november 2010 nummer 7

INFORMATIEBEVEILIGING

Hack in the box 2010 Amsterdam

Stuxnet - de zomerhit van 2010

DDoS-protectie service in de Cloud

De crypto life cycle

PvIB
Platform voor InformatieBeveiliging

ib

Stuxnet - de zomerhit van 2010

Auteurs: Lex Borger en Maarten Hartsuijker > Lex Borger is een principal consultant bij Domus Technica. Hij is te bereiken via e-mail: lex.borger@domustechnica.com.

Maarten Hartsuijker is security consultant bij Classity Informatiebeveiliging. Hij helpt organisaties met security management, security audits en website penetratietesten. Volg Maarten via @classityinfosec.

Het zal niemand die zijn ogen ook maar enigszins op het nieuws gevestigd houdt zijn ontgaan. Deze zomer infecteerde een computerworm massaal industriële ICT-omgevingen. Hierbij bleek de worm een vrij expliciete voorkeur te hebben voor Windowssystemen die Siemens-apparatuur aansturen. Het overgrote deel van de besmette systemen bevindt zich in Iran, wat leidde tot uitgebreide speculatie over de mogelijke betrokkenheid van de Israëlische en Amerikaanse overheid. Deze zouden geïnteresseerd zijn in meer informatie over het Iranese atoomprogramma en deze informatie via een intelligent computerworm hebben willen achterhalen. Is dit waar? En heeft dit gewerkt? Op dergelijke vragen zullen we vermoedelijk geen antwoord krijgen. Maar dat we met het verschijnen van Stuxnet te maken hebben gekregen met een interessant, nieuw type computerworm... dat is wel duidelijk. Dit artikel schets de opvallende aspecten hiervan.

SCADA-systemen worden gebruikt voor de besturing van fabricage- en andere mechanische processen. Ze zijn categorisch minder goed beveiligd dan bedrijfsnetwerken. Ze zijn oud en nooit ontworpen om aan het internet te hangen. Wachtwoorden zijn niet te wijzigen zonder uitgebreide testen, wat in de huidige stand van zaken tot gevolg heeft dat een fabriek enige tijd buiten gebruik is. Dat is voor een bedrijf over het algemeen niet acceptabel.

Stuxnet infecteert gericht

Stuxnet is zich bewust van zijn omgeving. Het heeft niet tot doel om zich zoveel mogelijk te verspreiden, het heeft veel meer een opdracht om op bedrijfsnetwerken onopgemerkt te blijven en op zoek te gaan naar SCADA-systemen. Het lijkt dus geïnteresseerd te zijn in de besturing van de traditionele wereld, een interesse die we in kwaadaardige software nog niet eerder zagen.

Stuxnet gebruikt meerdere kwetsbaarheden

De eerste berichten over Stuxnet in juli hadden het alleen nog maar over de LNK-kwetsbaarheid. Nooit eerder was bedacht dat 'shortcuts', de behulpzame icoontjes die verwijzen naar bestanden elders, door computervirussen of -wormen effectief misbruikt konden worden. Later kwam men erachter dat zeker drie andere kwetsbaarheden misbruikt werden. De combinatie van verschillende kwetsbaarheden maken Stuxnet een hybride worm. Het kan via het netwerk misbruik maken van een systeem (via misbruik van het printmechanisme), via het gedrag van fysieke personen machines besmetten (USB-stick) en zichzelf meer rechten toekennen indien een gebruiker op een systeem geen beheerrechten heeft (lokale, privilege verhogende, kwetsbaarheden).

We noemen alle kwetsbaarheden zonder oplossing bij publicatie een 'zero-day', en een interessante parameter is hoe lang de kwetsbaarheid dan al bestond, omdat dat het tijdvak aangeeft wat hackers eventueel hebben gehad om deze kwetsbaarheid onopgemerkt te gebruiken. Ook is het interessant om in archieven van onderzoekers te zoeken naar tekenen van eerder misbruik. Meestal zijn deze tijdvakken niet groot (weken, maanden), omdat kwetsbaarheden over het algemeen door onderzoekers worden opgemerkt op het moment dat ze door aanvallers actief misbruikt worden.

De kwetsbaarheden zijn 'zero-day's'

Opvallend is dat alle door Stuxnet gebruikte kwetsbaarheden tot het moment dat Stuxnet werd gedetecteerd volledig onbekend waren. Veel computervirussen en -wormen ontlenen hun succes aan het onderzoekswerk van derden en misbruiken bekende kwetsbaarheden. Dit maakt ze gemakkelijker te detecteren, maar omdat grote aantallen systemen ook tegen bekende kwetsbaarheden onvoldoende bescherming bieden is dit voor de verspreiding van het virus over het algemeen geen probleem. Stuxnet is voor 100% opgebouwd uit nieuw en uniek materiaal, waarbij kwetsbaarheden misbruikt werden die publiek niet, maar kennelijk bij de makers wel bekend waren. De kans op detectie heeft Stuxnet verder ingeperkt door zich in zijn verspreiding te beperken tot systemen met specifieke kenmerken. Dit maakt het gemakkelijker om uit handen van onderzoeksgroepen en antivirusbedrijven te blijven, waardoor de worm ook lang als zero-day zijn effectiviteit behoudt.

