Myndigheten för samhällsskydd och beredskap

Stuxnet

IT som vapen eller påtryckningsmedel

Säkerhet i industriella informations- och styrsystem

MSB:s kontaktpersoner:
Åke J. Holmgren, 010-240 42 78
Daniel Haglund, 010-240 44 15

Publikationsnummer MSB331

Förord

Industriella informations- och styrsystem (SCADA) blir allt mer en förutsättning för viktiga samhällsfunktioner såsom vatten och avlopp, energi, transporter, fastighetsautomation och tillverkningsindustri. Den här utvecklingen skapar nya möjligheter och nya risker i hela samhället och ökar kraven på arbetet med samhällets informationssäkerhet.

Störningar i industriella styrsystem kan inte enbart leda till att dyrbar utrustning förstörs, utan kan även orsaka avbrott i kritiska verksamheter och i värsta fall riskera människors liv och hälsa. Följderna kan också bli omfattande kostnader och förlorat förtroende, för såväl det enskilda företaget som samhället i stort.

Stuxnet utmärker sig i det brus av skadlig kod som ständigt översköljer dagens IT-system och kan sägas representera en milstolpe i utvecklingen av skadlig kod. Ett av skälen till detta är att koden är särskilt riktad mot specifika IT-system inom industrin, det vill säga vissa typer av industriella styrsystem.

Myndigheten för samhällsskydd och beredskap (MSB) har, i samverkan med andra aktörer däribland Totalförsvarets forskningsinstitut (FOI), studerat Stuxnet inom ramen för myndighetens program för ökad säkerhet i industriella informations- och styrsystem.

Denna rapport är en delredovisning av studierna om Stuxnet och den har författats av Robert Malmgren (Robert Malmgren AB). Arbetet har skett i nära samverkan med Daniel Haglund (ansvarig teknisk samverkansplattform säkerhet i styrsystem) och Svante Nygren (programansvarig omvärldsanalys), båda från Enheten för samhällets informationssäkerhet, MSB. Synpunkter på rapporten har även lämnats av Arne Vidström, FOI.

Författaren ansvarar för rapportens innehåll.

Stockholm, oktober 2011

Åke J. Holmgren

Programansvarig säkerhet i industriella informations- och styrsystem, MSB

Innehållsförteckning

Sammanfattning

Stuxnet utmärker sig i det brus av skadlig kod som kontinuerligt attackerar våra IT-system och anses allmänt representera en milstolpe i utvecklingen av sådan programkod. Ett av skälen till detta är det faktum att koden innehåller en elektronisk stridsspets riktad mot speciella IT-system inom industrin, så kallade industriella styrsystem. Stuxnet är det första allmänt kända exemplet på skadlig kod som skapats i direkt syfte att angripa sådana system. Koden är storleksmässigt mycket omfattande och har utformats för att kunna ta sig från Windowsmiljön till styrsystemsmiljön, installera nya programmoduler samt ersätta delar av existerande program. Detta genom att utnyttja avancerade funktioner som inte är välkända för styrsystemutvecklare i allmänhet.

Stuxnet upptäcktes och började diskuteras öppet under juni-juli 2010[1] [2]. Allt tyder emellertid på att Stuxnet i olika programgenerationer och versioner existerat under en längre tid dessförinnan. Bland annat säger sig antivirusföretaget Symantec ha hittat kopior vars ursprung är från juni 2009[3].

Så snart Stuxnet blev allmänt känd inleddes analys av koden på många håll i världen, liksom spekulationer om modus operandi och diskussioner om upphovsmän och tänkbara mål. Detta pågick med varierande intensitet under mer än ett halvår i bloggartiklar, vitbokspublikationer från antivirusföretag, och inte minst i alla former av nyhetsmedia.

Den tekniska analysen av Stuxnets programkod omfattade främst dess logiska struktur, attackmekanismer, inbyggda skyddsmekanismer och spridningsmekanismer. Analysen kom huvudsakligen att fokusera på den Windowsorienterade delen av koden[4]. Detta kom sig av det enkla faktum att i princip alla analytiker blev tagna på sängen och stod utan kunskaper, verktyg och möjligheter att analysera den andra delen av Stuxnet, den som manipulerade specialmaskinvara och specialprogramvara som ofta skräddarsys per användare och användningsområde.

