CRNA GORA

MINISTARSTVO JAVNE UPRAVE

IZVJEŠTAJ O INCIDENTNIM SITUACIJAMA NA INTERNETU U CRNOJ GORI ZA 2017. I 2018.GODINU

Podgorica, decembar 2018.godine

SADRŽAJ

UVOD

Od 2014. godine Nacionalni tim za odgovor na računarske incidente (NCIRT) izrađuje godišnji izvještaj o incidentnim situacijama na Internetu u Crnoj Gori. Cilj ovog izvještaja je da se kroz prikaz novih statističkih podataka ukaže aktuelno stanje u sajber prostoru Crne Gore.

Zbog konstantnog rasta broja usluga koje javni i privatni sektor pružaju putem Interneta, kako građanima, tako i drugim pravnim subjektima, moramo težiti ka bezbjednom sajber prostoru Crne Gore. S toga je ključno da, prije svega, razumijemo prijetnje koje su aktuelne u crnogorskom sajber prostoru.

U izradi izvještaja korišćeni su podaci sa kojima raspolažu Ministarstvo javne uprave, Zavod za statistiku, kao i ključna međunarodna organizacija na polju sajber bezbjednosti ENISA.

Svjesna značaja razvoja i primjene sajber bezbjednosti, Crna Gora je u prethodnom periodu napravila značajne korake u tom pravcu.

Formiranjem nacionalnog CIRT-a Crne Gore, postavljene su osnove za uspostavljanje kvalitetne zaštite sistema, podataka i infrastrukture u cilju stvaranja održivog informacionog društva. Jedan od ciljeva je i da se omogući rano otkrivanje sajber prijetnji i incidenata na nacionalnom nivou i da se adekvatno reaguje i odgovori na iste.

AKTERI U SAJBER PROSTORU

Kao i prethodnih godina, za aktere u sajber prostoru koristićemo zvanične podatke EU. Prethodnih godina evidentiran je porast broja aktera u sajber prostoru. Prema izvještaju koji je objavila ENISA (Agencija EU za mrežnu i informacionu bezbjednost) za 2017. godinu, prepoznati su sljedeći akteri, tj. napadači, u sajber prostoru:

- **Sajber kriminalci:** Ove grupe su najpoznatije i najaktivnije od svih sajber napadača. Procjenjuje se da su odgovorni za dvije trećine prijavljenih napada. Njihova glavna motivacija je sticanje profita nelegalnim sajber aktivnostima. Konstantno napreduju i unapređuju svoje mogućnosti. Umiješani su u sve vrste prevara sa elektronskim finansijama, trgovinom, ucjenama, sajber kriminalnim uslugama, isporučivanje i izrada malicioznog koda itd. Ove grupe imaju velike mogućnosti u sprovođenju zadataka, mogu biti globalno povezane i mogu lako ostvariti pristup neophodnim resursima za sprovođenje napada. Prethodne godine smo svjedočili masivnim DDoS napadima kroz IoT uređaje, sofisticiranim ransomware kampanjama, a sve kroz održavanje svoje anonimnosti.

- **Zaposleni (bivši, aktuelni, interni i eksterni):** Motivisani osvetom, sabotažom, iznudom ili profitom, ova grupa ima značajnu ulogu u materijalizaciji sajber prijetnji, naročito onih koje dovode do curenja podataka. Prijetnje koje dolaze od ove grupe mogu biti namjerne ili nenamjerne, i pod njima spadaju i nepoštovanje pravilnika i procedura, ljudske greške i sl.

- **Sajber špijuni (države, korporacije):** Jasno je da su dimenzije ovih napada u konstantnom širenju. Više država je razvilo sposobnosti koje mogu biti korišćene za različite vrste napada, bilo protiv drugih vlada ili privatnih institucija. Napadi su najviše usmjereni ka otkrivanju državnih i vojnih tajni, obavještajnih podataka, kao i prema kritičnoj infrastrukturi. Metode napada izrazito variraju i imaju veoma visok procenat uspješnosti.
  Glavni cilj korporacija je da steknu kompetetivnu prednost u odnosu na konkurenciju. Obično se radi o sakupljanju informacija vezanih za biznis, preuzimanje zaštićenih intelektualnih dostignuća, otkrivanje tuđih ponuda prilikom tendera i sl. Korporacije ili unajmljuju plaćenike za ove poslove ili ako su dovoljno velike imaju svoje odsjeke za sajber špijunažu.

