erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

Aaron Lye

Techniken und Möglichkeiten digitaler Kriegsführung am Beispiel Stuxnet

Der Computerwurm W32.Stuxnet, kurz Stuxnet, bekam weltweit von Analyst.innen, Forscher.innen, Hacker.innen, Medien und Politiker.innen in den Jahren 2010/2011, aber auch in den Folgejahren, große Aufmerksamkeit. Dieses lag daran, dass Stuxnet eine große und komplexe Bedrohung war und technisch einiges zu bieten hatte. Die Techniken und Möglichkeiten digitaler Kriegsführung sollen an diesem Beispiel verdeutlicht werden.

Technische Beschaffenheit von Stuxnet

Stuxnet ist ein Computerwurm, der sich in 32-Bit-Windowsnetzwerken verbreitet mit dem Ziel, eine spezielle Art von Anlagensteuerungssystemen der Firma Siemens – im Speziellen *SCADA Industrial Control Systems* – anzugreifen. Durch die Infektion des Steuerungsrechners war es dann möglich, auch auf *Programmable Logic Controllers* (PLC) zuzugreifen und diese umzuprogrammieren. Bei Stuxnet handelt es sich also um eine gezielte Attacke, die hochspezifisch für die Kompromittierung eines vorher genau spezifizierten Systems entwickelt wurde. Dies geht aus verschiedenen unabhängigen Analysen des Wurms hervor. Wesentliche Teile der technischen Analyse, bei der der Wurm *reverse-engineered* wurde, wurden gemeinsam von unterschiedlichen Unternehmen, wie Symantec und Microsoft, zusammen mit Einzelpersonen entwickelt, sind gut verstanden und der interessierten Öffentlichkeit zugänglich. Die Art und Beschaffenheit von Stuxnet, die Anzahl der Exploits und auch die Angriffe auf PLCs sind sehr ungewöhnlich. Ein PLC wird im Deutschen auch speicherprogrammierbare Steuerung (SPS) genannt und ist ein Digitalrechner zur Steuerung oder Regelung von Pumpen, Ventilen, Motoren oder im Allgemeinen von Maschinen oder Anlagen. Die Hardware ist üblich und wird weltweit in Millionen von Systemen verwendet. Die Einsatzgebiete erstrecken sich von Produktionsanlagen mit relativ simplen Steuerungen bis hin zur Steuerung von Robotern und Zentrifugen mit komplexen Abläufen, Kraftwerken (Kern, Kohle, Wasser, Wind), Mineralabbau, petrochemischer Industrie, Wasserwiederaufbereitung und Wassertransport, Zügen etc. Anzumerken ist, dass dieselbe Hardware sowohl in zivilen als auch in militärischen Anlagen benutzt wird.

Der Wurm lässt sich in zwei Teilen betrachten, die jeder für sich interessant sind. Der erste Teil ist die Infektion und Verbreitung des Wurms auf Betriebssystemebene; der zweite Teil ist die Infektion des PLC. Beide Teile sollen im Folgenden kurz erläutert werden. Details zu den Exploits sind beispielsweise in Symantecs Analyse[1] zu finden.

Für die Infektion und Verbreitung des Wurms auf Betriebssystemebene werden vier Zero-Day-Exploits genutzt. Ein Exploit ist ein Programm, das eine Sicherheitslücke ausnutzt, um nicht intendiertes Verhalten zu ermöglichen. Bei einem Zero-Day-Exploit ist die Sicherheitslücke nur wenigen bekannt bzw. existiert kein Patch, der diese Lücke schließt. Zwei dieser Exploits dienten dem Zugang und der Verbreitung. Die zwei anderen waren *Privilege Escalation Exploits* – dienten also dem Erlangen höherer Nutzerrechte.