Stuxnet blev för den stora allmänheten det "datorvirus" som blev en ögonöppnare för att IT, i form av skadlig kod, kan användas som en form av vapen och utnyttjas som ett påtryckningsmedel av aktörer, för att uppnå politiska eller andra mål.

---

[1] Sergey Ulasen från VirusBlokAda öppnade en diskussionstråd på ett e-forum där han beskrev en ny skadlig kod som hade lite märkliga egenskaper
http://www.wilderssecurity.com/showthread.php?p=1712146

[2] Frank Boldewin var den förste att peka på den nyupptäckta skadliga koden rootkit.tmphider innehöll mystiska referenser till Siemens Step7 och WinCC
http://www.wilderssecurity.com/showpost.php?s=dbe8d9e87d81f36d8b43db04245e34aa&p=1712134&postcount=22

[3] "The Stuxnet Dossier", ver 1.4, Sid 4

[4] Antivirusföretaget ESETs vitbok om Stuxnet handlar uteslutande om Windowsdelarna.
http://eset.ru/.company/.viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf

1. Bakgrund

Denna text är en sammanställning av Stuxnetincidenten fram till oktober 2011. När detta skrivs har över ett år förflutit sedan händelsen blev allmänt känd, vilket ur analysperspektiv är en fördel. En mängd artiklar och analyser har gjorts av såväl programvaruuppbyggnaden som av Irans kärnteknikprogram, vilket av många betraktas som måltavlan för Stuxnet.

Det vitryska antivirusföretaget VirusBlokAda upptäckte den 17:e juni 2010 ett nytt datorvirus som det kallar Trojan-Spy.0485, Malware-Cryptor.Win32. Inject.gen.2[5]. Viruset visade sig vara medvetet skadlig kod som innehöll många tekniskt intressanta mekanismer i form av en datormask[6] och ett rootkit[7] som installerade drivrutiner på Windows-baserade datorer. I fallet med Stuxnet skedde spridningen med hjälp av flera olika metoder för att på ett så effektivt och precist sätt som möjligt ta sig fram till och in i målmiljön.

Det som var utmärkande och ovanligt med denna skadliga kod, som snart skulle komma att döpas till Stuxnet, var bland annat att den använde sig av flera sedan tidigare publikt okända säkerhetshål i Windows och att de Windowsdrivrutiner som ingick i Stuxnet var elektroniskt signerade med legitima signaturer från kända företag. Till listan över ovanligheter kunde, efter ytterligare analys, läggas att programkoden var tvådelad – dels den del man först upptäckt och som riktade sig mot Windowsplattformen, dels en del som skapats för en helt annat typ av målsystem, nämligen industriella styrdatorer. I detta fall från tillverkaren Siemens.

Namnet Stuxnet, som skapades av antivirusföretagen som analyserade programmet, påstås[8] komma från teckensträngarna ”.stub” och filnamnet ”MrxNet.sys” som förekommer i själva Stuxnetkoden.

I oktober 2011 framkom att en annan skadlig kod, benämnd Duqu, uppvisat många likheter med Stuxnet. Vid publikationstillfället är analysen av Duqu inte färdigställd och kommenteras därför inte i denna rapport.

[5] http://www.anti-virus.by/en/tempo.shtml

[6] En mask är ett datorprogram som via nätverket sprider sig från dator till dator

[7] Ett rootkit är en programvara som skaffar sig höga åtkomsträttigheter på en infekterad dator, och när väl rootkitet aktiverats så gömmer det sig väl och kringgår aktivt olika aktiviteter för upptäckt

[8] http://twitter.com/#!/search/mrxnet.sys%20.stub

2. Analysarbetet

Under det första halvåret efter upptäckten av Stuxnet var det fortfarande en hel del diskussion i media, på Internet och inom säkerhetssamfundet om ursprung, mål, måluppfyllnad och tillvägagångssätt. Huvuddelen av analysen under denna tid fokuserade på Windowsplattformen och flera olika organisationer och personer bidrog till den öppna spridningen av kunskap om Stuxnet.

