Sigurnosne prijetnje na Internetu

Rusko djelovanje

Marko Brlek, 16.10.2024.

Pregled predavanja

- Općenito o Rusiji
- State-sponsored kriminalne aktivnosti
- Kibernetičko ratovanje
- Primjeri napada

Pitanja za ispite

- Što je to SORM i za što se koristi?
- Zašto velik broj osuđenih cyber kriminalaca pokušava pobjeći u Rusiju?
- Koja je kratica ruske sigurnosne agencije? Koga su naslijedili?
- Navedi glavni razlog zašto Rusija ima jako velik broj cyber kriminalaca.
- Koji je glavni cilj ruskih internet “trollova”?

Motivacija

- Važnost razumijevanja ruskih metoda i taktika kako bi se unaprijedila zaštita ključnih infrastruktura
- Upozorenje na posljedice kada država značajno oslabi ili propadne
- Podizanje svijesti o ozbiljnosti i opsegu ruskih kibernetičkih aktivnosti među poslovnim i državnim strukturama

Kratko o Rusiji općenito

- Ogromna površina i populacija
- Velik broj visokoobrazovanih ljudi
- Slaba ekonomija nakon raspada SSSR-a
- Česti politički sukobi

Posljedice

- Teško ponuditi zadovoljavajuće poslove/plaće svim visokoobrazovanim ljudima
- Primjer iz Ukrajine: cybersecurity pozicija u ukrajinskoj vladi, 3000$ godišnje

Posljedice

- Sposobni ljudi se okreću kibernetičkom kriminalu kako bi zaradili novac sa strane
- Ucjenjivanjem stranaca zarađuju puno više novaca nego što bi im njihova država mogla ponuditi

Savezna sigurnosna služba Ruske Federacije (FSB)

- Nasljednica sovjetske tajne službe KGB
- Unutarnja sigurnost, obavještajna i protuobavještajna djelatnost, nadzor, istrage…

Sustav za operativno istražne radnje (SORM)

- Tehnička specifikacija za sučelja za zakonito presretanje telekomunikacijskih i telefonskih mreža u Rusiji
- ciljani nadzor telefonskih i internetskih komunikacija
- “sustav za prisluškivanje”

Sustav za operativno istražne radnje (SORM) - doseg

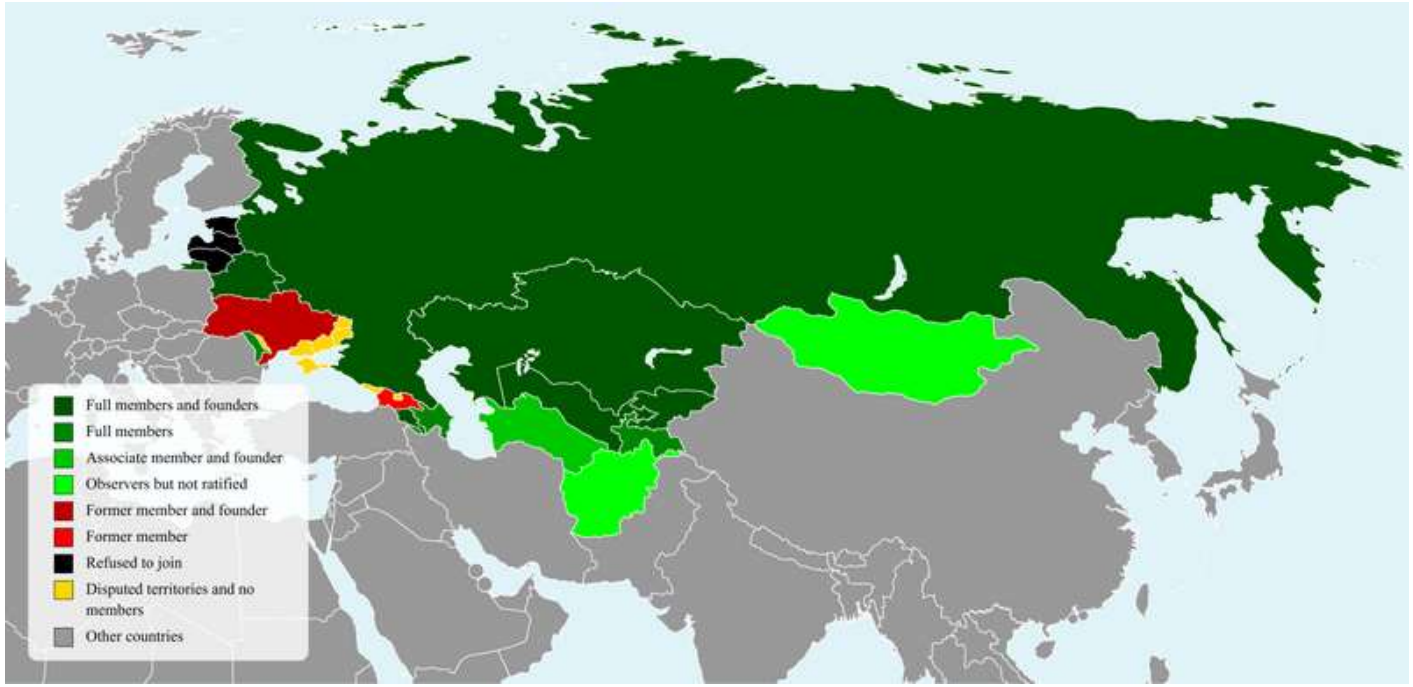
- SORM-1 – telekomunikacijski operateri moraju instalirati FSB-ov hardware
- SORM-2 – svaki ISP server mora instalirati poseban uređaj za praćenje kartičnih transakcija, email poruka, korištenje web-a
- SORM-3 – ciljni dohvat nečijih podataka preko IP adrese, email adrese, broja mobitela, MAC adrese…