Als Propagationsmethode verwendet der Wurm Wechseldatenträger wie USB-Sticks, des Weiteren Netzwerkdrucker und gemeinsame Verzeichnisse. Der erste Exploit ermöglicht, dass der Wurm automatisch beim Laden des USB-Sticks ausgeführt wird, wobei sich der Wurm allerdings nach drei Infektionen automatisch vom USB-Stick löscht. Der zweite Exploit nutzt einen Fehler im Rechtesystem von gemeinsam genutzten Druckern unter Windows-XP aus und kann so beliebige Dateien auf dem Zielsystem schreiben.[1] Anzumerken ist, dass sich der Wurm durch diese beiden Methoden nur lokal verbreiten kann. Es ist beachtlich, dass sich Stuxnet so weit verbreitet hat.

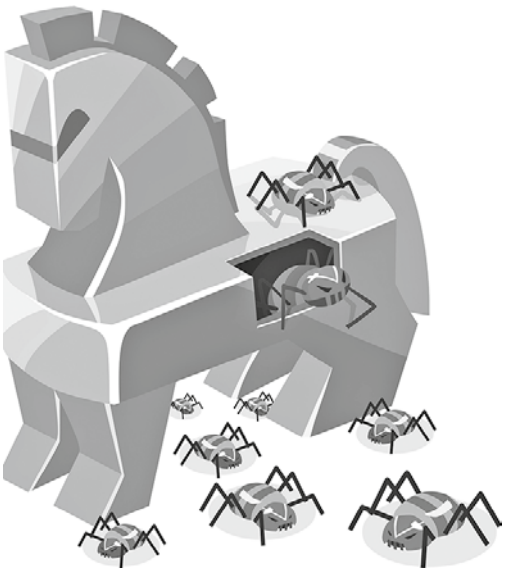
Außerdem ist interessant, dass zwei Privilege Escalation Exploits verwendet wurden, um sowohl Windows-2000-Systeme als auch -Vista und Folgesysteme anzugreifen. So funktioniert der Wurm auf einer Reihe von 32-Bit-Windows-Betriebssystemen: Win2k, XP, 2003, Vista, Server 2008, Win7, Server 2008 R2. Er nutzt die erweiterten Rechte von Antivirenprogrammen offensiv, indem er je nach installiertem Programm unterschiedliche infizierte dynamisch gelinkte Bibliotheken (DLLs) in das System injiziert.[1] So kann sich der Wurm an einen vertrauenswürdigen Prozess hängen.

Außerdem kann Stuxnet auch beim Starten des Betriebssystems geladen werden.[1] Dafür nutzt er einen digital signierten Treiber mit gestohlenem Zertifikat. Der signierte Treiber half, ein *Kernel Mode Rootkit* zu installieren, ohne dass der Nutzer darüber benachrichtigt wird, um länger unerkannt zu bleiben.

Ebenfalls kann der Wurm eine Verbindung zu einem Command-and-Control-Server aufbauen, die Konfiguration des Systems übermitteln und Updates herunterladen. Dabei umgeht er viele Firewalls und Intrusion-Detection-Systeme, da die Kommunikation auf HTTP basiert und wie normale Webseitenanfragen aussieht. Die Konfiguration des Systems wird dabei als Argument der Anfrage übergeben. Er kann sich aber auch lokal durch eine neue Infektion aktualisieren.[1]

Einem Mitarbeiter von Microsoft gemäß, der sich ebenfalls mit dem Wurm beschäftigt hat, waren zwei der vier Zero-Day-Exploits allerdings seit Jahren (mehr oder weniger) bekannt. Die Sicherheitslücke der Wechseldatenträger zum Ausführen von beliebigem Code mit den angemeldeten Nutzerrechten war 2011 schon seit sieben Jahren bekannt. Da die beiden Sicherheitslücken aber nicht oft ausgenutzt wurden, wurden sie von Microsoft nicht durch einen Security-Patch gefixt, was nach Stuxnet allerdings nachgeholt wurde.[2]

Der PLC war das eigentliche Ziel. Zunächst scannt Stuxnet das infizierte System, um die Systemkonfiguration zu analysieren. Siemens Step-7-Software oder WinCC, die üblicherweise zur Wartung von PLCs verwendet werden, muss installiert sein. Falls die Software vorliegt, werden mit Schadcode infizierte DLLs injiziert, über die der Wurm mit dem PLC kommuniziert. Außerdem muss eine Verbindung zu einem PLC mit spezifischen CPUs vorhanden sein. Nur dann wird der Wurm aktiv.[1]



