Stuxnet

Carsten Grønbjerg Lützen (140488)
Oliver Finn Madsen (250685)

25. April, 2012

DM830
Netværkssikkerhed

IMADA
Syddansk Universitet

Contents

1 Introduktion

Stuxnet er en meget avanceret orm med det specifikke mål at inficere og sabotere specifikke enheder ofte benyttet i større anlæg som eksempelvis atomkraftværker. Ligesom andre orme er det et selvstændigt program som kopierer sig selv for at inficere andre maskiner. Stuxnet blev udgivet i tre forskellige udgaver og nåede at inficere talrige anlæg og maskiner før den blev opdaget og stoppet. Ormen er meget sofistikeret og benytter mange forskellige teknikker til at nå dens mål og forblive uopdaget undervejs.

2 Bagom

Det er aldrig blevet afsløret hvem der stod bag Stuxnet. Selve ormen er meget avanceret og det må forventes at et sådant stykke programmel har krævet et stort og velorganiseret hold af programmører for at udvikle. Der har været spekulationer om hvorvidt Israel i samarbejde med USA har stået for udviklingen, på grund af den primært har inficeret deres fælles fjende, Iran, og deres atomprogram. Der er dog ingen endegyldige beviser for disse påstande. Det er derfor vigtigt at man ikke drager forhastede konklusioner, da bagmændene måske bevidst har plantet spor for at rette mistanken mod USA og Israel.

Stuxnet skulle sabotere de såkaldte SIMATIC WinCC og PCS7 systemer som kan styre f.eks. centrifuger. Over længere tid ændrede Stuxnet omdrejningerne i minuttet for at sabotere centrifugen, og derved minimerede den risikoen for at blive opdaget. Derved var dens inficering af andre maskiner kun et middel for at nå målet og ville derefter kun blive benyttet til opdateringer og videreformidling af ordrer.

En statistik over ramte mål tegner et tydeligt billede hvorpå næsten 60% af alle mål var lokaliseret i Iran. Det forventes at de resterende infektioner var et nødvendigt onde grundet Stuxnets aggressive spredning. Den første udgave af Stuxnet, en simpel udgave som er blevet dateret til juni 2009, var ikke så effektiv i forhold til dens spredning og det formodes at de to efterfølgende versioner forsøgte at forbedre dette. Stuxnet blev to gange signeret med certifikater fra henholdsvis Realtek Semiconductor Corps. og JMicron Technology Corp. som begge ligger i samme erhvervsbygning. De to certifikater kan have blevet stjålet fysisk fra virksomhederne - endnu et tegn på bagmændenes seriøse tilgang til udviklingen.

3 Teknikker

Stuxnet benytter flere forskellige teknikker til at nå dens mål. En vigtig teknik er den såkaldte zero-day exploit som udnytter huller i softwaren der endnu ikke er kendt af andre, ej heller de som udvikler softwaren. Ordet indikerer at hullet i softwaren bliver udnyttet før eller samme dag som den bliver opdaget af udviklerne, altså før en løsning kan blive udsendt til brugerne af softwaren.

En anden teknik Stuxnet benytter er at placere et rootkit på den inficerede maskine. Et rootkit er et hemmeligt program som forsøger at gemme bestemte processer fra brugeren og operativsystemet og samtidig give administrator adgang til maskinen. Dette giver rootkittet fuldstændig adgang og mulighed for at agere så det har størst mulig chance for at nå dets mål. Stuxnet inkluderede både et Windows rootkit samt PLC rootkit, hvor PLC er Programmable Logic Controller, hvilket er en anordning der kan styre en centrifuge eller lignede apparatur.

Desuden benyttes der en teknik kaldet hooking code, netop for at forhindre afsløringen af rootkitets tilstedeværelse på maskinen. Dette betyder at rootkittet forfalsker det output som ellers kunne have afsløret det. Desuden benyttes der også teknikken betegnet som code injection hvor der bliver indført kode ind i programmer så eksekvering bliver ændret for at tilgodese Stuxnets formål.

Stuxnet benyttede også; teknikker til at undvige mulige installerede antivirus programmer, at inficere netværks rutiner, at skabe et peer-to-peer netværk internt mellem maskinerne samt at benytte et Command & Control interface til at kalde internet servere. Disse teknikker vil blive behandlet i de kommende afsnit hvor Stuxnets opførsel vil blive diskuteret nærmere.

De teknikker som er beskrevet ovenfor giver et skræmmende billede af ormen Stuxnet. Det er tydeligt at den er professionelt designet og udviklet og benytter sofistikerede teknikker for at nå dens mål.