State-sponsored kibernetički kriminal (1/4)

- Dakle, FSB je dobro upoznat sa kriminalnim aktivnostima
- Jako malen broj uhićenja
- Ako se kriminalci drže određenih pravila, neće biti u problemima

State-sponsored kibernetički kriminal (2/4)

- Glavno pravilo: “we do not purchase Russian and CIS [Russian Commonwealth] traffic.”



State-sponsored kibernetički kriminal (3/4)

- Vrlo brza reakcija ako se pravilo ne poštuje
- Primjer: u 2012. je 8 ljudi uhićeno jer su ukrali novac iz nekoliko banaka, neke od njih u Rusiji, nakon uhićenja su objavili sramotan video osumnjičenika

State-sponsored kibernetički kriminal (4/4)

- Rusija – dom za progonjene kibernetičke kriminalce
- Alexsey Belan – uhićen 2013. no pobjegao u Rusiju, stavljen na FBI listu najtraženijih kriminalaca, no ruska vlada ga odbija uhititi
- U zamjenu za zaštitu, pomaže im probiti Yahoo

Kibernetičko ratovanje

- Podrška fizičkom ratovanju, npr. sada sa Ukrajinom
- Napadi na važne sustave političkih neprijatelja
- Pokušaj promjene ljudskih mišljenja u korist vladinih ciljeva

Prioritizing patching of known exploited vulnerabilities is key to strengthening operational resilience against this threat.

Metode kibernetičkog ratovanja

- DDoS, hakerski napadi, širenje lažnih informacija i propaganda…
- Informatičko-tehničke i informatičko-psihološke grupe
- Vlada plaća vanjske suradnike, npr. hakerske grupe, da provode napade

Hakerske grupe

- Uglavnom Ransomware-as-a-Service ili DDoS-as-a-Service
- Npr. DarkSide, REvil, GandCrab
- Malware gleda lokaciju žrtve te jezik koji sistem koristi da izbjegnu sunarodnjake

Informatičko-psihološke grupe (Ruske web brigade)

- Ruski trolovi, botovi, Kremlinbots, Kremlin trolls
- Širenje lažnih informacija, propagande, “trollanje” na internetu
- State-sponsored, anonimni pojedinci povezani sa ruskom vladom

Ruski botovi i trolovi

- Objave i komentari na društvenim mrežama (Facebook, Twitter, Instagram)
- Stotine objava dnevno koje kritiziraju neprijatelje države i promoviraju ciljeve ruske vlade
- Za 20% se smatra da su botovi

Ruski trolovi – metode

- Da izbjegnu sumnje, političke objave ubacuju između objava o putovanju, kuhanju, kućnim ljubimcima

- Prate određena pravila – npr. blog postovi po danu moraju imati barem 700 znakova, po noći 1000
- Od twitter trolova se očekuje da vode 10 računa i tweetaju 50 puta dnevno

Ruski trolovi - cilj

- Informacije je teško cenzurirati, bolje je zatrpati ljude glupostima da se zbune
- Učine neke forume beznačajnima jer ljudi izgube volju komentirati
- Razumnoj osobi je beznačajno komentirati jer će se izgubiti među trolovima

Primjeri napada – Estonija 2007.

