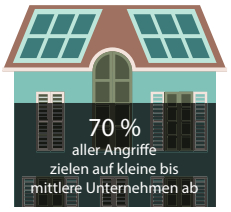
Abwehr bekannter, unbekannter und schwer fassbarer Bedrohungen mit WatchGuard Threat Detection and Response

Inhaltsverzeichnis

Welchen Malware-Bedrohungen sind kleine und mittlere Unternehmen ausgesetzt?

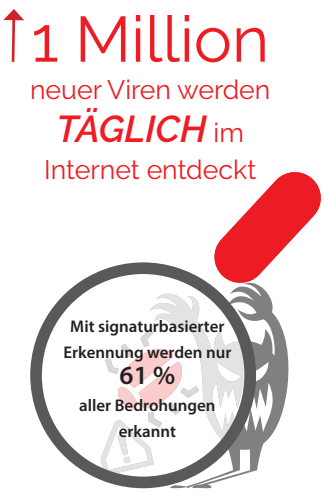
Während Schlagzeilen über Cyberangriffe und Datensicherheitsverletzungen bei Großkonzernen die Runde machen, wird über Malware-Bedrohungen für mittelständische Unternehmen nur selten berichtet. Tatsächlich ist die Zahl kleiner und mittlerer Unternehmen (KMU), die Cyberattacken und ausgefeilter Schadsoftware zum Opfer fallen, unverhältnismäßig hoch. Laut der Cyber Security Alliance zielen über 70 Prozent aller Cyberangriffe auf mittelständische Unternehmen ab.



Meldungen über erfolgreiche Cyberangriffe auf bekannte Marken sind zwar die Aufmacher in den Nachrichten, verschleiern aber zugleich die im Verborgenen lauernde, weitaus größere Schadsoftwarebedrohung. Organisationen jeder Größe sind heute einem endlosen Ansturm von Schadsoftware ausgesetzt. Tagtäglich werden eine Million neuer Malware-Samples entdeckt, und für Windows kommen jeden Monat 12 Millionen hinzu. Großkonzerne können sich dank umfangreicher Sicherheitsbudgets, fachkundiger Sicherheitsteams und modernster Technologie vor diesem Ansturm von Schadprogrammen schützen, die versuchen, sich durch Hintertüren Zutritt zu verschaffen. Für mittelständische Unternehmen hingegen, die den gleichen Bedrohungen ausgesetzt sind, und denen deutlich weniger Ressourcen zur Verfügung stehen, stellt Schadsoftware eine besonders große Herausforderung dar.

Was trägt zur Verschärfung dieser Bedrohungen bei?

Hacker rüsten auf und entwickeln Malware, wie es sie derart ausgeklügelt und perfide bisher noch nicht gab. Sie nutzen Zero-Day-Bedrohungen und Ausweichmanöver, um sich unerkannt an Netzwerkabwehrmechanismen vorbeizustehlen. Angesichts dieser virulenten Bedrohungslandschaft ist eine wirksame Malware-Erkennung unerlässlich. Dieses White Paper beschreibt, warum traditionelle Schadsoftware-Erkennungsansätze fehlschlagen. Es veranschaulicht die Bedeutung der Datenkorrelation von Ereignissen im Netzwerk und am Endpunkt für eine wirksame Erkennung und Abwehr ausgereifter Malware. Abschließend erörtern wir, wie wichtig eine schnellere Erkennung und Abwehr für die Bekämpfung schwer fassbarer und gezielter Bedrohungen ist.



Bekannte, unbekannte und schwer fassbare Malware

Mehr als eine Million neue Malware-Samples werden täglich im Internet entdeckt. Diese Zahl ist allerdings etwas irreführend, was zum Teil darauf zurückzuführen ist, dass sich Malware durch Morphing verändern und dadurch bekannten, signaturbasierten Erkennungsmodulen entgehen kann. Bedrohungen durch Schadsoftware sind vielfältig, verbreiten sich in rasantem Tempo und entwickeln sich permanent weiter. Um diese Bedrohungslandschaft eingehender darstellen zu können und Ansätze aufzuzeigen, die Sie in Ihrem Unternehmen für eine erfolgreiche Abwehr benötigen, klassifizieren wir Bedrohungen als bekannte, unbekannte und schwer fassbare Bedrohungen.

