AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Raportimi i situatës mbi sulmet FLUBOT

25/06/2021

Autoriteti Kombëtar për Certifikim Eletronik dhe Sigurinë Kibernetike
Rruga. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Shqipëri 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

Indeksi

Hyrje

Ky raport ofron një azhurnim të patcheve përsa i përket sulmeve që po përhapen dhe zgjerohen shpejtë, të malware-s së Flubot Android në Evropë, që nga fillimi i vitit 2021. Raporti bazohet në burime të hapura (Open Sources) për incidentet e Flubot, siç raportohet në Shtete të ndryshme anëtare.

Çfarë është Flubot:

Malware-i Android i njohur si FluBot, po vazhdon të zgjerohet me shpejtësi në një numër në rritje të Vendet evropiane. FluBot vjedh fjalëkalimet dhe informacionin e hyrjes në llogaritë tuaja personale, detajet personale, dhe informacionin bankar. Informacioni përdoret për të bërë pagesa nga llogaritë e rrezikuara si dhe për vjedhjet e identitetit në internet. FluBot gjithashtu u dërgon mesazhe SMS viktimave të reja dhe përhapet vetë më tej. E gjithë kjo bëhet pa dijeninë e përdoruesve.

Gjeografia e synuar

Evropa

Sektorët e synuar

Sektori bankar, publiku i gjerë

Si funksionon

Nëse një viktimë joshet nga sulmuesi në fushatën me qëllim të keq, e gjithë pajisja e tyre Android bëhet e arritshme për mashtruesin. Kjo përfshin potencialin për të vjedhur numrat dhe aksesin e kartës së kreditit, kredencialet në llogaritë bankare në internet. Për të shmangur heqjen, sulmuesi zbaton mekanizmat për të ndaluar mbrojtjen e integruar të ofruar nga Android OS dhe ndalon shumë paketa sigurie të palëve të treta nga instalimi, një veprim që shumë përdorues do të bënin për të hequr softuerin me qëllim të keq.

Viktima së pari merr një mesazh që imiton një markë të njohur logjistike të dërgesave, të tilla si FedEx, DHL dhe Correos (në Spanjë), një njoftim i postës zanore të re (Zvicër) ose ndoshta disa njoftime te tjetra specifike për vendin e sulmuar. Thirrja për veprim e mesazhit është që përdoruesi të klikoje në një lidhje në mënyrë që të shkarkoje dhe instaloje një aplikacion që ka të njëjtën markë të njohur si SMS, por në të vërtetë është me qëllim të keq dhe e ka ne permbajtje malware-in FluBot.

Sapo të instalohen dhe të jepen Accessibility Service permissions, FluBot në thelb ka kontroll te plotë mbi telefonin e kompromentuar. Vendos veten si aplikacioni standard për SMS dhe jep grante vetë aksesi për të lexuar librin e telefonit, për të lexuar ose bllokuar njoftime dhe më shumë përmes Accessibility Service controls. Lista e kontakteve shkarkohet nga pajisja dhe u dërgohet serverëve nën kontrollin e një aktori të keq, duke u ofruar atyre informacion shtesë personal dhe duke u mundësuar atyre të lëshojnë më tej sulmet ndaj viktimave të tjera të mundshme. Mesazhet dhe njoftimet nga transportuesit e telekomit mund të jenë të përgjuara, faqet e shfletuesit mund të hapen dhe mbishkrimet për të kapur kredencialet mund të shfaqen. Një aplikacion i dëmshëm gjithashtu I heq të drejtën Google Play Protect për të shmangur zbulimin nga sistemi operativ i integruar. Gjithashtu, për shkak të lejeve të të dhënave, aktori i kërcënimit është në gjendje të bllokojë instalimin e shumë të palëve të treta antimalware.

Duke shmangur zbulimin e antivirusit pasi të instalohet, FluBot e bën veten të pazbulueshme duke modifikuar regjistrin. Gjithashtu bllokon hyrjen në Google Play Store në mënyrë që përdoruesi të mos jetë në gjendje të shkarkojë antivirus të ri. Kjo do të thotë që jo vetëm që është pothuajse e pamundur të mbroheni nga infektimi, madje sapo të kuptoni se pajisja juaj është infektuar, është shumë e vështirë të hiqet pa një rivendosje të plotë të fabrikës të telefonit.