Från perioden årsslutet 2010 och framåt ansåg allt fler personer[9] [10] att Stuxnet representerade ett försök att med hjälp av IT, i form av avsiktligt skadlig kod, slå mot det iranska kärnteknikprogrammet.

Symantec var det företag som bidrog till huvuddelen av analysen, och en av de få organisationer som analyserade och publicerade information om PLC-koden, främst genom publiceringen av sin "Stuxnet Dossier"[11].

Flera IT-säkerhetsföretag, t.ex. Symantec och ESET, kom efterhand ut med nya, ofta mycket uppdaterade versioner av sina tekniska vitböcker. Från att i början enbart ägnat sig åt statisk kodanalys av binärfiler, så inkluderade Symantec även en dynamisk översikt av tidsförlopp och spridning av Stuxnet. Denna analys möjliggjordes främst av följande två egenskaper:

1. Stuxnet använder sig av en fil i vilken den registrerar lyckade spridningar. Denna information används dels för att undvika försök till återinfektion, dels för att ha kontroll över infekterade systernoder i nätverket med vilken det går att hämta eller skicka uppdateringar och styrkommandon.
2. Vid en lyckad infektion så försöker Stuxnet kontakta förbestämda nätverksadresser för att hämta uppdateringar eller nya styrkommandon.

Symantec styrde efter upptäckten[12] om och övervakade uppkopplingsförsök från infekterade datorer mot de förbestämda nätadresserna. På så sätt gick det att få en överblick av den pågående infektionen och spridningen. Genom att samla in kopior av Stuxnet från infekterade datorer kunde man också pussla ihop bilden över hur och när Stuxnet har spridit sig[13].

Symantecs djupanalys av PLC-delen är något som byggts upp över tid, från de relativt informationsfattiga bloggposterna i början av analysen till en ganska avancerad analys av PLC-programmets struktur, vad PLC-programmet faktiskt avser att göra och mot vem. PLC-programmets tillståndsmaskin var ganska avancerad, med start och förändring av olika programaktiviteter över tid[14].

---

[9] http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf

[10] http://www.langner.com/en/2010/12/27/breaking-news-417-centrifuge-safety-system/

[11] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[12] 20 juli 2010, enligt "Stuxnet Dossier", ver 1.4, sid 4

[13] "The Stuxnet Dossier", ver 1.4, Sid. 8-11

[14] "The Stuxnet Dossier", ver 1.4, Sid. 41

3. Kort teknisk fördjupning

Tekniskt kan Stuxnet ses som ett IT-vapen med kapacitet att överbrygga såväl olika typer av datorutrustning, som olika sätt att sprida sig mellan datorerna.

3.1 Spridningsmekanismer

Det sättet Stuxnet var uppbyggt på förenklar spridningen av kod mellan organisationer och därefter till en fysiskt avskild IT-miljö. T.ex. kan Stuxnet sprida sig via infekterade USB-minnen. Det sker genom att utnyttja en säkerhetsbrist i filhanteraren Windows Explorer som felaktigt och prematurt exekverar programkod när filhanteraren ska lista innehållet i en filkatalog som innehåller en manipulerad fil. Denna spridningsmetod är en god angreppstaktik för någon som vill att omedvetna offer eller involverad personal, ska flytta smittad kod mellan fysiskt separerade (isolerade) IT-miljöer. Likaså sprider sig Stuxnet genom att infektera vissa Siemens S7 projektfiler[15], filer som beskriver kontrollsystemets uppsättning och programkod. Dessa infekterade filer automatexekverar Stuxnetkod när filen öppnas med mjukvarorna WinCC eller Step7. Även denna metod får anses vara väl uttänkt för att kunna sprida smittan mellan fysiskt separerade IT-miljöer. Förutom spridningen via S7-projekt eller smittade USB-minnen kan Stuxnet även använda andra metoder för att sprida sig direkt till nya datorer via nätverket.

När Stuxnet väl har etablerat kontroll över en infekterad dator så sker kommunikation direkt mellan noder via såkallad peer-to-peer-trafik (P2P). Via denna direktkanal kan uppdaterad programkod skickas eller tas emot mellan noderna. Detta är en metod som Stuxnet använder för att se om någon av noderna har modernare eller äldre kod än andra noder, och i förekommande fall uppdatera äldre Stuxnetinfektioner.

