

ჩინეთის საიდუმლო კიბერტავდასხმები

თბილისი
2024



2024 წლის მარტში მსოფლიო მედია საშუალებები ჩინეთის სახალხო რესპუბლიკასთან დაკავშირებული ორგანიზაციების/პირების მხრიდან, დიდი ბრიტანეთის დემოკრატიული ინსტიტუტებისა და პარლამენტარების წინააღმდეგ განხორციელებულმა მავნებლური კიბერშეტევების შესახებ ინფორმაციებმა მოიცვა. ამის შესახებ წერდნენ CNN, BBC, The New York Times, The Guardian და სხვა.



World / China

China hits back at US, UK for sanctions on espionage hacks as coordinated pressure on Beijing grows



By Nectar Gan, CNN

4 minute read · Updated 5:21 AM EDT, Tue March 26, 2024



BBC

Home News Sport Business Innovation Culture Travel Earth Video Live

UK imposes sanctions after Chinese-backed cyber-attacks

26 March 2024

By Sam Francis & Jennifer McKiernan, Political reporters, BBC News

Share



The deputy PM says the UK and international partners will expose China for "ongoing patterns of hostile activity".

[“China hits back at US, UK for sanctions on espionage hacks as coordinated pressure on Beijing grows” –](#)
[“ჩინეთი პასუხობს აშშ-ს და დიდ ბრიტანეთს საღაზვერვო თავდასხმების საპასუხო საწვავებისთვის, რამდენადაც პეკინზე კოორდინირებული ზეწოლა იზრდება”](#)

წყარო:

<https://edition.cnn.com/2024/03/26/china/china-cyber-hacking-accusations-intl-hnk/index.html>

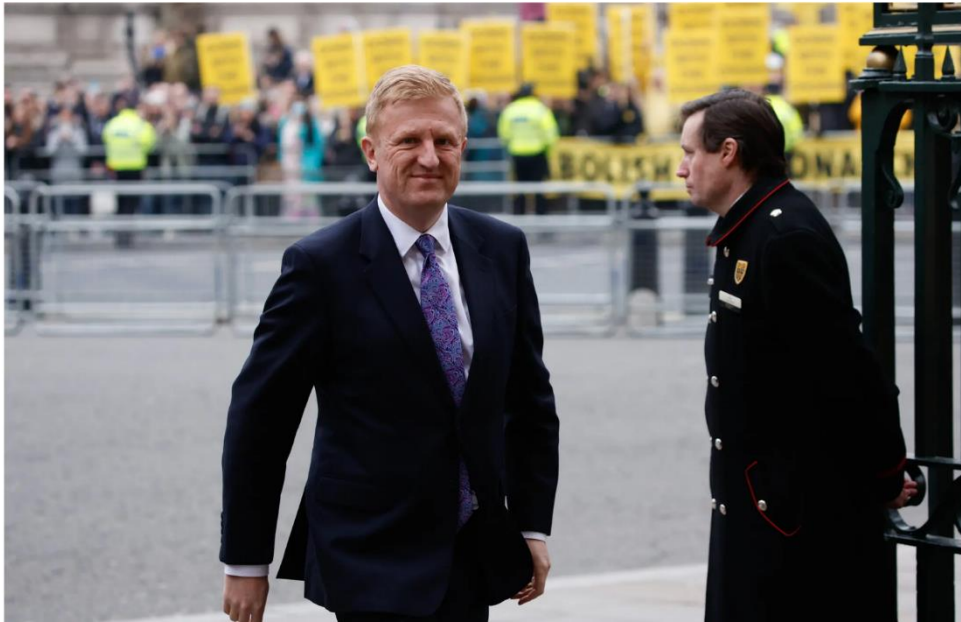
[“UK imposes sanctions after Chinese-backed cyber-attacks” –](#)
[„გაერთიანებული სამეფო ჩინეთის მიერ მხარდაჭერილი კიბერთავდასხმების შემდეგ საწვავებს აწესებს“](#)

წყარო:

<https://www.bbc.com/news/uk-politics-68654533>

U.K. Accuses China of Cyberattacks Targeting Voter Data and Lawmakers

The British government believes China has overseen two separate hacking campaigns, including one that yielded information from 40 million voters.



