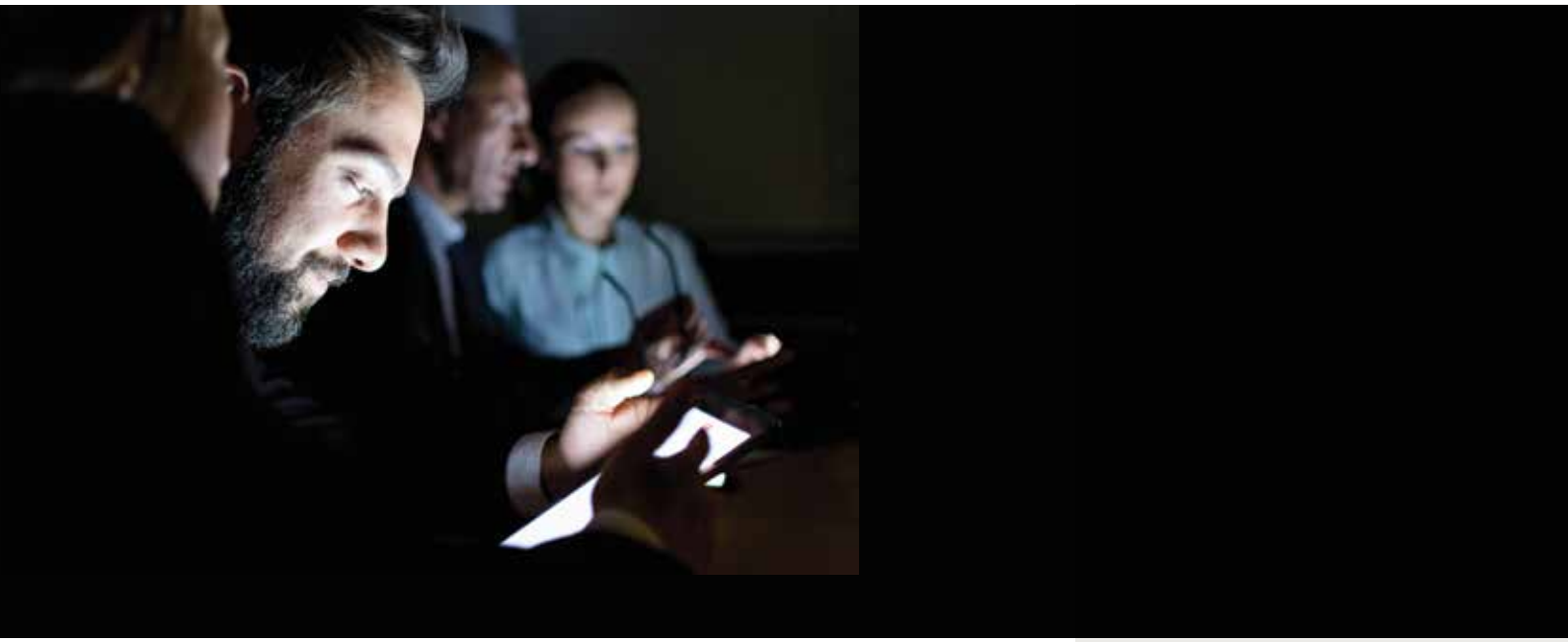
FORTINET

WHITE PAPER

Erst einmal in die Sandbox

Sandboxing-Technologie und ihre praktische Anwendung in der heutigen Bedrohungslandschaft im Fokus



Einleitung

Erst einmal in die Sandbox

Bei Computern steht der Bergriff Sandboxing schon lange für eine sichere, isolierte Umgebung, in der Schadcode ausgeführt werden kann, damit die Forscher ihn analysieren können. Dasselbe Konzept wird jetzt auch von Appliances für die Netzwerksicherheit angewendet, um Netzwerkverkehr auszuführen und zu untersuchen, um Schadcode zu enttarnen, der die herkömmlichen Sicherheitsvorkehrungen bisher unbemerkt passieren konnte.