Bekannte Malware

Bezeichnet Malware, die zuvor bereits in freier Wildbahn in Erscheinung getreten ist und mithilfe reputations- und signaturbasierter Erkennungsmethoden identifiziert werden kann. Malware fällt in die Kategorie bekannter Schadsoftware, wenn Sicherheitsanalysten in der Lage sind, die Bedrohung zu analysieren und eine Signatur für Erkennungsmodule zu erstellen. Es ist ein manueller und zeitraubender Vorgang, der Analysten angesichts der schieren Bedrohungsflut schnell überfordert. Heute lassen sich mit signaturbasierten Erkennungsmethoden nur 61 Prozent aller Bedrohungen aufspüren – in vielen Fällen erst zwei Wochen nachdem die Malware selbst entdeckt wurde.1 Auch wenn die signaturbasierte Erkennung gegenüber den neuesten Bedrohungen ineffizient ist, muss darauf hingewiesen werden, dass die Infektionswahrscheinlichkeit von Endgeräten ohne diese Schutzmaßnahme 5,5-mal höher ist.2

Unbekannte Malware

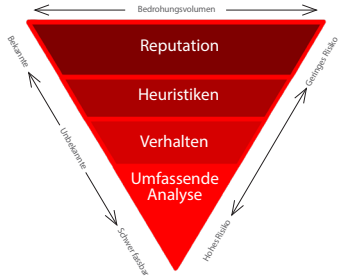
Unbekannte Malware ist Schadsoftware, die bislang nicht in freier Wildbahn entdeckt wurde oder für die noch keine bekannte Signatur existiert. Sie kann komplett neu oder eine Variante einer bekannten Schadsoftware sein, die sich durch Morphing verändert, um der signaturbasierten Erkennung zu entgehen. Mittels heuristischer Ansätze lässt sich die Erkennung unbekannter Malware deutlich verbessern, da Heuristiken nach bösartigem Code in verdächtigen Dateien suchen, um Bedrohungen zu identifizieren. Auch die Überwachung von Endpunkten auf Verhaltensweisen, die auf das Vorhandensein von Schadsoftware hindeuten, hat sich als wirkungsvoll erwiesen.

1 https://www.lastline.com/labsblog/antivirus-isnt-dead-it-just-cant-keep-up/
2 https://news.microsoft.com/2013/04/17/malware-infections-5-5-times-more-likely-without-antivirus-software-finds-new-research-from-microsoft/

Schwer fassbare Malware

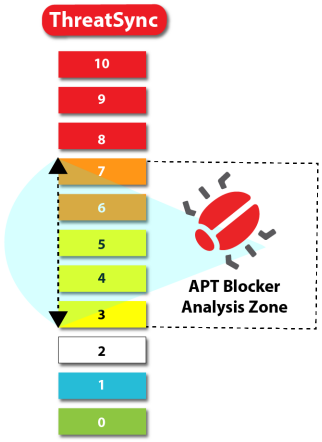
Schwer fassbare Malware nutzt verschlüsselte Kommunikationskanäle, Rootkits auf Kernel-Ebene, Zero-Day-Exploits sowie Umgebungserkennung, um Abwehrmechanismen ungehindert zu passieren. 2014 entwickelte sich diese Form der Malware zum Mainstream: Innerhalb weniger Monate stieg die Zahl der Schadsoftwareprogramme, die traditionelle Erkennungsmethoden umgehen, explosionsartig um 2000 Prozent an.3 Heute machen sich schätzungsweise 70 Prozent aller Malwareprogramme diese raffinierte Technologie in irgendeiner Form zunutze.4 Die Erkennung schwer identifizierbarer Malware erfordert umfassende Dateianalysen in einer Umgebung, die ein komplettes Betriebssystem nebst Hardwareplattform emuliert.

