**რევერსული ინჟინერია:**

1. **10** კრიმინალურმა პოლიციამ აღმოაჩინა საეჭვო სერვერი, რომელიც ჰაკერების მიერ არის კონტროლირებადი და დაცულია პაროლით. თქვენი მიზანია გამოიცნოთ პაროლი.

დავალება: https://github.com/CERT-GOV-GE/Cybercube-2017/raw/master/stage\_1\_JS.zip

პაროლი არქივზე: Cyb3rCub3\_2017!

1. 15 კრიმინალურმა პოლიციამ აღმოაჩინა საეჭვო სერვერი, რომელიც ჰაკერების მიერ არის კონტროლირებადი და დაცულია პაროლით. თქვენი მიზანია გამოიცნოთ პაროლი.

დავალება: https://github.com/CERT-GOV-GE/Cybercube-2017/raw/master/stage\_2\_JS.zip

პაროლი არქივზე: Cyb3rCub3\_2017!

1. 20 კრიმინალურმა პოლიციამ აღმოაჩინა საეჭვო სერვერი, რომელიც ჰაკერების მიერ არის კონტროლირებადი და დაცულია პაროლით. თქვენი მიზანია გამოიცნოთ პაროლი.

დავალება: https://github.com/CERT-GOV-GE/Cybercube-2017/raw/master/stage\_3\_JS.zip

პაროლი არქივზე: Cyb3rCub3\_2017!

1. 15 კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფმა მოიპოვა საეჭვო ფაილი, რომელიც დაცულია პაროლით. თქვენი მიზანია გამოიცნოთ პაროლი.

დავალება: https://github.com/CERT-GOV-GE/Cybercube-2017/raw/master/Stage\_1\_BIN.zip

პაროლი არქივზე: Cyb3rCub3\_2017!

1. 20 კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფმა მოიპოვა საეჭვო ფაილი, რომელიც დაცულია პაროლით. თქვენი მიზანია გამოიცნოთ პაროლი.

დავალება: https://github.com/CERT-GOV-GE/Cybercube-2017/raw/master/stage\_2\_BIN.zip

პაროლი არქივზე: Cyb3rCub3\_2017!

1. 25 კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფმა მოიპოვა საეჭვო ფაილი, რომელიც დაცულია პაროლით. თქვენი მიზანია გამოიცნოთ პაროლი.

დავალება: https://github.com/CERT-GOV-GE/Cybercube-2017/raw/master/stage\_3\_BIN.zip

პაროლი არქივზე: Cyb3rCub3\_2017!

**მავნე ფაილის ანალიზი:**

კომპანიაში აღმჩენილ იქნა მავნე ფაილი, თქვენი მიზანია გაანალიზოთ ფაილი და გასცეთ პასუხი კითხვებს.

დავალება: https://github.com/CERT-GOV-GE/Cybercube-2017/raw/master/AdobeReader.zip

პაროლი არქივზე: Cyb3rCub3\_2017!

1. 15 Windows API-ს რომელ ფუნქციას იყენებს ფაილის გადმოსაწერად?
2. 20 რა სახელით ინახება და ეშვება გადმოწერილი ფაილი?

ერთერთი მსხვილი საფინანსო ორგანიზაცია გახდა კიბერ-შეტევის მსხვერპლი, მათი მთლიანი ინფორმაცია დაიშიფრა, თქვენი მიზანია გამოიკვლიოთ ინციდენტი და გასცეთ პასუხი კითხვებს.

დავალება: https://github.com/CERT-GOV-GE/Cybercube-2017/raw/master/xRansom.zip

პაროლი არქივზე: Cyb3rCub3\_2017!

1. 15 რომელი გაფართოების ფაილები იშიფრება? (დაალაგეთ ანვანის მიხედვით, მაგ.: doc, exe, pdf)
2. 30 გამოიცანით დაშიფრვისას გამოყენებული გასაღები.
3. 50 ამ ორგანიზაციის ერთერთ წარმომადგენელი დაინფიცირდა აღნიშნული რანსომვეარით და password.txt ფაილი დაეშიფრა, სადაც ინახავდა მისთვის მნიშვნელოვან პაროლს, მოცემული გაქვთ დაშიფრული ფაილი აღადგინეთ პაროლი.

ლოგ ფაილის ანალიზი

კომპანია “ვიქტორია სექიურითის” ვებსერვერზე განხორციელდა შეტევა, მაგრამ მისი ყველა დეტალი უცნობია. თქვენ გადმოგცეს სერვერის ე.წ. „access log“-ი შეტევის მომენტში და უნდა გაიგოთ, თუ რა მოხდა შეტევის დროს?

https://github.com/CERT-GOV-GE/Cybercube-2017/raw/master/access.rar

(პაროლი არქივზე არის: "Cyb3rCub3\_2017!")

