Forfatter: Snorre Ledal

Emnekode: TK2100

Emnenavn: Informasjonssikkerhet

Innleveringsdato: 7. april 2022

Arbeidskrav



Høyskolen Kristiania

Semester Vår 2022

Denne besvarelsen er gjennomført som en del av utdannelsen ved Høyskolen Kristiania. Høyskolen er ikke ansvarlig for oppgavens metoder, resultater, konklusjoner eller anbefalinger.

StuxNet

Et virus som har tjent sitt navn med å være første i sitt slag og med sine presentasjoner den har gjort. Den skapte stor internasjonal oppmerksomhet kort tid etter sitt funn og gjorde større fysiske skader fra det mange tenkte var en isolert verden, datamaskiner. Trolig det største med Stuxnet var bruker av 4 forskjellige zero day exploits[[1]](#footnote-1). Dette var første av sitt slag og tyder på at de som laget denne skadevaren la alle sine egg oppi en kurv for full effekt.

Den 17. juni 2010 fikk sikkerhetsfirma VirusBlokAda fra Hviterussland en epost om at serverne til en av kundene har problemer, det mistenkes at et virus stod bak dette. VirusBlokAda sendte ned konsulent Sergey Ulasen ned for videre utbedring av problemet som har oppstått. Omtrent en uke etter Sergey hadde ankommet de fysiske serverne, ble det konkludert at serverne er infisert med et ukjent virus. Det som var overraskende, var at det ble funnet flere .SYS filer som var signert med Realtek sine private sertifikat[[2]](#footnote-2).

For å gi mer innhold til hva denne trusselen hadde klart å infiltrere, må vi skjønne hva som har blitt påvirket. Vi snakker om SCADA PLC (Supervisory control and data acquisition[[3]](#footnote-3) og programmable logic controller[[4]](#footnote-4)) i korte trekk er dette datamaskiner laget for å drifte og styre meget store industrielle bygg og anlegg[[5]](#footnote-5). Disse spesialiserte maskinene som har blitt påvirket av Stuxnet, er ansvarlig å drift atomreaktorer i Iran! Heldigvis var ikke målet å få en reaktor til å bryte ned å eksplodere, men i dette tilfelle å hindre berikelse av uranium igjennom sentrifuger. Hvordan klarte Stuxnet dette? med å benytte rootkit for å skjule seg selv og vise feile tall til operatøren, men i virkeligheten drev rotoren til sentrifugen og senket og øket hastigheten så hyppig at det brøt ned rotoren[[6]](#footnote-6).

Fra hva man klarte å hente så var SCADA maskinene infisert med dette siden juni 2009 og resultatet har vært at ca. 1000 sentrifuger fra november 2009 til juni 2010 blitt rapportert ødelagt fra Institute of Science and International Security[[7]](#footnote-7). Fra disse tallene kan man hente ut at måle var å hindre utvikling av potent uranium, øke kosten av dette prosjektet for pårørte landet og siste fjerne tiltro til forskerne som jobbet med dette.

Tilbake til hvordan Stuxnet klarte denne jobben, så nevnte jeg at det benyttet zero day exploits. Trolig den viktigste er en feil med Windows .LNK filer (Snarvei-filer). I korte trekk så kommer feilen når Windows prøver å laste inn ikonet for USB-pinnen som er stikket inn[[8]](#footnote-8). Som Bengt Østby skrev   
«På grunn av at Windows Shell, for en spesifikk – ikke dokumentert, Item ID brukte LoadLibrary og ikke LoadLibraryEx ble kode i DLLen kjørt»[[9]](#footnote-9). Dette skaper muligheten for Stuxnet å kjøre ikke administrert kode bare ved å sette inn USB-pinnen i en maskin. Fra dette punktet var målet for skadevaren å jobbe seg innover i det lokale nettverket med bruk av sårbarheter med RPC og Print Spooler[[10]](#footnote-10). Etter et par hopp ville skadevaren stoppe seg selv å spre videre for å ikke gå ut av kontroll. Som nevnt tidligere, når Stuxnet fant ønsket maskin med riktige kriterier så slo det seg til rette for å begynne sitt ondsinnede formål.

