კიბერუსაფრთხოების ახალი გამოწვევები და საქართველო

ინტერნეტის განვითარების ინიციატივა

განვითარების პროცესი

- 1990 – 1991 წლები - სპარსეთის ყურის ომი;
- 1999 წელი - ომი ბალკანეთზე/კოსოვოს კონფლიქტი;
- 2001 წლის 11 სექტემბერი;
- 2001 წლის ნოემბერი - ბუდაპეშტის კონვენცია კიბერდანაშაულის შესახებ;
- 2007 წელი - მასირებული კიბერშეტევა ესტონეთის კიბერ სივრცეზე;
- 2008 წელი - მასირებული კიბერშეტევები ლიტვისა და საქართველოს კიბერ სივრცეზე;
- 2008 წელი - კიბერშეტევები „რადიო თავისუფლებისა“ და „თავისუფლების“ ოფისებზე;
- 2008 წლიდან - იწყება სტრატეგიებზე და განვითარების პოლიტიკაზე აქტიური მუშაობა;
- 2014 – 2015 წლები - უკრაინა-რუსეთის ომი/ჰიბრიდული ომის დროს გამოიყენებოდა კიბერშეტევითი ელემენტები;
- 2015 - ახალი გამოწვევები/გაიზარდა დაპირისპირება კიბერ სივრცეში.

კიბერშეტევებში ძირითადი მოთამაშეები

- შეერთებული შტატები;
- რუსეთი;
- ირანი;
- ჩინეთი;
- ჩრდილოეთ კორეა;
- ისრაელი.

წყარო: FireEye, 2015

ყველაზე დაუცველი და მოწყვლადი სექტორები

- საბანკო სექტორი და სხვა საფინანსო ინსტიტუტები;
- საფონდო ბირჟები;
- ბირთვული ელექტროსადგურები;
- წყლის მომარაგებისა და გამწმენდი სისტემები;
- პერსონალური მონაცემები/ელექტრონული მმართველობა.

წყარო: FireEye, 2015

კიბერუსაფრთხოების განზომილებები

- პოლიტიკური დონე;
- სამხედრო დონე;
- ეკონომიკური დონე;
- ტექნიკური დონე;
- სამოქალაქო საზოგადოება და მოქალაქეები.

წყარო: Aapo Cederberg (GCSP), 2015

არსებული ვითარება

- 2015 წლის აპრილში გამოქვეყნდა შეერთებული შტატების კიბერუსაფრთხოების ახალი სტრატეგია;
- 2015 წლის 8 მაისს რუსეთსა და ჩინეთს შორის გაფორმდა თორმეტპუნქტიანი ხელშეკრულება, სადაც ერთერთი „მსხვილი“ პუნქტი ეხება თანამშრომლობას კიბერუსაფრთხოების სფეროში;
- 2015 წლის 13 ივნისს რუსეთსა და ირანს შორის დაიწყო მუშაობა მემორანდუმზე კიბერუსაფრთხოების სფეროში;
- 2015 წლის 25 სექტემბერს შეერთებულ შტატებსა და ჩინეთს შორის გაფორმდა ხელშეკრულება კიბერ სივრცეში თანამშრომლობის შესახებ.

საქართველოს კიბერუსაფრთხოების სამართლებრივი სივრცე

1) 2011 წლის დეკემბერი - საქართველოს ეროვნული უსაფრთხოების კონცეფცია;
2) 2012 წლის ივნისი - კანონი ინფორმაციული უსაფრთხოების შესახებ;
3) 2013 წლის მაისი - კიბერუსაფრთხოების სტრატეგიისა და განხორციელების 2013 – 2015 წლების სამოქმედო გეგმის დამტკიცება;
4) განისაზღვრა კრიტიკული ინფრასტრუქტურის სუბიექტები;
5) 2014 წლის აგვისტო - ევროკავშირთან ასოცირების ხელშეკრულება.

საქართველოს კიბერუსაფრთხოების სუბიექტები

1. 2010 წლის იანვარი - იუსტიციის სამინისტროს საჯარო სამართლის იურიდიული პირი **მონაცემთა გაცვლის სააგენტო**;
2. 2012 წლის დეკემბერი - შინაგან საქმეთა სამინისტროს ცენტრალური კრიმინალური პოლიციის დეპარტამენტის **კიბერდანაშაულთან ბრძოლის სამმართველო**. იქვე ფუნქციონირებს **კომპიუტერულ ციფრული ექსპერტიზის ქვეგანყოფილება;**
3. 2014 წლის თებერვალი - თავდაცვის სამინისტროს საჯარო სამართლის იურიდიული პირი **კიბერუსაფრთხოების ბიურო**;
4. 2011 წლის იანვარი - მონაცემთა გაცვლის სააგენტოს ფარგლებში ფუნქციონირებას იწყებს **CERT.GOV.GE.**

კიბერშეტევები 2008 – 2014/FireEye

Malware	Targeting	Russian Attributes
Evolves and Maintains Tools for Continued, Long-Term Use • Uses malware with flexible and lasting platforms • Constantly evolves malware samples for continued use • Malware is tailored to specific victims' environments, and is designed to hamper reverse engineering efforts • Development in a formal code development environment **Various Data Theft Techniques** • Backdoors using HTTP protocol • Backdoors using victim mail server • Local copying to defeat closed/air gapped networks	**Georgia & the Caucasus** • Ministry of Internal Affairs • Ministry of Defense • Journalist writing on Caucasus issues • Kavkaz Center **Eastern European Governments & Militaries** • Polish Government • Hungarian Government • Ministry of Foreign Affairs in Eastern Europe • Baltic Host exercises **Security-related Organizations** • NATO • OSCE • Defense attaches • Defense events and exhibitions	**Russian Language Indicators** • Consistent use of Russian language in malware over a period of six years • Lure to journalist writing on Caucasus issues suggests APT28 understands both Russian and English **Malware Compile Times Correspond to Work Day in Moscow's Time Zone** • Consistent among APT28 samples with compile times from 2007 to 2014 • The compile times align with the standard workday in the UTC + 4 time zone, which includes major Russian cities such as Moscow and St. Petersburg

კიბერშეტევები 2015

- 2015 წლის იანვარი - ფრანგული ჰიპერმარკეტის Carrefour - ის ოფიციალური ვებ - გვერდი http://carrefour.com.ge/ (the Middle Eastern Cyber Army - MECA);

- 2015 წლის აპრილი - "საქართველოს მოსამართლეთა ერთობის" ვებ-გვერდი ("ელ მოჰაჯირი");

- 2015 წლის მაისი - საფინანსო ინსტიტუტები (უცნობია).

არსებული პრობლემები

- საკანონმდებლო ბაზის არარსებობა;
- საზოგადოებაში დაბალი ცნობიერება;
- სპეციალისტების არარსებობა/არასაკმარისი რაოდენობა;
- საერთაშორისო სტანდარტების არარსებობა.

კითხვები/დისკუსია