EVROPSKA KOMISIJA

SPOROČILO ZA MEDIJE

Bruselj, 10. februar 2014

Evropski center za boj proti kibernetski kriminaliteti – eno leto od odprtja

Katere so glavne grožnje kibernetske kriminalitete v prihodnosti? Kako je Evropski center za boj proti kibernetski kriminaliteti pomagal zaščititi evropske državljane in podjetja od njegove ustanovitve januarja 2013?

Na ti vprašanji poskuša odgovoriti poročilo o Evropskem centru za boj proti kibernetski kriminaliteti, ki ga je Komisija predstavila danes, bili pa sta tudi v ospredju na konferenci, ki jo je organizirala Komisija in na kateri so bili prisotni organi pregona ter predstavniki nacionalnih organov, institucij EU in zasebnega sektorja.

„Storilci kaznivih dejanj hitro spreminjajo svoje ravnanje in izkoriščajo tehnološki razvoj in pravne vrzeli. Še naprej bodo ustvarjalni in uporabljali kompleksne oblike napadov, da bi zaslužili več denarja, mi pa moramo biti na to pripravljeni. Strokovno znanje in izkušnje Evropskega centra za boj proti kibernetski kriminaliteti nam pri tem pomagajo, hkrati pa spodbujajo tudi sodelovanje na evropski ravni. Evropski center za boj proti kibernetski kriminaliteti je z več uspešnimi in daljnosežnimi operacijami lansko leto že pridobil zaslužen sloves med organi kazenskega pregona," je dejala Cecilia Malmström, članica Komisije, pristojna za notranje zadeve.

Troels Örting, vodja Evropskega centra za boj proti kibernetski kriminaliteti, je dodal: „V 12 mesecih od odprtja Evropskega centra za boj proti kibernetski kriminaliteti smo izredno veliko pomagali organom kazenskega pregona EU pri njihovih dejavnostih preprečevanja in preiskovanja čezmejne kibernetske kriminalitete. Ponosen sem in zadovoljen z našimi rezultati do zdaj, vendar ne moremo počivati na lovorikah. Zlasti sem zaskrbljen zaradi vse bolj zapletenih oblik zlonamerne programske opreme, ki se pojavljajo, ter vse bolj tehnološko naprednih računalniških prevar („cyber-scams") in spolnega izsiljevanja („sextortion") mladoletnikov. Zaenkrat vidimo le vrh ledene gore, vendar si Evropski center za boj proti kibernetski kriminaliteti, ki ga podpirajo naši dragoceni deležniki in partnerji, prizadeva, da bi podprl prihodnje vodilne operacije boja proti kibernetski kriminaliteti v državah članicah."

Po nedavni raziskavi Eurobarometra ima 12 % evropskih uporabnikov interneta izkušnje z vdori v svoje račune pri družbenih medijih ali račune elektronske pošte. 7 % jih je bila žrtev goljufije pri spletnih nakupih s kreditnimi karticami ali spletnem bančništvu.

Glavni dosežki Evropskega centra za boj proti kibernetski kriminaliteti

Glavna naloga Evropskega centra za boj proti kibernetski kriminaliteti je uničiti dejavnosti mrež organiziranega kriminala, odgovorne za huda in organizirana kazniva dejanja na področju kibernetske kriminalitete (za več podrobnosti glej MEMO/13/6 in infografični prikaz). Evropski center za boj proti kibernetski kriminaliteti podpira in usklajuje dejavnosti in preiskave, ki jih na več področjih opravljajo organi držav članic. Nedavni primeri njegovih dejavnosti vključujejo:

Kazniva dejanja z visokimi tehnologijami (kibernetski napad, zlonamerna programska oprema)

V svojem prvem letu je Evropski center za boj proti kibernetski kriminaliteti pomagal pri usklajevanju 19 večjih operacij boja proti kibernetski kriminaliteti, na primer:

- zaključeni sta bili dve večji mednarodni preiskavi (Ransom in Ransom II), ki sta bili povezani z zlonamerno programsko opremo, imenovano Police Ransomware, ki je vrsta zlonamerne programske opreme, ki blokira računalnik žrtve in jo obtoži, da je obiskala nezakonite spletne strani z gradivom o zlorabi otrok ali o drugih nezakonitih dejavnostih. Storilci kaznivega dejanja zahtevajo izplačilo „globe" za deblokado računalnika žrtve napada, zaradi česar se zdi, da je vir te zlonamerne programske opreme zakonit organ kazenskega pregona. Storilci kaznivega dejanja skušajo žrtev prepričati, da je treba plačati „globo" v višini približno 100 evrov prek dveh vrst portalov za spletna plačila, ki sta virtualna in anonimna. Storilci kaznivih dejanj, ki jih preiskuje Evropski center za boj proti kibernetski kriminaliteti, so okužili več deset tisoč računalnikov po vsem svetu in zaslužili več kot milijon evrov na leto. Izvedenih je bilo 13 aretacij (v glavnem v Španiji), poleg tega pa so bile razbite tudi kriminalne mreže.
- Evropski center za boj proti kibernetski kriminaliteti je podprl tudi več mednarodnih pobud na področjih razbitja omrežja robotskih računalnikov (botnetov), prekinitev in preiskav forumov z vsebinami o kaznivih dejanjih ter napadov zlonamerne programske opreme proti finančnim institucijam, kot je nedavno razbitje botneta ZeroAccess v sodelovanju z Microsoftom in enotami za boj proti kriminaliteti visoko razvite tehnologije iz nemškega BKA, Nizozemske, Latvije, Luksemburga in Švice.