Die Bedeutung der Korrelation für die Erkennung und Abwehr von Malware



Jede Schadsoftware weist ein bestimmtes Infektionsmuster auf, das zu ihrer Erkennung beitragen kann. Ein Angriff beginnt in der Regel damit, dass ein Anwender auf einen Link in einer bösartigen E-Mail klickt, einem Drive-by-Download zum Opfer fällt oder das Endgerät über einen Malware-beladenen USB-Stick infiziert wird. Hat sich die Malware erst im Zielsystem eingenistet, kann sie sensible Daten ausspionieren, Berechtigungen eskalieren, zusätzliche Schadprogramme herunterladen oder versuchen, andere Geräte im Netzwerk zu infizieren. Jedes einzelne Verhaltensmuster hinterlässt Spuren auf dem Endgerät und im Netzwerk, die zur Visualisierung einer potenziellen Bedrohung herangezogen werden können. Dessen ungeachtet dauert die Aufdeckung einer Datensicherheitsverletzung in Unternehmen in der Regel mehr als 200 Tage. Je länger eine Datensicherheitsverletzung unentdeckt bleibt, um so größere Chancen hat der Angreifer, dem Opfer zu schaden. Wenn so viel auf dem Spiel steht, ist es von entscheidender Bedeutung, unbekannte und schwer fassbare Schadprogramme schneller zu erkennen und die dafür benötigten Ressourcen zu reduzieren. Dies wird durch die Korrelation von Sicherheitsereignissen im Netzwerk und am Endpunkt erreicht. Mithilfe der Korrelation können Administratoren darüber hinaus neue Bedrohungen mit unbekannter Signatur identifizieren, feststellen, welche Endgeräte befallen sind, dem Infektionsweg folgen und den Ursprung der Bedrohung bestimmen. Sie bietet Administratoren die erforderliche Visualisierung, um unbekannte und schwer fassbare Bedrohungen zu stoppen, bevor sie Schaden anrichten und sich im Unternehmen ausbreiten können.

Threat Detection and Response – eine Einführung



Signaturen sind notwendig und nützlich, wenn es um die Abwehr bekannter Bedrohungen geht, aber Unternehmen brauchen darüber hinaus auch wirksame Maßnahmen, um unbekannte oder neue Malware-Varianten zu stoppen. Threat Detection and Response (TDR) ist eine leistungsstarke Sammlung hochentwickelter Werkzeuge von WatchGuard. Sie korrelieren die von Firebox-Appliances und Host-Sensoren gemeldeten Bedrohungsindikatoren für die automatisierte Abwehr bekannter, unbekannter und schwer fassbarer Bedrohungen in Echtzeit.

Kernkomponenten der TDR-Lösung:

- ThreatSync. Ein innovatives Modul für die Bedrohungskorrelation. Es erfasst Sicherheitsereignisse im Netzwerk und am Endpunkt, setzt diese zu externen Informationen zur Bedrohungslage in Beziehung und bewertet den Schweregrad der Bedrohung, sodass umgehend automatische oder manuelle Abwehrmaßnahmen ergriffen werden können.
- Host Sensor. Der Host Sensor ermöglicht die Visualisierung am Endpunkt und erleichtert Abwehrmaßnahmen, sobald eine Bedrohung erkannt wird. Er umfasst zudem das Host Ransomware Prevention-Modul, das die Ausführung von Ransomware verhindert, bevor eine Verschlüsselung am Endpunkt erfolgt.
- APT Blocker. APT Blocker arbeitet mit einer prämierten Sandbox der nächsten Generation von Lastline, um Dateien umfassend zu analysieren. Eine Aufgabe, die üblicherweise ein Team aus erfahrenen Sicherheitsanalysten erfordert, um Hunderttausende Verhaltensmerkmale zu analysieren und so bösartige Absichten zu ermitteln. In TDR ist APT Blocker das Haupttool zur Sichtung von Bedrohungen. Sie können Dateien senden, um detailliertere Einblicke zu gewinnen, und den Sichtungsprozess zu einem großen Teil automatisieren.
- WatchGuard Firebox. Mit TDR fungiert die Firebox nicht nur als erste Abwehrinstanz gegen Malware, die ein Netzwerk zu infizieren versucht, sondern auch als Netzwerksensor, der Daten zu Sicherheitsereignissen erfasst und zwecks Korrelation an ThreatSync überträgt.