Da in einer Sandbox komplette Betriebssysteme virtuell emuliert werden können, können verdächtige Programme dort sicher ausgeführt werden, um ihre Aktivitäten zu beobachten. Schädliche Aktivitäten, wie Datei-/Festplattenoperationen, Netzwerkverbindungen, Änderungen der Registrierung/Systemkonfigurationen usw. werden enttarnt, damit Bedrohungen neutralisiert werden können.

Traditionell wurden Sandboxes für Programmdateien verwendet. Neuerdings werden damit auch Anwendungsdaten ausgeführt, in denen sich Schadcode verbergen kann, wie beispielsweise Adobe Flash und JavaScript. Einige Anwendungen, wie Adobe Reader X, verfügen aus demselben Grund über eine eigene integrierte Sandbox. Wenn Reader X beispielsweise beim Öffnen einer PDF bösartigen Code entdeckt, wird dieser in einer Sandbox isoliert, sodass er das Betriebssystem nicht infizieren kann.

Sandboxing – warum jetzt?

Bei Computern steht der Bergriff Sandboxing schon lange für eine sichere, isolierte Umgebung, in der Schadcode ausgeführt werden kann, damit die Forscher ihn analysieren können. Dasselbe Konzept wird jetzt von Appliances für die Netzwerksicherheit angewendet, um Netzwerkverkehr auszuführen und zu untersuchen, um Schadcode zu enttarnen, der die herkömmlichen Sicherheitsvorkehrungen bisher unbemerkt passieren konnte. Da in einer Sandbox komplette Betriebssysteme virtuell emuliert werden können, können verdächtige Programme dort sicher ausgeführt werden, um ihre Aktivitäten zu beobachten. Schädliche Aktivitäten, wie Datei-/Festplattenoperationen, Netzwerkverbindungen, Änderungen der Registrierung/Systemkonfigurationen usw. werden enttarnt, damit Bedrohungen neutralisiert werden können.

Traditionell wurden Sandboxes für Programmdateien verwendet. Neuerdings werden damit auch Anwendungsdaten ausgeführt, in denen sich Schadcode verbergen kann, wie beispielsweise Adobe Flash und JavaScript. Einige Anwendungen, wie Adobe Reader X, verfügen aus demselben Grund über eine eigene integrierte Sandbox. Wenn Reader X beispielsweise beim Öffnen einer PDF bösartigen Code entdeckt, wird dieser in einer Sandbox isoliert, sodass er das Betriebssystem nicht infizieren kann.
Sandboxing – warum jetzt?

Wenn die Sandbox-Technologie so alt ist, warum wird sie dann plötzlich so wichtig? Cyberkriminelle bringen immer mehr über die gängigen Methoden der Sicherheitssysteme in Erfahrung und arbeiten verstärkt an der Erforschung und Entwicklung von Methoden, um Sicherheitsmaßnahmen zu umgehen. Die Sandbox kann uns heute dabei helfen, gut getarnte neue Bedrohungen oder alte Bedrohungen im neuen Gewand aufzuspüren.

Sandbox und proaktive Signaturerkennung

Leider ist Sandboxing ressourcenintensiv. Programme müssen in der Sandbox vollständig ausgeführt werden, damit sie analysiert werden können, und das Erforschen aller Ausführungspfade, einschließlich weiterer Module die der Schadcode möglicherweise zu laden versucht, benötigt Zeit. Deshalb kombiniert Fortinet das Sandboxing mit der proaktiven Signaturerkennung, um Datenverkehr bereits vor Erreichen der Sandbox zu filtern. Im Vergleich zu einer einzelnen Sandbox, geht das viel schneller.

