2017-0273, CVE-2017-0280 და Remote Code Execution სისუსტეები, როგორიცაა CVE-2017-0272, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279.

ყველაზე ცნობილი SMBv1 ექსპლოიტებია: EternalRomance, ETERNALBLUE, EternalChampion. აქვე უნდა ვახსენოთ, მასშტაბური გამომძალველი ვირუსი WannaCry, რომელმაც 2017 წელს რამდენიმე საათში 230 ათასზე მეტი კომპიუტერი დააინფიცირა. ასევე, Petya/NotPetya, რომელმაც სერიოზული ზიანი მიაყენა უკრაინის ელექტროსისტემას და მილიონობით ადამიანი ელექტრო ენერგიის გარეშე დატოვა. ამ ვირუსების სამიზნე სწორედ SMBv1 პროტოკოლი იყო.

WannaCry - მალვეარი სწორედ SMBv1-ის სისუსტეს იყენებს

რამდენიმე კრიტიკული სისუსტე SMBv2 ვერსიაზეც არის ნაპოვნი, რომელთა საშუალებით დისტანციურ თავდამსხმელს შეუძლია (CVE-2009-2526, CVE-2009-3103) სერვერზე განახორციელოს DoS შეტევა.

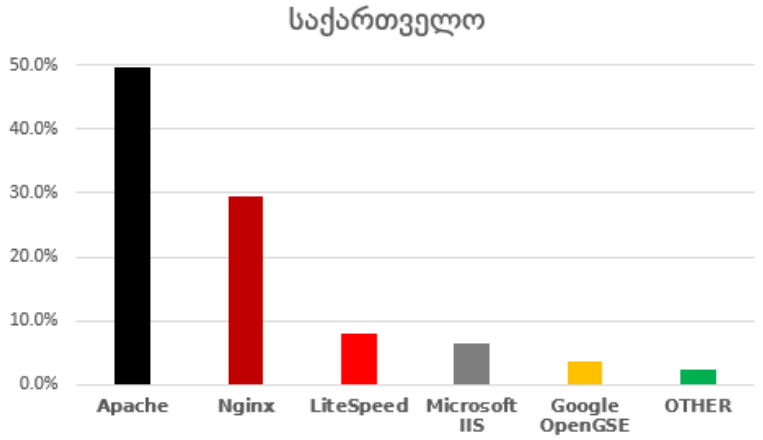
აღსანიშნავია, რომ 2020 წლის მარტში აღმოაჩინეს ვინდოუსის SMBv3 ვერსიის RCE სისუსტე CVE-2020-0796. მოცემული დაუცველობით დისტანციურ თავდამსხმელს შეეძლო სრული კონტროლი მოეპოვებინა ინფიცირებულ სისტემაზე.

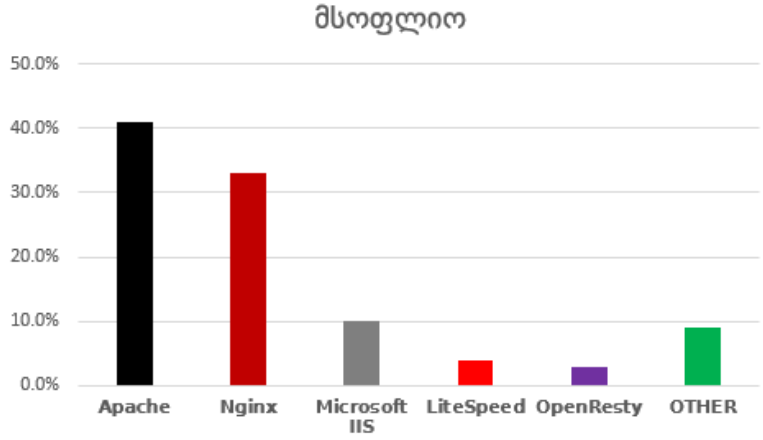
.GE გვერდების ტექნოლოგიური სტატისტიკა

ქვემოთ მოცემული სტატისტიკა აჩვენებს ქართლ ინტერნეტ სივრცეში გამოყენებულ ტექნოლოგიებს. ჩვენი მაჩვენებლები შედარებულია გლობალურ მაჩვენებლებთან, რომელიც აღებულია Wappalyzer-ს ოფიციალური საიტიდან. ნახავთ, რომ ქართული ტრენდი ახლოს მისდევს გლობალურს, თუმცა არის განსხვავებებიც, რასაც ვიზუალიზაციებზე შეამჩნევთ.