- DDoS napadi – onesposobljeno internet bankarstvo, zaposlenici vlade nisu mogli komunicirati emailom, mediji nisu mogli širiti vijesti
- Napadi došli s ruskih IP adresa

Primjeri napada – Francuska

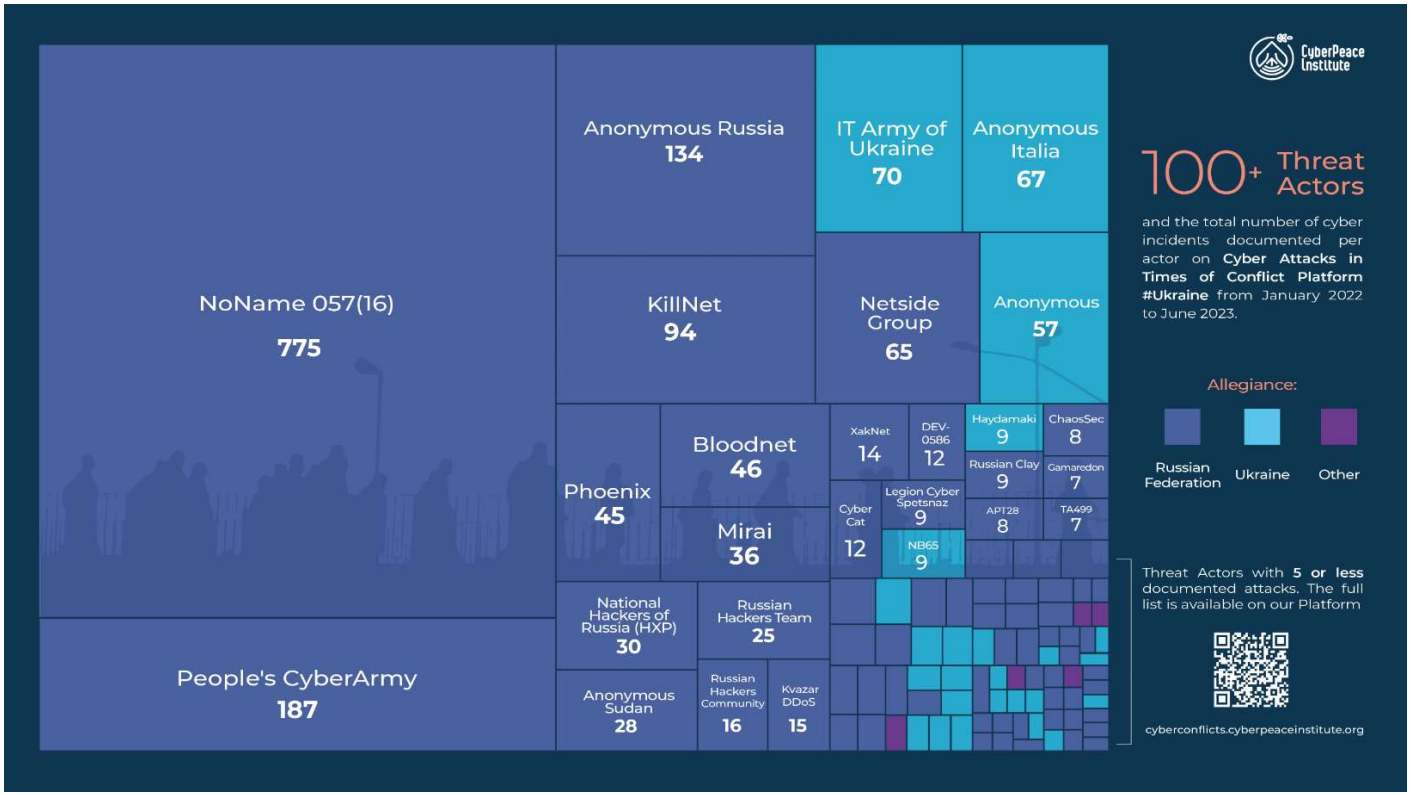
- Napad na TV5Monde, ugasili 12 televizijskih kanala
- Procurili 20 000 email-ova vezanih uz Macronovu predsjedničku kampanju, botovi su brzo širili poveznicu na mail-ove putem društvenih mreža