Die traditionelle Signaturerkennung ist reaktiv, denn Signaturen sind nur Fingerabdrücke von Bedrohungen, die bereits erkannt wurden. Fortinets patentierte Compact Pattern Recognition Language (CPRL) ist eine Technologie zur gründlichen, proaktiven Signaturerkennung, die im Rahmen jahrelanger Forschungsarbeit von FortiGuard Labs entwickelt wurde. Eine einzige CPRL-Signatur kann mindestens 50.000 Tarnungen abfangen, in die eine Malware verpackt ist. Zusammen mit dem Sandboxing, kann die proaktive CPRL-Signaturerkennung aktuelle komplexe und persistente Bedrohungen (Advanced Persistent Theats, APT) sowie raffinierter Tarnmechanismen (Advanced Evasion Techniques, AET) engmaschiger bekämpfen.

> „Cyberkriminelle bringen immer mehr über die gängigen Methoden der Sicherheitssysteme in Erfahrung und investieren daher in die Forschung und Entwicklung von Methoden zur Umgehung von Sicherheitsmaßnahmen.“

Komplexe persistente Bedrohungen

Komplexe persistente Bedrohungen sind maßgeschneiderte, gezielte Angriffe. Sie umgehen normale Erkennungsmechanismen, indem sie bisher unbekannte (oder „Zero-Day“) Malware, Exploit-Schwachstellen (nicht geschlossene Sicherheitslücken) verwenden, die von ganz neuen oder anscheinend unverdächtigen URLs und IPs stammen. Ziel ist es, das Zielobjekt mithilfe von ausgeklügelten Programmiermethoden zu infizieren, die Sicherheitsmaßnahmen zu umgehen und möglichst lange unentdeckt zu bleiben.

Advanced Evasion Techniques

Es gibt mehrere Möglichkeiten, wie Bedrohungen Sicherheitshürden umgehen können. Hier einige gängige Methoden zur Umgehung von Sandboxes.

Logikbomben

Die gängigsten Logikbomben sind Zeitbomben, die bereits in groß angelegten Angriffen zum Einsatz kamen. Bei einer Zeitbombe bleibt der Schadcode bis zu einem festgelegten Zeitpunkt verborgen. Der Angreifer kann Malware unbemerkt auf mehreren Systemen installieren und zu einem bestimmten Zeitpunkt alle Bomben gleichzeitig platzen lassen. Andere Logikbomben werden durch Nutzerinteraktionen (Mausklicks, Systemstarts usw.) ausgelöst, die nahe legen, dass sich die Bombe auf einem echten Computer befindet und nicht zur Überprüfung in einer Sandbox-Appliance. Logikbomben sind schwer zu enttarnen, da die Wahrscheinlichkeit, dass ihre auslösenden Bedingungen in der Sandbox erfüllt werden und der manipulierte Ausführungspfad während der Untersuchung aktiviert wird, sehr gering ist. Fortinet schafft die passende Umgebung, um Logikbomben mithilfe von CPRL und einer Analyse der Codeemulation zu enttarnen, bevor der eigentliche Code ausgeführt wird. CPRL führt eine Echtzeitanalyse der tatsächlichen Betriebsanweisungen durch, damit die logischen Bedingungen, die die Bombe auslösen, beobachtet werden können.

Rootkits und Bootkits

Hoch entwickelte Malware enthält häufig eine Rootkit-Komponente, die das Betriebssystem mit Code auf Kernel-Ebene unterwandert, um die Kontrolle über das System zu erlangen. Sandboxes sind für diese Art der Tarnung potenziell anfällig, da auch das Ausgabeverhalten manipuliert sein kann. Darüber hinaus wird das System beim Systemstart durch Bootkits mit Malware infiziert, ein Umstand, den die Sandbox normalerweise nicht beobachtet. Fortinet löst auch dieses Problems mithilfe der CPRL-Erkennung, um raffinierte Rootkit-Bootkit-Routinen aufzuspüren, bevor Sie ausgeführt werden.

