FAGOMRÅDER

- Digital sikkerhet
  - Nasjonalt cybersikkerhetssenter
    - Varsler fra NCSC
    - Håndtering av dataangrep
    - Tekniske sikkerhetstjenester
    - Råd og anbefalinger
    - Kontakt NCSC
    - NCSC Cyberforum 2020
  - Råd og anbefalinger innenfor digital sikkerhet
  - Kryptosikkerhet
  - Kommunikasjonssikkerhet
  - Informasjonssystemsikkerhet
  - IT-sikkerhet
- Personellsikkerhet
- Fysisk sikkerhet
- Sikkerhetsstyring

Varsel om løsepengevirus

Publisert: 10.01.2021

NSM NCSC, DSB og Kommune-CSIRT er kjent med et pågående angrep knyttet til løsepengevirus mot en kommune og har utarbeidet dette varselet i fellesskap.

Merk at følgende kun beskriver kjente handlinger og verktøy, det kan ikke utelukkes at en angriper benytter andre verktøy. Man bør derfor undersøke bredt dersom man mistenker at man kan være truffet.

Det aktuelle løsepengeviruset er kjent som "Mespinoza/Pysa" og man er kjent med lignende angrep mot lokale myndigheter i Frankrike[1] og andre hendelser[2].

Fra disse og andre kjente hendelser vet man at aktøren bak angrepet vil forsøke å komme seg inn i nettverket gjennom blant annet "brute force"-angrep mot internetteksponerte tjenester og brukere. For eksempel vil angriper forsøke å koble seg til fjernaksessløsningen RDP dersom dette er tilgjengelig.

Dersom angriper kommer seg inn i nettverket har man observert at de vil forsøke å bevege seg mellom maskiner ved hjelp av RDP eller andre metoder for å bevege seg lateralt. Man har observert bruk av verktøyet "Mimikatz" for å hente ut passord og man vet at angriperen vil forsøke å dumpe passorddatabaser for å kunne få tilgang til flere brukere.

Angriper tar seg tid til å kartlegge nettverket de har fått tilgang til og man har sett at angriper har utført flere av følgende handlinger:

* Skrudd av antivirusløsninger. For eksempel har angriper skrudd av Microsoft Defender igjennom lokale gruppe policyer.
* Unntak for alle filer som har filendelsen ".exe" har blitt opprettet i Microsoft Defender
* Slette backup og skyggekopier av systemet
* Hente ut detaljer om nettverk, brukere, databaser og backup
* Bruk av flere PowerShell skripts for å kartlegge og automatisere
* Bevege seg lateralt ved hjelp av "PsExec"

Avhengig av hvor lett angriper oppnår tilgang til en administratorbruker, vet man at angriperen kan bruke alt fra timer til dager før man aktiverer løsepengeviruset.

I etterkant av kartlegging, infeksjon og handlinger utført av angriper ser man at angriper starter løsepengeviruset for å kryptere filene. Filene får en ny filendelse som slutter på ".pysa", i tillegg vil man få opp en beskjed om hvordan man skal kontakte angriper for å få dekryptert filene sine. Som regel vil angriper oppgi en tilfeldig generert e-post hos ProtonMail, for eksempel "[tilfeldig tekst]@protonmail.com".

Hva kan man se etter?

* Mistenkelig trafikk inn og ut av nettverket til TOR-nettverket
* Mistenkelige RDP tilkoblinger fra internett mot egen infrastruktur
* Påloggingsforsøk gjennom "brute force"-angrep
* Mistenkelige påloggинger
* Deaktivering av antivirus
* Bruk av verktøy som "PsExec" og "procdump"

Anbefalinger og tiltak:

* Ha oversikt over hvilke tjenester som er internetteksponert, deriblant åpne RDP tjenester og andre fjernaksessløsninger
* Benytt tofaktorautentisering der mulig
* Ha gode gjenopprettelsesrutiner og om mulig ha egen backup offline.
* Overvåk aktivitet på administrator kontoer
* Vurder blokkering av trafikk mot TOR-nettverket dersom dette ikke er strengt nødvendig
* Vurder geofiltrering/-blokkering av trafikk fra land man normalt ikke har trafikk til/fra
* Ha kontroll over og overvåkning av trafikk mellom sikkerhetssoner
* Ha tilstrekkelig logging av tjenester man benytter og bevar disse loggene i tilstrekkelig tid, gjerne lenger enn tre måneder.

Ut over de anbefalingene gitt over vil følgende generelle tiltak kunne virke forebyggende:

1. Installer sikkerhetsoppdateringer så fort som mulig
2. Ikke tildel sluttbrukere administratorrettigheter
3. Blokker kjøring av ikke-autorisert programvare
4. Oppgrader program- og maskinvare

Dersom man er offer for løsepengevirus anbefales det å ikke betale angriper for å gjenopprette filene da dette vil være med på å finansiere kriminell aktivitet.

I tillegg anbefales det at man anmelder forholdet til lokalt Politi.

Se forøvrig følgende for ytterligere råd og generelle tiltak [3] [4] [5].

[1]:https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-003/__;!!Nq5e9Ls!z4kBQ9WxqLbVGAeOiFrvxsVznBsh8omBUyr4uXQ41P1XeX18Vu0U0Zo6R-a83kh0mWOkaQ$

[2]:https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/__;!!Nq5e9Ls!z4kBQ9WxqLbVGAeOiFrvxsVznBsh8omBUyr4uXQ41P1XeX18Vu0U0Zo6R-a83kgP6jxRDgS

[3]: https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/fire-effektive-tiltak-mot-dataangrep

[4]: https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/losepengevirus

[5]: https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt

Del på:

Finner du det du leter etter?

JA NEI