mnemonic

KONFIDENSIELL

TRUSSELRAPPORT

TRUSSELVURDERING AV NY LØSNING FOR DIGITAL SMITTESPORING BASERT PÅ GAEN

Folkehelseinstituttet (FHI)

Sted	OSLO
Dato	04.11.2020
Versjon	1.0

Sammendrag

mnemonic mottok 29. oktober en forespørsel fra FHI om å gjøre en trusselvurdering av «trusler eller angrep mot andre nasjoners smittesporingsapper, da med et spesielt fokus på smittesporingsappene i Danmark og Irland»

Oppdraget ble gitt en ramme på 12 timers arbeide som skulle resultere i en skriftlig rapport overlevert til FHI innen 4. november 2020.

Oppdraget ble akseptert og arbeidet med trusselvurdering startet opp dagen etter.

Denne rapporten er resultatet av arbeidet og viser konklusjon, arbeidsmetodikk og datagrunnlag.

Innholdsfortegnelse

1 Konklusjon

Vi har ikke funnet bevis for angrep mot nasjonale smittesporingsapper og vi konkluderer derfor med at det er lite sannsynlig at det har vært vellykkede angrep. Det er ikke vanlig å finne dokumentasjon av angrep som ikke har vært vellykket, vi kan derfor ikke konkludere på om det har vært angrep som ikke har vært vellykket.

Spesifikt for smittesporingsappene til Danmark og Irland finner vi ingen indikasjon på at disse har blitt utsatt for noe angrep.

Vi finner bevis for at kriminelle aktører utnytter tematikk rundt smittesporingsapper til phishing og spredning av skadevare. Når myndigheter informerer befolkningen om smittesporingsapper er det sannsynlig at kriminelle vil benytte anledningen til å sende ut falsk informasjon med tema fra det offisielle budskapet for å spre phishing og skadevare.

2 Bakgrunn

FHI ba om bistand fra mnemonic for å innhente informasjon vedrørende historiske og nåværende trusler eller angrep mot andre nasjoners smittesporingsapper. FHI ba om spesielt fokus på smittesporingsappene i Danmark og Irland, da det er disse som likner mest på den norske versjonen som er under utvikling.

Smittesporingsappene i Danmark og Irland er begge basert på "Google Apple Exposure Notification" (GAEN), dette gjelder også den nye norske appen under utvikling. Det vil derfor være mest relevant å se på aktuelle trusler og angrep på apper som benytter GAEN grensesnittet.

Med angrep på smittesporingsapper menes her utnyttelse av apper på mobiler, sentral infrastruktur for disse apper og tilhørende data. Omdømme, økonomi, offenliggjøring av sårbarheter og andre faktorer som også kan omtales som et angrep er ikke vurdert.

3 Metodikk

For å besvare spørsmålet fra FHI om trusler og angrep mot smittesporings-applikasjoner har vi benyttet en standard metodikk som er delt opp i følgende faser:

1. Planlegging og definering av omfang
2. Definere søkekriterier og kilder som skal dekkes i datainnsamling
3. Datainnsamling
4. Analyse og rapportering

To analytikere har jobbet i tandem med datainnsamling, analyse og konklusjon.

4 Scenarier og analyse av data

Følgende trussel og angreps-scenarier er identifisert og brukt som grunnlag for analysen:

4.1 Falsk app som utgir seg for å være den offisielle smittesporingsappen

Kriminelle trusselaktører vil være i stand til å utvikle falske apper som utgir seg for å være den offisielle smittesporingsappen.

Motivasjonen er økonomisk profitt ved at trusselaktøren kan tilegne seg informasjon som kan benyttes til utpressing, eller omsettes ved salg.

I våre kildesøk har vi funnet eksempler på at dette scenariet har forekommet. I juni 2020 meldte sikkerhetsselskapet ESET om at de hadde oppdaget, analysert og varslet canadiske myndigheter om en falsk smittesporingsapp som utga seg for å være den offisielle canadiske smittesporingsappen "Covid Alert" som fortsatt var under utvikling. Den falske appen infiserte android telefoner med "CryCryptor" løsepengevirus.

Vi anser det som lite sannsynelig at den norske smittesporingsappen vil kunne utnyttes av kriminelle trusselaktører til dette formålet.

4.2 Phishing epost eller phishing SMS som utnytter seg av tillit til smittesporingsappen

Kriminelle trusselaktører vil kunne utnytte tilliten til smittesporingsappen ved å sende ut phishing eposter eller phishing SMS som utgir seg for å stamme fra smittesporingsappen.

Motivasjonen er økonomisk profitt ved at trusselaktøren kan tilegne seg informasjon som kan benyttes til utpressing, eller omsettes ved salg.