Sandbox-Erkennung

Eine weitere ausgeklügelte Umgehungsstrategie besteht darin, die Umgebung zu erkennen. APT-Code kann Routinen enthalten, die versuchen herauszufinden, ob er in einer virtuellen Umgebung ausgeführt wird (könnte auf eine Sandbox hinweisen), oder nach Fingerabdrücken von Sandbox-Umgebungen bestimmter Anbieter suchen. Wenn der Code merkt, dass er sich in einer Sandbox befindet, führt er sein zerstörerisches Werk nicht aus. Mit CPRL kann Code, der nach einer Sandbox sucht, gründlich untersucht, erkannt und aufgezeichnet werden.

Botnet-Befehls- und Steuerungsfenster

Die Befehls- und Steuerungsaktivitäten von Botnets beginnen in der Regel mit einem Dropper. Der Dropper ist ein sauberes Programm, das keine Routine ist. Es stellt eine Verbindung zu einer URL-/IP-Adresse her, um auf Befehl eine Datei herunterzuladen. Der Befehl kann vom Angreifer Stunden, Tage oder Wochen nach der ersten Ausführung gegeben werden. Wenn der Server, mit dem sich der Dropper verbindet, in der Zeit, in der die Sandbox den Code ausführt, schläft, kann keine bösartige Aktivität beobachtet werden. Mit CPRL können ungewöhnliche Programmiertechniken entdeckt werden, die Malware enttarnen, auch wenn sie sich nicht in diesem Zeitfenster offenbart. Zudem ist die Botnet-Überwachung, die Botnet-Aktivitäten in freier Wildbahn aufdeckt, Teil des globalen FortiGuard Verteidigungsnetzwerks.

Netzwerk-Fast-Flux

Raffinierte Malware setzt gegebenenfalls auch Fast-Flux- oder DNS-Technik ein, um eine URL-/IP-Adresse zu ändern, mit der sich der Virus verbindet. Währen der Prüfung in der Sandbox ruft der Virus eine unverdächtige Adresse auf. Im Laufe der Zeit jedoch ändert der Schadcode auf dem Zielcomputer den Pfad zu einer anderen Adresse, die dann die infizierten Daten einschleust. FortiGuard verfolgt Fast-Flux-Netzwerke und meldet die erfassten Daten zu möglichen Bedrohungen an die Sandbox zurück, damit diese sie in den Vorab-Scans nutzen kann. Dabei schaut sich Fortinet, im Gegensatz zur gängigen Praxis anderer Anbieter, die DNS-Ebene an und gleicht nicht nur Listen manipulierter IP-Adressen ab.

Verschlüsselte Archive

Ein uralter Trick bei dem Angreifer Malware einfach in Archiven verschlüsseln. Mit etwas Social Engineering im Nachgang, veranlassen sie das Opfer, die infizierte Datei durch Eingabe eines Kennworts zu öffnen. Da eine Sandbox das Kennwort nicht automatisch eingeben kann, wird die Malware während der Prüfung nicht ausgeführt. Fortinets patentierte Header-Prüfung für komprimierte Archive ermöglicht die Erkennung von Malware-Fingerabdrücken, die durch Verschlüsselung getarnt wurden.

Binär-Packer

Binär-Packer verstecken Malware, indem sie sie in unkenntliche Teilstücke verschlüsseln, die von herkömmlichen Antivirus-Programmen so gut wie nicht analysiert werden können. Der Code wird beim Ausführen entpackt und infiziert den Host. Ähnliche Methoden werden verwendet, um Schadcode in Programmiersprachen, wie JavaScript und Adobes ActionScript für Flash, einzubetten Als Arbeitsspeicher noch ein Thema war, wurde diese Technologie verwendet, um Programmcode zu komprimieren. Heute ist Arbeitsspeicher kein Problem mehr, dennoch werden Binär-Packer häufig verwendet, um Virenscans zu umgehen. Bei JavaScript und ActionScript kann diese Methode auch offiziell als Kopierschutz

eingesetzt werden. Die Antivirus-Engine von FortiGate unterstützt die Enthüllung von Script und die Erkennung vieler Binär-Packer. Sie entpackt Malware in ihr Ursprungsformat, um sie einer gründlichen CPRL-Analyse zu unterziehen. Das ermöglicht die Erkennung und Abwehr in Echtzeit oder verlagert die weitere Ausführung in die Sandbox.