Spolno izkoriščanje otrok na spletu

Evropski center za boj proti kibernetski kriminaliteti trenutno podpira 9 velikih policijskih operacij na področju spolnega izkoriščanja otrok v Evropski uniji. V prvem letu delovanja Evropskega centra za boj proti kibernetski kriminaliteti je ta skupaj z veliko državami članicami in sodelujočimi partnerji izven EU veliko energije usmeril v boj proti nezakonitim dejavnostim pedofilov, ki sodelujejo pri spletnem spolnem izkoriščanju otrok in za to uporabljajo skrite storitve.

Evropski center za boj proti kibernetski kriminaliteti je vključen v veliko operacij in skupnih preiskav, usmerjenih v izdelavo in distribucijo gradiv o zlorabi otrok na različnih internetnih platformah. Zagotavlja operativno in analitično podporo pri preiskavah o darknetu, kjer pedofili trgujejo z nezakonitimi gradivi o zlorabi otrok na skritih forumih, ter pri preiskavah o spolnem izsiljevanju („sextortion"). Spolno izsiljevanje je izraz, ki se uporablja, kadar osebe, ki spolno zlorabljajo otroke, pridobijo dostop do neprimernih slik mladoletnikov in jih uporabijo, da jih prisilijo v nadaljnja dejanja, ali pa jih posredujejo družini in prijateljem žrtve.

Goljufija v zvezi s plačili

Evropski center za boj proti kibernetski kriminaliteti trenutno zagotavlja operativno in analitično podporo 16 preiskavam o goljufiji v zvezi s plačili. Leta 2013 je podprl preiskave, na podlagi katerih so prekinili tri različne mednarodne mreže goljufov s kreditnimi karticami:

- pri eni operaciji so aretirali 29 osumljencev, ki so zaslužili 9 milijonov evrov z zlorabo podatkov 30 000 imetnikov kreditnih kartic.

- pri razkritju druge mreže je bilo med operacijo aretiranih 44 oseb (ki jih je treba prišteti 15 že aretiranim osebam, tj. skupaj 59 aretacij) v več državah članicah, uničeni sta bili dve nezakoniti delavnici za proizvodnjo naprav in programske opreme za upravljanje prodajnih terminalov ter zaseženi nezakonita elektronska oprema, finančni podatki, ponarejene kartice in gotovina. Organizirana kriminalna združba je prizadela približno 36 000 bank / imetnikov kreditnih kartic iz 16 evropskih držav.
- tretja operacija je bila usmerjena na azijsko kriminalno mrežo, odgovorno za nezakonite transakcije in nakup letalskih vozovnic. Dva člana kriminalne združbe, ki sta potovala s ponarejenimi dokumenti, sta bila aretirana na letališču v Helsinkih. Približno 15 000 zlorabljenih številk kreditnih kartic so našli na zaseženih računalnikih. Mreža je uporabljala podatke iz kartic, ki so bile ukradene imetnikom po vsem svetu. V Evropi so imetniki kartic in banke utrpeli več kot 70 000 evrov izgub.
- letalske operacije proti goljufom uporablja goljufive kreditne kartice za nakup letalske vozovnice je usklajeval Evropski center za boj proti kibernetski kriminaliteti na 38 letališčih iz 16 evropskih držav. Med operacijo so letalske družbe poročale o več kot 200 sumljivih transakcijah, 43 oseb je bilo prijetih (po operaciji pa še nadaljnjih 74 oseb, tj. skupaj 177 prijetih oseb). Za vse je bilo ugotovljeno, da so povezane z drugimi kriminalnimi dejavnostmi, kot so distribucija podatkov o kreditnih karticah prek interneta, vdor v zbirke podatkov finančnih institucij, druge sumljive transakcije, promet s prepovedanimi drogami, tihotapljenju ljudi, ponarejevanje dokumentov, vključno z osebnimi izkaznicami ter druge vrste goljufij. Nekatere priprte osebe so že iskali pravosodni organi z evropskimi nalogi za prijetje.