1) რომელი IP მისამართებიდან განხორციელდა შეტევა? (IP მისამართები დაალაგეთ ზრდადობის მიხედვით და გამოყავით ";" სიმბოლოთი)

2) რა ტიპის შეტევა გამოიყენა შემტევმა წვდომის მოსაპოვებლად?

3) რომელი ანონიმური ქსელით განხორციელდა კიბერ შეტევა?

4) რა ხელსაწყო გამოიყენა შემტევმა ვებ გვერდის სკანირებისთვის?

5) რა სახელის მქონე ფაილი ატვირთა შემტევმა?

6) რომელი კიბერ შეტევის ვექტორი განახორციელა ჰაკერმა აღნიშნულ ვებ გვერდზე?

კრიფტოგრაფია

1) ჰაკერმა ზედმეტ სახელად “კეისარი”, თავის მეტოქეებს შემდეგი დაშიფრული შეტყობინება გაუგზავნა. თუ შეძლებთ მის გაშიფვრას?

"Jevgvat nobhg zhfvp vf yvxr qnapvat nobhg nepuvgrpgher."

2)

x XOR y = 0x52

y XOR z = 0xa2

x XOR z = ?

3)

თავისი გამჭრიახობით განთქმული ჰაკერი ზედმეტ სახელად „ლიკვიდა“, როგორც იქნა დაიჭირეს. მის პირად ფაილებში იპოვეს ქვემომოცემული სტრინგი, რომელშიც, სავარაუდოდ, მისი პაროლია დაშიფრული. თუ შეძლებთ, გაშიფროთ „ლიკვიდას“ პაროლი?

VWtoS2FHUXliSFZhZVVKMlltbENkR1ZUUW0xaFZ6VnNTVWRPZG1KWE1XaGliVkZuWWpKWloySkhSblZhTTFab1dqSlZjMGxGYTJkak1rWndXa05DZFdJelVtOWhWelZ1VEdjOVBRPT0=

კრიფტოგრაფია/სტეგანოგრადია

1)

ცერტის აგენტებმს ორი ჰაკერის შიდა მიმოწერა აღმოაჩინეს, და მისი გარჩევა სცადეს, რათა მათი სერვერის პაროლი გაეგოთ. სამწუხაროდ, ჰაკერებს თავისი პაროლი ღია ფორმით არსად დაუწერიათ. ერთ-ერთ მეილზე მიმაგრებული იყო ეს უცნაური სურათი. შეძლებთ თუ არა მის დახმარებით ჰაკერების სერვერის პაროლის გაგებას? [ფაილი:<https://github.com/CERT-GOV-GE/Cybercube-2017/raw/master/steg.zip> ]

(პაროლი არქივზე არის: "Cyb3rCub3\_2017!")

კრიფტოგრადია/პროგრამირება

1)

ჰაკერებმა პაროლების გაგზავნის ახალი სქემა შემოიმუშავეს, რომლის ერთადერთი კვალი მოცემული ფაილია. შეძლებთ თუ არა გაიგოთ მათი ახალი პაროლი? [ფაილი:<https://github.com/CERT-GOV-GE/Cybercube-2017/raw/master/crypto1.zip> ]

2)

ჰაკერებმა კიდევ უფრო დახვეწეს სქემა, რომელსაც პაროლების გადაცემისთვის იყენებენ და ახლა მას უკვე შემდეგი ფაილის ფორმა აქვს. თქვენი მიზანია ჰაკერების მიერ დაშიფრული ინფორმაცია წაიკითხოთ. [ფაილი:<https://github.com/CERT-GOV-GE/Cybercube-2017/raw/master/crypto2.zip> ]

(პაროლი არქივზე არის: "Cyb3rCub3\_2017!")

ლოგ ფაილის ანალიზი

კომპანია “ალიგატორის” ვებსერვერზე განხორციელდა შეტევა, მაგრამ მისი ყველა დეტალი უცნობია. თქვენ გადმოგცეს სერვერის ე.წ. „access log“-ი შეტევის მომენტში და უნდა გაიგოთ, თუ რა მოხდა შეტევის დროს. [ფაილი:<https://github.com/CERT-GOV-GE/Cybercube-2017/raw/master/log.zip> ]

(პაროლი არქივზე არის: "Cyb3rCub3\_2017!")

1)

რომელი IP მისამართი ჰქონდა შემტევს?

2)

რა ხელსაწყოები გამოიყენა შემტევმა (დაალაგეთ ანბანის მიხედვით)?

3)

რომელი შეტევის მეთოდით მოახერხა მან სერვერზე შეღწევა?

4)

რა სახელის მქონე ე.წ. „პლაგინი“ ატვირთა შემტევმა?

5)

სერვერზე არსებული რომელი ფაილის შიგთავსი წაიკითხა მან?