Polymorphe Malware

Polymorphe Malware ändert ihre Gestalt bei jeder Ausführung. Dabei fügt sie unsinnige Programmteile hinzu, um der Entdeckung durch Muster- oder Prüfsummenerkennung zu entgehen. Der Schadcode wird ausgeführt, sobald er durch ein Betriebssystem entpackt wird. Polymorpher Code stellt für traditionelle reaktive Prüfungen eine Herausforderung dar. Fortinet begegnet diesem Problem durch eine Kombination aus proaktiver Antivirus-Engine-Technologie, CPRL und Sandbox. Die Engine kann die Malware in ein natives Format entpacken, um möglichst viel Datenverkehr ressourcensparend zu filtern, um dann den Rest zur gründlicheren Inspektion in der Sandbox auszuführen.

Reproduktion in der Sandbox

Ziel des Sandboxing ist es, das Verhalten von Schadcode in vollem Umfang zu reproduzieren. Im Idealfall entspricht die Ausgabe in der Sandbox dem, was der Code bei Ausführung in der Nutzerumgebung ausgeben würde. In der Praxis sind identische Ergebnisse, aufgrund der Anzahl der beteiligten Variablen, schwer zu erzielen. Das ist, als ob man aus Samenkörnern identische Pflanzen ziehen wollte. Selbst kleinste Abweichungen bei der Menge an Wasser, Licht, Temperatur und Bodenbeschaffenheit führen zu unterschiedlichen Ergebnissen.

Exploits und Zpplications

Hoch entwickelte Malware kann auch in Dokumenten versteckt sein, die ihre Anwendungen (wie Word, Excel oder Adobe Reader) dazu bringen, bösartigen Code auszuführen. Um dieses Verhalten zuverlässig zu reproduzieren, muss die Sandbox eine ganze Reihe von Betriebssystemen durchtesten, auf denen jeweils mehrere Versionen von Anwendungen ausgeführt werden. Dieser Prozess beruht auf Versuch und Irrtum und ist zeit- und kostenintensiv. Viele Sandbox-Lösungen versuchen diesem Problem mit mehr Leistung beizukommen – schnellere Prozessoren, mehr virtuelle Maschinen, mehr Arbeitsspeicher. Aber das ist ineffizient und teuer. Der bessere Ansatz ist es, die Betriebssysteme und Anwendungen nach Marktanteil oder Einsatzhäufigkeit zu gewichten, und sich auf die Umgebungen zu konzentrieren, die das schädliche Verhalten am wahrscheinlichsten auslösen.

32-Bit vs. 64-Bit, Windows XP vs. Windows 7/8

32-Bit-Programme laufen sowohl in 32-Bit- als auch in 64-Bit-Umgebungen, deshalb bevorzugen die Entwickler von

> „Cyberkriminelle bringen immer mehr über die gängigen Methoden der Sicherheitssysteme in Erfahrung und investieren daher in die Forschung und Entwicklung von Methoden zur Umgehung von Sicherheitsmaßnahmen.“