4 Adgang til anlægget

Et atomanlæg kræver et meget lukket og sikkert netværk udad til, for at det kan modstå mulige udefra kommende angreb. Hvis et ondsindet angreb ikke bliver modstået vil det kunne resultere i en fysisk katastrofe omkring anlægget. Derfor forventes det også at anlæggene har den sikkerhed der er påkrævet for at stå imod sådanne angreb. Derfor er det også mere sandsynligt at adgangen til anlægget skete ved at transportere et inficeret flytbart medie ind og benytte den på en af terminalerne.

Der var tidligere spekulationer hvorvidt starten på inficeringen skete via en gratis USB pind givet til ansatte på anlægget ved messer eller lignende. For nyligt er der dog kommet yderligere informationer frem og det formodes at ormen kom ind via et hukommelseskort eller USB som blev leveret af en iransk dobbelt agent.

5 Spredning internt i anlægget

Et anlæg som bearbejder atomart materiale kræver høj sikkerhed og det forventes at det interne netværk er opdelt i flere lukkede dele som kommunikerer via faste rutiner og protokoller. Derfor har Stuxnet skulle arbejde sig ned fra den første spredning til dens specifikke mål. Det er dog langt fra sikkert at

strukturen er en lukket lagdeling da eksterne ingeniører vil kunne kræve adgang til de dybere lag for at kunne udføre deres arbejde. Hvis de, uvidende eller ej, benytter et inficeret flytbart medie vil dette være kritisk, netop fordi man omgår de elektroniske sikkerhedscheck. Dette er dog på sin vis ligegyldigt da Stuxnet er så sofistikeret at den uden problemer ville kunne have nået mål fra det øverste lag. Dette har bare fremskyndet processen.

Grundet Struxnets avancerede design benytter den flere forskellige metoder for at sprede sig internt i anlægget når først en maskine er inficeret. Det formodes at ormen opnåede stor spredning via USB eller andre former for flytbare medier.

Den første udgave af Stuxnet udnyttede ikke de zero-day exploits, den senere blev udstyret med, og måtte derfor ty til andre metoder for at kunne inficere den maskine hvorpå det flytbare medie blev indsat. Dens `autorun.inf` fil var blevet omskrevet af Stuxnet og ville først blive benyttet som en reel autorun fil, men også en executable fil senere. For at forøge dens chance for at inficere maskinen blev der tilføjet et ekstra menupunkt når Windows brugeren højre klikkede på ikonet til det flytbare medie. Dette ekstra menupunkt var `Open` som allerede eksisterede, men denne gang fungerede det så maskinen ville blive inficeret.

De senere udgaver af Stuxnet var udstyret med zero-day exploits og behøvede derfor ikke denne tilgang. Den kunne altså tilgå maskinen direkte uden at brugeren skulle gøre noget specifikt. Ormen ønskede dog ikke at forblive på den flytbare disk og efter den havde inficeret tre maskiner ville den slette sig selv igen. På denne måde, er sandsynligheden for at opdage at der mangler en lille smule plads på sin USB pind meget lille, og det gør det sværere at sporre kilden til inficeringen.

Et aktivt og opdateret antivirus ville muligvis kunne fange Stuxnet via nogle af de metoder den benytter, en kæmpe risiko for dens videre inficering af anlægget hvis dette skete. Derfor agerer Stuxnet i forhold til hvilken antivirus der er installeret på den pågældende maskine den forsøger at inficere. Ud fra type og version vil ormen inficere et forudbestemt mål. Hvis det eksempelvis er Kaspersky's antivirus version 8 eller 9 vil Stuxnet inficere Kaspersky's egen proces. Ved andre, eksempelvis ETrust version 5 eller 6 vurderer ormen at risikoen er for stor og dropper inficerings forsøget.

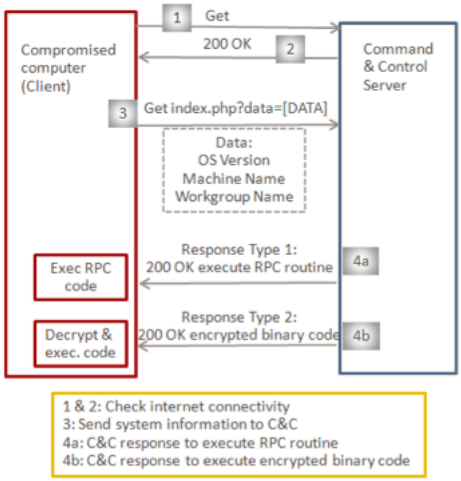
Foruden spredning via flytbare medier udnyttede Stuxnet også andre huller i software og systemer. Den brugte det interne netværk, heriblandt netværksdrev, til at inficere andre maskiner. Af zero-day exploits i Windows, brugte den et hul i netværksprintere hvor dens print spooler blev inficeret og udnyttet. Denne funktionalitet gjorde brug af Windows' egen Remote Procedure Call (RPC) og ville derfor ikke gøre noget væsen af sig selv.