Stuxnet har alltså skapat en effektiv kombination av:

- *Spridningsteknik* (on-line samt off-line med USB-minne)
- P2P-teknik för att *behålla* och *underhålla* infekterade noder relativt lokalt, samt
- Call-back – infekterade noder försöker kontakta förbestämda nätadresser, s.k. command and control-noder, och där hämta kod eller kommandon. Denna metod möjliggör tillägg av *ny funktionalitet* eller *större förändringar* av Stuxnets programkod. Detta är inte olikt de på Internet vanligt förekommande bot-nät där många infekterade noder kontrolleras.

Med hjälp av denna struktur möjliggörs en spridning som inte bara kan hoppa över så kallade luftgap in till isolerade miljöer, utan också skapa underhållslinjer som potentiellt kan upprätthållas ända in till den isolerade miljön för de tillfällen då nya programversioner finns tillgängliga eller nya

[15] "The Stuxnet Dossier", ver 1.4, Sid 32

kommandon ges. Stuxnet har en inbyggd enkel databas[16] som håller konfigurationsinställningar, referenser och datumstämplar. Med hjälp av databasen kan Stuxnet veta vilka andra noder som den lyckats infektera och därmed ha kunskap om vilka noder som P2P-nätet ska kommunicera med. Denna fil går även att använda som en loggfil över spridningsförfarandet. Genom att samla in många kopior av Stuxnet och dess databasfil går det att kartlägga när, var och hur Stuxnet spridit sig. Symantec analyserade filen för att kartlägga spridningen och har därmed relativt väl lyckats ringa in troliga startpunkter, starttillfällen, spridningstakt och spridningsvolym[17].

3.2 Undvikande av upptäckt

Stuxnet har ett visst inbyggt skydd mot att kunna undgå upptäckt, t.ex. kryptering av sina egna filer[18] och för sin nättrafik[19]. Den har också programkod för att aktivt undvika och motverka populära antivirusprogram från de vanligaste tillverkarna[20]. Detta genom att först detektera programmen, etablera tillräckligt höga systemprivilegier och sedan stänga ner antivirusprogrammet.

3.3 Utnyttjande av sårbarheter

Windowskomponenten av Stuxnet använder sig av såväl enklare säkerhetshål, såsom hårdkodade lösenord i databaskomponenten i WinCC-plattformen, som mer avancerade angrepp via tidigare opublicerade eller för allmänheten okända sårbarheter i Windows. Förutom att dessa var allmänt okända, så hade inte heller leverantören kännedom om dem. Därmed saknades patchar för dessa sårbarheter och de kunde inte åtgärdas direkt av systemägarna. Sårbarheterna fanns bland annat i skrivarhanteringen, hanteringen av schemaläggning (schedulering) av program, fildelningsmodulen och filhanteraren. Vissa av säkerhetshålen användes för att Stuxnet skulle kunna sprida sig själv, andra säkerhetshål användes som attackvektor för att kunna lyfta sig själv från låg behörighetsnivå med få systempriviligier till hög behörighetsnivå. Ett exempel på det senare är det säkerhetshål som lagas med säkerhetspatchen MS10-073.

Stuxnet innehöll programkomponenter som signerats med falska programutgivarcertifikat[21]. Det var lågnivåkomponenter som betroddes och laddades av Windows operativsystemkärna eftersom programutgivar-certifikaten var betrodda. Olika versioner av komponenterna signerades med först en signeringsnyckel och vid en senare variant av Stuxnet med den andra signeringsnyckeln. Certifikaten tillhörde ursprungligen de två taiwanesiska hårdvarutillverkarna RealTek och JMicron. Hur angriparna kunnat skaffa sig tillgång till dessa för signering är idag inte känt. Det är dock anmärkningsvärt med både förekomsten av signerade filer samt att angriparen kommit över två olika organisationers signeringsnycklar.