- **Haktivisti:** Haktivisti predstavljaju grupu napadača koji uživaju veliki publicitet, npr. Anonimusi. Oni su ideološki motivisani pojedinci, koji dinamički formiraju grupe, obično bez centralne organizacione strukture. Njihova glavna motivacija je odbrana ideja. Biraju mete koje će stvoriti što veći odraz u medijima, pa zato biraju sajtove vlada, velikih kompanija i slično.

- **Sajber borci:** Grupa građana koji su motivisani na nacionalnoj ili religijskoj osnovi. Oni iz ideoloških razloga pokreću koordinisane sajber napade. Ova grupa spade u "sivu zonu" između haktivista, terorista, sajber špijuna i sajber vojske. Napadači iz ove grupe (npr.

Syrian Electronic Army) se nalaze na spisku najtraženijih sajber kriminalaca od strane organa za sprovođenje reda.

- **Sajber teroristi:** Ovakve grupe obično ciljaju nacionalnu bezbjednost i cjelokupno društvo. Karakterišu se primjenjivanjem represivnih mjera, kako bi uticali na proces donošenja odluka, a sve u cilju postizanja svojih ciljeva. Uobičajeno je da napadaju kontrolu saobraćaja, vojnu infrastrukturu, vladine sisteme i sl.

- **Skript prepisivači** (***script kiddies***): su pojedinci koji tek ulaze u svijet sajber napada. Oni ne poznaju dovoljno tehnike i alate, već samo kopiraju napade iskusnijih hakera. Zbog ovog oni obično nisu upoznati ni sa posljedicama koje mogu da proizvedu.

SAJBER PRIJETNJE NA GLOBALNOM NIVOU

Imajući u vidu prekograničnu prirodu sajber napada, kako bi na najbolji način razumjeli prijetnje na nacionalnom nivou, prvo moramo sagledati trenutno stanje kada su u pitanju sajber prijetnje na globalnom nivou.

U nastavku ćemo sagledati izvještaje ENISA-e za 2017.godinu.

ENISA – PREGLED SAJBER PRIJETNJI U 2017. GODINI

Za izradu ovog dokumenta, ENISA je koristila javno dostupne izvore, izvještaje nacionalnih i međunarodnih organizacija kao što su CERT/CIRT timovi, državne institucije, akademija, industrija, štampa, kao i individualne eksperte za sajber bezbjednost.

Na osnovu prikupljenih informacija iz 2017. godine, glavni zaključak koji se može donijeti je da su svi izloženi sajber prijetnjama. Jasno je da je glavni motiv sajber napada novac, a tokom prethodne godine bili smo svjedoci vrlo efikasne monetizacije sajber kriminala. Odavno je poznato da krupniji akteri u sajber prostoru imaju razvijenu infrastrukturu i alate za sajber napade. Ono što je novi trend je nuđenje takvih alata i infrastrukture u formi usluga (eng. *as a service*). Očigledan je napredak kada je u pitanju zrelost napadača sa jedne, ali i organa koji se bave zaštitom sa druge strane. Organi koji se bave zaštitom su demonstrirali pojačan nivo saradnje i zajedničkog odgovora na sajber prijetnje. Međutim, napadači su, kao i obično, korak ispred.

U nastavku je prikazana tabela najvećih prijetnji u 2017. godini sa trendom rasta u odnosu na prethodnu godinu (Tabela 1), kao i tabela učešća identifikovanih grupa napadača kod najvećih prijetnji (Tabela 2).

	Glavne prijetnje - 2016	Trend rasta 2016	Glavne prijetnje – 2017	Trend rasta 2017	Promjena pozicije
1	Malver		Malver		
2	Web bazirani napadi		Web bazirani napadi		
3	Napadi na web aplikacije		Napadi na web aplikacije		
4	DoS, DDoS		Phishing		
5	Botnetovi		Spam		
6	Phishing		DoS, DDoS		
7	Spam		Ransomware		
8	Ransomware		Botnetovi		
9	Prijetnja od unutrašnjih napada (Insider threat)		Prijetnja od unutrašnjih napada (Insider threat)		
10	Fizička šteta/gubitak/krađa		Fizička šteta/gubitak/krađa		
11	Exploit kitovi		Kompromitovanje podataka (Data Breach)		
12	Kompromitovanje podataka (Data Breach)		Krađa identiteta		
13	Krađa identiteta		Curenje podataka (Information leakage)		
14	Curenje podataka (Information leakage)		Exploit kitovi		
15	Sajber špijunaža		Sajber špijunaža		