15. juli 2010 ble det offentlig gjort en blogg for første gang om StuxNet, skrevet av Brian Krebs. Raskt fulgt opp blir nettsiden som har denne bloggen et offer for Denial-of-service attack samt flere epostlister spammet ned for å hindre informasjonene å nå ut til forskere og drifts administrasjon til SCADA-nettverk[[11]](#footnote-11). Kommende dager blir raskt hetet opp når Microsoft offentlig kommer ut med at denne .LNK feilen er «as designed» og ikke vill bli fikset. Samt som denne uttalelsen kommer har skadevare forfattere offentliggjort hvordan man kan implementere denne feilen inn i nye koder.  
For å gi innhold til panikken som står nå, så er denne .LNK utnyttelsen mulig på alle Windows-typer etter win98 fram til nyeste versjon av Windows. Dette er på grund av at kjernekoden er like på alle OS-variantene fra win98. Heldigvis så trekker Microsoft tilbake på ordet tidligere og lanserer en oppdatering til Windows som fjerner denne utnyttelsen den 02. august 2020[[12]](#footnote-12).

Fra dette punktet her begynner ting å bli uklart. Siden det er mange kilder som har sine oppfatninger pluss at mye av dette er mest sannsynlig kontrollert lekket informasjon fra statlige organisasjoner fra USA. De som står bak dette er faktisk NSA, CIA (USA) og Israelsk etterretning i det kalles Operation Olympic Games. Denne operasjonen har blitt godkjent av Bush administrasjonen tilbake i 2006 og hadde som intensjon å stoppe Iran med å anrike uranium, trolig for bruk av atom våpen[[13]](#footnote-13).

Det som ikke er nevnt tidligere at dette skadevaren har sprett seg til mange flere maskiner enn kun SCADA-maskinene i Iran. Stuxnet har klart å spre seg til trolig 12 000 maskiner[[14]](#footnote-14) og til flere land som; Indonesia, India, Eqador, Pakistan, Libanon, Taiwan og Azerbaijan[[15]](#footnote-15). Fra hva offentlige kilder har å si om dette så var det en «feil» med viruset som gjorde at det spredde mer enn det skulle. Fra kilden jeg jobber med så vil det tyde på at intensjonen trolig var større og mer utbredt enn det som blir offentlig uttalt. Hele tre forskjellige institusjoner i Iran har blitt utsatt for StuxNet, men fra uttalelser fra USA var målet kun anlegget Natanz målet[[16]](#footnote-16).

Så i skyggen til alt dette ble sikkerhet for SACADA miljøet en mye større prioritering for nyere løsninger, USA sin sikkerhets policy blir endret til å ta til rette cyberangrep som en trussel til nasjonale interesser og kan bli returnere med «kinetisk angrep», pent sakt for at USA kan angripe tilbake med bomber[[17]](#footnote-17).

Skrekkscenario

I mitt eget personlige skrekkscenario som involvere fysiske resultater av skadevare så er trolig hacking av GPS utstyr av typen satellitter. Her skal det sies at jeg ikke har kjennskap til hvordan programvare eller sikkerhetstiltaket det er gjort for å hindre uønsket kontakt med en satellitt.

Man har flere Global Navigation Satellite Systems (GNSS) som er det tekniske fagbegrepet. Vi har totalt seks systemer, GPS av USA. BeiDou av China, Galileo av Europa, Glonass av Russland, NavIC av India og QZSS fra Japan[[18]](#footnote-18). Uten direkte kilder å støtte meg på har jeg av oppfatning at GPS av USA er den mest benyttede GNSS systemet som er i bruk. Uavhengig om dette er sant så vill mitt skrekkscenario føre til globale forstyrrelser på alle nivåer.

I et slikt system så er det fire viktige ledd for at GNSS system skal funke. Vi har den tydeligste komponenten, selve satellitten. Monitorstasjon, Stasjon for satellittoppdatering og kontrollstasjon[[19]](#footnote-19). Ut av alle disse leddene så er det minst av kontrollstasjon og trolig der man får mest utnytte av å snike inn skadevare for å hemme eller ødelegge et slikt system.