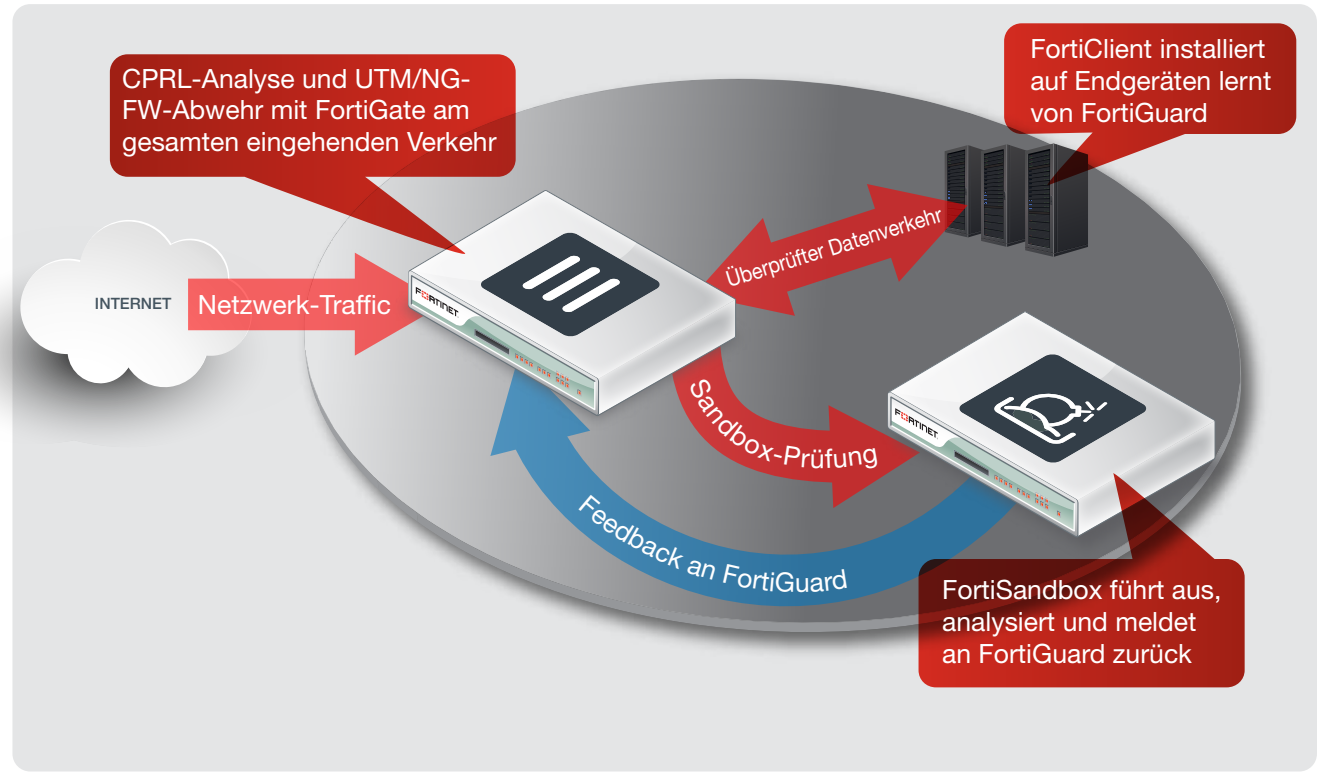
Malware 32-Bit, um möglichst großen Schaden anzurichten. Auch heute noch findet sich der größte Teil der Malware in Programmdateien, speziell Portable Executables im 32-Bit-Format (PE32). PR32-Dateien werden sowohl in Windows XP- als auch in Windows 7/8-Umgebungen ausgeführt. Daher kann der Großteil ihres bösartigen Verhaltens unter XP (das keinen 64-Bit-Code ausführt) beobachtet werden, ohne dass unter Windows 7/8 getestet werden muss. Die Antivirus-Engine von Fortinet, die mit CPRL in der FortiSandbox läuft, unterstützt sowohl 32-Bit- als auch 64-Bit-Code und mehrere Plattformen: Windows, Mac, Linux, Android, Windows Mobile, iOS, Blackberry sowie Symbian.