[“U.K. Accuses China of Cyberattacks Targeting Voter Data and Lawmakers” –](#)
[“გაერთიანებული სამეფო ჩინეთს ადანაშაულებს კიბერ თავდასხმებში, რომლებიც მიმართული იყო ამომრჩევლებისა და პარლამენტარების წინააღმდეგ”](#)

წყარო:
<https://www.nytimes.com/2024/03/25/world/europe/uk-china-cyberattack-hacking.html>

News

Opinion

Sport

Culture

Lifestyle



The Guardian

World UK Climate crisis Ukraine Environment Science Global development Football Tech

Hacking

Explainer

China cyber-attacks explained: who is behind the hacking operation against the US and UK?

Chinese hacking group APT 31 has been accused by UK and US officials of targeting critics of Beijing, while New Zealand's systems have also been attacked



[“China cyber-attacks explained: who is behind the hacking operation against the US and UK?”](#)
– „ჩინეთის კიბერ-თავდასხმების ასსნა: ვინ ღვას აშშ-სა და გაერთიანებული სამეფოს წინააღ-მდეგ ჰაკერული ოპერაციების უკან?“

წყარო:
<https://www.theguardian.com/technology/2024/mar/26/china-cyber-attack-uk-us-explained-hack-apt-31>

დიდი ბრიტანეთის ეროვნული კიბერუსაფრთხოების ცენტრის [შეფასებით](#), გაერთიანებული სამეფოს ინსტიტუტები და პარლამენტარები 2021-2022 წლებში სხვადასხვა კიბერთავდასხმის სამიზნეებს წარმოადგენდნენ. 2021 წლის აგვისტოში ქვეყნის საარჩევნო სისტემებში მავნებლური ქმედებები [დაფიქსირდა](#). ამავდროულად, 2022 წლის ოქტომბერშიც გაერთიანებული სამეფოს საარჩევნო კომისიაზე კიბერთავდასხმები [განხორციელდა](#), თუმცა თავდასხმაზე ეჭვმიტანილების ვინაობა უცნობი იყო. აღსანიშნავია, რომ კიბერთავდამსხმელებს წვდომა ჰქონდათ 2014-2022 წლებში ჩრდილოეთ ირლანდიაში, ბრიტანეთსა და საზღვარგარეთ ამომრჩევლად რეგისტრირებული დაახლოებით 40 მილიონი მოქალაქის პერსონალურ მონაცემებზე (სახელი, მისამართი). აღსანიშნავია, რომ საარჩევნო კომისიის [განცხადების](#) მიხედვით, აღნიშნულ კიბერაქტივობებს გაერთიანებული სამეფოს არჩევნების შედეგებზე გავლენა არ მოუხდენია.

გარდა საარჩევნო კომისიაზე თავდასხმისა, გაერთიანებული სამეფოს თემთა პალატის 2024 წლის 25 მარტის [განცხადების](#) თანახმად, 2021 წელს პარლამენტარების ანგარიშებზე ცალკე სადაზვერვო კამპანია განხორციელდა. პარლამენტარების ელექტრონულ ფოსტებზე თავდასხმები წარუმატებელი აღმოჩნდა. თუმცა, ნიშანდობლივია, რომ თავდასხმის სამიზნეები იყვნენ ის პირები, რომლებიც ღიად აკრიტიკებდნენ ჩინეთის მავნებლურ პოლიტიკურ ქმედებებს.

აღწერილი კიბერთავდასხმების საპასუხოდ, გაერთიანებულმა სამეფომ სანქციები დაუწესა ჩინეთის ორ მოქალაქესა (ჟაო გუაძონგს და ნი გაობინს) და ჩინურ კომპანიას ("Wuhan Xiaoruizhi Science and Technology Company Ltd"). გარდა ამისა, გაერთიანებულ სამეფოში ჩინეთის ელჩს [მოსთხოვეს](#) ინციდენტის შესახებ ინფორმაციის მიწოდება.