By Starkus01 (Own work), CC BY-SA 4.0

Aus der Analyse des Wurms geht hervor, dass er nach niedrigharmonischen Frequenzumrichtern *(low-harmonic Frequency Converter Drives)* der Unternehmen Vacon (Finnland) und Fararo Paya (Iran) suchte, und zwar anhand eines 16-Bit-Wortes, mit dem Geräte identifiziert werden, die am Profibus des PLC angeschlossen sind.[3] Diese Frequenzumrichter, die von den PLCs gesteuert werden, steuern wiederum die Geschwindigkeit eines anderen Geräts, wie beispielsweise eines Motors. (Anmerkung: Diese Art von Frequenzumrichtern sind in vielen Ländern exportbeschränkt; in den USA sind beispielsweise Frequenzumrichter über 600 Hz von der U.S. Nuclear Regulatory Commission exportbeschränkt, da sie sich für die Urananreicherung nutzen lassen.[4])

Stuxnet hatte zwei Payloads für die PLCs: Der erste veränderte die Rotationsgeschwindigkeit des Motors, um das angetriebene Gerät zu beschädigen. Iterativ wird die Geschwindigkeit in kurzen Abständen von 1410 Hz auf 2 Hz und dann wieder auf 1064 Hz gesetzt. Die normale Frequenz liegt zwischen 807 und 1210 Hz. Der zweite war eine Art *Man-in-the-Middle-Attack*, um die Aktion des ersten Payloads zu verstecken, indem normales Verhalten vorgetäuscht wird. Dafür zeichnete es die Kommunikation zwischen PLC und Steuerungsrechner auf und sendete diese Daten anstatt den tatsächlichen, während es die modifizierten Operationen des PLC ausführte (nach Mikko Hypponen, Chief-Research-Officer, F-Secure[5]).

Einordnung

Das eigentliche Ziel von Stuxnet war also nicht die Infektion von Millionen von Systemen, sondern die Zerstörung eines vorher genau spezifizierten Systems. Der Wurm wurde am 17. Juni 2010 von Sergey Ulasen, Leiter des russischen IT-Security-Unternehmens VirusBlokAda, entdeckt, als er über ein ungewöhnliches

Problem auf Rechnern informiert wurde, die im Zusammenhang mit dem Iranischen Atomprogramm stehen.[5] Die Umstände seines Auftretens im Zusammenhang mit Anlagen des iranischen Atomprogramms, der primäre Offline-Verbreitungsweg und der extrem hohe Aufwand zur Programmierung des Wurms legten den Schluss nahe, dass Stuxnet eine gezielte Attacke auf das iranische Atomprogramm war.[6] Wahrscheinliches Ziel war die Urananreicherungsanlage in Natanz, Iran.[5] Aber auch in China waren mehrere Millionen Systeme infiziert.[6] Allerdings hat im November 2010 der damalige iranische Präsident Ahmadinejad öffentlich zugegeben, dass ein Angriff auf die Zentrifugen der Anlage stattfand.[5] Laut Symantec erfolgte der Angriff in drei Wellen mit drei leicht geänderten Varianten des Wurms.[1]

Durch die Anzahl an Exploits und die Vielzahl an Möglichkeiten, durch die sich der Wurm verbreiten und seine Schadroutinen ausführen konnte, lässt sich schließen, dass die Angreifer eine hohe Infektionsrate beabsichtigt haben. Es ist außerdem davon auszugehen, dass die Komponenten des Wurms von unterschiedlichen Personen entwickelt wurden und dann in ein gemeinsames Framework gefügt wurden.[6] Hier ist auch die Zuverlässigkeit des Wurms bemerkenswert. Die Angreifer zielten auf 100 %ige Zuverlässigkeit. So funktionieren die Exploits und Rootkits nicht probabilistisch – sie hätten damit auch zu Fehlern führen können, die das System zum Absturz gebracht hätten –, sondern exakt und wie bereits angemerkt mit einem hohen Wirkungsgrad.