Windows 7/8-Sicherheitsmechanismen

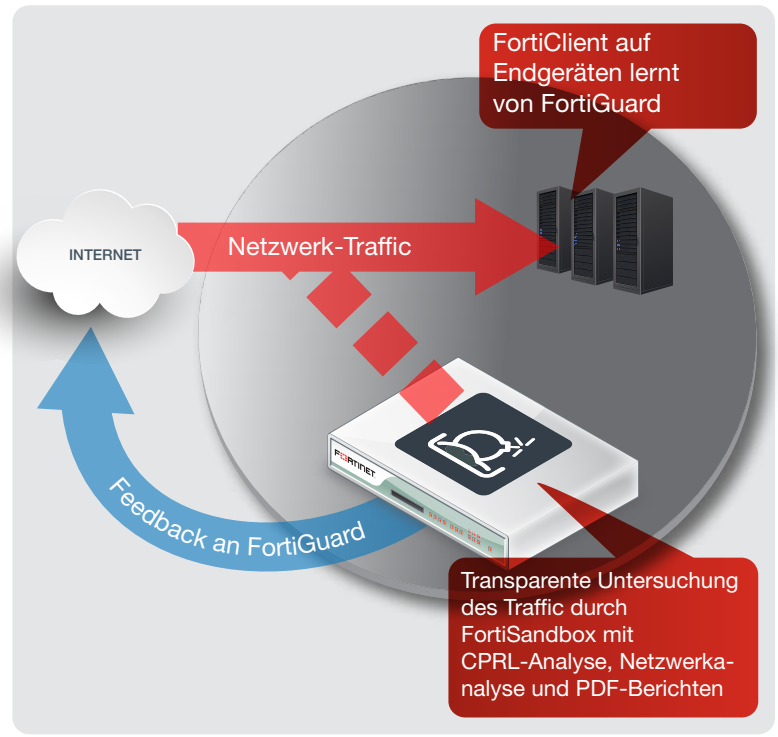
Microsoft hat in Windows 7/8 Sicherheitstechnologie eingeführt, die Schadcode und Dokumenten-Exploits an der Ausführung hindern sollen. Da Windows XP noch nicht über diese Technologie verfügt, erhöht sich die Erkennungsquote, wenn der Code in der Sandbox unter XP ausgeführt wird, auch wenn der Virus speziell für Windows 7/8 geschrieben wurde.

Einstellung von Windows XP

Windows XP ist ein guter Nährboden für Infektionen und das ideale Betriebssystem, um Bedrohungen in der Sandbox zuverlässig zu reproduzieren. Aber nach dem 8. April 2014 wird XP von Microsoft nicht mehr unterstützt. Ab dann gibt es keine Sicherheits-Updates mehr und in XP-Umgebungen werden sich immer mehr Sicherheitslücken auftun. Sie werden also noch anfälliger für Infektionen. Die gute Nachricht ist, dass in der Sandbox unter XP noch mehr Malware umfassend enttarnt werden kann. Die schlechte Nachricht ist, XP wird für Angreifer zum besonders lohnenden Ziel. Es besteht kein Zweifel, dass Malware entwickelt wird, um gezielt die Endbenutzer abzuschöpfen, die nicht auf Windows 7/8 umsteigen. Und ein Blick zurück lässt vermuten, dass die Migration nicht über Nacht erfolgen wird.



FortiSandbox-Konfiguration mit FortiGate



FortiSandbox Standalone-Konfiguration

Übersicht über die Bedrohungslandschaft

Die meisten von FortiGuard Labs beobachteten Bedrohungen sind im 32-Bit-Format geschrieben und auf Windows XP-Umgebungen ausgerichtet. Windows XP ist immer noch weit verbreitet und ein leichtes Ziel. So lange Entwickler 32-Bit-Malware programmieren können, die heute auf XP und später, nach einem Betriebssystemwechsel auch auf Windows 7/8 funktioniert, gibt es keinen Grund Malware speziell auf Windows 7/8 zuzuschneiden Das heißt nicht, dass FortiGuard Labs eine unmittelbare Explosion von 64-Bit-Bedrohungen erwartet. Fortinet ist aber dennoch bereits darauf vorbereitet, mit einer Kombination aus CPRL, Antivirus-Engine und FortiSandbox beides abzufangen.