I våre kildesøk er det flere eksempler på at trusselaktører benytter seg av tillit til smittesporingsapper, offisiell kommunikasjon om Covid-19 og generelt tillit til myndigheter som "agn" i phishing-kampanjer.

Vi anser det som sannsynlig at den norske smittesporingsappen vil kunne utnyttes av kriminelle trusselaktører til dette formålet.

4.3 Målrettet falsk informasjon som utnytter seg av tillit til smittesporingsappen

Hacktivister eller avanserte statlige trusselaktører vil kunne utnytte tilliten til smittesporingsappen ved å spre falsk informasjon via epost, sosiale media eller SMS som utgir seg for å stamme fra smittesporingsappen.

Motivasjonen vil være å spre falsk informasjon som ledd i en påvirkningskampanje som kan ha som mål å skape usikkerhet og svekke tillitsgrunnlaget for demokratiske prosesser. Fokus 2020 peker på den russiske etterretningstjenesten som en trusselaktør som i særlig grad utnytter det digitale domenet for sine påvirkningsoperasjoner, som i større grad enn før er tilpasset publikum i ulike land. Falske profiler og automatiserte kontoer (såkalte "bot"er) på sosiale medier vil typisk utnytte polariserende temaer for å spre desinformasjon. Personvern og smittesporingsappen har vist seg å være et kontroversielt tema, og falsk informasjon om datalekkasjer fra appen kan muligens misbrukes i en påvirkningsoperasjon.

Vi har ikke funnet noen eksempler på at dette har forekommet i vårt begrensede kildesøk.

Vi anser det som lite sannsynelig at den norske smittesporingsappen vil kunne utnyttes til dette formålet, men sannsynligheten vil kunne øke avhengig av den politiske situasjonen.

4.4 Offentliggjøring av sårbarheter i smittesporingsappen

Hacktivister kan offentliggjøre informasjon om sårbarheter i smittesporingsappen med formål om å skade appens og/eller myndighetenes omdømme. Sikkerhetsforskere vil også kunne finne sårbarheter i smittesporingsappen, men skiller seg fra hacktivister ved at de vil ha en intensjon om å varsle om sårbarheter til appens utviklere slik at sårbarhetene kan fikses innen offentliggjøring. Hvis det ikke legges til rette for at sikkerhetsforskere enkelt kan ta kontakt for å varsle om sårbarheter (såkalt "coordinated vulnerability disclosure"), eller kommunikasjon og samarbeid med sikkerhetsforskeren ikke fungerer, kan også sikkerhetsforskere offentliggjøre sårbarheter som skader myndighetenes omdømme.

I våre kildesøk har vi funnet flere eksempler på at dette har forekommet.

Vår vurdering er at det er like sannsynlig som usannsynlig at dette vil ramme den norske smittesporingsappen, gitt at det var stor interesse rundt sårbarheter i den tidligere versjonen av den norske smittesporingsappen.

4.5 Målrettet falsk informasjon som spres via utnytting av sårbarheter i smittesporingsappen

Hacktivister eller avanserte statlige aktører vil kunne utnytte potensielle sårbarheter i smittesporingsappen for å spre falsk informasjon. Dette kan for eksempel være i form av falske meldinger som ber personer gå i karantene. Motivasjonen vil være å skape usikkerhet rundt appen, eller rundt demokratiske prosesser. Et eksempel kan være å få bestemte grupper av personer til å holde seg hjemme på en valgdag, eller mer målrettet begrense bevegelsesfriheten til personer med viktige stillinger.

Vi har ikke funnet noen eksempler på at dette har forekommet i vårt begrensede kildesøk.

Vår vurdering er at det er lite sannsynlig at dette vil forekomme i dagens trussellandskap, men sannsynligheten vil kunne øke avhengig av den politiske situasjonen.

4.6 Tilgang til sensitiv data via utnyttelse av sårbarheter i smittesporingsappen

Kriminelle, hacktivister eller avanserte statlige aktører vil kunne utnytte seg av sårbarheter i smittesporingsappen for å få tilgang til sensitiv data, som for eksempel bevegelsesmønstre eller persondata. Motivasjonen vil være økonomisk profitt ved utpressing eller salg av data, overvåkning av personer, eller tilgang til informasjon om smittespredning.

Appens desentraliserte arkitektur basert på GAEN betyr at innsamling av sensitiv data begrenses, noe som også begrenser denne trusselen. Det har imidlertid vært rapportert om sårbarheter i andre apper basert på GAEN (såkalt "little thumb attack" demonstrert i en video) som utnytter svakheter i synkroniseringen av rullerende identifikatorer, som muliggjør sporing av personer med appen innen Bluetooth rekkevidde. Denne sårbarheten er demonstrert i smittesporingsappene i Sveits, Østerrike, Italia og Tyskland.