Sannsynligheten for hva tror kommer å skje er så liten pga. effekten det vill påføre eget land at resultatet ikke ville være vært det på økonomisk plan. Eneste tilfelle jeg kan se for meg dette er i sammenheng med gjensidig selvdestruksjon situasjon. Hvis et land klarer å ødelegge et GNSS system igjennom skadevare for en slik stasjon før et militært angrep så vil en side ha betrakting større fordel på alle planer. Skipsfart som står for majoriteten av all internasjonal handel vill senkes kraftig og økonomisk vekst er ute av bordet. Lite har det å si hvis en nasjon allerede ønsker å gå ut i full krig.

Skal vi se på tallene er det 53.2% stedsbaserte tjenester og 38% veitrafikk som benytter GNSS tjenester mest[[20]](#footnote-20). Så man kan fort se at innlands infrastruktur som lastebiler senke effektiviteten meget og mobile enheter som telefoner og andre mindre gjenstander miste mye funksjonalitet. Verden vill trolig på kort tid ha fullt kaos og med tydelige eksempler fra Covid-epidemien i 2020 hvor toalett papir var trolig det mest etterspurte varen pga. folk panikk kjøpte av redsel av å gå tom[[21]](#footnote-21).

Om det blir en økonomisk avslutning av samfunnet eller en voldelig en med krig. Så vill alle lide en form eller annet hvis et av de større og mest brukte GNSS systemene går ned. Hvis nasjoner klare å infiltrere atomkraftverk som mulig kan gi deg atomvåpen eksplosjoner, så tror jeg også at de kan klare å infiltrere kontrollstasjoner for GNSS nettverk hvis de virkelig ville gå fult ut.

Referanser

Forssell, Børje, og Norvald Kjerstad. «GPS». I *Store norske leksikon*, 30. november 2021. http://snl.no/GPS.

«GPS.gov: Other Global Navigation Satellite Systems (GNSS)». Åpnet 23. februar 2022. https://www.gps.gov/systems/gnss/.

Mao, Frances. «Coronavirus Panic: Why Are People Stockpiling Toilet Paper?» *BBC News*, 4. mars 2020, pargr. Australia. https://www.bbc.com/news/world-australia-51731422.

«Programmable Logic Controller». I *Wikipedia*, 13. februar 2022. https://en.wikipedia.org/w/index.php?title=Programmable\_logic\_controller&oldid=1071602524.

«SCADA». I *Wikipedia*, 19. januar 2022. https://en.wikipedia.org/w/index.php?title=SCADA&oldid=1066724217.

Østby, Bengt. «TK2100\_04\_Kinetisk.pdf», u.å.

1. Østby, «TK2100\_04\_Kinetisk.pdf», Side 19. [↑](#footnote-ref-1)
2. Østby, Side 15. [↑](#footnote-ref-2)
3. «SCADA», l. 1. [↑](#footnote-ref-3)
4. «Programmable Logic Controller», l. 1. [↑](#footnote-ref-4)
5. Østby, «TK2100\_04\_Kinetisk.pdf», Side 20. [↑](#footnote-ref-5)
6. Østby, Side 21. [↑](#footnote-ref-6)
7. Østby, Side 38. [↑](#footnote-ref-7)
8. Østby, Side 23. [↑](#footnote-ref-8)
9. Østby, Side 36. [↑](#footnote-ref-9)
10. Østby, Side 19. [↑](#footnote-ref-10)
11. Østby, Side 17. [↑](#footnote-ref-11)
12. Østby, Side 18. [↑](#footnote-ref-12)
13. Østby, Side 39. [↑](#footnote-ref-13)
14. Østby, Side 42. [↑](#footnote-ref-14)
15. Østby, Side 22. [↑](#footnote-ref-15)
16. Østby, Side 43. [↑](#footnote-ref-16)
17. Østby, Side 37. [↑](#footnote-ref-17)
18. «GPS.gov: Other Global Navigation Satellite Systems (GNSS)». [↑](#footnote-ref-18)
19. Forssell og Kjerstad, «GPS». [↑](#footnote-ref-19)
20. Forssell og Kjerstad, fig. 3. [↑](#footnote-ref-20)
21. Mao, «Coronavirus Panic». [↑](#footnote-ref-21)