ვებ სერვერები

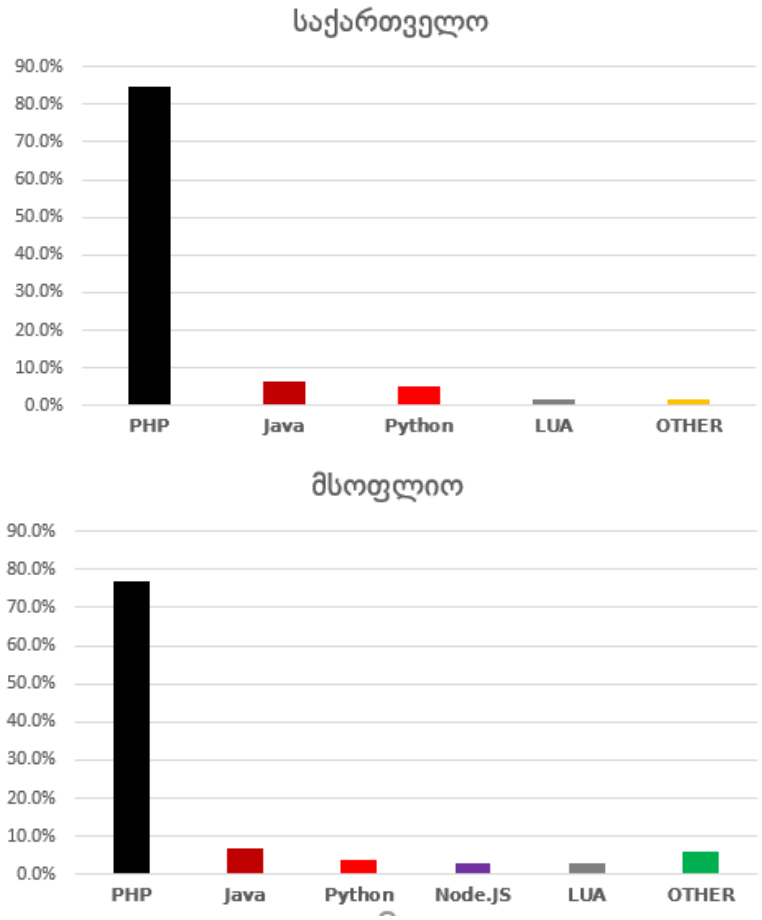
სკანირებული 17185 ვებ-გვერდიდან wappalyzer-ის საშუალებით მივიღეთ 7187 საიტის ანალიზის შედეგი. მიღებულ რეზულტატებში ჭარბობს Apache-ს ვებ-სერვერი (49.7%), შემდეგ მოდის Nginx - 29.5%, LiteSpeed - 8%.





პროგრამირების ენები

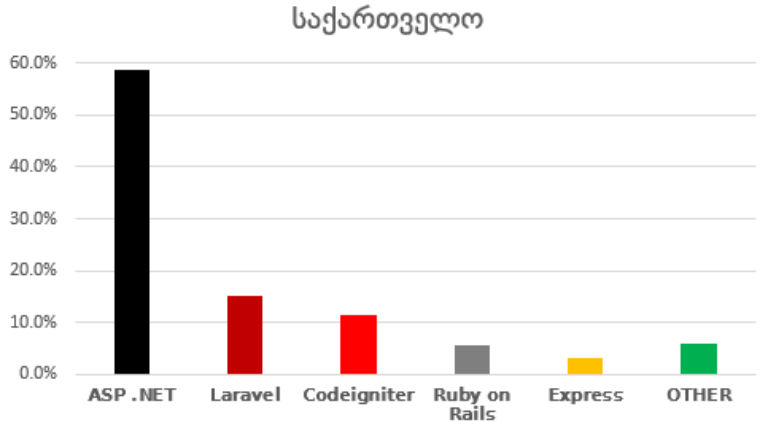
სკანირებული 17185 ვებ-გვერდიდან wappalyzer-ით მივიღეთ 5162 გვერდის შედეგი, რომელიც გადანაწილდა შემდეგნაირად: PHP - 84.8%, Java - 6.6%, Python - 5.3%, Lua - 1.8%.