Stuxnet ondersteunt zichzelf

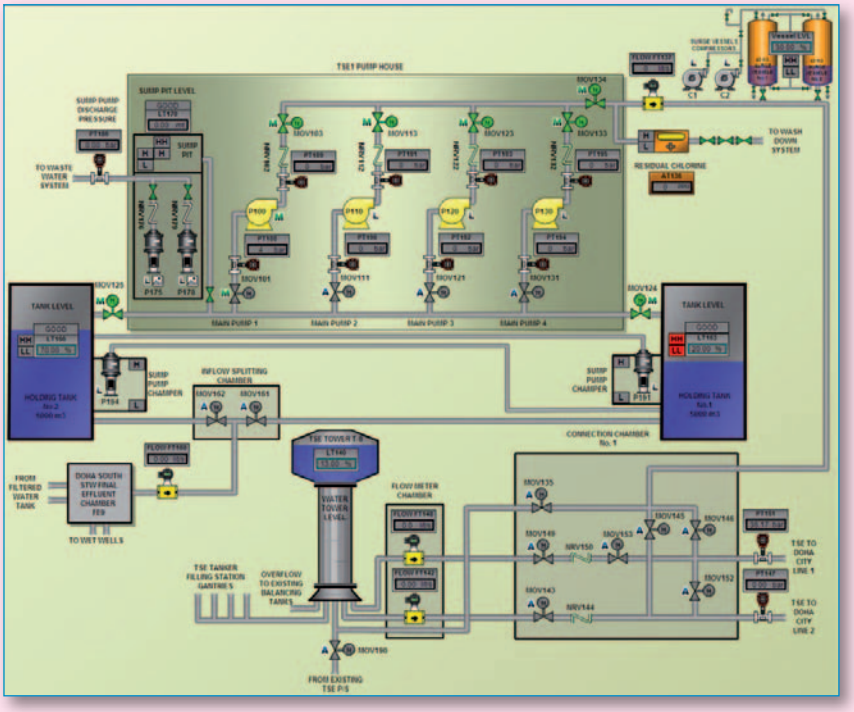
Stuxnet wordt niet alleen bestuurd vanuit een centrale aansturing, maar gebruikt ook zijn eigen 'peer-to-peer'-functionaliteit om in zijn omgeving verbinding te houden met andere geïnfecteerde computers en de software zo actueel mogelijk te houden door versies te vergelijken en vernieuwingen door te sturen. Hiermee kan het actief blijven, ook al valt de centrale aansturing weg.

Een 'payload' is het doel van de worm. Veel computervirussen en -wormen uit het verleden hadden geen payload. De verspreiding was hun doel, daarmee kon de hacker roem verkrijgen. Toen virussen en wormen in criminele circuits gebruikt gingen worden kwam de payload aan bod. Moderne criminele payloads bieden criminelen volledige toegang tot een computer en/of netwerk, verzamelen wachtwoord- of creditcardgegevens of stellen de crimineel tot andere handelingen in staat waarmee geld valt te verdienen.

Stuxnet heeft een complexe 'payload'
In dit geval richt Stuxnet zich specifiek op Siemens-systemen. Op deze systemen breidt het de functionaliteit van de besturingssoftware zodanig uit dat de beheerders van Stuxnet de aan de pc gekoppelde machines kunnen besturen. Het doel is niet duidelijk, de commando's die Stuxnet kan geven zijn geheel afhankelijk van de context. Het lijkt erop dat Stuxnet in een SCADA-netwerk snel veel commando's kan geven aan een groot aantal gelijksoortige machines. De geruchten dat het ultieme doel van Stuxnet is om een verrijkingscentrale met duizenden centrifuges te besturen behoren daarom technisch tot de mogelijkheden. Of Iran hierin daadwerkelijk een specifiek doelwit was blijft zoals gezegd speculeren. Ook netwerken in India zijn bovengemiddeld getroffen. Iran neemt de aanval in elk geval zeer serieus. De minister van de Iranese inlichtingendienst heeft begin oktober in een persconferentie te laten weten diverse verdachten te hebben aangehouden en beschuldigt het Westen van pogingen tot sabotage. Medio oktober werden deze beschuldigingen genuanceerd en legde de minister de nadruk op het succes waarmee Iran het virus gedetecteerd en onschadelijk gemaakt heeft. Ondertussen speculeren andere experts verder over de betrokkenheid van China. Stuxnet houdt de gemoederen dus flink bezig en gelet op het technische hoogstandje van de worm is dat ook niet zo verwonderlijk.

Enric Martinez [attribution], from Flickr

Stuxnet is kwaliteitssoftware
Onderzoekers staan verbaasd over hoe geavanceerd Stuxnet is. Het is modulair opgebouwd, heeft verschillende mechanismen voor zeer verschillende doelen (zie hiervoor), en is hierdoor ook snel in te zetten met een hele andere payload. Het is puur speculatie, maar we weten niet of we nu alles van Stuxnet ontdekt hebben, of slechts het topje van de ijsberg.