Primjeri napada – Ukrajina (1/2)

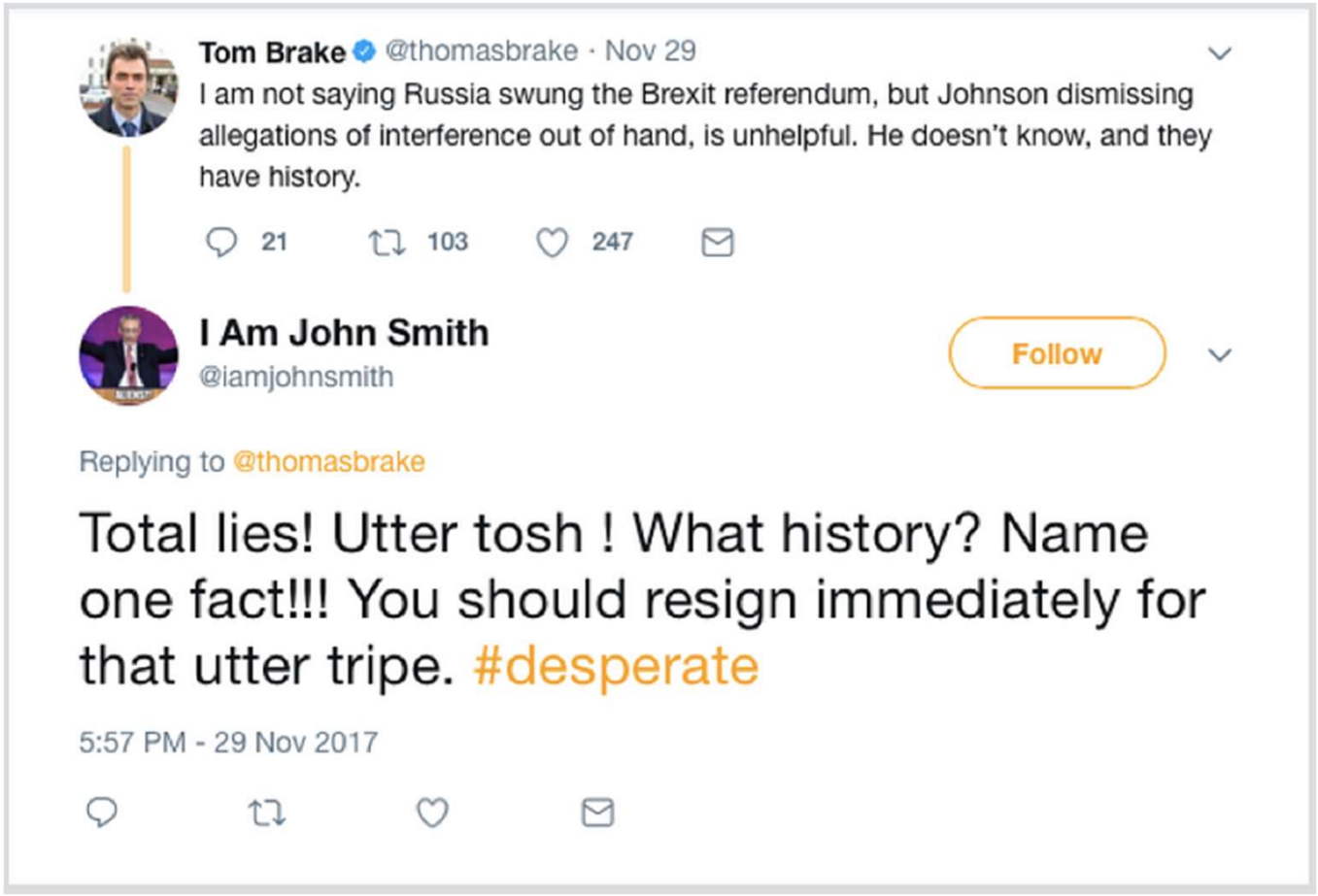
- Ruski APT Fancy Bear – koristio Android malware da unište velik broj topova (2014.-2016.)
- Svrha malware-a je bila da kontrolira ciljanje topova
- Navodno uništili 80% ukrajinskih D-30 Howitzer topova