Von FortiSandbox unterstützte Betriebssysteme

Um Bedrohungen effizient und effektiv abzufangen, weist die FortiSandbox den virtuellen Windows XP- und Windows 7/8-Umgebungen auf Basis der aktuellen Bedrohungslandschaft Ressourcen zu. Eine Veränderung in dieser Landschaft, zieht auch eine Änderung der unterstützten Umgebungen nach sich. Verbesserungen bei der Erkennung neuer Verschleierungstechniken und der angegriffenen Plattformen werden umgehend in FortiGate und FortiSandbox integriert. Darüber hinaus unterstützt Forti-Sandbox die betriebssystemunabhängige Erkennung durch Code-Emulation und Vorabfilterung per Antivirus-Engine.

Proaktive Gefahrenabwehr und Endgeräteschutz

Mit der Sandbox-Technologie lassen sich Bedrohungen aufspüren, um sie jedoch zu stoppen, sind erprobte Appliances zur Verwaltung der Netzwerksicherheit oder Firewall-Appliances besser geeignet. Werden bösartige Aktivitäten entdeckt, können sie mithilfe von UTM-Appliances (Unified Threat Management) und dem Schutz vor komplexen Bedrohungen (Advanced Threat Protection, ATP) in Next-Generation Firewalls (NGFW) aufgehalten werden.

FortiGate und andere Produkte von Fortinet wurden als erste Verteidigungsebene gegen ausgefeilte Bedrohungen von außen und innen entwickelt. Sie verwenden vorausschauende Technologie, die Angriffe in Echtzeit erkennt und konterkariert, bevor sie Schaden anrichten können. FortiSandbox ist eine Erweiterung von Fortinets führender UTM-/NGFW-Lösung, die ihre gesammelten Daten an FortiGate und/oder FortiGuard zurückmeldet. Erneute Angriffe mit durch FortiSandbox aufgedeckten Bedrohungen können bereits an vorderster Front abgewehrt werden, während ihr Lebenszyklus sich noch weiter entwickelt.

Schlussfolgerung

Tatsache ist, dass die Entwickler von Malware alle Sicherheitstechnologien kennen. Einige von ihnen entwickeln daher Tarnungen und verwenden hoch entwickelte Verschleierungsmethoden. Um die Malware zu erkennen, müssen möglichst viele Ebenen auf alle potenziellen Angriffsrichtungen überprüft werden. Dabei, hat sich eine Mischung aus Prüfung am Gateway und in der Sandbox als der beste Ansatz erwiesen.

Sandboxing ergänzt die Verteidigung in der modernen Bedrohungslandschaft um eine sinnvolle Ebene. Richtig eingesetzt, ist die Sandbox lernfähig und letztlich in die Gateway-Sicherheit eingebunden, sodass sie Aktivitäten durch neue Bedrohungen im Netzwerk schnell erkennen und Gegenmaßnahmen einleiten kann. Dabei ist die Integrationsfähigkeit dieser Appliances von entscheidender Bedeutung. FortiGuard Labs entdeckt und überwacht häufig neue Verschleierungstaktiken, sodass Fortinet-Lösungen schnell mit entsprechenden Updates und Daten aktualisiert werden können. Derzeit unterstützt Fortinet die Integration von FortiSandbox mit den Sicherheits-Appliances FortiGate, FortiManager und FortiMail.

www.fortinet.com

Deutschland
Feldbergstraße 35
60323 Frankfurt
Deutschland
Verkaufsabteilung: +49 69 310 192 0

Schweiz
Riedmuehlestr. 8
CH-8305 Dietlikon/Zürich
Schweiz
Verkaufsabteilung: +41 44 833 68 48

Österreich
Wienerbergstrasse 7/D/12th floor
1100 Wien
Österreich
Verkaufsabteilung: +43 1 22787 120

KONZERNSITZ
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
USA
Tel.: +1 (408) 235 7700
www.fortinet.com/sales

VERTRIEBSBÜRO EMEA
120 rue Albert Caquot
06560, Sophia Antipolis,
Frankreich
Tel.: +33 (0)4 8987 0510

VERTRIEBSBÜRO APAC
300 Beach Road 20-01
The Concourse
Singapur 199555
Tel.: +65 6513 3730

VERTRIEBSBÜRO LATEINAMERIKA
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel.: +52 (55) 5524 8480