Die Angreifer mussten eingehende Kenntnisse gehabt haben und auch die Möglichkeit, die Angriffe in realen Systemen zu testen.[6] Das heißt, sie mussten die Rechner- und Netzwerkarchitektur relativ gut kennen; wichtiger ist aber die genaue Spezifikation der Zentrifugen, um diese tatsächlich zu zerstören. Diese Informationen wurden wahrscheinlich durch Geheimdienste beschafft. Anzumerken ist, dass weltweit in Urananreicherungsanlagen zwar zum Teil unterschiedliche Hardware eingesetzt wird, der Prozess zur Urananreicherung aber überall derselbe ist (nach Olli Heinonen, *International Atomic Energy Agency*).[3] Diese Kenntnisse waren aber offensichtlich vorhanden, da beispielsweise die genaue Anzahl der Zentrifugen im Quellcode einprogrammiert wurde. So berichtet der Control-System-Security-Consultant Ralph Langner[7,8], dass es sechs Gruppen von Zentrifugen gab, wobei jede Gruppe aus 164 Einträgen bestand. Diese Zahlen stehen im Quellcode und sind in öffentlich zugänglichem Bildmaterial zu finden. Es ist also anzunehmen, dass den Angreifern die Hardware zur Evaluation der Schadensroutinen zur Verfügung stand, da Testen durch reine Simulation hier extrem unwahrscheinlich ist.[6,8] Dadurch sind erhebliche Kosten entstanden. Da es sich aber um Standard-Hardware handelt, ist das Beschaffen ohne Weiteres möglich.

Stuxnet selbst ist vollkommen konstruiert und auch aus den Command-and-Control-Servern lässt sich nichts folgern – es gibt aus technischer Sicht keine Indizien, wer hinter dem Angriff steckt. Folglich ist so keine sichere Attribution möglich. Die oben ausgeführten Indikatoren wie Komplexität und Kosten sind starke Indizien für staatliches Mitwirken.

Die am weitesten verbreitete Theorie, wer hinter diesem Angriff steckt, wurde vor allem durch den Autor David Sanger propagiert. Er ist der Washington-Korrespondent der *New York Times* sowie National-Security-Korrespondent und schrieb in dem 2012 erschienenen Buch *Confront and Conceal* über Stuxnet. Laut Sanger wurde Stuxnet vom US-Geheimdienst NSA gemeinsam mit einer geheimen israelischen Einheit entwickelt.[9,10,11] Seine Darstellung basiere auf in 18 Monaten geführten Interviews mit gegenwärtigen und ehemaligen amerikanischen, europäischen und israelischen Beamten, die in das Programm involviert gewesen sein sollen. Keine der Quellen wird namentlich genannt und weite Teile des Programms seien „bis heute streng geheim“[11]. Es gab allerdings nie öffentlich einen stichhaltigen Beweis, Israel oder die USA mit Stuxnet in Verbindung zu bringen, weder Israel noch die USA haben offiziell zugegeben, in irgendeiner Weise in die Entwicklung oder Verbreitung von Stuxnet involviert gewesen zu sein. Die *New York Times* berichtete,[10] dass Stuxnet Teil einer größeren Operation mit dem Namen *Olympic Games* sei. Später berichtete die *Washington Post*[12], dass die Malware mit dem Namen *Flame* ebenfalls Teil dieser Operation sei. Nach der Analyse des Codes berichtete *Kaspersky Lab*, dass es eine starke Beziehung zwischen Stuxnet und Flame gibt.[13]