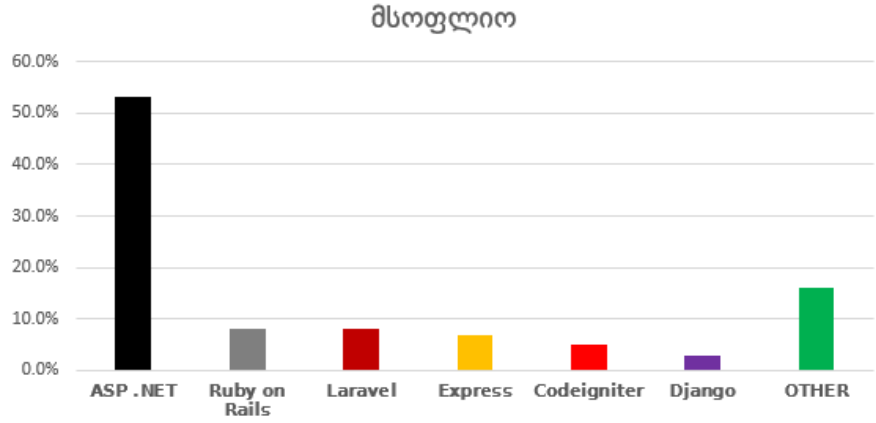


შემდეგ გვერდზე ნახავთ ვებ ფრეიმვორკების სტატისტიკას, სადაც ASP .NET ლიდერობს. პროგრამირების ენებში PHP-სა და ვებ ფრეიმვორკებში ASP .NET-ის ლიდერობაზე ბევრს შეიძლება გაუჩნდეს კითხვა. რეალურად, სკანირების ხელსაწყოები ASP .NET-ზე აგებულ სერვერებს ვერ აფიქსირებენ პროგრამირების ენების სიაში. ამიტომაც გვაქვს მსგავსი შეუსაბამობა.

ვებ ფრეიმვორკების სტატისტიკა

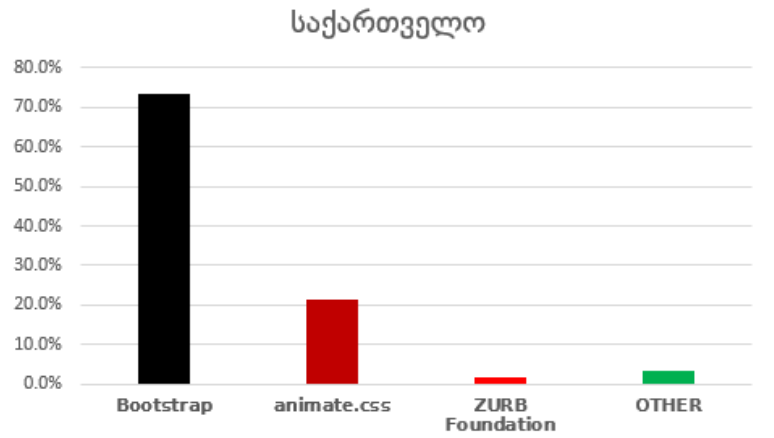
Wappalyzer-მა შედეგი ათასამდე ვებსაიტისთვის დაგვიბრუნა. 58.8% ASP.NET-ზე მოდის, მეორე ადგილზეა Laravel - 15.1%, მესამეზე კი CodeIgniter 11.5%-ით.