Ashtu siç sugjeron emri, sapo brenda një Banker Trojan shpejt fillon mbledhjen e zbulimeve për të misioni përfundimtar - vjedhja e parave. Kur malware është instaluar në terminal, ai përdor emri i brendshëm i aplikacionit bankar / pagesa për të zbuluar momentin kur hapet. Tjetra ajo dërgon këtë informacion te serveri C&C, i cili më pas dërgon mbivendosjen e përputhshme që imiton identikisht faqen e hyrjes së aplikacioneve për të kapur detajet e hyrjes në llogari. Pasi të përfundojë kjo fazë, kriminelët mund të fillojnë të zbrazin fondet nga llogaria ose duke bërë blerje të dëmshme.

RAPORTI OSINT

Ekzistojnë disa variante të Flubot si *Android / Trojan.Bank.Acecard*, *Android / Trojan.BankBot*, ose *Android / Trojan.Spy.Agent*.

Vektori fillestar i sulmit është një mesazh me tekst me një link që shkarkon malware-in. Gjatë instalimit malware do të tregojë udhëzime mashtruese për t'u instaluar dhe për të marrë Accessibility Service permissions. Këto permissions, e lejojnë atë të marrë akses të mëtejshm të nevojshme për të kryer qëllimet e synuara. Këto aksese e lejojnë atë të:

- Dërgoje mesazhe te kontaktet tuaja

- Të veprojë si spiun dhe vjedh informacionin

Në varësi të variantit, Flubot gjithashtu mund të:

- Përgjojë mesazhet hyrëse
- Ndaloje njoftimet
- Hape faqet e internetit
- Çaktivizoje Google Play Protect
- Çinstaloje aplikacionet e tjera
- Kontaktoje një server të komandimit dhe kontrollit bazuar në një algoritëm gjenerues të domenit (DGA)

Figura 1 tregon një shembull të komandës dhe kontroll panelit të gjetur online, i cili shfaq aftësitë e ndryshme të malware-it:

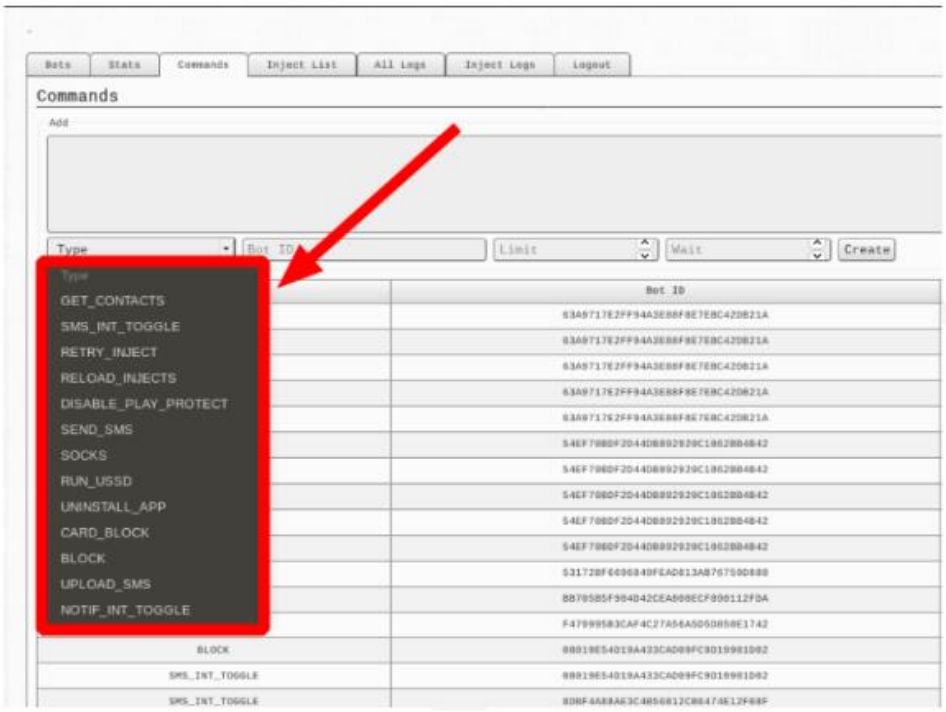
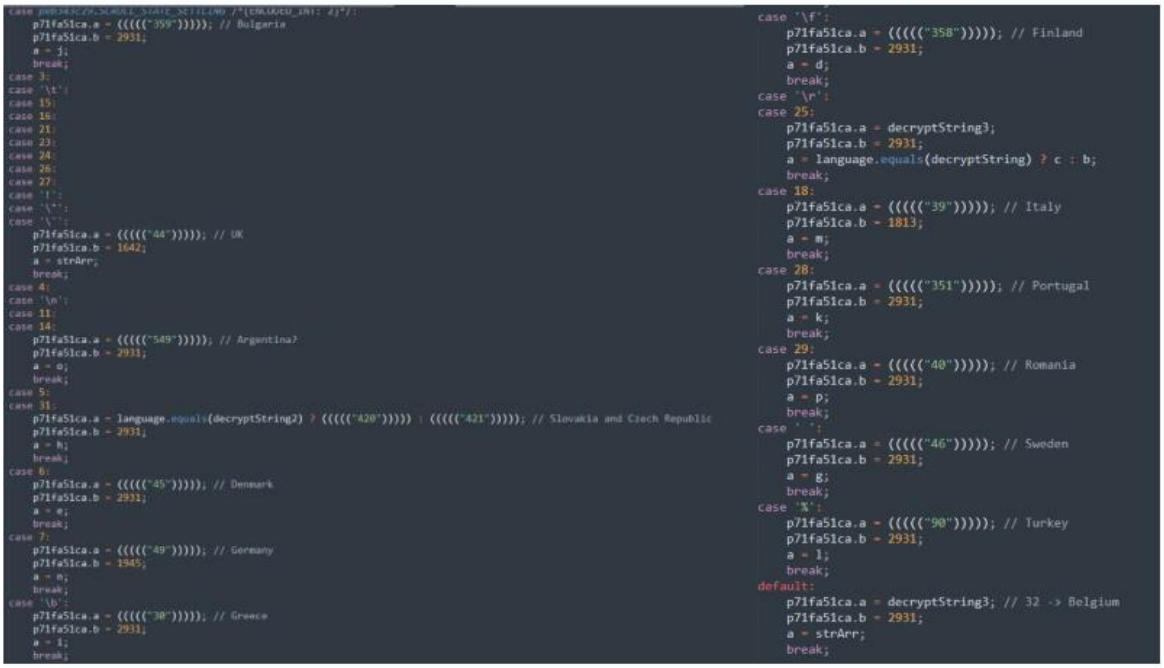


Figure 1: Example of a FluBot Command and Control interface[1]

1

Në vendet ku FluBot-i nuk është aktiv, ose në pajisje jo të suportuara, një viktimë që klikon në link çohet në një faqe me përmbajtje phishing në vend të shkarkimit të malwares. In ekstraktim të kodit më poshtë, një pjesë e mekanizmit të zbulimit të vendit tregohet në Figurën 2:

[1] https://raw.githubusercontent.com/prodaft/malware-ioc/master/FluBot/FluBot.pdf



```
    p71fa51ca.a = (((((("359")))))); // Bulgaria
    p71fa51ca.b = 2931;
    a = j;
    break;
case 3:
case '\t':
case 15:
case 16:
case 21:
case 23:
case 24:
case 26:
case 27:
case '!':
case '\"':
case '\'':
    p71fa51ca.a = (((((("44")))))); // UK
    p71fa51ca.b = 1642;
    a = strArr;
    break;
case 4:
case '\n':
case 11:
case 14:
    p71fa51ca.a = (((((("549")))))); // Argentina?
    p71fa51ca.b = 2931;
    a = o;
    break;
case 5:
case 31:
    p71fa51ca.a = language.equals(decryptString2) ? (((((("420"))))) : (((((("421"))))); // Slovakia and Czech Republic
    p71fa51ca.b = 2931;
    a = h;
    break;
case 6:
    p71fa51ca.a = (((((("45")))))); // Denmark
    p71fa51ca.b = 2931;
    a = e;
    break;
case 7:
    p71fa51ca.a = (((((("49")))))); // Germany
    p71fa51ca.b = 1945;
    a = n;
    break;
case '\b':
    p71fa51ca.a = (((((("30")))))); // Greece
    p71fa51ca.b = 2931;
    a = i;
    break;
case '\f':
    p71fa51ca.a = (((((("358")))))); // Finland
    p71fa51ca.b = 2931;
    a = d;
    break;
case '\r':
case 25:
    p71fa51ca.a = decryptString3;
    p71fa51ca.b = 2931;
    a = language.equals(decryptString) ? c : b;
    break;
case 18:
    p71fa51ca.a = (((((("39")))))); // Italy
    p71fa51ca.b = 1813;
    a = m;
    break;
case 28:
    p71fa51ca.a = (((((("351")))))); // Portugal
    p71fa51ca.b = 2931;
    a = k;
    break;
case 29:
    p71fa51ca.a = (((((("40")))))); // Romania
    p71fa51ca.b = 2931;
    a = p;
    break;
case ' ':
    p71fa51ca.a = (((((("46")))))); // Sweden
    p71fa51ca.b = 2931;
    a = g;
    break;
case '%':
    p71fa51ca.a = (((((("90")))))); // Turkey
    p71fa51ca.b = 2931;
    a = l;
    break;
default:
    p71fa51ca.a = decryptString3; // 32 -> Belgium
    p71fa51ca.b = 2931;
    a = strArr;
    break;
```

Figure 2: Code fragment with country detection[2]

2

Lista tregon plane të mundshme të zgjerimit nga aktorët e kërcënimit.

Rekomandime për masat që duhen marrë dhe këshilla

Përdoruesit e përparuar mund të ndjekin udhëzimet për heqjen e malwares:

- https://www.youtube.com/watch?v=dIIDh1AqUKQ&ab_channel=AndroidInfosec

Shumica e përdoruesve do të duhet të bëjnë një factory reset, e cila pastron të gjitha aplikacionet dhe informacionin në telefon.
Udhëzimet e factory reset-it: https://support.google.com/android/answer/6088915?hl=en

Nëse merrni një mesazh SMS të panjohur ose të papritur me një link të klikueshëm, përmbahuni nga klikimi i linkut dhe në vend të kësaj fshini mesazhin. Në skenarin më të keq, kur malware është instaluar në një pajisje duke bërë veprimtari bankare ose tjetër aktivitet që ka ndodhur që nga momenti i instalimit, atëherë kontaktoni menjëherë organizatat në fjalë për të bllokuar

[2] https://twitter.com/alberto__segura/status/1404098461440659459/

aksesin dhe kur është e nevojshmë të ndryshoni fjalëkalimet, duke mos harruat t'i bëni ato unike dhe të forta.

KUJDES !!!

Sulmet Flubot pritet të rriten në përmasa dhe shkallë në zonën e BE, duke u zgjeruar në vendet e tjera nga ato që janë vërejtur tashmë.

Referenca:

[2] https://twitter.com/alberto__segura/status/1404098461440659459/
[3] https://youtu.be/dIlDh1AqUKQ
[4] https://github.com/prodaft/malware-ioc/tree/master/FluBot

1. https://www.virustotal.com/gui/file/ab9c2ff18bf62e816b96003be65cc7cc1c439988f4803046ec7fa109de681e19/relations
2. https://blogs.protegerse.com/2021/01/18/delincuentes-siguen-suplantando-a-correos-para-propagar-amenazas/
3. https://raw.githubusercontent.com/prodaft/malware-ioc/master/FluBot/FluBot.pdf