---

[16] ”The Stuxnet Dossier”, ver 1.4, Sid. 15

[17] ”The Stuxnet Dossier”, ver 1.4, Sid. 7-11

[18] Algoritm och kryptonyckel beskrivs på sid 65 i ”Stuxnet under the Microscope”, ver 1.1

[19] Algoritm och kryptonyckel beskrivs på sid 58 i ”Stuxnet under the Microscope”, ver 1.1

[20] ”The Stuxnet Dossier”, ver 1.4, Sid. 14

[21] ”Stuxnet under the Microscope”, ver 1.1, sid 11-13

3.4 Målsystem

Den programkod som kör i Windowsdatorn är en spridningskomponent för att nå slutmålet, att infektera PLC-komponenter. De infekterade PLC-komponenterna styr en fysisk process som består av maskiner, sensorer, reglage och styrreglage. Genom att påverka dessa PLC-komponenter gick det att manipulera den fysiska processen, vilket kan påverka såväl den anslutna utrustningen som det resultat den fysiska processen arbetar med.

Det finns flera skäl att tro att Stuxnet är en skräddarsydd attack mot en viss processautomationslösning:

- Den infekterar enbart specifika versioner av Siemens PLC-utrustning[22]: 6ES7-315-2 och 6ES7-417
- Stuxnet kontrollerar att dessa PLC-system har en specifik programuppsättning[23]
- Stuxnet kontrollerar att dessa PLC-system har specifikt anslutet nätverkskort och specifik ansluten utrustning som den kontrollerar [24]
- Stuxnet innehåller styr- och kontrollrutiner samt parametersättning för att styra en viss typ av fysisk process.

En viktig observation av manipulationen av PLC-systemet var att ny programkod installerades i flera delar av PLC:n. Bland annat så installerades en ny programmodul, kallad DP_RECV, som närmast kan liknas vid en ny enhetsdrivrutin (device driver) för kommunikationsgränssnittet mot Profibus[25]. Denna programmodul innehöll funktioner för att kunna fånga nätverkstrafik[26] innan den nådde PLC:ns egentliga hantering av inkommen nättrafik. En annan aspekt av manipulationen av PLC:n var att de in- och utgångar som användes för att hämta in mätvärden eller styra utrustning frikopplades från den överliggande operatörskopplingen. Genom att skicka manipulerad (förskönad) information mot operatörerna, så kunde den skadliga koden i själva PLC:n jobba ostört med att med ökande avvikelse styra och manipulera de anslutna maskinerna. Upplägget är inte helt olikt de spelfilmer där förövarna visar en förinspelad bildsekvens av ett tomt bankvalv under själva bankrånet.

[22] "White Paper: How Stuxnet Spreads" sid 8

[23] "The Stuxnet Dossier", ver 1.4, sid 39

[24] "The Stuxnet Dossier", ver 1.4, sid 39

[25] Profibus är en fältbuss (industriell digital kommunikationsbuss för distribuerad realtidskontroll)

26 "The Stuxnet Dossier", ver 1.4, sid 39

4. Efterspel

Stuxnet lär i dagsläget vara ett av de mest analyserade och dokumenterade exemplen på skadlig kod som existerar. Det har skapats åtskillig dokumentation om de tekniska aspekterna av Stuxnet och dess modus operandi. IT-tekniskt och IT-säkerhetsmässigt beskrivs Stuxnet framför allt i:

- de tekniska vitböcker som getts ut av Symantec, ESET[27], Joe Langill[28] m.fl.
- de bloggartiklar som skrivits av Ralph Langner[29], Mark Russinovich[30] m.fl.
- den återskapade källkod som tagits fram av Amr Thabet[31] m.fl.[32]

Man får anta att upphovsmännen till Stuxnet hade räknat med att deras kod skulle analyseras, men frågan är om de tänkt sig att det skulle bli en så ingående och omfattande insats? En viktig, än så länge obesvarad, fråga är hur mycket av Stuxnets arkitektur, uppbyggnad, design eller programmoduler som går att inspireras av, eller återanvändas, för framtida angrepp.