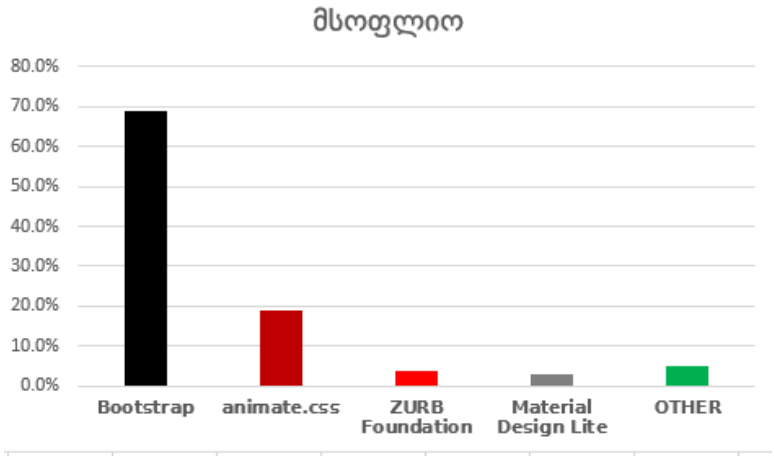




UI ფრეიმვორკები

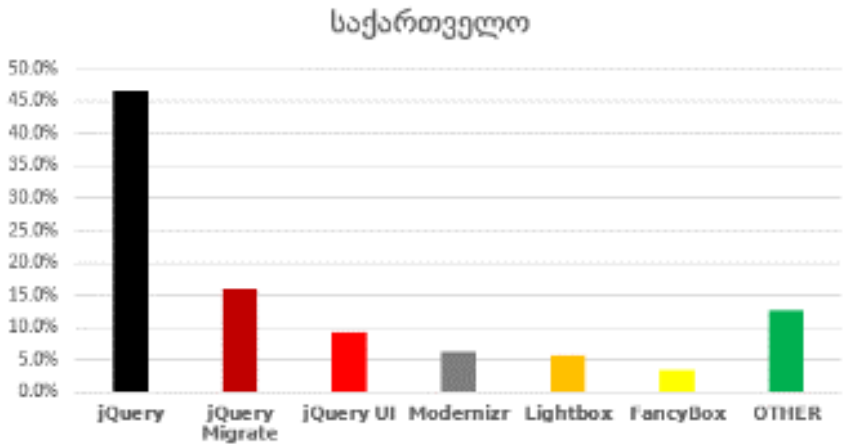
გავაანალიზეთ 2728 IP-ის შედეგი. სკანირების შედეგად მიღებული მონაცემების 73.3% Bootstrap-ზე მოდის, მეორე ადგილზეა 21.6%-ით animate.css.

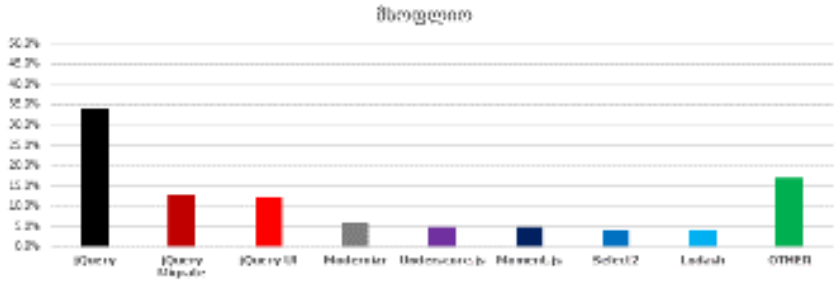




Javascript-ის ბიბლიოთეკების სტატისტიკა

გაანალიზდა 11311 ქართული ვებ გვერდი. შედეგები შემდეგნაირია: jQuery - 46.7%, jQuery Migrate - 16%, jQuery UI - 9.4%, Modernizr - 6.3%.

