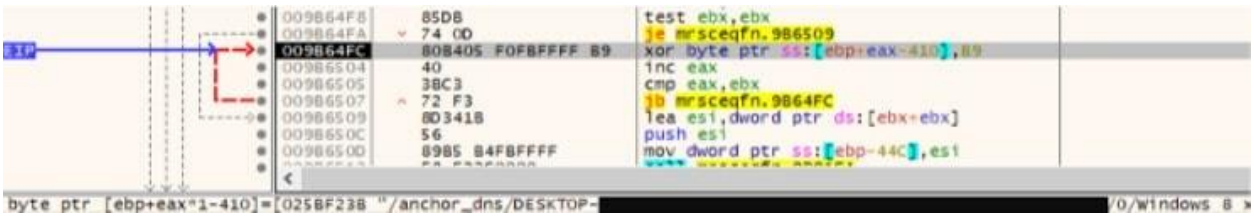
დღევანდელი მდგომარეობით მსოფლიო COVID-19 პანდემიას ებრძვის და ამ სამწუხარო რეალობას კიბერ-კრიმინალური დაჯგუფება ბოროტად იყენებს თავიანთი მიზნებისთვის, როგორც წესი, ფინანსური სარგებელის მისაღებად.

ერთ-ერთი ასეთი დაჯგუფებაა „**Ryuk UNC1878**“, რომელმაც ამერიკის შეერთებულ შტატებსა და ევროპის მასშტაბით ჯანდაცვის სისტემებზე მიიტანა იერიში. ეს ძალზედ მნიშვნელოვანი პოტენციური საფრთხეა საქართველოს ჯანდაცვის სისტემებისთვისაც, რადგან ჩვენი მცირე რესურსების პარალელურად, კიბერ-კრიმინალების მიერ მოყენებული ზარალით უფრო უკან დახევა გამოიწვევს ძალზედ ცუდ შედეგებს.

კიბერუსაფრთხოების და ინფრასტრუქტურის უსაფრთხოების სააგენტოს (CISA), აშშ ფედერალური ბიუროს (FBI) და ჯამრთელობის და სერვისების დეპარტამენტის (HHS) ერთობლივი მუშაობის შედეგად მოგვაწოდეს ინფორმაცია მიმდინარე საფრთხეზე, რომელიც ხდება აშშ-ში და დიდი შანსია საქართველოშიც განხორციელდეს.

კიბერ-კრიმინალური დაჯგუფება „**Ryuk UNC1878**“ იყენებს **Trickbot** მალვეარს, რომელსაც გააჩნია მოდული: **Anchor_DNS**. მისი დანიშნულებაა კომპრომიზირებულ სისტემას და C2C (command and Control) სერვერს შორის კავშირის ინფორმაციის მიმოცვლა DNS ტუნელინგის დახმარებით, რომელიც გულისხმობს DNS პროტოკოლში სასურველი ინფორმაციის ჩასმას და გაგზავნას. ამ გზით ქსელის პერიმეტრზე ცალსახად არ გამოჩნდება მავნე მოქმედებები და აღიქმება როგორც ჩვეულებრივი DNS პაკეტები. აღსანიშნავია ისიც, რომ Anchor_DNS სასურველ კომუნიკაციის ტექსტს პირდაპირ არ უთითებს DNS პროტოკოლში და არ აგზავნის. არამედ იგი თავდაპირველად XOR მეთოდს იყენებს ბაიტების ენკოდირებისთვის 0xB9 ბაიტით.:



დეკრიპტაციის შემდგომ გამოჩნდება „Anchor_DNS“ სტრინგი DNS პაკეტში.

Trickbot მალვეარი ძირითადად ვრცელდება ელ.ფოსტით, რომლებსაც მიბმული აქვთ მავნე ფაილები MS Office დოკუმენტების სახით და იყენებენ როგორც Macro, ასევე DDE მექანიზმებს მავნე კოდის ასამოქმედებლად. გაშვებისას იგი აკეთებს საკუთარი თავის კოპირებას შემდეგ დირექტორიებზე და იცვლის სახელს, რომელიც შედგება 12 შემთხვევითი სიმბოლოსგან (მაგ: qwedfrty.exe):

- C:\Windows\
- C:\Windows\SysWOW64\
- C:\Users\%username%\AppData\Roaming

ასევე შესაძლებელია Trickbot მალვეარმა შექმნას ფაილი: anchorDiag.txt რომელიმე ზემოთ აღნიშნულ დირექტორიაში.

მსხვერპლის კომპიუტერში მოხვედრის შემდეგ, სანამ C2C დაუკავშირდება მეხსიერებაში ქმნის სტრინგს: Global\fde345tyhoVGYHUJKIOuy, რომელიც Memory Dump-ში უნდა გამოჩნდეს, თუ საჭირო გახდება მეხსიერების დამპის აღება.

