CERT.at Technical Report

Erkennung von Stuxnet im eigenen Unternehmen

Karlsplatz 1/2/9
A-1010 Wien
Tel: +43 1 505 64 16 / 78
Fax: +43 1 505 64 16 / 79
office@cert.at
www.cert.at

Release Date: 2010/09/27
Last Updated: 2010/09/27, public version 1

Author: Christian Proschinger, L. Aaron Kaplan
Email: {proschinger,kaplan}@cert.at

Zusammenfassung

Aktuell kursiert Schadsoftware, die die Manipulation von industriellen Steuerungsanlagen der Marke Siemens SIMATIC zum Ziel hat. Die aktuelle Schadsoftware („Malware“) verbreitet sich über mehrere Schwachstellen in Microsoft Windows und infiziert, über die zur Steuerung und Programmierung der Anlagen (SIMATIC, WinCC, PCS7) verwendeten Windows PCs, die industriellen Anlagen selbst. Die Auswirkungen können von Industriespionage, über sicherheitsrelevante Fehlfunktionen in den Steuerungssystemen bis zu Systemausfällen führen. Es sind daher entsprechende Maßnahmen zur Erkennung von Infektionen und Absicherung der Anlagen zu treffen.

Der Hersteller Siemens stellt eine Anleitung zur Kontrolle und Bereinigung der Systeme zur Verfügung.

Der vorliegende Bericht zeigt auf, wie man lokal und mittels Netzwerkmonitoring feststellen kann, ob potentiell eine Infektion im eigenen Unternehmen stattgefunden hat.

Zielpublikum

Der vorliegende Bericht ist öffentlich. Er richtet sich an System- und Netzwerkadministratoren in österreichischen Unternehmen und hat das Ziel, Hinweise auf eine Infektion mit dem sogenannten “Stuxnet”-Trojaner zu liefern. Der Bericht erhebt keine Ansprüche auf Vollständigkeit oder Korrektheit. Die angeführten Informationen sind zum aktuellen Zeitpunkt nach bestem Wissen recherchiert. Neuere Versionen bzw. Korrekturen zu diesem Bericht werden auf der CERT.at Homepage publiziert.

Technische Detailbeschreibung

Die aktuelle kursierende Malware Stuxnet nutzt für die Infektion diverse Schwachstellen von Microsoft Windows aus, um sich danach mittels Rootkit-Technologien am infizierten System zu verstecken. Dabei manipuliert sie am zur Programmierung verwendeten Rechner den Programmcode für die PLCs (Programmable Logic Controllers). Manipulationen an PLCs sind durch infizierte Windows-PCs nicht mehr feststellbar, da die Malware die Read/Write Requests verändert.
Insbesondere ist es notwendig, vor einer Reprogrammierung der Siemens Steuerungsanlage sicher zu gehen, dass der hierfür verwendete PC (Laptop) definitiv nicht von Stuxnet infiziert wurde.

Betroffene Systeme:

- Windows XP
- Windows Vista
- Windows 7
- Windows Server 2003
- Windows Server 2008

- Siemens SIMATIC Steuerungen
- WinCC
- Step7

CERT.at möchte betonen, dass sämtliche Windows PCs, also auch jene, die nicht mit einer Siemens SIMATIC Steuerung verbunden sind, genauso infiziert sein können. Betroffen sind somit auch Heim-PCs oder PCs in Unternehmen. Dort allerdings wird derzeit kein Schadcode ausgeführt, sondern diese PCs werden nur zur Weiterverbreitung verwendet.

Folgende Schwachstelle wird aktuell für die Verbreitung benutzt

- MS10-061: lnk. Schwachstelle
- MS08-067: "Conficker Schwachstelle"
- MS10-046
- MS10-061

Verbreitungsvektor

- Netzwerk
- Fileshares
- MS-SQL Datenbanken
- USB Stick
- div. Datenträger
- Step 7 Projektdateien

Es wird ersucht, in der eigenen Organisation zu überprüfen, ob Steuerungs- PCs und PLCs infiziert sind. Bitte nehmen Sie dies auch zum Anlassfall und überprüfen die Sicherheit Ihrer Steuerungssysteme:

- Sicherheitsupdates (z.B. vom Basis Betriebssystem), insbesondere MS 10-061, MS 08-067
- Einfallsvektoren (z.B. USB Sticks, Fernwartungen)
- Netzwerksegmentierung

Schadensszenarien

- Industriespionage
- Manipulation von Industrieanlagen
- Ausfälle von Industrieanlagen

Anleitung zur Erkennung von Stuxnet

Offizielle Anleitung von Siemens

Siemens stellt unter

http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&lang=en&objid=43876783&caller=view

eine detaillierte Anleitung zur Überprüfung und Bereinigung eines einzelnen PCs zur Verfügung. CERT.at empfiehlt auch eine Erstüberprüfung mittels Netzwerkmonitoring, sollten Proxy-Logs, Netflow Logs, DNS Query-Logs oder Firewall-Logs vorhanden sein.

Erkennung im Netzwerk

Es können somit IDS-Systeme, Firewall, Proxy- und DNS Server Logfiles zur Erkennung genutzt werden.

Mehrere Wurmvarianten rufen die URL

```
www.mypremierfutbol.com
```

und/oder

```
www.todaysfutbol.com
```

über TCP Port 80 (HTTP) auf.

Im Parameter der URL war jedes Mal der String "66a96e28" enthalten

Obige URLs lösten bisher zu folgenden IP Adressen auf:

```
mypremierfutbol.com
78.111.169.146
193.95.161.220

todaysfutbol.com
193.95.161.220
```

Durch Inspizieren von Proxy- oder Firewall-Logs kann man somit für das gesamte Netzwerk einen ersten Hinweis auf eine Infektion erhalten. Sollte kein verdächtiger Netzwerkverkehr erkennbar sein, heisst das allerdings noch nicht, dass keine Infektion stattgefunden hat.

Referenzen

Windows LNK. Schwachstelle: http://www.microsoft.com/technet/security/Bulletin/MS10-061.mspx

ICS-CERT: http://www.us-cert.gov/control_systems/pdf/ICSA-10-238-01B%20-%20Stuxnet%20Mitigation.pdf

Analyse von Stuxnet: http://research.zscaler.com/2010/07/lnk-cve-2010-2568-stuxnet-incident.html

http://www.symantec.com/connect/de/blogs/exploring-stuxnet-s-plc-infection-process

Weiterführende Hilfe

CERT.at: Computer Emergency Response Team Austria
Karlsplatz 1/2/9
A-1010 Wien
Austria
Telefon: +43 1 5056416 78
Fax: +43 1 5056416 79

Credits

Wir möchten sowohl dem Siemens CERT, BFK als auch Ikarus Software für die freundliche Unterstützung danken.