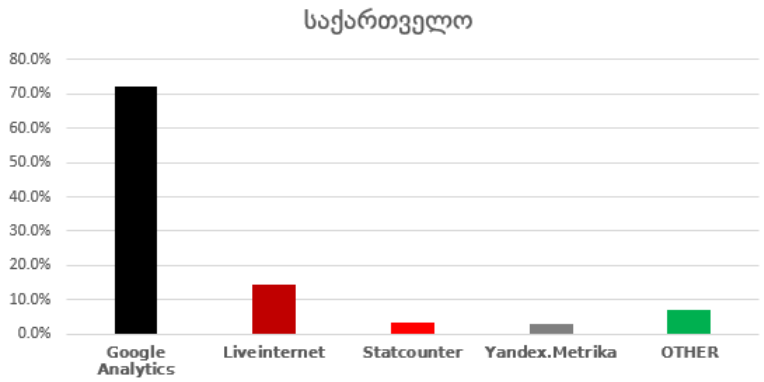


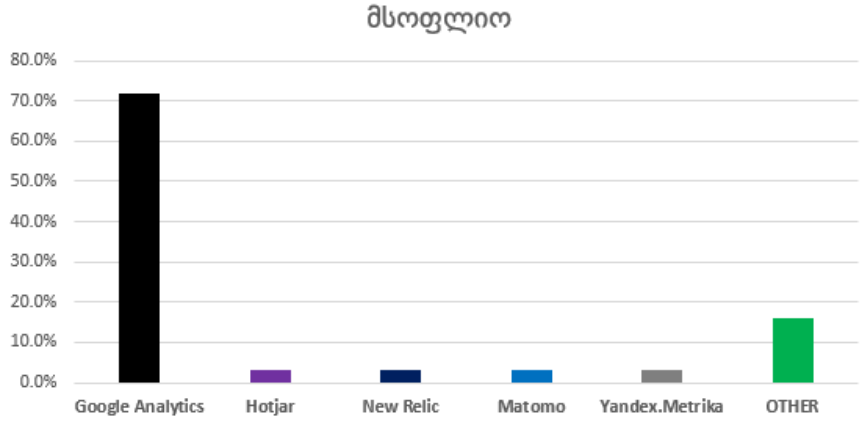


ანალიტიკური სერვისები

სკანირებული მონაცემებიდან ხელსაწყოს საშუალებით მივიღეთ 3336 ვებ-გვერდის ანალიზის შედეგი. მიღებული მონაცემების 71.9%-ს Google Analytics იკავებს, შემდეგ მოდის Liveinternet - 14.4%, Statcounter - 3.4%, Yandex.Metrika - 3.1%.

გავამახვილებთ თქვენს ყურადღებას Yandex.Metrika-ზე, რომელიც რუსული პროდუქტია. საიტზე განთავსებული ანალიტიკური სერვისები მრავალ ინფორმაციას აგროვებს მომხმარებელზე. რუსული კომპანიები ზოგჯერ ნებით, ზოგჯერ კი კრემლის ზეწოლით მჭიდროდ თანამშრომლობენ რუსულ სპეცსამსახურებთან.





დასკვნა

კვლევის შედეგები გვაძლევს საშუალებას დავასკვნათ, რომ ზოგადი დადებითი დინამიკის მიუხედავად, ქართული ინტერნეტ სივრცე კვლავ დაუცველია და უსაფრთხოება მეტ ძალისხმევას მოითხოვს. კვლავაც მრავლად გვხვდება კრიტიკული სისუსტეები.

შეიძლება გაჩნდეს კითხვა - თუ ამდენი კრიტიკული სისუსტეა, რატომ არ ხორციელდება მათი ექსპლუტაცია. პირველ რიგში, უნდა აღვნიშნოთ, რომ ხორციელდება. ამის დასტურად მხოლოდ 2019 წლის ოქტომბრის კიბერ შეტევაც კმარა (თუმცა სხვა მაგალითებიც არსებობს).

ქართულ ინტერნეტ სივრცეში კვლავ მრავლად გვხვდება კრიტიკული სისუსტეები

მეორეს მხრივ კი უნდა გავითვალისწინოთ 2008 წლის გამოცდილება: საქართველო-რუსეთის ომის დროს, მოწინააღმდეგე კარგად მომზადებული აღმოჩნდა კიბერ ოპერაციებისთვის. მაშინდელი თავდასხმების ანალიზით გამოჩნდა, რომ კარგად იყო შესწავლილი ქართული საიტების უსაფრთხოების დონე და კონკრეტულად ომის დროს მოხდა მრავალი სისუსტის ექსპლუატაცია.