Fyra viktiga konsekvenser som skett i efterdyningarna av Stuxnet är att:

- Fokuseringen på IT-vapen (Cyber Warfare) allmänt har ökat. Politiker, militärer, försvarsanalytiker, IT-säkerhetsbranschen och andra tittar på såväl offensiva som defensiva aktiviteter.
- Flera länder har ökat sina försvarsorienterade IT-aktiviteter, både defensiva och offensiva, efter Stuxnetincidenten. T.ex. har Iran, riktigt eller oriktigt, pekats ut som källa i mängder av nya IT-angrepp runt om i världen.
- Det går att dela in historieskrivningen för IT-säkerhet i ”tiden innan Stuxnet” och ”tiden efter Stuxnet”. Efter Stuxnet så kom frågan om IT-angrepp mot industriella kontrollsystem upp på agendan inom många organisationer där kontrollsystem används.
- Angripare som bygger IT-vapen eller planerar attacker av Stuxnets typ i framtiden kommer att bygga på erfarenheterna från Stuxnetincidenten. Frågor såsom ”Hur hantera att koden analyseras publikt”, ”hur bygga en mer robust bot-nät-del?”, ”hur hålla konfiguration och programtillstånd, utan att detta kan användas för forensisk analys” kommer att beaktas.

---

[27] ”Stuxnet under the Microscope”, ver 1.1 http://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf

28 http://www.tofinosecurity.com/how-stuxnet-spreads

29 http://www.langner.com/en/2010/09/13/stuxnet-is-a-directed-attack-hack-of-the-century/

[30] http://blogs.technet.com/b/markrussinovich/archive/2011/03/30/3416253.aspx

31 http://www.codeproject.com/KB/web-security/StuxnetMalware.aspx

32 https://github.com/Laurelai/decompile-dump

5. Viktiga lärdomar

När vi nu med distans till själva incidenten kan summera ihop händelsen så går det att dra olika lärdomar utifrån sådant som attackmetodik, händelseförlopp, mediahantering, tekniska detaljer, etc.

- Risken är stor att de som inte direkt påverkades av Stuxnetincidenten, genom att vara måltavla eller få sin miljö infekterad utan att vara primärmål, fortsätter att driva en processkontrollmiljö som inte håller fullgott skydd. Samma attackmetoder, liknande säkerhetshål, motsvarande arkitektur på attackprogram samt liknande camouflagemetodik går att utnyttja vid angrepp mot såväl Siemens S7 som för produkter från andra leverantörer.
- Stuxnet har visat att det finns många *faktorer* som användare eller utvecklare av industriella styrsystem inte känner till eller tagit hand om på ett adekvat sätt:
  - Möjligheten att bli utsatt för IT-attacker i allmänhet.
  - Att drabbas av skräddarsydd, skadlig kod.
  - Att få tag i relevant information om säkerhetsbrister eller angrepp.
  - Vid egna eller mediarapporterade incidenter ha rätt kanaler eller rätt information för att snabbt och enkelt kunna upprätta dialoger med systemintegratörer och leverantörer om hotbild, tillfälliga eller permanenta lösningar, etc.
  - Att man, främst inom större organisationer, inte skapar sig en klar och korrekt bild över innehav av system, programversioner, etc. Detta är inom många organisationer ofta bättre utvecklat på kontors-IT-sidan än för industriella informations- och styrsystem.
- Organisationer behöver ta fram bättre skydd av sina processkontrollmiljöer och ha processer och rutiner på plats för att över tid förstärka och utveckla skydden mot nya hot och ny teknisk utveckling.
  Tiden mellan det att Stuxnet började spridas till det att någon antivirusanalytiker fick en kopia, gjorde viss analys samt gick ut med varningar var lång, cirka ett år[33]. Med ställtider som dessa kan både angrepp ske och spåren kallna innan någon fått upp ögonen för att något ovanligt inträffat.
- Mycket av analysen publicerades öppet. Denna öppenhet finns tack vare att antivirusföretag publicerade sina analyser som öppna nyhetsinslag i form av bloggpostningar, sammanställningar av dessa i form av längre tekniska vitböcker[34] eller presentationer på IT-säkerhetskonferenser[35]. Ägare av utrustning som använder Siemens PLC-komponenter samt IT-säkerhetskollektivet i stort hade i princip bara dessa informationskanaler att tillgå för snabb information.