აღსანიშნავია, რომ დიდ ბრიტანეთზე კიბერშეტევებს [გამოეხმაურა](#) ევროკავშირი და ჩინეთს მოუწოდა გაეროს ფარგლებში კიბერსივრცესთან დაკავშირებით დაკისრებული [ვალდებულებების](#) შესრულებისაკენ. კერძოდ კი, [განცხადების თანახმად](#), ჩინეთის ხელისუფლებამ მისი ტერიტორიიდან განხორციელებული კიბერშეტევების წინააღმდეგ საჭირო ზომები უნდა მიიღოს.

ჩინეთის სახალხო რესპუბლიკასთან აფილირებული ორგანიზაციების მზარდი კიბერთავდასხმების ფონზე, აშშ-ში ჩინეთთან დაკავშირებულ 7 პიროვნებას [ბრალი წაუყენეს](#). [დოკუმენტის თანახმად](#), ბრალდებულები (ნი გაობინი, ვენგ მინგი, ჩენგ ფენგი, პენ იაოუენი, სუნ სიაოჰუი, სიონგ ვანგი, ჟაო გუაძონგი) ჰუბეის სახელმწიფო უსაფრთხოების დეპარტამენტის ფარგლებში მოქმედი კიბერთავდამსხმელი ჯგუფის წევრები არიან. კიბერუსაფრთხოების მკვლევარების მიერ ეს ჯგუფი ცნობილია სახელწოდებით: „[გაზრდილი მუდმივი საფრთხე 31](#)“ („Advanced Persistent Threat 31“ – „APT31“). აღსანიშნავია, რომ გაერთიანებული სამეფოს პარლამენტარებისა და ინსტიტუტების წინააღმდეგ განხორციელებულ თავდასხმებში ეჭვმიტანილი პირებიც აღნიშნულ დაჯგუფებასთან [არიან დაკავშირებულნი](#).

გამოძიებით გაირკვა, რომ 2010 წლიდან მოყოლებული, APT31-ის წევრები ახორციელებდნენ კიბერშეტევებს აშშ-ს ოფიციალური პირების, აქტივისტების, აკადემიკოსებისა და კონგრესმენების, ისევე როგორც აშშ-ს ეკონომიკისა და თავდაცვის წინააღმდეგ. აშშ-ს სახაზინო დეპარტამენტმა ორ ბრალდებულს სანქციები [დაუწესა](#), ხოლო აშშ-ს სახელმწიფო დეპარტამენტმა ბრალდებულებზე, მათ ორგანიზაციაზე ან მათთან დაკავშირებულ გაერთიანებებზე ინფორმაციის გაცემის სანაცვლოდ ჯილდო (10 მლნ) [გამოაცხადა](#).

APT31 ჯგუფის წევრები სამიზნე პირებს წერილებს [უგზავნიდნენ](#) ელექტრონული ფოსტით, რომლებშიც ჩასმული იყო ფარული სადაზვერვო (tracking) ბმულები. აღნიშნული ელექტრონული წერილები იგზავნებოდა ცნობილი მედია საშუალებების (მაგ, CNN, Vox) ან ჟურნალისტების სახელით. ელექტრონული ფაილის გახსნის შემთხვევაში კი, მიმღები პირის შესახებ ინფორმაცია (მისი ადგილმდებარეობა, ინტერნეტ

პროტოკოლის მისამართი, ელექტრონულ ფოსტაზე წვდომის მექანიზმები კონკრეტული მოწყობილობები და ა.შ) იგზავნებოდა ბრალდებულების მიერ კონტროლირებად სერვერზე. შემდგომში, APT31-ის წევრები ამ ინფორმაციას უფრო პირდაპირი და რთული კიბერშეტევების განსახორციელებლად იყენებდნენ. 2018 წლის ივნის-სექტემბერში დაახლოებით 10 000-ზე მეტი ელექტრონული ფოსტა [გაეგზავნა](#) აშშ-ს მაღალი თანამდებობის პირებსა და მათ მრჩეველებს.