Som tidligere beskrevet formodes det at de ramte anlæg er opdelt i flere mindre, delvist uafhængige netværk. Stuxnet udnyttede at ingeniører muligvis havde anmodet om data fra et stærkt beskyttet netværk via et mindre sikkert og inficeret netværk. Disse anmodninger ville Stuxnet hæfte sig på og derved inficere maskinen der returnerede data. Afslutningsvis skal Siemens S7 projekt filer også nævnes. Disse type filer benyttes meget i anlæg med netop Siemens udstyr

og var en filtype som Stuxnet havde held med at inficere. Da denne type fil benyttes på maskiner meget tæt på kernen i anlægget ville det være en effektiv måde at komme fra en lav risiko maskine som kun benyttes til at udarbejde og teste filen inden direkte implementering.

6 Opdatering af inficeringen

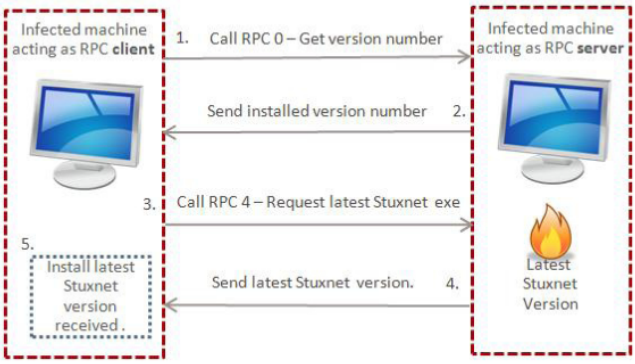
Ved en længerevarende inficering af et anlæg kunne det blive nødvendigt at opdatere Stuxnet for at tage hensyn til opdateringer af antivirus, Windows eller lignede som ville begrænse Stuxnet. Skaberne af ormen konstruerede et internetbaseret opdateringssystem for de maskiner der måtte have adgang til internettet. Dette Command & Control (C&C) interface benyttede to servere, en i Malaysia og en i Danmark, med relativt anonyme domæne navne: www.mypremierfutbol.com og www.todaysfutbol.com.



Interaktionsdiagram af Command & Control kommunikation

De inficerede maskiner med internet adgang ville først sende en simpel anmodning til disse servere, hvis der blev svaret ville de anmode om mulig opdatering, en anmodning der ville indeholde informationer omkring den maskine den blev sendt fra. Anmodningen var en kodet streng for at undgå opmærksomhed. Svaret sendt fra serveren ville være i binær form, dog krypteret med en statisk 31-byte lang XOR nøgle som Stuxnet benyttede for at kunne dekryptere svaret.

Problemet med overstående C&C interface er at det forventes kun at være få maskiner der vil kunne skabe adgang til serverne, enten på grund af manglende internet adgang eller blokering af ikke godkendte domæner. Den opdaterede udgave af Stuxnet vil dog stadig kunne sprede sig ved at bruge de metoder beskrevet i det forrige afsnit. Ormen kan dog benytte sig af et internt peer-to-peer netværk for opdateringer som ville kunne sprede den nye version hurtigere mellem maskinerne der var inficerede.

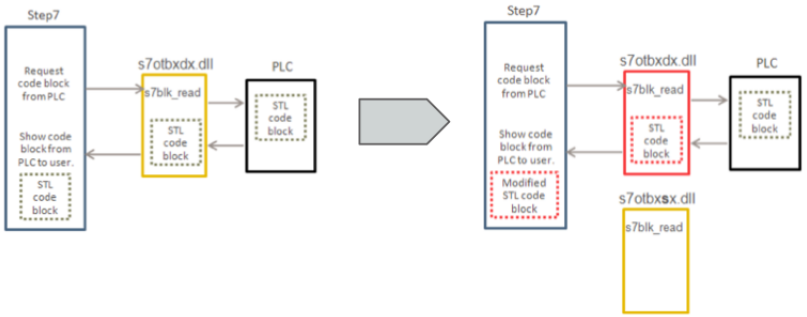


Interaktionsdiagram af peer-to-peer kommunikation

De inficerede maskiner i netværket vil både agere som servere og klienter hvor der udveksles informationer om Stuxnet's version samt mulig opdatering af denne hvis forbindelsen mellem to maskiner viser at den ene er af ældre version. Det skabte peer-to-peer netværk benytter Windows' egen protokol, den førnævnte RPC, og vil derfor ikke skabe stor opmærksomhed da den bruges til mange former for netværks kommunikation mellem Windows maskiner.

