Wer steckt tatsächlich hinter den Angriffen auf ICS-Ausrüstung?

Autor: Kyle Wilhoit, Senior Threat Researcher bei Trend Micro

Inhaltsverzeichnis

Einleitung

ICS-Systeme (Industrial Control Systems) sind Geräte, Systeme, Netzwerke und Kontrollmechanismen für den Betrieb und/oder die Automatisierung von Industrieprozessen. Diese werden in fast allen Branchen eingesetzt – von der Fahrzeugherstellung und dem Transportwesen bis hin zur Energie- und Wasserversorgung.

SCADA-Netzwerke (SCADA = Supervisory Control and Data Acquisition) stellen Systeme und/oder Netzwerke dar, die mit ICS kommunizieren und den Betreibern Daten für die Überwachung und auch Kontrollmöglichkeiten für das Prozessmanagement liefern. Mit steigender Automatisierung nimmt auch der Einsatz von ICS-/SCADA-Systemen zu.

Infolge der Bedrohungen und Angriffe wie beispielsweise Stuxnet und Flame in den vergangenen zwei Jahren ist die Bedeutung der Sicherheit für ICS-/SCADA-Systeme viel diskutiert worden. Deren Sicherheitsmängel sind wohlbekannt und dokumentiert. Dieser Forschungsbericht geht der Frage nach, wer tatsächlich die mit dem Internet verbundenen ICS-/SCADA-Systeme angreift und aus welchem Grund dies geschieht. Des Weiteren stellt der Bericht Techniken und Best-Practice-Methoden für die Sicherung dieser Systeme vor.

Wie sehen typische ICS-Installationen aus?

ICS-Installationen bestehen in der Regel aus einem vorgelagerten SCADA-Netzwerk, das entweder über eine Firewall oder eine Air-Gap (auch Luftspalte oder Luftpolster genannt) vom Internet abgetrennt ist. Da in vielen ICS-Installationen keine Firewalls vorhanden sind, fehlen sie sowohl in den folgenden Abbildungen und werden auch im Text nicht mehr berücksichtigt.

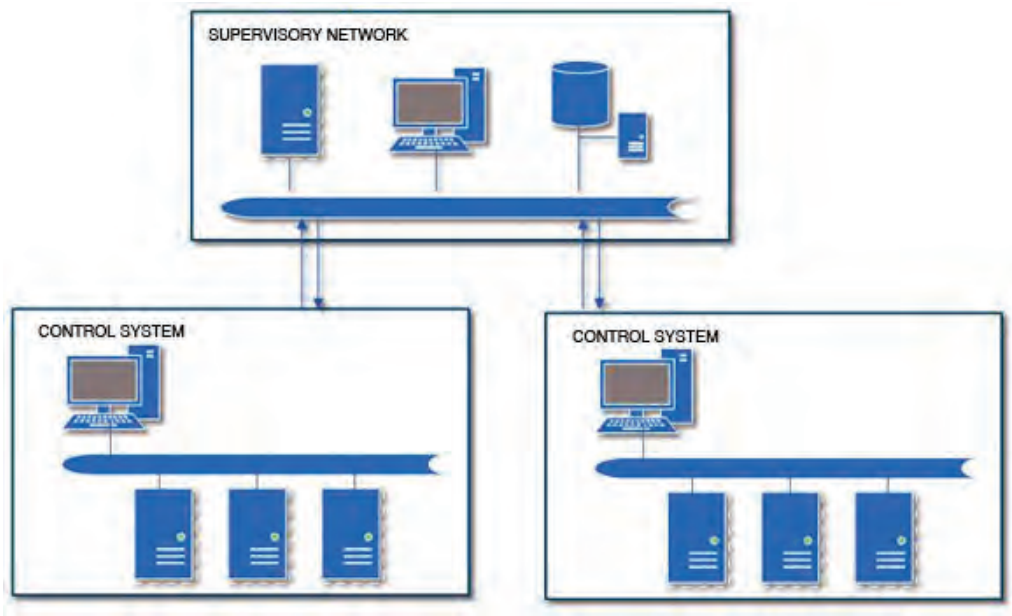

Abbildung 1: Einfache ICS-/SCADA-Systemumgebung

Unterschiede zwischen ICS-/SCADA- und IT- Systemen

Die Sicherheit von ICS-/SCADA-Systemen ähnelt der von IT-Systemen hinsichtlich der Funktionen, doch gibt es große Unterschiede bezüglich der Prioritäten. Die Betreiber dieser Systeme sind leider unterschiedlicher Auffassungen darüber, was Sicherheit bedeutet und wie sie zu gewährleisten ist. Auch die Anforderungen an Verfügbarkeit, Taktiken zur Risikovermeidung, Architektur, Ziele und Leistungsanforderungen sind unterschiedlich.
Vorrang bei der Sicherheit von IT-Systemen hat bekanntlich der Schutz der Daten sowie die Gewährleistung der störungsfreien Arbeit der Mitarbeiter. Sicherheit für ICS-/SCADA-Systeme hingegen konzentriert sich darauf, die Zuverlässigkeit der Daten zu gewährleisten, ohne die Produktivität zu behindern. Aufgrund dieser jeweils spezifischen Schwerpunkte muss die Sicherheit von ICS-/SCADA-Systemen im Vergleich zur IT-Sicherheit aber auch entsprechend spezifisch behandelt werden.

Sicherheit nur als „Beiwerk“

Sicherheit in einem ICS-/SCADA-Netzwerk wird häufig nur nachträglich betrachtet. Vor etwa 20 Jahren, als diese Systeme erstmals in Betrieb gingen, war Sicherheit noch kein Thema. Außerdem hatten viele dieser Systeme auch keine Verbindung zum Internet oder zu LANs. Physische Isolation gewährleistete die Sicherheit am besten.
Mit den Jahren hat sich auch die Zielsetzung der Systeme verändert und damit einhergehend auch deren Konfiguration. Ein System, auf das früher lediglich ein einziger Computer neben einem Förderband Zugriff hatte, wurde nun, ohne große Mühe, über das Internet zugänglich.

Warum sind ICS-/SCADA-Systeme mit Internetverbindung so unsicher?

Vor nicht allzu langer Zeit wurde der Öffentlichkeit die mangelnde Sicherheit von ICS-/SCADA-Geräten deutlich vor Augen geführt. Und trotzdem werden mehr und mehr Geräte ans Internet angeschlossen. Es ist kinderleicht, über „Google-dork-Abfragen“ im Web solche Systeme zu finden, einige von ihnen gibt es dort schon seit 2010 oder noch früher.

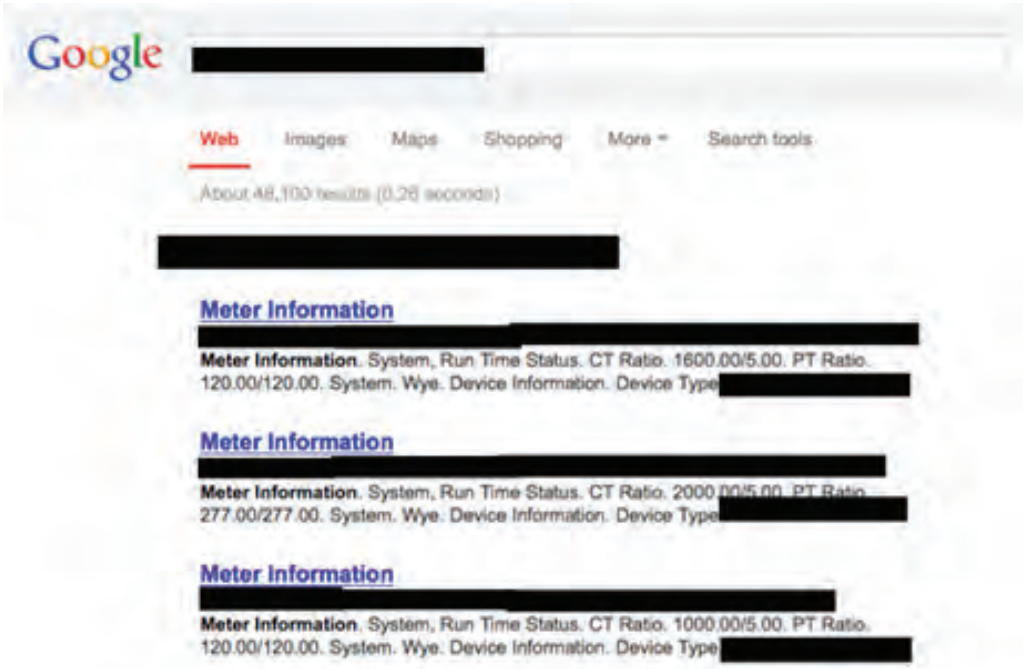

Abbildung 2: Google-dork-Abfragen, die ICS-/SCADA-Systeme als Ergebnis anzeigen

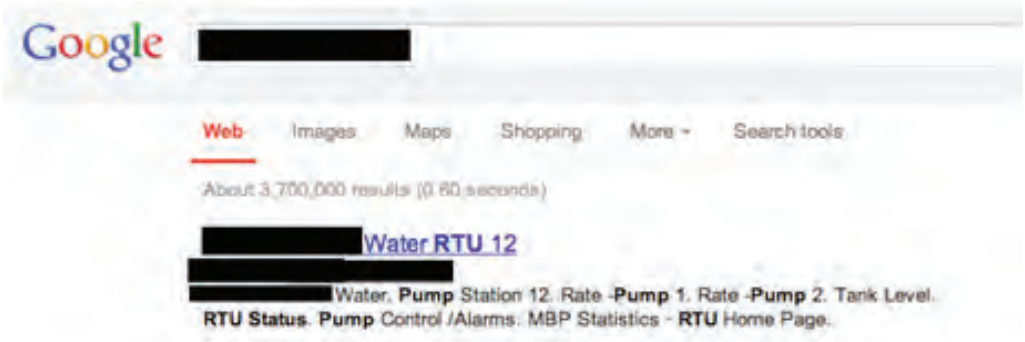

Abbildung 3: Google-dork-Abfrage, die ein Wasserpumpwerk als Ergebnis anzeigt

Zum Zeitpunkt des Tests umfassten diese Geräte trotz Verbindung zum Internet leider keine Sicherheitsvorkehrungen, die einen nicht autorisierten Zugriff verhindert hätten. Das Testteam setzte sich mit den betroffenen Unternehmen und Strafverfolgungsbehörden in Verbindung, und nun sind einige dabei, aufgrund der Testergebnisse Verbesserungen an der Sicherheit vorzunehmen.

Google-dork-Abfragen sind sicherlich hilfreich, um Maschinen zu identifizieren, doch nutzen Angreifer eine andere beliebte Site, nämlich Pastebin, um dort ihre Ergebnisse zu verbreiten. Auch gibt es auf Pastebin immer mehr Einträge, die Daten über ICS-/SCADA-Geräte veröffentlichen, etwa IP-Adressen oder andere der Identifizierung dienliche Informationen.

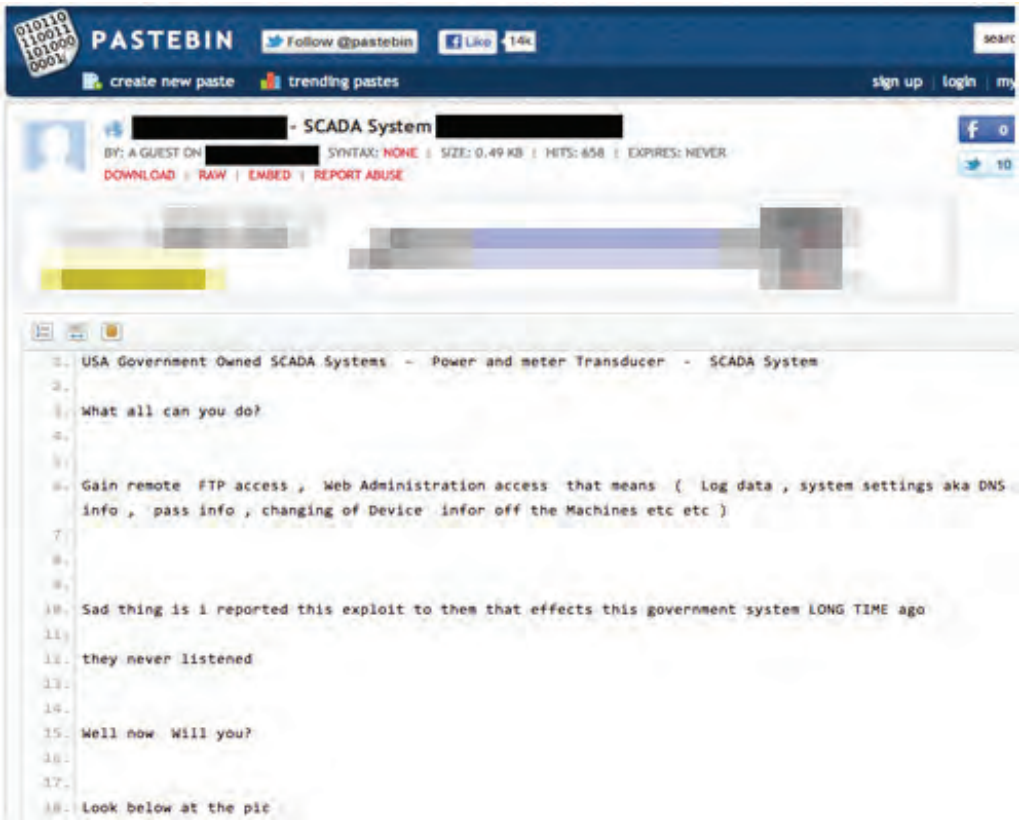

Abbildung 4: Pastebin-Veröffentlichung mit ICS-/SCADA-Geräteinformationen

ICS-/SCADA-Systeme werden immer angegriffen

Nachdem Flame, Duqu und Stuxnet in den Medien so viel Aufmerksamkeit erregt hatten, beschloss Trend Micro Muster zu sammeln, um zu erforschen, was diese tatsächlich angreifen und welche Methoden dabei verwendet werden. Ohne zu wissen, ob sich Angreifer für mit dem Internet verbundene ICS-/SCADA-Systeme tatsächlich interessieren, entwickelte das Team eine Honeypot-Architektur, die verschiedene Typen von ICS-/SCADA-Geräten emuliert und diejenigen nachahmen sollte, die meistens mit dem Internet verbunden sind. Die Honeypots enthielten herkömmliche Schwachstellen, wie sie in den meisten Systemen dieser Art vorkommen, und präsentierten so eine sehr realistische Umgebung.

Zweck des Honeypot-Einsatzes ist es zu prüfen, wer (beziehungsweise was) mit dem Internet verbundene ICS-/SCADA-Geräte angreift und warum. Zudem wollte das Team herausfinden, ob die Angriffe auf diese Systeme zielgerichtet ausgeführt wurden.

Die Sicherheitsvorfälle und Angriffe auf ICS-/SCADA-Systeme haben in der Sicherheitsbranche immer wieder zu Kontroversen über ihre Aussagekraft geführt. Untersuchungen des ICS CERT zufolge hat es allein im Jahr 2012 171 verschiedene Schwachstellen gegeben, wovon eine 55 ICS-Anbieter betroffen hat[1].

Das Honeypot-Architekturdesign setzt auf eine Kombination aus Honeypots mit hoher Interaktion und solchen mit reiner Produktion. Um die Angriffsfläche zu maximieren wurden drei Honeypots erstellt. Alle hatten Verbindung zum Internet und verwendeten drei verschiedene statische IP-Adressen in quer durch die USA verstreuten unterschiedlichen Subnetzen. Ein Honeypot mit hoher Interaktion ahmt die Aktivitäten der realen Systeme nach, und zwar einen PLC-System (Programmable Logic Controller) in einer virtuellen Ubuntu-Instanz auf Amazon EC2.

Diese Cloud-basierte Amazon EC2-Instanz war als Webseite konfiguriert, welche die Seite einer Wasserpumpe imitierte. Als Webserver fungierte ein Apache Webserver mit selbst entwickelten Webseiten, welche die genauen Funktionen eines PLC-Systems nachahmten.

Für die Analyse nutzte das Team die Tools Snort, Honeyd (für SCADA-Protokolle modifiziert), tcpdump und andere Werkzeuge für das Monitoring des Systems[2]. Zusätzlich wurden lokale Log-Dateien an einen zentralen Syslog-Server gesendet, um sicherzustellen, dass die Logs intakt blieben.

[1] *http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf*

[2] *https://www.snort.org/ und http://www.honeyd.org/*

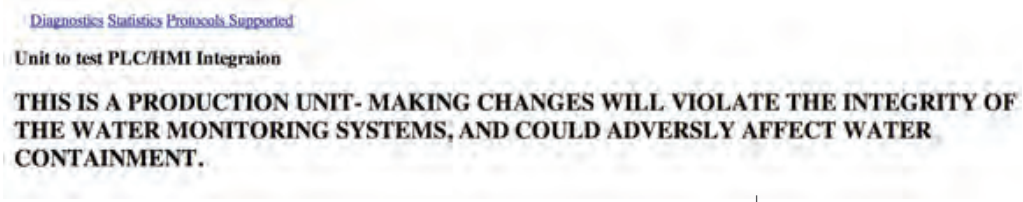

Abbildung 5: Webseite auf dem hochgradig interaktiven Honeypot mit Verbindung zum Internet

Der herkömmliche Webserver, der die vorgebliche Seite der Anlage für Wasserpumpen hostete, konnte auch Port 502- oder Modbus-, FTP und HTTP-Dienste emulieren.

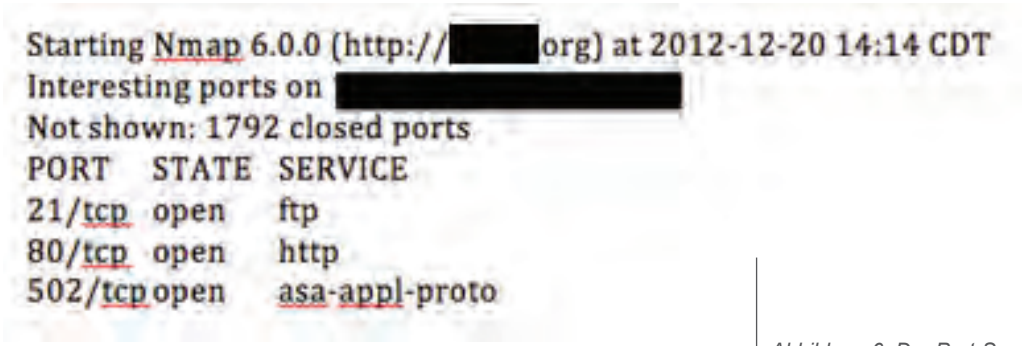

Abbildung 6: Der Port-Scan zeigt offene Ports auf dem hoch interaktiven Honeypot an.

Zusätzlich gab es noch den reinen Produktions-Honeypot, der auf einem Dell DL360-Server mit PLC-Software und einem Webserver gehostet wurde.

Ein reiner Produktions-Honeypot ist ein physischer Server, der ein richtiges Produktionssystem desselben Typs widerspiegelt. In diesem Fall ahmte der Server einer Benutzerschnittstelle (Human Machine Interface, HMI) nach. Wird dieser Server verändert, so modifiziert er hypothetisch einen PLC, der mit dem die HMI verbunden ist.

Abbildung 7: Screenshot des reinen Produktions-Honeypot auf dem Dell DL360-Server

Schließlich setzte das Team noch ein PLC-Gerät namens „nano-10“ von Trangle Research[3] ein, das als reiner Produktions-Honeypot gelten konnte. Es ahmte Temperatur-Controller in einem Werk nach und hatte modifizierbare Einstellungen für die Temperatur, die Gebläsestärke (fan speed) und Licht. Der PLC war mit Standard-Zugangsdaten ausgestattet, eine übliche Vorgehensweise beim Einsatz der Controller. Der Admin-Bereich war kennwortgeschützt und ebenfalls über Standard-Zugangsdaten erreichbar. Alle Einstellungen waren ohne jede Änderung auf „Standard” gestellt, um Angreifer glauben zu lassen, das PLC-System sei eben erst aufgesetzt worden.

Modifizierungen an dem Gerät hätten physisch das PLC-System geändert, was eine katastrophale Änderung für ein SCADA-System im Backend vorgaukeln würde.

Architektur

Es gab also die beiden Architekturtypen für das Honeypot-Design: den hoch interaktiven Honeypot als Falle, welche die Aktivitäten eines Produktionssystems nachahmt und häufig, wie beim vorliegenden Honeypot, auf einem Produktionssystem läuft.

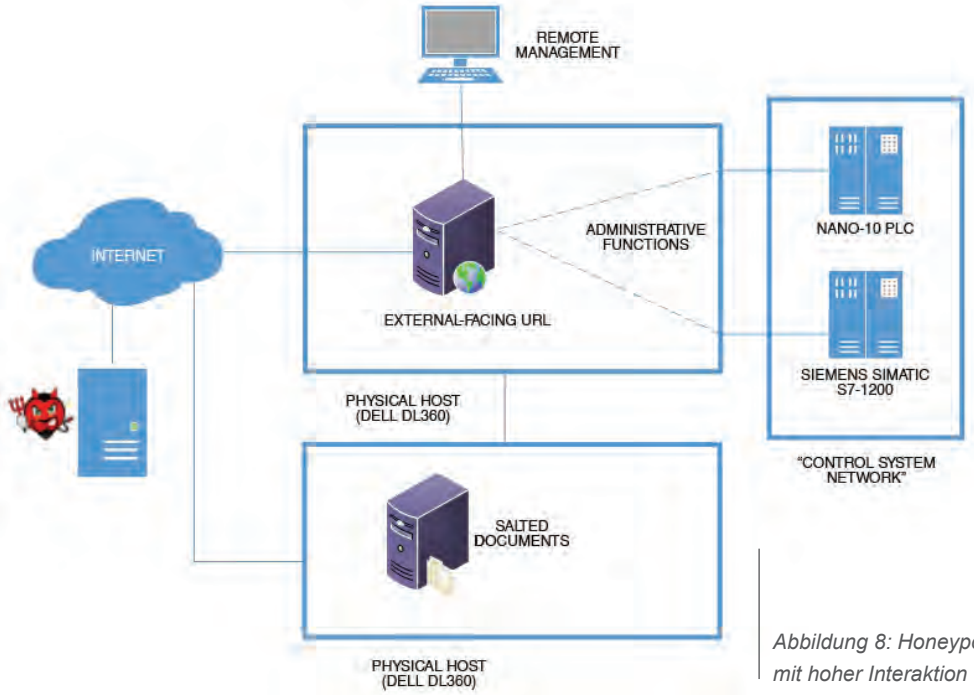

Abbildung 8: Honeypot-Architekturtypus mit hoher Interaktion

[3] *http://www.tri-plc.com/nano10.htm*

Zusätzlich nutzte der ICS-Honeypot auch einen mit geringer Interaktion, also eine Falle, die die Services simuliert, die ein Produktionssystem liefert. Diese Honeypots haben einen sehr geringen Ressourcenverbrauch und ermöglichen bei Bedarf das Erzeugen von mehreren Instanzen

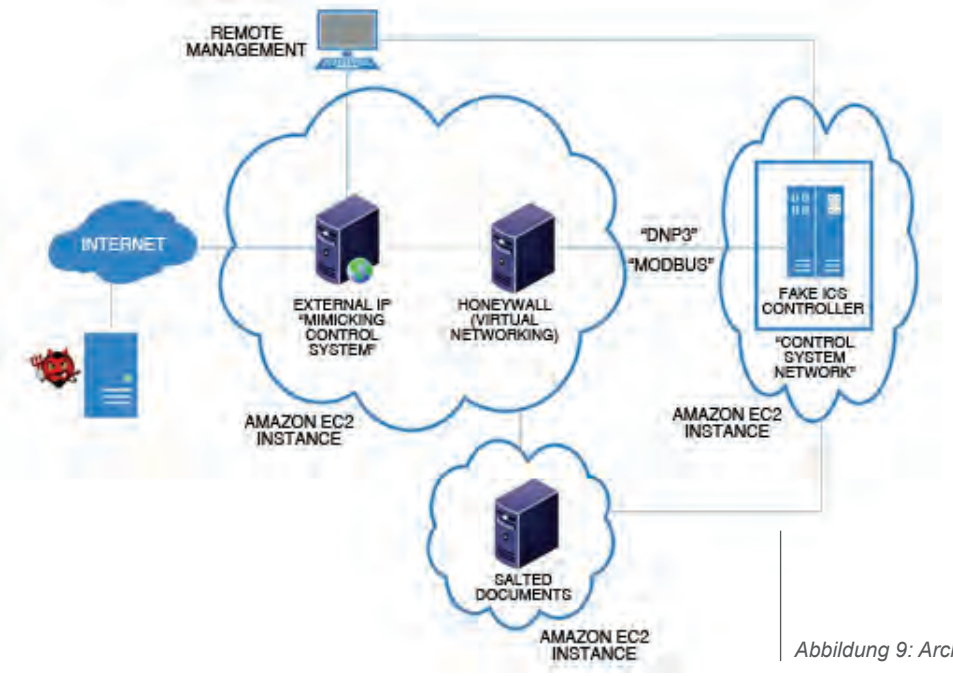

Abbildung 9: Architektur mit Honeypots für geringe Interaktion

Ergebnisse und Metriken

Dem Team ging es nicht um Berichte aufgrund von Port-Scans, Versuchen von automatisierten Angriffen wie SQL Injection oder andere so genannte „Drive-by-Angriffen".

Als Angriff zählte alles, was als Bedrohung für mit dem Internet verbundene ICS-/SCADA-Systeme gelten konnte. Dazu gehören nicht autorisierte Zugriffe auf sichere Bereiche der Site, Änderungen auf erkannten Controllern oder jeder Angriff auf ein für ICS-/SCADA-Geräte typisches Protokoll wie etwa Modbus. Hinzu kommen Versuche des gezielten Zugriffs oder Verursachens eines Sicherheitsvorfalls auf Server.

Beim Launch der Honeypots platzierte das Team die Geräte auf mehrere Arten. Als erstes optimierten die Bedrohungsforscher die Sites für Suchläufe und veröffentlichten diese bei Google, um die Aufmerksamkeit dafür sicherzustellen. Außerdem benannten sie die Server in „SCADA-1", „SCADA-2" und so weiter. Ferner sorgten sie dafür, dass die anderen Honeypot-Einstellungen auf Geräten vorgenommen wurden, die Teil von HD Moores Shodan-Projekt[4] waren, damit interessierte Angreifer diese Server einfach finden konnten.

[4] *http://www.shodanhq.com/*

Bereits nach nur 18 Stunden gab es erste Anzeichen eines Angriffs auf einen der Honeypots. Die Honeypots sammelten weiter Angriffsdaten, und die Ergebnisse waren Besorgnis erregend. Die Berichte enthielten die Daten für 28 Tage, und es gab in der Zeitspanne 39 Angriffe aus 14 verschiedenen Ländern. Davon waren zwölf zu diesem Zeitpunkt jeweils unbekannt („unique“) und ließen sich als „gezielt“ klassifizieren, während 13 von mehreren oder auch demselben Autor an mehreren Tagen wiederholt wurden. Auch diese ließen sich als „gezielt“ und/oder „automatisiert“ beschreiben. Vor allen Angriffen gab es Port-Scans, die von derselben IP-Adresse oder einer IP-Adresse in demselben Netzblock (/27) ausgingen. Die restlichen 14 Angriffe, allesamt ebenfalls gezielt, werden derzeit noch weiter untersucht.

Aus China kamen mit 35 Prozent insgesamt die meisten Angriffsversuche, gefolgt von den USA mit 19 Prozent und Laos mit zwölf Prozent.

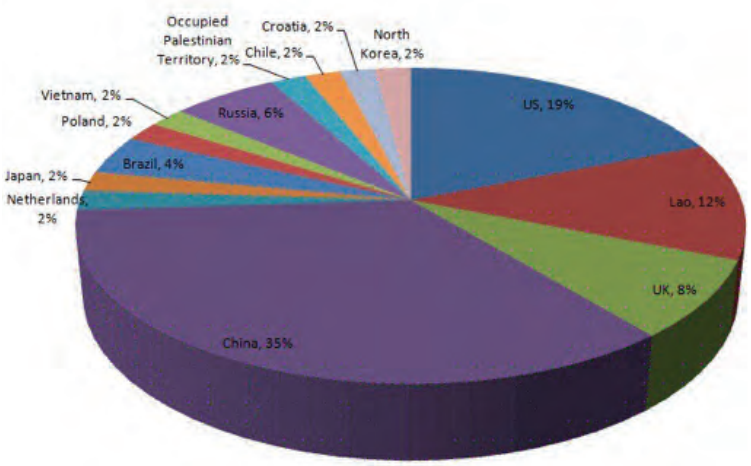

Abbildung 10: Anteil der Angriffsversuche nach Ländern

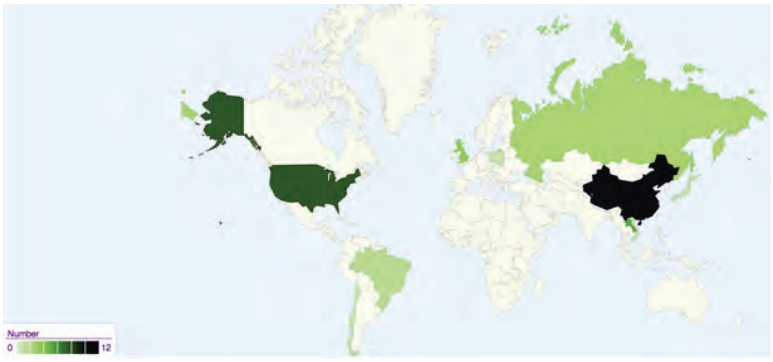

Abbildung 11: Weltkarte mit den Regionen, aus denen die meisten Angriffe (schwarz gefärbt) kamen

Neben der hohen Zahl von Angriffen erschreckt die Häufigkeit derAngriffswiederholungen fast noch mehr. Die meisten Wiederholungstäter gab es in Laos, dicht gefolgt von China. Diese Angreifer kamen häufig zu bestimmten Zeiten alle 24 Stunden wieder und versuchten nicht nur dieselben Schwachstellen auf den Geräten auszunützen, sondern probierten neue Mittel aus, wenn sie in den vorangegangenen Versuchen gescheitert waren. Dies zeigt das hohe Interesse der Täter am Zugang zu den Geräten und auch darum, weitere Schäden zu Verursachen.

Zusätzlich zu den vielen Angriffen auf die Honeypot-Umgebungen gab es eine erstaunlich hohe Zahl von Versuchen, mithilfe von Malware in Server einzudringen. Über den bekannten Malware-Honeypot, Dionaea, konnten die Forscher während des Testlaufs vier Muster sammeln, von denen zwei noch unbekannt waren, denn sie hatten eindeutige MD5-Prüfsummen. Trend Micro analysiert die Muster gerade, um ihre Funktionalität zu bestimmen.

Land	Angriffstypus	Angriffsklassifizierung
USA	Versuch des nicht autorisierten Zugriffs auf diagnostics.php, Versuch der Änderung des Modbus-Verkehrs, Änderung der Lüftergeschwindigkeit der CPU der Wasserpumpe	Versuch des nicht autorisierten Zugriffs und der nicht autorisierten Änderung, Veröffentlichen von Informationen
Großbritannien	Versuch der Änderung der Seite diagnostics.php	Änderung der php Scripts auf der Site
Laos	Versuchter Zugriff auf die Seite diagnostics.php, Änderung der Lüftergeschwindigkeit der CPU der Wasserpumpe	Versuch des nicht autorisierten Zugriffs, Veröffentlichen von Informationen, Änderung des SCADA-Systems
China	Zugriff auf statistics.php, diagnostics.php und protocols.php, Spearphishing-Versuch; versuchte Änderung des Modbus-Verkehrs	Versuch des nicht autorisierten Zugriffs, Veröffentlichen von Informationen
Niederlande	Versuchte Änderung des Modbus-Verkehrs, Änderung der Lüftergeschwindigkeit der CPU der Wasserpumpe	Versuch des nicht autorisierten Zugriffs, Änderung des SCADA-Systems
Japan	Zugriff auf statistics.php-, diagnostics.php- und protocols.php-Seiten	Versuch des nicht autorisierten Zugriffs, Veröffentlichen von Informationen
Brasilien	Versuchte Änderung des Modbus-Verkehrs	Nicht autorisierter Änderungsversuch
Polen	Versuchter Zugriff auf die Seite diagnostics.php-Seite	Versuch des nicht autorisierten Zugriffs, Veröffentlichen von Informationen
Russland	Versuchter Einbruch mithilfe von Malware; Zugriff auf statistics.php, diagnostics.php und protocols.php	Versuchter Einbruch mithilfe von Malware -- unbekannte Malware, Versuch des nicht autorisierten Zugriffs, Veröffentlichen von Informationen
Vietnam	Versuchter Einbruch mithilfe von Malware	Versuchter Einbruch mithilfe von Malware – bekannte Malware - ROJ_MEREDROP.II und WORM_ATAK.AM
Nord Korea	Zugriff auf statistics.php, diagnostics.php und protocols.php	Versuch des nicht autorisierten Zugriffs, Veröffentlichen von Informationen
Chile	Versuchter Zugriff auf diagnostics.php	Versuch des nicht autorisierten Zugriffs, Veröffentlichen von Informationen
Palästinensische Autonomiegebiete	Versuchter Zugriff auf alle sicheren Bereiche des Site, versuchte Änderung des Modbus-Verkehrs	Versuch des nicht autorisierten Zugriffs, Veröffentlichen von Informationen

Tabelle 1: Angriffsversuche

Snort-Ergebnisse

Nicht nur die Honeypot-Umgebung sammelte Daten, sondern auch die Instanzen in Snort, die auf jedem Gerät liefen. Dieses beliebte IDS-System (Intrusion Detection System) bringt mit den Standard-Regeln auch einen sehr hilfreichen Satz an ICS-Regeln mit und zusätzlich solche, die adhoc aufgrund der Angriffsversuche erstellt werden. Für die Honeypot-Umgebung nutzte das Team die Regeln von Digital 5 Bond.

Der Top-Snort-Alarm, der in der Umgebung erzeugt wurde, war Modbus TC non-Modbus-Kommunikation auf TCP-Port 502. Diese Regel wird dann angestoßen, wenn jemand eine Verbindung über Modbus kapert oder nachahmt, um Befehle oder Angriffe an ein anderes Gerät zu schicken.

Außerdem wurden auch die folgenden zwei Regeln angestoßen:
- Nicht autorisierte Read-Anfrage für einen PLC
- Nicht autorisierte Write-Anfrage für einen PLC

Dies passiert üblicherweise dann, wenn ein nicht autorisierter Modbus-Client versucht, Informationen von oder zu einem PLC- oder SCADA-Gerät zu lesen oder zu schreiben. Beide Regeln sind ein Indiz dafür, dass ein ICS-Netzwerk ausspioniert wird – der erste Schritt zu einem Einbruch in ein ICS-Netzwerk.

Die Quellen aller drei Alarme waren die USA, Russland sowie China, wobei die letzteren zwei alle drei Alerts erzeugten, während die USA nur zwei davon generierten. Die Angriffe waren so aufgesetzt, dass es keine Indizien für Drive-by-Scanversuche gab. Jeder Alert wurde auf einer einzigen Instanz und von unterschiedlichen IP-Adressen erzeugt, ohne weitere Port-Scan-Aktivitäten von besagten IP-Adressen – ein Indiz dafür, dass sie sie gezielt ausgesucht worden waren.

Empfehlungen

Glücklicherweise gibt es Kontrollmechanismen, die dafür sorgen, dass ICS-/SCADA-Systeme nicht in Listen auf Websites wie Pastebin landen oder über Google-Suchläufe gefunden werden können.

Einige grundlegende Konfigurations- und Architekturüberlegungen können dazu beitragen, einen entfernten Zugriff auf vertrauenswürdige ICS-Ressourcen zu verhindern. Die meisten Empfehlungen beruhen auf dem Konzept, Sicherheit schon beim Design und bei der Installation ins ICS einzubauen. Dazu gehören fogende Maßnahmen:

- Den Internet-Zugang zu den vertrauenswürdigen Ressourcen soweit möglich deaktivieren.
- Gewährleisten, dass die vertrauenswürdigen Ressourcen immer auf aktuellem Stand sind.
- Dort, wo es sinnvoll ist, Anti-Malware-Schutz in Echtzeit aufzusetzen ebenso wie ein lokales Netzwerk-Scanning von vertrauenswürdigen Hosts in Echtzeit (einige PLC-Systeme unterstützen keine Anti-Malware-Produkte).
- Kombination aus Nutzername/Kennwort für alle Systeme verpflichtend aufsetzen, auch für diejenigen, die nicht als vertrauenswürdig eingestuft sind.
- Einführen sicherer Zugriffsdaten. Keine Default-Daten zulassen!
- Einführen von Zwei-Faktor-Authentifizierung für jedes Nutzerkonto auf allen vertrauenswürdigen Systemen.
- Deaktivieren von unsicheren Remote-Protokollen wie Telnet.
- Deaktivieren aller Protokolle, die nach innen mit den vertrauenswürdigen Ressourcen kommunizieren und nicht unbedingt für die Geschäftsfunktionen vonnöten sind.
- Kontrolle des Auftragnehmerzugriffs; viele ICS-/SCADA-Netzwerke haben nicht lokale Auftragnehmer, und bei diesen ist die Kontrolle der Art ihres Zugriffs auf vertrauenswürdige Ressourcen unerlässlich.
- Netzwerksegmentierung in sichere Ressourcen wie VES-Systeme, ICS- und SCADA-Geräte (zu diesem Thema gibt es einen sehr informativen Blogeintrag zum Thema Netzwerksegmentierung unter http://www.tofinosecurity.com/blog/controlling-stuxnet-%E2%80%93-no-more-flat-networks-please-lets-embrace-security-zones).
- Zugriffskontrolle zu vertrauenswürdigen Geräten aufsetzen. So sollte beispielsweise für den Zugang zu einem segmentierten Netzwerk ein „Bastions-Host“ mit Access Control Lists (ACL) für den Zutritt und Austritt verwendet werden.
- Verbessern der Anmeldung an vertrauenswürdige Umgebungen zusätzlich zur Weitergabe von Log-Dateien an SIEM-Geräte für Backup/Analysen.
- Entwickeln eines Bedrohungs-Modellierungssystems für das Unternehmen. Verständnis dafür schaffen, wer und warum die Systeme angreift.

Schlussfolgerungen

Dieses Papier zeigt, dass mit dem Internet verbundene ICS-Systeme sich bei Angreifern hoher Beliebtheit erfreuen. Solange keine entsprechende ICS-Sicherheit aufgesetzt ist, werden diese Angriffe nicht aufhören und immer raffinierter und destruktiver werden. Sicherheitsexperten gehen davon aus, dass der Trend zu Angriffen geht, die noch weiter reichende Konsequenzen haben. Weitergehende Forschungsarbeiten konzentrieren sich auf die Motive, Quellen, Techniken und die steigende Rafinesse der kriminellen Angreifer.

Über Trend Micro

Trend Micro, der international führende Anbieter für Cloud-Security, ermöglicht Unternehmen und Endanwendern den sicheren Austausch digitaler Informationen. Als Vorreiter bei Server-Security mit mehr als zwanzigjähriger Erfahrung bietet Trend Micro client-, server- und cloud-basierte Sicherheitslösungen an. Diese Lösungen für Internet-Content-Security und Threat-Management erkennen neue Bedrohungen schneller und sichern Daten in physischen, virtualisierten und Cloud-Umgebungen umfassend ab. Die auf der Cloud-Computing-Infrastruktur des Trend Micro Smart Protection Network basierenden Technologien, Lösungen und Dienstleistungen wehren Bedrohungen dort ab, wo sie entstehen: im Internet. Unterstützt werden sie dabei von mehr als 1.000 weltweit tätigen Sicherheits-Experten. Trend Micro ist ein transnationales Unternehmen mit Hauptsitz in Tokio und bietet seine Sicherheitslösungen über Vertriebspartner weltweit an.
www.trendmicro.de

Securing Your Journey to the Cloud

Ihr kostenfreier Kontakt zu Trend Micro:

D: 0800 330 4533 oder sales_info@trendmicro.de
AT: 0800 880 903 oder sales_info@trendmicro.at
CH: 0800 330 453 oder sales_info@trendmicro.ch

TREND MICRO Deutschland GmbH

Central & Eastern Europe
Zeppelinstraße 1
85399 Hallbergmoos
Tel: +49 811 88990-700
Fax: +49 811 88990-799
www.trendmicro.com

Trend Micro (Schweiz) GmbH

Schaffhauserstrasse 104
CH-8152 Glattbrugg
Tel: +41 44 828 60 80
Fax: +41 44 828 60 81
www.trendmicro.com