Tabela 1: Najveće prijetnje i trend rasta

Prikaz prijetnji i mogućih aktera								
	Sajber kriminalci	Zaposleni	Države	Korporacije	Haktivisti	*Sajber borci*	Sajber teroristi	*Script kiddies*
Malver	✓	✓	✓	✓	✓	✓	✓	✓
Web bazirani napadi	✓		✓	✓	✓	✓	✓	✓
Napadi na web aplikacije	✓		✓	✓	✓	✓	✓	✓
DoS, DDoS	✓		✓	✓	✓	✓	✓	✓
Botnetovi	✓		✓	✓	✓	✓		✓
Phishing	✓	✓	✓	✓	✓	✓		
Spam	✓	✓	✓	✓				
Ransomware	✓	✓	✓	✓		✓		✓
Prijetnja od unutrašnjih napada (Insider threat)	✓		✓	✓		✓	✓	
Fizička šteta/gubitak/krađa	✓	✓	✓	✓	✓		✓	✓
Exploit kitovi	✓		✓	✓		✓		
Kompromitovanje podataka (Data Breach)	✓	✓	✓	✓	✓	✓	✓	✓
Krađa identiteta	✓	✓	✓	✓	✓	✓	✓	✓
Curenje podataka (Information leakage)	✓		✓	✓	✓	✓	✓	✓
Sajber špijunaža		✓	✓	✓		✓		

Tabela 2: Prikaz prijetnji i mogućih aktera

(✓ -Primarna grupa za prijetnju; ✓ -Sekundarna grupa)

PREGLED PRIJETNJI U SAJBER PROSTORU CRNE GORE

Nacionalni CIRT Crne Gore, u sklopu svojih svakodnevnih aktivnosti, obavlja poslove koordinacije i odgovora na incidentne situacije u crnogorskom sajber prostoru. Incidenti se prijavljuju online, putem web portala www.cirt.me ili putem email-a na kontakt@cirt.me.

Vlada Crne Gore je usvojila Strategiju Sajber bezbjednosti u Crnoj Gori od 2018-2021. godine. Implementacija Strategije treba da doprinese podizanju ukupnog stepena sajber bezbjednosti. Neke od ključnih aktivnosti koje su sprovedene u tom cilju su: Analiza prijetnji u sajber prostoru Crne Gore, Metodologija izbora kritične informatičke infrastrukture, Zakon o izmjenama i dopunama Zakona o informacionoj bezbjednosti, uspostavljanje lokalnih CIRT timova, itd.

Kroz analizu prijetnji i izvještaje o incidentnim situacijama u sajber prostoru Crne Gore za period od 2014. do 2018. godine vidjeli smo da su računarski sistemi i korisnici u Crnoj Gori izloženi sajber prijetnjama i napadima koje pogađaju i ostatak svijeta.

Analizom trenutnog stanja, možemo zaključiti da se i tokom 2018. godine nastavio trend rasta broja prijavljenih incidenata u odnosu na prethodne godine. Tokom 2017.godine CIRT-u je prijavljeno ukupno 532 incidenta, dok je od 1. januara do 1. decembra 2018.godine CIRT registrovao 490 prijava.

Ovaj trend se ogleda i u činjenici da je CIRT-u, tokom 2017. i 2018 godine, prijavljen veliki broj incidenata koji se odnose na malver, uključujući maliciozne programe za ucjenu, tj. *ransomware*, pomoću kojih napadač kriptuje podatke na računaru i traži novac za dekripciju. Broj napada ove vrste je u velikom porastu na globalnom nivou, i prepoznat je kao jedna od glavnih prijetnji u gore navedenim izvještajima ENISA-e, a svjedoci smo da je ova prijetnja itekako prisutna i u crnogorskom sajber prostoru.

U Crnoj Gori su registrovani slučajevi u kojima su računari zaraženi “WannaCry” ransomware-om. Radi se o jednom od najopasnijih ransomware-a koji se pojavio 2017.godine, a koji se se proširio ogromnom brzinom i tokom prva dva dana kampanje zarazio je preko 170 hiljada uređaja širom svijeta. Tokom 2018. godine primijetan je veliki broj napada povezanih sa više hakerskih grupa, kao što su "Fancy Bear", "Sandworm", "Strontium", "APT 28", "CyberCaliphate", "Sofacy", "BlackEnergy Actors".