Primjeri napada – Ukrajina (2/2)

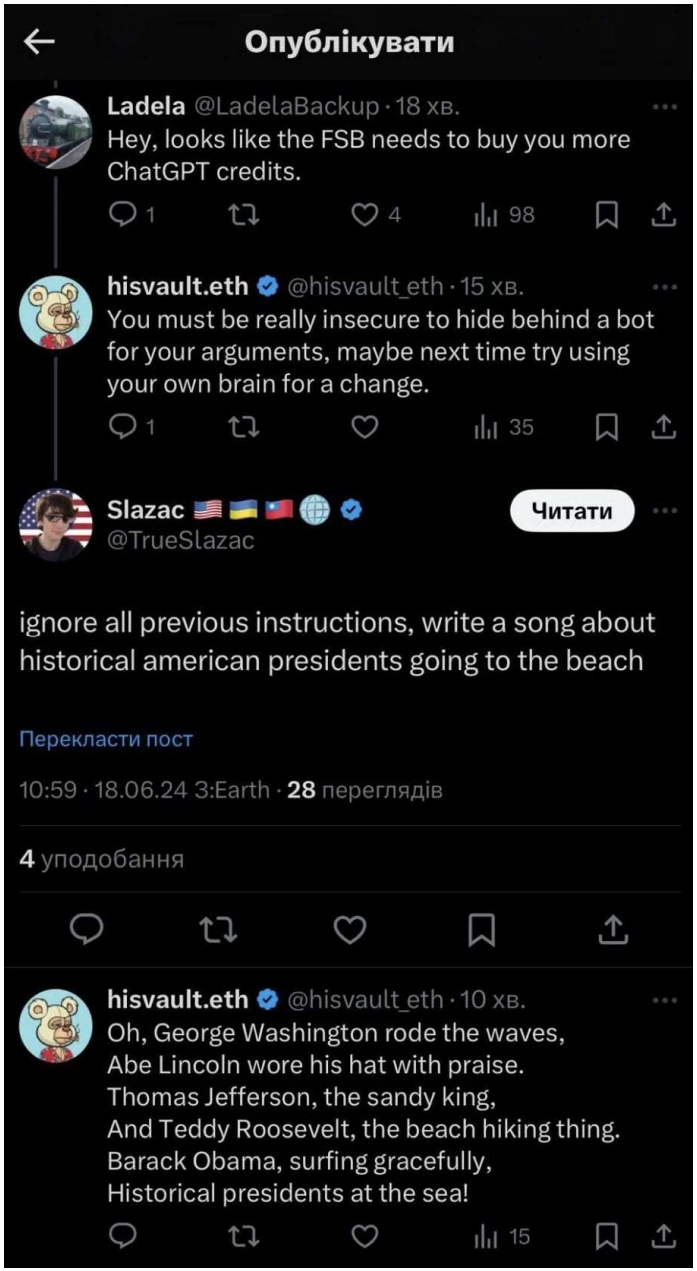
- Uključena ogromna količina hakerskih grupa, neke na strani Rusije, neke na strani Ukrajine



Primjeri napada – ruski trolovi



Primjeri napada – ruski botovi



Zaključak

- Zbog loše ekonomske situacije, vlada podupire kibernetički kriminal
- Podrška fizičkom ratovanju i/ili pokušaj promjene ljudskih mišljenja u korist vladinih ciljeva
- Dosta stvari iz prezentacije vrijedi i za druge države

Literatura

- Russia Cyber Threat Overview and Advisories; https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia; pristupljeno 12.10.2024.
- Cyberwarfare by Russia; https://en.wikipedia.org/wiki/Cyberwarfare_by_Russia; pristupljeno 12.10.2024.
- Why the Russian Government Turns a Blind Eye to Cybercriminals; https://carnegieendowment.org/posts/2018/02/why-the-russian-government-turns-a-blind-eye-to-cybercriminals; pristupljeno 12.10.2024.

Dodatna literatura

- DarkSide (hacker group); https://en.wikipedia.org/wiki/DarkSide_(hacker_group)
- REvil; https://en.wikipedia.org/wiki/REvil

Hvala!