კიბერთავდასხმები მიმართული იყო სენატის წევრების, რესპუბლიკური თუ დემოკრატიული პარტიის წარმომადგენლების და აშშ-ს იმ ოფიციალური პირების წინააღმდეგ, რომლებიც მუშაობდნენ თეთრ სახლში, იუსტიციის, ვაჭრობის, ხაზინის და სახელმწიფო დეპარტამენტებში. რიგ შემთხვევებში კიბერთავდასხმების სამიზნეები იყვნენ მაღალი თანამდებობის პირების მეუღლეებიც. საყურადღებოა, რომ თავდასხმის მსხვერპლებს შორის იყვნენ აშშ-ს პოლიტიკური პარტიების საარჩევნო კამპანიის პერსონალის წევრებიც. 2021 წელს ჩინეთის მიერ მხარდაჭერილი კიბერთავდასხმების სამიზნეებს შორის [იყვნენ](#) ჩინეთის შესახებ პარლამენტთაშორისი ალიანსის (“Inter-Parliamentary Alliance on China” – “IPAC”) წევრები. აღნიშნული დაჯგუფების მიზანია ჩინეთის კომუნისტური პარტიის ანტიდემოკრატიულ ქმედებებთან და საფრთხეებთან გამკლავება.

კიბერთავდასხმის სამიზნეებს შორის, ასევე, [არიან](#) კომპანიები/პირები, რომლებიც მოქმედებენ ისეთ სტრატეგიულად მნიშვნელოვან დარგებში, როგორიცაა თავდაცვა, ინფორმაციული ტექნოლოგიები, ტელეკომუნიკაციები და სხვა. გარდა ამისა, ბრალდებულები ეჭვმიტანილნი არიან იმ დისიდენტების წინააღმდეგ კიბერთავდასხმების განხორციელებაში, რომლებიც ღიად აპროტესტებენ ჩინეთის ანტიდემოკრატიულ ქმედებებს, მათ შორის არიან ჰონგ-კონგში დემოკრატიის მომხრე აქტივისტები და მათი პარტნიორები.

შესაბამისად, აშშ-ს სადაზვერვო საზოგადოების „საფრთხის ყოველწლიური შეფასების“ [დოკუმენტის](#) დასკვნაში ვკითხულობთ, რომ ქვეყანაში სამოქალაქო განხეთქილების ხელშესაწყობად „ჩინეთის სახალხო რესპუბლიკამ შესაძლოა გარკვეულ დონეზე სცადოს აშშ-ს 2024 წლის არჩევნებზე გავლენის მოხდენა“.

აშშ-ს (ნიუ-იორკის) სასამართლოს მიერ გამოქვეყნებული საბრალდებო აქტის [თანახმად](#), ჩინეთის სახალხო რესპუბლიკამ სადაზვერვო აქტივობები განახორციელა რიგი ინსტიტუტების, მათ შორის სახელმწიფო უსაფრთხოების სამინისტროს მეშვეობით. სამინისტროს დეპარტამენტები ცდილობენ სხვა ქვეყნების პოლიტიკური, ეკონომიკური თუ უსაფრთხოების საკითხების შესახებ ინფორმაციის მოპოვებას და მათ საგარეო პოლიტიკაზე გავლენის მოხდენას. ამ თვალსაზრისით, სამინისტრო, სხვა მრავალ ქვეყანასთან ერთად, აშშ-ზეც ახორციელებდა სადაზვერვო ოპერაციებს.

2010 წელს ჰუბეის სახელმწიფო უსაფრთხოების დეპარტამენტმა შექმნა კომპანია (“Wuhan Xiaorui Science & Technology Co., Ltd”), რომლის ოფიციალურ სამუშაო სფეროებს წარმოადგენდა კვლევა და ტექნოლოგიური განვითარება. თუმცა, რეალურად, აღნიშნული კომპანია იყო ერთგვარი მექანიზმი, რომლის გამოყენებითაც ჰუბეის სახელმწიფო უსაფრთხოების დეპარტამენტი კიბერთავდასხმებს [ახორციელებდა](#). ამიტომ 2024 წელს აშშ-მ და გაერთიანებულმა სამეფომ ამ კომპანიას სანქციები [დაუწესეს](#).

აღსანიშნავია, რომ გაერთიანებულ სამეფოსა და აშშ-ს წინააღმდეგ კიბერთავდასხმაზე ეჭვმიტანილები სწორედ ჰუბეის სახელმწიფო უსაფრთხოების დეპარტამენტის ფარგლებში ოპერირებდნენ. აღნიშნული დეპარტამენტი კი, ჩინეთის უსაფრთხოების დეპარტამენტის პროვინციულ განშტოებას [წარმოადგენს](#).