Primjetan je značajan porast broja napada na informacione sisteme državnih organa i pravnih lica. Informatička infrastruktura državnih organa, a naročito portal Vlade Crne Gore, bili su često meta DDoS napada.

CIRT je preduzeo sve mjere iz svoje nadležnosti u koordinaciji sa državnim organima, privatnim sektorom, kao i međunarodnim partnerima, kako bi napadi bili spriječeni, servisi nesmetano funkcionisali, a javnost bila pravovremeno informisana. U toku 2018. godine Ministarstvo javne uprave u saradnji sa Agencijom za nacionalnu bezbjednost je obezbijedilo redudantni Internet link kod drugog provajdera, koji je omogućio nesmetano funkcionisanje servisa tokom napada.

Veliki broj prijava koje je primio CIRT odnosi se na zloupotrebu profila na društvenim mrežama. Ovo saznanje ukazuje na opasnosti kojima se korisnici izlažu prilikom postavljanja ličnih podataka i sadržaja na Internet.

Pored navedenih, bitno je napomenuti da je zabilježen i veliki broj finansijskih prevara i *phishing* napada.

Ovaj trend je nastavljen i u 2018.godini.

U nastavku (Tabela 4, Tabela 5) je statistički prikaz prijavljenih incidenata.

Godina	Napad na web sajtove i IS	Prevare putem Interneta	Zloupotreba profila na društvenim mrežama	Neprikladan sadržaj na Internetu	Malver	Ostali	Ukupno
2011	1	-	-	-	-	-	1
2012	3	2	-	1		-	6
2013	5	3	10	-	1	3	22
2014	5	6	20	5		6	42
2015	6	17	37	19	17	36	132
2016	18	20	36	14	50	25	163
2017	91	18	34	9	368	12	532
2018 (do 1 dec)	13	68	39	4	333	33	490

Tabela 4: Statistika incidenata prijavljenih CIRT-u

Godina	Broj predmeta
2011	1
2012	6
2013	22
2014	42
2015	132
2016	163
2017	532
2018 (do 1 decembra)	490
UKUPNO	**1388**

Tabela 5: Ukupan broj prijava po godinama

ZAKLJUČAK

Na osnovu podataka navedenih u ovom Izvještaju, možemo zaključiti da su globalne sajber prijetnje itekako prisutne u Crnoj Gori, i da se statistika najvećih globalnih sajber prijetnji ne razlikuje u velikoj mjeri u odnosu na crnogorski sajber prostor.

Najbolji način za borbu protiv sajber prijetnji jeste proaktivno djelovanje i podizanje nivoa svijesti o ovoj problematici kroz edukaciju građana i korisnika.

Shodno tome, Ministarstvo javne uprave u saradnji sa Upravom za kadrove, organizuje obuku za sve državne i lokalne službenike i namještenike na temu sajber bezbjednosti. U periodu od 2016 do 2018.godine organizovan je veći broj obuka kojima je prisustvovalo oko 350 službenika.

Osim osnovne obuke za sve državne i lokalne službenike i namještenike, Ministarstvo javne uprave organizuje ekspertske obuke za službenike koji rade na poslovima informacione bezbjednosti. Imajući u vidu sve veći broj napada na državnu informacionu infrastrukturu, smatramo da je neophodno jačanje ekspertskog kadra iz ove oblasti

Borba protiv sajber kriminala zahtijeva upotrebu modernih tehničkih znanja, radi preventivnog djelovanja i sprječavanja hakera. Potrebno je izvršiti sinhronizaciju djelovanja, uskladiti zakone između država, djelovati na globalnom nivou, a države moraju imati jake obrazovane kadrove u ovoj sferi, kako bi se procedura otkrivanja, gonjenja i procesuiranja što bolje izvela. Svaka aktivnost u zemlji treba da bude organizovana tako da postoji saradnja između državnih organa i istovremeno djelovanje bezbjednosnih službi (obavještajne službe, policije, vojne obavještajne službe), kao i saradnja u javno-privatnom obliku.

Ministarstvo javne uprave će nastaviti i sa aktivnostima na edukaciji građana o bezbjednom korišćenju interneta, objavljivanju savjeta za zaštitu i upozorenja o aktuelnim prijetnjama.