Bilal.dweik [public domain], from Wikimedia Commons

Onderzoekers zijn het er wel over eens dat Stuxnet veel geavanceerder is dan Conficker. Toen Conficker in november 2008 de wereldpers haalde werd de worm gezien als het summum van kwaadaardige software. Het slaagde er echter niet in om lang onzichtbaar te blijven.
We weten echter niet hoe lang Stuxnet al bestaat. Het is beter in staat onopgemerkt te blijven. Het is geheel niet ondenkbaar dat het al meer dan een jaar actief is.

Staan we aan de vooravond van een nieuwe generatie malware?
Net zoals alle succesvolle aanvallen van kwaadaardige software eerder, zal Stuxnet van invloed zijn op toekomstige aanvallen. In de vorige eeuw was het ontwikkelen van kwaadaardige software hoofdzakelijk een hobby van enthousiaste hackers die wilden laten zien hoe slim ze waren. De afgelopen jaren zijn virussen ontwikkeld door criminele organisaties (crimeware) de overhand gaan voeren. Er wordt geschat dat creditcardfraude op internet inmiddels zeker zoveel opbrengt als porno. Het feit dat geheime diensten van overheden en grootindustriëlen op dit vlak actief zijn behoort ook al langere tijd tot de vermoedens, maar blijft voorlopig nog speculatie. Stuxnet draagt hieraan bij. De methodes die gebruikt zijn om onder de radar te blijven en modulair inzetbaar te zijn zullen zeker bestudeerd en gekopieerd worden. Voorzien van een eigen payload kan de Stuxnet-aanpak vervolgens andere doelen gaan dienen.

Kunnen we onszelf hiertegen wapenen?
Om te beginnen horen we SCADA-systemen niet zomaar te koppelen met bedrijfsnet-

Zxctypo at en.wikipedia [public domain], from Wikimedia Commons

werken. Het overgrote deel van de SCADA-systemen van dit moment heeft een beveiligingsniveau dat niet voldoende bescherming biedt tegen de hedendaagse bedreigingen. We zullen daarom op zijn minst een goede isolatie moeten aanbrengen tot er een generatie SCADA-systemen is dat ontwikkeld is met betere beveiliging voor de bedreigingen van nu en de toekomst, met de inzichten van nu. Hierover is vorig jaar in dit blad al geschreven door Maarten Oosterink (2009 nummer 8, 'Process control security en SCADA security: een realitycheck')

Computervirussen en andere kwaadaardige programma's zullen steeds moeilijker op te sporen zijn door antivirusproducten. Dit heeft twee redenen. De pure hoeveelheid aan kwaadaardige programma's en het succes waarmee deze detectie kunnen ontduiken. Virusscanners zijn voor hun succes nog grotendeels afhankelijk van vaste signaturen en in beperkte mate van het constateren van overduidelijke afwijkingen van een normaal patroon. Als we succesvoller willen worden in het detecteren van virussen en degelijke, zullen we beter op de hoogte moeten zijn van het gedrag van de software in onze ICT-omgevingen. Op basis van deze kennis is het mogelijk om bekende patronen en programmatuur te 'whitelisten', zodat afwijkingen daarvan automatisch tot een reactie van antivirussoftware zal leiden. Onder andere omdat de kans op fouten en verstoringen met deze aanpak groter wordt, wordt deze aanpak nog niet breed gebruikt. We zullen nadelen als deze moeten oplossen en dit mechanisme op een slimme manier gaan toepassen. Als we hier succesvol in zijn kunnen we een volgend Stuxnet in de toekomst, zelfs al misbruikt het onbekende kwetsbaarheden, hopelijk eerder detecteren en weren van onze infrastructuren.
Het is de verwachting dat de detectie van verdacht gedrag naast detectie van infecties veel belangrijker zal worden. In grote netwerken wordt hier al mee gewerkt, dat kan veel gerichter. Het werkstation is op een hele andere wijze dan het netwerk dat kan, in staat om verdacht gedrag te herkennen.

Ook de consumentenmarkt zal meer en meer met deze vorm van security monitoring geconfronteerd worden. Toen het aantal netwerkaanvallen toenam werd elke pc rap van zijn eigen firewall voorzien. De impact die wormen als Stuxnet op het dreigingenlandschap hebben maken een security monitor per systeem daardoor eigenlijk niet meer dan logisch.

Baytownbert [CC-BY-SA-3.0 or GFDL], from Wikimedia Commons

Links
Bruce Schneier blog entry: http://www.schneier.com/blog/archives/2010/09/the_stuxnet_wor.html
Graham Cluley's blog entry: http://www.sophos.com/blogs/gc/g/2010/09/24/stuxnet-vancouver-virus-bulletin/
•Symantec's Stuxnet Dossier: http://www.symantec.com/connect/blogs/w32stuxnet-dossier
•Informatiebeveiliging 2010 nummer 5: 'Internationale aanpak Cybercrime in Proces Control Systems' door Hans Baars
•Informatiebeveiliging 2009 nummer 8: 'Process control security en SCADA security: een reality check' door Maarten Oosterink