გვინდა რამდენიმე პუნქტად ჩამოვაყალიბოთ კვლევის ყველაზე მნიშვნელოვანი მიგნებები:

- ქართულ ინტერნეტ სივრცეში არსებობს მრავალი სერვერი, რომელსაც გააჩნიათ კრიტიკული სისუსტეები. ისეთები, რომელთა ექსპლუატაციის ხელსაწყოები ფართოდ არის გავრცელებული ინტერნეტში
- მაღალი კრიტიკულობის სისუსტეები გააჩნია HTTPS ვებსაიტების ნახევარზე მეტს
- მხოლოდ ქართული რესურსებითაც კი შესაძლებელია საქართველოსთვის მძლავრი მასშტაბის DDoS შეტევის ორგანიზება (DNS და NTP ამპლიფიკაციის შეტევების საშუალებით)
- გაკვირვებას იწვევს მოძველებული და არა ერთი, არამედ მრავალი კრიტიკული სისუსტის მქონე SMB v1.0-ის ფართოდ გამოყენება
- ანალიტიკური სერვისების შედეგებიც (Yandex.Metrika) კმარა რუსული პროდუქტების გამოყენების პრობლემის თვალსაჩინოებისთვის

იმედი გვაქვს, მოცემული ანგარიში პოზიტიურად აისახება ქართული ინტერნეტ სივრცის უსაფრთხოებაზე, რასაც თავის მხრივ, 2021 წლის ანგარიშში დავინახავთ.

კიბერჰაუსის შესახებ

კიბერჰაუსი არის გამოცდილი კადრებით დაკომპლექტებული კომპანია, რომელიც კლიენტებს მათ საჭიროებებზე მორგებულ სერვისებს სთავაზობს.

რას ვაკეთებთ:

- უსაფრთხოების და IT აუდიტი
- კონსალტინგი და შესაბამისობა: NIST კიბერუსაფრთხოების ჩარჩო, ISO 27001, SWIFT CSP, COBIT, BCP & DR
- აუთსორსინგი: უსაფრთხოების ოპერაციები და SOC
- შეღწევადობის ტესტი

საკუთარი პროდუქტი:

Cyberclass.ge - კიბერ ჰიგიენის ტრენინგის ონლაინ პლატფორმა ფიშინგის პორტალითა და მრავალფეროვანი მასალებით

ჩვენი გუნდის პროფესიული სერტიფიკატები:

- CISSP (Certified Information Systems Security Professional)– (ISC)²
- CCSP (Certified Cloud Security Professional) - (ISC)²
- CISM (Certified Information Security Manager) – ISACA
- CISA (Certified Information Systems Auditor) – ISACA
- CRISK (Certified in Risk and IT) – ISACA
- ISO 27001 Lead Implementer – British Standards Institute
- ISO 22301 Lead Implementer – British Standards Institute
- COBIT 5 – ISACA
- CEH (Certified Ethical Hacker) – EC-Council
- OSCP (Offensive Security Certified Professional)

რესურსები

www.cvedetails.com

cve.mitre.org

www.us-cert.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_WannaCry_Ransomware_S508C.pdf

www.apriorit.com/qa-blog/428-mail-server-security-testing

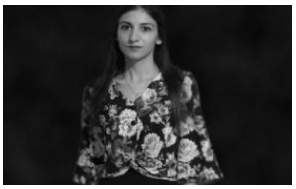
github.com/zkikvidze/scandata/tree/master/results-2018

pingvinuka.blogspot.com

testssl.sh

heartbleed.com

კვლევაზე მუშაობდნენ



მარიამ დემურაშვილი

მონაცემების მოგროვება და ანალიზი

მიხეილ ბასილაია

მონაცემების ანალიზი, რეპორტის რედაქტირება

დავით აღნიაშვილი

რეპორტის რედაქტირება

განსაკუთრებული მადლობა **ზვიად კიკვიძეს** 2018 წელს მის მიერ მოგროვებული ინფორმაციისთვის

კითხვებისა და შენიშვნებისთვის დაგვიკავშირდით:

info@cyberhouse.ge

+995 577 27 88 19

+995 599 63 63 00

www.cyberhouse.ge

www.cyberclass.ge