7 Inficeret dets mål

Hvis, eller måske rettere når, Stuxnet får inficeret den maskine som er forbundet med den PLC enhed den skal bruge for dens sabotage benytter den sig af en teknik kendt som masquerade. Dette betyder at den ligger sig imellem maskinen som benytter de tidligere omtalte Siemens S7 projekt filer og selve PLC enheden hvor den opfanger al kommunikation mellem de to enheder og handler ud fra dette.



Før og efter inficering af PLC

Den originale .dll fil, som blev benyttet til denne kommunikation bliver omdøbt og gemt hvorefter Stuxnet erstatter denne fil. Ved at lade kommunikationen løbe igennem dens egen fil vil den kunne styre PLC enheden og samtidig give forkerte data tilbage til de ingeniører som forgæves forsøger at styre enheden. Ingeniørerne vil ikke fatte mistanke da det output de får er som forventet, men de er fabrikeret af Stuxnet's egen .dll fil for at maskere dens sabotage.

Grunden til at denne gemmer den originale .dll fil er at Stuxnet havde en udløbsdato. Denne dato var sat til efter den blev opdaget og nåede derfor ikke at slette sig selv fra alle inficerede maskiner. I tilfældet af at datoen var nået ville ormen havde genindsat den originale .dll fil og Stuxnet ville formentlig aldrig have været blevet opdaget.

8 Fremtiden

Alt i alt er Stuxnet ufattelig avanceret og meget skræmmende. At det lykkes at inficere anlæg med atomart materiale bør få enhver til at få bange anelser. Skaberne af Stuxnet ville sabotere anlæggene, men hvem ved om den næste orm vil gøre noget der forårsager voldsomme skader. Dog kan man ud fra et data teknologisk synspunkt kun blive imponeret over hvad den har opnået og med hvilke midler og teknisk overlegenhed at den gør dette. Spredning eksternt er godt nok langsomt, men så snart den har inficeret en maskine i anlægget sker spredningen ufattelig hurtigt. Den agerer alt efter forsvarsforanstaltninger på maskinen, den kan opdatere sig selv via internettet og propagerer de opdateringer ud via det interne netværk. Den bruger teknologier som rootkit og zero-day exploits. Alt dette uden at blive opdaget.

Generelt set er tidligere orme blevet skabt af fritids cracker programmører uden stor finansiering, ej heller med en seriøst udviklings øjemed. De tidligere orme har også været lavet med et generelt formål, såsom at lave DDoS angreb eller sende spam. Dette er helt anderledes med Stuxnet. Selvom det ikke vides hvem der står bag Stuxnet er dens opførsel så sofistikeret at det formodes at have været et meget fokuseret og velstruktureret udviklingsteam der samtidig var velfinanseret. Stuxnet er uhyre målrettet og bruger alle kneb til at nå dens mål.

Stuxnet er den første af næste generation af elektronisk terror/krigsførelse og man må forvente at se flere af dens kaliber. Man kan allerede se eftervirkningerne, feks. har man fornyligt opdaget ormen Duqu, som er baseret på samme platform som Stuxnet, den såkaldte Tilded ($\sim$ d). Den er næsten identisk med Stuxnet, men med det mål at opsamle informationer, spørgsmålet er til hvad. Det kunne være en rekognoscering inden Duqu for alvor går til angreb, måske via en ny orm i samme genre som Stuxnet

9 Afrunding

Stuxnet er en god historie, der er tilpas med konspirationsteorier til at underholde menigmand, og der er teknisk snilde nok til at gøre professionelle IT folk bange.

Ormen er ikke en enkeltpersons værk, det er produktet af en grunding research og en grundig udvikling der varsler en ny og meget farlig type software, som bliver uhyre svært at slippe af med. Som Symantec slutter af med at skrive i deres rapport om Stuxnet: "*Stuxnet is the type of threat we hope to never see again*", og man kan kun give dem ret.

10 Kildeliste

Symantic Security Response. (2011). W32.Stuxnet Dossier (1st ed.). Cupertino, CA: Nicolas Falliere, Liam O Murchu & Eric Chien.

Tofino Security. (2011). White Paper (1st ed.). Appleton, WI: Eric Byres, Andrews Ginter & Joel Langill.

Zetter, Kim. (2011, July 11). How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History. Wired.
Retrived from http://www.wired.com

Goodin, Dan. (2011, April 13). Stuxnet worm reportedly planted by Iranian double agent using memory stick. Ars Technica.
Retrieved from http://www.arstechnica.com