[33] "The Stuxnet Dossier", ver 1.4, Sid 4

[34] Som exempelvis Symantecs "The Stuxnet Dossier" eller ESET:s "Stuxnet under Microscope"

[35] Exempelvis VirusBulletinkonferensen 2010-09-30

- Angripare kan hitta oväntade attackvägar och nyttja oväntade IT-tekniska grepp, t.ex. uppvisade Stuxnet följande icke-traditionella funktionalitet:
  - Stuxnet är en hybrid som påverkar två olika typer av IT-miljöer. Detta tog det tid för analytikerna att förstå.
  - Smittan kunde spridas via Siemens projektfiler. Detta är ett grepp som de flesta sannolikt inte förväntat sig.
  - Ersättandet av en relativt okänd programmodul för nätverkshantering i en ovanlig hårdvarumiljö (PLC).
  - I Windows-delen av Stuxnet använde de sig av programkomponenter som hade försetts med falska elektroniska utgivarsignaturer. Detta öppnar vägar in i operativsystemet. Samtidigt döljer det spåren av angreppen eftersom det är komponenter som tros komma från kända leverantörer. Detta var en av orsakerna till att Stuxnet kunde etablera en typ av rootkit[36]-funktionalitet för att både aktivt manipulera styrningen av den fysiska processen och samtidigt rapportera normalläge till operatören eller ignorera styrkommandon.
- Angripare kan ha stor kunskap om allmänna attacktekniker men även djup kunskap om:
  - Hur man upptäcker nya säkerhetsluckor för vilket det inte finns färdiga skydd.
  - Specifika tekniska detaljområdet såsom filformat för en nischprodukt eller hårdvaruarkitektur på en udda plattform. I detta fall MCS- och S7P-filer och Siemens PLC-utrustning.
  - Detaljer för en viss specifik fysisk process som hanteras av processkontrollsystem. I detta fall något så ovanligt som anrikning av kärnbränsle.
  - Detaljer om produktval och IT-miljö för en viss specifik anläggning. I detta fall vilka Siemens S7-enheter och hur dessa var uppsatta.
- Mediabevakning av händelser där IT-system är måltavla eller där IT-system används kan få stort genomslag. Detta kan förenkla lägesbedömning och omvärldsbevakning men samtidigt innebära informationsläckage eller störande moment när den egna organisationen får hantera frågor från journalister eller allmänhet.
- Mycket av de säkerhetsfunktioner som ryggmärgsmässigt används – såsom exempelvis antivirusprogram - skulle inte ha skyddat mot skadlig kod av Stuxnets kaliber. Detta beror på att Stuxnetkoden dels använde sig av okända eller icke-publika säkerhetshål för sin spridning, dels hade inbyggda funktioner för att manipulera antivirusprogram eller andra säkerhetsmekanismer såsom lokala brandväggar på de datorer som angreps.

[36] Mjukvara som döljer sin närvaro i systemet men samtidigt har systemåtkomst på hög behörighetsnivå och kan manipulera systemet.

- Målet för Stuxnet var av allt att döma ett väl skyddat högsäkerhetsmål, där:
  - såväl personal som säkerhetskultur får anses vara riskmedveten,
  - delar av IT-miljön får antas vara skyddad i form av fysisk separation,
  - den fysiska säkerheten får antas vara god i form av vakter och fysiska skydd, och
  - informationssäkerheten får antas vara god i form av att ritningar, beskrivningar av den fysiska processen, källkod och liknande skyddas.

  Trots detta förefaller det som om Stuxnet lyckas väl i sin penetration av IT-miljön och infekterade PLC-systemen med skador på utrustning i den fysiska processen (centrifuger) som en fördröjd och/eller undermålig slutprodukt[37]. Detta visar hur svårt det är att skydda sig mot en angripare, som i detta fall troligen är välmotiverad och/eller resursstark.
- De IT-säkerhetspåverkande sårbarheter som Stuxnet utnyttjade har tagit lång tid att att åtgärda eller reparera[38]. Eller som i flera delar av fallet med Siemens-produkterna, inte ändrats alls[39].

[37]"Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf

[38] Microsoft släppte under 2010 följande patchar för att hantera hålen i Stuxnet: MS10-046 i augusti, MS10-061 i september, MS10-073 i oktober, MS10-092 i december.

[39] Det går inte att byta det standardlösenord som finns hårdkodat i databaskomponenten i Siemens WinCC-produkt, det går inte att blockera eller autentisera sättet som Stuxnet via manipulerade.dll-filer pratar mellan Windowsplattformen och S7 PLC-systemet.

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB331