MEDIENMITTEILUNG

Hochkarätige Lösungen gegen Cyber-Bedrohungen

Ontrex nimmt ReversingLabs ins Vertriebs- und Kompetenzprogramm auf

Die Lösungen von ReversingLabs erkennen und analysieren Schadcode im Webverkehr, in E-Mail Anhängen, im internen Netzwerkverkehr und in vorhandenen Dateibeständen mit einer industrieweit einzigartigen Technologie: Die Active File Decomposition analysiert Dateien innert Millisekunden und ermittelt das Bedrohungsniveau. Im Vergleich zu anderen Threat-Detection-and-Analysis-Lösungen ist diese statische Analyse massiv schneller und auch zuverlässiger. Ontrex hat die Produkte von ReversingLabs neu ins Portfolio aufgenommen und unterstützt Unternehmen mit Proofs-of-Concept und Schulungen.

Brüttisellen, 17. September 2015 – Gezielte Cyber-Attacken mit raffiniert versteckten und spezifisch auf die avisierten Unternehmen programmierten Schadcodes nehmen weiter zu. Mit konventionellen Sicherheitslösungen werden solche Attacken oft erst erkannt, wenn es zu spät ist. In der Industriebranche beispielsweise liegt der Durchschnitt bei 237 Tagen nach dem Befall. Die Gründe dafür liegen unter anderem im hohen Aufwand zur Untersuchung des gesamten Datenverkehrs. Um solchen Angriffen wirkungsvoll zu begegnen, müssen Unternehmen ein tiefergehendes Verständnis der Bedrohungslage entwickeln. Der Sicherheitsspezialist ReversingLabs mit Sitz in Cambridge, Massachusetts und Niederlassungen in Zürich und Zagreb hat bahnbrechende neue Technologien namens Active File Decomposition (AFD) und RHA (Reverse Hashing Algorithm) zum Aufspüren, Analysieren und Einordnen von Cyber-Bedrohungen entwickelt. Die Produkte von ReversingLabs ermöglichen dank bisher unerreicht hoher Geschwindigkeit eine umfassende Bedrohungsanalyse des gesamten Web-, E-Mail- und Datenverkehrs respektive heruntergeladenen Dateien aller Art und können riesige bereits vorhandene Datenbestände analysieren. Somit werden auch ältere, noch nicht identifizierte Schadcodes entdeckt und lösen eine bekannte Problematik herkömmlicher Sicherheitslösungen (Anti-Virus und sogar Sandbox-basierender Schadcode-Analyse). Diese liegt darin, dass die Entwickler von Malware wissen, wie die Lösungen funktionieren. Sie können ihre Programme dadurch «unsichtbar» an solchen Plattformen vorbeischleusen. Das US-amerikanische Forschungsinstitut Lastline Labs hat vom Mai 2013 bis im Juni 2014 47 Hersteller von Anti-Virus-Lösungen untersucht. Das Ergebnis: Keine der Lösungen entdeckte alle Angriffe und selbst ein über zwölf Monate alter Schadcode wurde von 10 Prozent der Hersteller nicht identifiziert.

Einzigartige Technologie

Die Active File Decomposition (AFD) kombiniert verschiedene Analysetechniken, um in Dateien versteckten Schadcode zu ermitteln. Jede Datei wird dabei in ihre Komponenten zerlegt: AFD identifiziert, dearchiviert, entschleiert und entpackt die gesamte Objektstruktur der Datei. Jede so gefundene Komponente wird einzeln auf vorhandene Bedrohungsindikatoren (Proactive Threat Indicators, PTI) untersucht. Daraus ergeben sich das Bedrohungsniveau und eine Sofortreputation für die gesamte Datei. Die einzigartige Technologie von ReversingLabs funktioniert

betriebssystemunabhängig mit Dateien von Windows, Unix und OS X sowie Mobilplattformen wie iOS oder Android.

In Millisekunden analysiert
Die ganze Analyse ist innert Millisekunden erledigt, und im Gegensatz zur Analyse anderer Cyberthreat-Lösungen wird kein Code ausgeführt. Somit besteht auch keine Manipulationsmöglichkeit für den Ersteller des Schadcodes. AFD bietet hohe Geschwindigkeit bei höherer Analyse-Genauigkeit, Zuverlässigkeit und Sicherheit und deckt ein breites Spektrum von möglichen Bedrohungen ab.

Über 2 Millionen Updates täglich
Die lokale Analyse wird durch den File-Reputation-Dienst von ReversingLabs unterstützt. Die TitaniumCloud enthält gegen 2 Milliarden Malware- und Goodware-Samples mit über 3000 PTIs pro Datei, darunter detaillierte Informationen über den Inhalt, Angaben zur Herkunft sowie historische Daten zu Bedrohungsfaktoren und Antivirus-Scans: Die Malware-Datenbank wird zweimal täglich mit den Antivirus-Lösungen von 29 Herstellern gescannt. Insgesamt erhält die TitaniumCloud über 2 Millionen Updates pro Tag und kann täglich 7 Milliarden Abfragen bewältigen.

Entdeckt Zero-Day-Malware
RHA ermittelt den Hash-Wert einer Datei, der zum Abgleich mit bestehenden Malware-Informationen benötigt wird, im Gegensatz zu klassischen Hashing-Algorithmen wie MD5 oder SH-1 nicht aufgrund der enthaltenen Bits, sondern berücksichtigt die Eigenschaften der Datei: Verschiedene Dateien erhalten den gleichen RHA-Wert, wenn sie sich funktional ähnlich sind. Ein bestimmter RHA-Wert identifiziert so potenziell tausende leicht unterschiedliche Malware-Dateien, und RHA kann selbst «Zero-Day»-Malware entdecken, die es bisher noch nicht gab.

Differenzierte Produktpalette
Die ReversingLabs-Technologien sind in Form mehrerer sich ergänzender Produkte erhältlich:

- Die Network Security Appliance N1000 extrahiert und analysiert alle Dateien aus dem Web-, E-Mail und Datenverkehr (HTTP, FTP, SMTP, SMB) und entdeckt auf Basis der AFD- und RHA-Technologien auch ausgefeilte und auf Unternehmen individuell zugeschnittene Bedrohungen. Sie überwacht den ein- und ausgehenden sowie den internen Datenverkehr. Monitoring, Konfiguration und Reporting erfolgen über eine anschauliche Weboberfläche. Die N1000-Appliance lässt sich auch in unternehmensweite SIEM- und Datenanalyse-Lösungen integrieren.
- Die Malware Analysis Appliance A1000 ist eine Plug&Play-Lösung zur Schadcode-Analyse in Dateien, erhältlich als Hardware-Appliance, virtuelle Appliance oder Cloud-Service. Sie analysiert die Dateien, speichert die ermittelten PTIs in einer internen Datenbank und stellt die untersuchten Dateien und Dateikomponenten für weitere Analysen bereit. Sie nutzt die File-Reputation-Informationen der TitaniumCloud, optional auch über die File Reputation Appliance T1000.
- Die File Reputation Appliance T1000 ist eine ständig aktualisierte On-Site-Version der TItaniumCloud-Datenbank. Sie kommt dann zum Einsatz, wenn eine besonders hohe

Performance erwünscht ist oder aus Vertraulichkeitsgründen nicht auf einen Cloud-Service zugegriffen werden soll.

- Das Incident Response Toolkit AT1000 besteht aus einer USB-Solid-State-Disk, mit der Dateien auf verdachtsauffälligen Systemen oder in Disk-Images analysiert werden können. Mit dem AT1000 hat man eine portable Malware-Analyseplattform mit Onboard-Reputationsdatenbank zur Hand. Diese Lösung kann auch Schadcode in Firmware identifizieren, was einzigartig ist. - als absolutes Einzelstellungsmerkmal -.
- TItaniumCore setzt die AFD-Technologie in Form einer Softwarelösung für Windows oder Linux um. Die Desktop-Variante ist für die Analyse von bis zu 1000 Samples pro Tag konzipiert. Die Server-Variante bewältigt im selben Zeitraum 100'000 Samples und lässt sich über die Kommandozeile (CLI) und einen SDK für C, C++, .NET und Python in Workflow-Lösungen oder andere Plattformen einbinden.

Als IT-Dienstleister mit langjähriger Erfahrung berät, unterstützt und schult Ontrex seine Kunden unter der Firmenstrategie «Solution Integrity» insbesondere auch dabei, die Produkte von ReversingLabs mit anderen Lösungen aus dem Portfolio zu integrieren, um eine vielschichtige und ganzheitliche Sicherheitslösung mit zentraler Administration zu erreichen.

Ontrex
Ontrex ist ein Schweizer IT-Dienstleister, der sich auf Service-, Security- und System-Management sowie auf Enterprise Mobility Lösungen spezialisiert hat. Als Symantec-Master-Partner, Master-Reseller von helpLine und Nexthink-Platinum-Partner verkauft, entwickelt, implementiert und betreut Ontrex branchenunabhängig Software-Lösungen. In der Schweiz zählt die Ontrex AG derzeit rund 400 Kunden. Das Team besteht aus 55 Mitarbeitenden. www.ontrex.ch, www.ontrexmobile.ch

Medienkontakte:

Ontrex AG
Graziano Gaggioli, CEO
T: +41 44 835 10 38
M: +41 79 509 27 00
graziano.gaggioli@ontrex.ch

Rocco Leone, CTO
T: +41 44 835 10 21
rocco.leone@ontrex.ch

in marketing gmbh
Jolanda Brühwiler
T: +41 44 806 40 52
M: +41 79 671 00 24
jolanda@inmarketing.ch