Informasjon om datalekkasjer fra den nederlandske smittesporingsappen ble offentliggjort i et nyhetsoppslag i Security Affairs i april 2020. Det var en tidlig versjon av appen (ikke basert på GAEN) som ble analysert av sikkerhetsforskere der det viste seg at en kobling til en database med personopplysninger hadde blitt lagt inn ved en feiltagelse. Trusseletteretningsleverandøren FireEye verifiserer denne nyhetsartikkelen med sin "Media-on-target" klassifisering, noe som betyr at kilden har høy troverdighet.

Vår vurdering er at det er lite sannsynelig at et Bluetooth-basert angrep som knytter persondata til bevegelsesmønstre vil ramme den norske smittesporingsappen, siden gjennomføringen vil kreve betydelige ressurser og kapasiteter hos trusselaktør.

Appendix A: Kilder

A.1 Åpne kilder

Publiseringsdato	Tittel	Referanse eller lenke
Apr 03, 2020	Malicious Android Apps Exploit Coronavirus Panic	OSINT (*1)
Jun 10, 2020	Anomali Threat Research Identifies Fake COVID-19 Contact Tracing Apps Used to Download Malware that Monitors Devices, Steals Personal Data	OSINT (*2)
Jun 24, 2020	New ransomware posing as COVID-19 tracing app targets Canada; ESET offers decryptor	OSINT (*3)
Jul 20, 2020	A Survey of COVID-19 Contact Tracing Apps	OSINT (*4)
Sep 3, 2020	COVID-TRACING FRAMEWORK PRIVACY BUSTED BY BLUETOOTH	OSINT (*5)
Sep 4, 2020	Why Your Apple/Google Covid-19 Contact Tracing App Has An Awkward New Problem	OSINT (*6)
Sep 26, 2020	SECURITY ANALYSIS OF THE COVID-19 CONTACT TRACING SPECIFICATIONS BY APPLE INC. AND GOOGLE INC.	OSINT (*7)
Oct 19, 2020	Covid contact-tracing app not sharing data with police	OSINT (*8)

*1 https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/android-apps-coronavirus-covid19-malicious
*2 https://www.anomali.com/blog/anomali-threat-research-identifies-fake-covid-19-contact-tracing-apps-used-to-monitor-devices-steal-personal-data
*3 https://www.welivesecurity.com/2020/06/24/new-ransomware-uses-covid19-tracing-guise-target-canada-eset-decryptor/
*4 https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9144194
*5 https://hackaday.com/2020/09/03/covid-tracing-framework-privacy-busted-by-bluetooth/
*6 https://www.forbes.com/sites/zakdoffman/2020/09/04/apple-iphone-google-android-contact-tracing-app-upgrade-release-phone-tracking-warning/
*7 https://eprint.iacr.org/2020/428.pdf
*8 https://www.bbc.com/news/technology-54599320

A.2 Lukkede kilder

Publiseringsdato	Tittel	Referanse eller lenke
Apr 20, 2020	Proposed Government Coronavirus Contact Tracing App Leaked Data	FireEye News Analysis – Media on-target ref 20-00007123 9 sider
Mai 19, 2020	Governments Increasingly Reliant Upon Mobile Apps to Monitor and Contain COVID-19 Infections	FireEye TI – Strategic ref 20-00009002 2 sider
Jun 24, 2020	New Ransomware Masquerades as COVID-19 Contact-Tracing App on Your Android Device	FireEye News Analysis – Plausible ref 20-00011901 2 sider
Jul 09, 2020	Monthly Report on Cyber Crime Threats to the Financial Sector – June 2020	FireEye TI – Fusion ref 20-00012595 18 sider
Jul 16, 2020	Coronavirus Impact on Cyber Threat Landscape Remains Limited	FireEye TI – Strategic ref 20-00014235 12 sider
Aug 14, 2020	Iranian Actors Using Newly Identified SHIPTHIEF and BOSSRAT Likely Targeting Shipping- and Satellite-Tracking Services and Impersonating Australian COVID-19 Application	FireEye IT – Susion ref 20-00015153 10 sider
Sep 09, 2020	Overview: Mobile Malware Trends and Developments Between January and August 2020	FireEye TI – Susion ref 20-00016803 16 sider
Sep 09, 2020	COVID-19 Increases Cyber Threats to Healthcare, Pharmaceuticals	FireEye – Strategic ref 20-00018225 9 sider
Oct 23, 2020	Coronavirus-Themed Phishing Continues Gradual Decline as of October 2020	FireEye TI – Strategic ref 20-00021765 10 sider