2016 veröffentlichte Alex Gibney eine Dokumentation über Stuxnet mit dem Titel *Zero Days*[3]. Hier wird die gleiche Argumentation geführt. Im Film werden mindestens fünf geheime US-Militär- oder Geheimdienstquellen mit direktem Wissen von den Programmen und Operationen zitiert. Um die Identität zu verbergen, werden sie als „NSA Source“ zusammengefasst. Diese fiktive Quelle gibt zu, dass die NSA an Stuxnet beteiligt war und dass es sich um eine große internationale Operation handelt, bei der viele Militärs und Geheimdienstorganisationen beteiligt waren. Von US-Seite waren die USA Geheimdienste CIA und NSA wie auch das Military Cyber Command beteiligt. Der britische Geheimdienst GCHQ war für die Aufklärung zuständig. An anderer Stelle heißt es, er sei auch für das Deployment des Angriffes gegen die iranischen Anlagen zuständig gewesen. Der wesentliche Teil wurde allerdings von Israel durchgeführt. So war der israelische Auslandsgeheimdienst Mossad beteiligt und der technische Teil wurde von einer Einheit mit dem Namen *Unit 8200* durchgeführt. Durch die Ansiedlung des Cyber Commands beim Militär hat es die Autorität, solche Waffen zu entwickeln. Michael Hayden, der ehemalige Direktor der NSA und auch der CIA, hat es wie folgt kommentiert: „The NSA has the ability to do these things; Cyber-Command has the authority to do these things“.[3] Anzumerken ist, dass das *U.S. Cyber Command* in demselben Gebäude wie die NSA sitzt und die Zusammenarbeit äußerst eng ist. Es wird behauptet, dass Israel den Wurm vor dem Deployment modifiziert hat, um die Iranischen Atomanlagen anzugreifen. Sie machten ihn viel aggressiver im Vergleich zur vorherigen Version. Diese Version wurde dann eigenmächtig ausgeliefert und später von Security-Forschern entdeckt und analysiert.

Stuxnet sei aber auch im Zusammenhang mit der Operation NITRO ZEUS zu sehen. Im Film werden dazu folgende Behauptungen aufgestellt:[3] Die Operationen unter NITRO ZEUS beinhalten als Ziel Irans Industrieanlagen, Command-and-Control, Luftverteidigung, Transportwesen, aber auch das Stromnetz. Die Quellen behaupten, dass in NITRO ZEUS Hunderte von Personen über mehrere Jahre involviert waren und es schon Hunderte von Millionen Dollar gekostet hat. Das Ziel sei stören, abwarten und zerstören (*disrupt, degrade and destroy*) iranischer Infrastruktur mit Code, der keine Beweise liefert, wer für die An-

griffe verantwortlich ist. US-Hacker, die im Remote Operations Center (ROC) in Fort Meade, Maryland, USA, arbeiten, haben große Teile von Irans kritischer Infrastruktur unter ihre Kontrolle gebracht und sind in der Situation, diese jederzeit, beispielsweise zeitgleich mit militärischen Operationen, herunterfahren zu können. Im Film heißt es aber auch, dass es innerhalb des U.S. State Department und der NSA Menschen gibt, die diese Operation, also die Deaktivierung von ziviler als auch militärischer Infrastruktur, legal und ethisch bedenklich finden.

Diese Darstellung klingt plausibel. Andererseits ist diese Behauptung, die rein auf Interviews basiert, ohne jeglichen Beweis auch sehr zweifelhaft. Zwar ist spätestens durch die Enthüllungen von Edward Snowden bekannt, dass die NSA massiv an der Entwicklung von Exploits arbeitet, aber es sollte jeder/m auch klar sein, dass das Knowhow weltweit verfügbar ist und mindestens alle Industrieländer massiv an offensiven Waffen arbeiten. Die Komplexität und Kosten für Malware, die mit Stuxnet vergleichbar ist, sind zwar für die meisten Angreifer unrealistisch, für Nationalstaaten ist dieses aber keineswegs der Fall: Diese Waffen sind vergleichsweise günstig.

Fazit

Nationalstaaten haben die Ressourcen und das Know-how, um sowohl zivile als auch militärische Infrastruktur durch Schadsoftware anzugreifen und gegebenenfalls auch zu zerstören. Wahrscheinlich war Stuxnet der erste Fall, bei dem das auf einem hohen technischen Niveau passiert ist.

Weil die Attribution so schwierig bzw. oft unmöglich ist, wird bei der Suche nach den Verursachern oft nach dem Prinzip des *cui bono* (w*em zum Vorteil?)* verfahren. Diese Argumentation ist äußerst problematisch, da bestimmte Ereignisse sich aus unterschiedlichsten Gründen für unterschiedliche Akteure zum Vorteil entwickeln können. Oft werden Angriffe politisch instrumentalisiert, ohne dass eine klare Attribution gegen die Gegner möglich ist. Oft wird dabei wie folgt verfahren: Aus einer schwachen Argumentation beim ersten Fund wird ein leichter Verdacht beim zweiten Fund und ein erhärteter Verdacht beim dritten Fund, obwohl zu keinem Zeitpunkt echte Beweise vorliegen. Metadaten sind nachträglich fälschbar und echte Profis würden die Informationen nicht in der Malware mit ausliefern. Der Punkt ist aber: Aus Indizien werden – auch durch die Medien – Fakten. Deshalb bleibt es wichtig, die offensiven Fähigkeiten auf unterschiedlichen Ebenen genau zu analysieren. Das umfasst sowohl technische Analysen, um fundierte Kenntnisse und Beweise zu liefern, als auch strukturelle Analysen zu Gesetzesänderungen, dem Ausbau von Streitkräften, Hochrüsten von Geheimdiensten und Militärs, etc. Wichtig bleibt auch, Infrastrukturen und Rechte von Journalist.innen und Medien aufrecht zu halten, damit Whistleblower sicher Dokumente befreien können, um Licht ins Dunkel zu bringen.

Referenzen

1 *Falliere N, O'Murchu L, Chien E (2011) W32.Stuxnet Dossier. Symantec Security Response, Version 1.4, Feb. 2011, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf*

2 *Dang B, Ferrie P (2010) Adventures in analyzing Stuxnet, 27. Chaos Communication Congress (27c3), https://media.ccc.de/v/27c3-4245-en-adventures_in_analyzing_stuxnet*

3 *Gibnez A (2016) Zero Days. Dokumentation*

4 *Halliday J (2010) Stuxnet worm is aimed to sabotage Iran's nuclear ambition, new research shows. The Guardian, 16.11.2010, https://www.theguardian.com/technology/2010/nov/16/stuxnet-worm-iran-nuclear*

5 *Hammersley B (2014) Cybercrimes Episode 5: Cyber War. BBC News, Reportage*

6 *Gaycken S (2011) Cyberwar*

7 *Langner R (2013) To kill a centrifuge: A technical analysis of what Stuxnet's creators tried to achieve. The Langner Group, Nov. 2013, https://www.langner.com/wp-content/uploads/2017/04/To-kill-a-centrifuge.pdf*

8 *Langner R (2012) Stuxnet attack code deep dive. SCADA Security Scientific Symposium, https://www.youtube.com/watch?v=zBjmm48zwQU*

9 *Sanger DE (2012) Confront and conceal: Obama's secret wars and surprising use of American power. Crown*

10 *Sanger DE (2012) Obama order sped up wave of cyberattacks against Iran. The New York Times, 1.6.2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&hp&pagewanted=all*

11 *Stöcker C (2012) Enthüllung über Stuxnet-Virus: Obamas Cyber-Angriff auf Irans Atomanlagen. Spiegel Online, 1.6.2012, http://www.spiegel.de/netzwelt/netzpolitik/usa-und-israel-sollen-stuxnet-virus-gegen-iran-entwickelt-haben-a-836401.htm*

12 *Nakashima E, Miller G, Tate J (2012) U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say. The Washington Post, 19.6.2012, http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html*

13 *Kaspersky Lab (2012) Resource 207: Kaspersky Lab Research proves that Stuxnet and Flame developers are connected. Press Release, 11.6.2012, http://newsroom.kaspersky.eu/fileadmin/user_upload/en/Images/Lifestyle/20120611_Kaspersky_Lab_Press_Release_Flame_Stuxnet_cooperation_final_-_UK.pdf*

Aaron Lye

Aaron Lye ist Informatiker und wissenschaftlicher Mitarbeiter in der Arbeitsgruppe *Technische Informatik und IT-Sicherheit* an der Universität Bremen. Darüber hinaus engagiert er sich im Bereich Kriegsführung, Überwachung und Repression durch Informationstechnik unter anderem im FIfF.