პირველადი კომუნიკაციისას მალვეარი აგზავნის ბაზისურ ინფორმაცის ინფიცირებული სისტემის შესახებ: კომპიუტერის hostname, ოპერაციული სისტემის ვერსია და ე.წ. „Build“-ის ვერსია, რომლის ფორმატი არის შემდეგი სახის:

/anchor_dns/[COMPUTERNAME]_[WindowsVersionBuildNo].[32CharacterString]/.

ასევე, მალვეარი სტაბილურობისთვის იყენებენ Windows-ის Task Scheduler-ს, რომელიც ყოველ 15 წუთში ერთხელ ეშვება.

წარმატებული გაშვებისას Anchor_DNS ქმნის „.bat“ გაფართოების ფაილს powershell-ის დახმარებით და იგი მოიცავს შემდეგ ბრძანებებს:

- **cmd.exe /c timeout 3 && del C:\Users\[username]\[malware_sample]**
- **cmd.exe /C PowerShell \“Start-Sleep 3; Remove-Item C:\Users\[username]\[malware_sample_location]\“**

ეს ბრძანებები უზრუნველყოფენ იმას, რომ ორიგინალი მალვეარი წაიშალოს, ანუ მიმართავს თვით-დესტრუქციას.

თავდაპირველად დაფიქსირებული იყო შემდეგი დომეინ მისამართები, რომლებიც ასოცირებული იყო anchor_dns-თან, თუმცა ცხადია სია ამჟამად გაცილებით უფრო დიდია.

- kostunivo[.]com
- chishir[.]com
- mangoclone[.]com
- onixcellent[.]com

ასევე დაფიქსირებულია ის დომეინ მისამართები, რომლებიც გამოყენებულ იქნა იმისათვის, რათა მალვეარს შეემოწმებინა ინტერნეტთან წვდომის შესაძლებლობა:

- ipecho[.]net
- api[.]ipify[.]org
- checkip[.]amazonaws[.]com
- ip[.]anysrc[.]net
- wtfismyip[.]com
- ipinfo[.]io
- icanhazip[.]com
- myexternalip[.]com

ისტორიულად დაფიქსირებულია ეს IP მისამართები:

- 23[.]95[.]97[.]59
- 51[.]254[.]25[.]115
- 193[.]183[.]98[.]66
- 91[.]217[.]137[.]37
- 87[.]98[.]175[.]85

Trickbot მალვეარს აქვს Ryuk Ransomware-ის გამოყენების შესაძლებლობა და საკმაოდ აქტიურად გამოიყენება, რის შედეგადაც ძალზედ დიდ მაშტაბებს აღწევს აშშ-ში და ევროპის ტერიტორიაზე. აღსანიშნავია, რომ Ryuk Ransomware არის Hermes მავნე კოდისგან მიღებული, ანუ გამოყენებული აქვს მისი ფუნქციონალური შესაძლებლობები. ამის დასტურია ის, რომ დაკრიპტულ ფაილებში შეგვიძლია წავიკითხოთ სტრინგი: „**HERMES**“.

კიბერ-შეტევისას კრიმინალები აქტიურად გამოიყენებენ კომერციულ Cobalt Strike-სა და ღია კოდის მქონე Powershell Empire ხელსაწყოებს, რომლებსაც გააჩნიათ უამრავი მოდულები შიდა ქსელის და ლოკალური სისტემის ენუმერაციისთვის. ასევე აქვთ შესაძლებლობა მეხსიერებაში გააკეთონ DLL-ის ინექცია და მოიპოვოთ სიღრმისეული წვდომის უფლებები ინფიცირებულ სისტემაზე.

აღსანიშნავია ისიც, რომ კრიმინალები მაქსიმალურად თავს არიდებენ ზედმეტ ე.წ. „ჰაკერულ“ ხელსაწყოებს და ფონს გადიან ჩვეულებრივი სტანდარტული ე.წ. „native“ ხელსაწყოებით, როგორიცაა მაგალითად: powershell, net view, net localgroups და ა.შ. იქ სადაც არის Active Directory გარემო, იყენებენ BloodHound ხელსაწყოს, რომელიც სრულ სურათს იძლევა მთლიანად Active Directory-ზე, როგორიცაა მაგალითად არსებული domain ადმინები, დომეინებს შორის ე.წ. „Trust”-ები და ა.შ. შიდა ქსელში მოხვედრის შემდეგ მაქსიმალურად ცდილობენ შიდა ქსელის არეალში გავრცელებას.