Prihodnje grožnje ter trendi v kibernetski kriminaliteti

Trenutno ima dostop do interneta okoli 2,5 milijarde ljudi po vsem svetu, po ocenah pa naj bi v naslednjih štirih letih dostop pridobilo še približno 1,5 milijarde ljudi. Vse več življenja bomo preživeli na spletu, kar prinaša velike prednosti, hkrati pa bomo tam tudi bolj izpostavljeni kaznivim dejanjem. Evropski center za boj proti kibernetski kriminaliteti v svojem prvem letnem poročilu obravnava prihodnje grožnje in trende v zvezi z kibernetsko kriminaliteto. Med drugim opozarja na naslednje:

Vse več storilcev kaznivih dejanj. Vse lažje je priti do sodelovanja z organiziranimi združbami na področju kibernetske kriminalitete. Že zdaj se je razvila celovita podzemna ekonomija, kjer trguje z vsemi vrstami kazenskih proizvodov in storitev, vključno s prepovedanimi drogami, orožjem, naročenimi uboji, ukradenimi podatki o plačilnih karticah in zlorabami otrok. Do vseh vrst kibernetskih kaznivih dejanj je mogoče priti tudi brez tehničnih znanj — zlorabljanja gesel, vdorov v računalniške sisteme, prilagojene zlonamerne programske opreme ali napadov DDoS-a.

Večje povpraševanje. Pričakuje se, da se bosta povpraševanje po storitvah kibernetske kriminalitete in njihova uporaba povečevala, kar bo še nadalje spodbudilo razvoj, testiranje in distribucijo zlonamerne programske opreme; gradnje in uporabe botnetov; kraje in trgovanja s podatki o plačilnih karticah ter storitev pranja denarja.

Večja izpopolnjenost. Pričakuje se razvoj bolj agresivnih in odpornih vrst zlonamerne programske opreme. To vključuje t.i. ransomware z bolj naprednim in kompleksnim šifriranjem podatkov; odpornejše botnete; ter zlonamerno programsko opremo spletnega bančništva in izjemno kompleksne trojanske konje, da bi se zaobšli zaščitni ukrepi finančnih institucij.

Še večja globalizacija. Zaradi hitre širitve internetne povezljivosti, bo naraščala kibernetska kriminaliteta v jugovzhodni Aziji, Afriki in Južni Ameriki.

Uporaba mobilnih naprav. Pričakuje se premik zlonamerne programske opreme na mobilne naprave, prek katerih naj bi potekala tudi njihova distribucija.

Pametnejša distribucija. V naslednjih letih se pričakujejo novi načini distribucije agresivnih in odpornih vrst zlonamerne programske opreme. Povečuje se tudi zaskrbljujoči trend ponujanja zlorabe otrok prek prenosov v živo („live streaming"), pri čemer policija ostaja brez dokazov, če prenosa ne prestreže.

Večja potreba po pranju denarja. Storilci kaznivih dejanj bodo iskali preproste načine izplačila in pranja denarja. Osredotočanje na veliko število državljanov ter mala in srednja podjetja, katere se ogoljufa za razmeroma majhne zneske, se bo verjetno nadaljevalo. Povečevala se bo tudi uporaba podatkov o plačilnih karticah za spletne nakupe. Prav tako se bo povečalo povpraševanje po e-valutah in drugih anonimnih plačilnih sistemih.

Osredotočanje na storitve v oblaku. Vdiranje v storitve v oblaku postaja za storilce kaznivih dejanj vedno bolj zanimivo. Pričakuje se, da si bodo storilci kaznivih dejanj vedno bolj prizadevali, da bi vdrli v tovrstne storitve z namenom vohunjenja, pridobivanja plačilnih podatkov in izsiljevanja.

Da bi Evropski center za boj proti kibernetski kriminaliteti lahko odgovoril na ta razvoj dogodkov in obravnaval kazniva dejanja, ki po svoji naravi ne poznajo meja ali pristojnosti, bo še naprej zagotavljal operativno podporo organom kazenskega pregona iz držav članic EU in sodelujočih partnerskih držav izven EU. Obenem bo še nadgradil svoje strokovno znanje in izkušnje pri usposabljanju in gradnji zmogljivosti, strateški analizi in digitalni forenzični podpori.

Koristne povezave

Poročilo Evropskega centra za boj proti kibernetski kriminaliteti iz leta 2014

Evropski center za boj proti kibernetski kriminaliteti v okviru Europola

Posebno poročilo Eurobarometra št. 404 o KIBERNETSKI VARNOSTI (november 2013).

Spletišče Cecilie Malmström

Spremljajte evropsko komisarko Cecilio Malmström na Twitterju

Spletišče GD za notranje zadeve

Spremljajte GD za notranje zadeve na Twitterju

Kontakti:
Michele Cercone (+32 22980963)
Tove Ernst (+32 22986764)