Ryuk Ransomware ფაილებს შიფრავს AES-256 ალგორითმის მეშვეობით და იყენებს RSA public key-ს AES გასაღების ენკრიპტაციისათვის.

ასევე, ისინი ცდილობენ ისეთი პროგრამების გათიშვას, რომლებიც ხელს უშლიან მოქმედებაში: მაგალითად: Defender ანტივირუსის და თავს არიდებენ AMSI (Antimalware Scan Interface) მექანიზმს და ა.შ.

ფაილების ენკრიპტაციის შემდეგ იგი ტოვებს RyukReadMe ფაილს, სადაც წერია 1 ან 2 მეილ მისამართი კრიმინალებთან დასაკავშირებლად.

Ryuk Ransomware იყენებს ATT&CK ტექნიკებს, რომლებიც ჩამოთვლილია ქვემოთ მოცემულ ცხრილში:

ტექნიკა	შინაარსი
System Network Configuration Discovery [T1016]	Ryuk იძახებს WinAPI-ის GetIpNetTable ფუნქციას იმისათვის, რომ მიიღოს ინფორმაცია დამაუნთებულ დრაივებზე და ARP ცხრილზე.
Masquerading: Match Legitimate Name or Location [T1036.005]	GetWindowsDirectoryW ფუნქციის დახმარებით იღებს ინფორმაციას Windows დირექტორიაზე, იღებს ე.წ. „ფართიშენს“, სადაც სისტემაა დაყენებული და საბოლოო ჯამში ქმნის C:\Users\Public დირექტორიას.
Process Injection [T1055]	თავის თავის განთავსება პროცესში VirtualAlloc, WriteProcessMemory და CreateRemoteThread ფუნქციების დახმარებით.
Process discovery [T1057]	იძახებს CreateToolHelp32Snapshot-ს, რათა მიიღოს ინფორმაცია გაშვებული პროცესების შესახებ.
Command and Scripting Interpreter: Windows Command Shell [T1059.003]	cmd.exe-ს დახმარებით ქმნის რეესტრში ჩანაწერს persistence - სთვის.
File and Directory Discovery [T1083]	იძახებს GetLogicalDrives დამაუნთებული დრაივებზე და GetDriveTypeW დრაივის ტიპზე ინფორმაციის მისაღებად.
Native API [T1106]	იყენებს Native API ფუნქციებს, რომლებიც განსხვავდება WinAPI- სგან.
Access Token Manipulation [T1134]	იყენებს token-ებზე მანიპულაციებს, რათა მიიღოს Se-DebugPrivilege პრივილეგია.
Data Encrypted for impact [T1486]	Ryuk ფაილების შიფრაციისთვის იყენებს სიმეტრიულ და ასიმეტრიულ კრიპტოგრაფიას.
Service Stop [T1489]	იყენებს თავისივე შექმნილ kill.bat ფაილს სერვისების გასათიშათ.
Inhibit System Recovery [T1490]	იყენებს vssadmin Delete Shadow /all /quiet და vssadmin resize shadowstorage - ს, რათა წაშალოს ყველა შესაძლო backup-ები, რომლებიც სისტემაზე მდებარეობს.
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder [T1047.001]	აკეთებს startup ჩანაწერს HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run - ში persistence-ისათვის.
Impair Defenses: Disable ro Modify Tools [T1562.001]	თიშავს სერვისებს, რომლებიც დაკავშირებულია ანტი-ვირუსთან.

რეკომენდაციები:

- განაახლეთ ოპერაციული სისტემები და მასზე განთავსებული პროგრამები.
- რეგულარულად გამოცვალეთ პაროლები.

- გამოიყენეთ MFA, სადაც შესაძლებელია.
- გათიშეთ ისეთი სერვისები, რომლებსაც არ იყენებთ (მაგ: RDP, ssh, winrm და ა.შ.)
- სასურველია სისტემებზე გათიშული იყოს ლოკალური ადმინისტრატორის ანგარიში და წვდომა დაშვებული იყოს სტანდარტული მომხმარებლით ან დომეინ მომხმარებლით.
- სიფრთხილით მოეკიდეთ ყველა შემოსულ ელ.წერილს.
- თუკი იყენებთ Active Directory-ს გამოიყენეთ GPO და დაბლოკეთ powershell.exe AppLocker-ის დახმარებით.

ასევე რეკომენდირებულია გამოიყენოთ CERT-GOV-GE -ის მიერ მოწოდებული მავნე დომეინებისა და IP მისამართების სიები ინციდენტის პრევენციისათვის:

- Domain - http://blacklists.cert.gov.ge/unc1878_domains.txt
- IP - http://blacklists.cert.gov.ge/unc1878_ip.txt