3 https://www.sans.org/reading-room/whitepapers/forensics/detecting-malware-sandbox-evasion-techniques-36667
4 https://www.lastline.com/documents/lastLine_deep_content_inspec_tb.pdf

Korrelation und Bedrohungsbewertung mit ThreatSync

ThreatSync erfasst Ereignisdaten von der WatchGuard Firebox und dem WatchGuard Host Sensor, bezieht diese auf aktuelle Feeds zur Bedrohungslage und analysiert sie. Ereignisdaten von anderen Sicherheitsdiensten auf Firebox-Appliances, beispielsweise APT Blocker, Reputation Enabled Defense (RED), Gateway AntiVirus und WebBlocker, werden an ThreatSync gesendet und dort mit den vom Host Sensor gesammelten Endpunktdaten verglichen.

ThreatSync analysiert und bewertet Indikatoren – individuelle Ereignisse im Netzwerk und am Endpunkt – und bezieht sie zur Erstellung eines umfassenden Bedrohungsindex auf aufgetretene Vorfälle.

WatchGuard-Bedrohungsbewertungsmodell:

8, 9, 10 – schwerwiegend

6, 7 – hoch

3, 4, 5 – verdächtig

2 – fragwürdig

1 – abgewehrt

0 – harmlos

Stellt ThreatSync fest, dass Ereignisse, die sowohl im Netzwerk als auch am Endpunkt erfasst wurden, miteinander in Beziehung stehen, werden sie automatisch mit der höchsten Gefahrenstufe 10 versehen.

Bedrohungsbewertung und automatisierte Reaktion

Somit liefert ThreatSync nicht nur umfassende Einblicke in die Vorgänge, die im Netzwerk und am Endpunkt ablaufen. Durch die gezielte Bewertung können IT-Teams auch im Handumdrehen erkennen, welche Bedrohungen am gefährlichsten sind und umgehende Aufmerksamkeit erfordern. Auf Basis der Priorisierung der Gefahren lassen sich Angriffe deutlich schneller identifizieren und geeignete Abwehrmaßnahmen ergreifen. Darüber hinaus verringert sich die Anzahl der dedizierten Ressourcen, die zur Beseitigung von Bedrohungen erforderlich sind.

Wenn entsprechende Regeln hinterlegt und aktiviert wurden, grenzt ThreatSync sofort nach Erkennung einer Bedrohung den infizierten Host ab, damit sich die Infektion nicht auf weitere Bereiche Ihres Netzwerks ausbreiten kann. Diese Funktion kann beim Schutz Ihrer Umgebung vor „Patient Zero"-Zwischenfällen eine entscheidende Rolle spielen, wenn außerhalb des Netzwerks infizierte Endpunkte die Malware bei ihrer Rückkehr einschleusen.

Nach der Abgrenzung des Hosts verschiebt ThreatSync die Datei in Quarantäne, bricht den Prozess ab oder löscht den vorhandenen Registrierungsschlüssel am Endpunkt und zeigt Einzelheiten zum entschärften Netzwerkereignis an. Diese Aktionen können auch manuell ausgeführt werden – dank unserer Technologie ist dabei ebenfalls nur ein Klick nötig.

Intelligente Gefahrenerkennung auf Enterprise-Niveau

ThreatSync nutzt und analysiert Informationen zur Bedrohungslage für Unternehmen, um sicherzustellen, dass aktuelle Gefährdungsindikatoren verwendet werden. Diese sogenannten „Threat-Feeds" enthalten Listen mit bekannten Malware-Signaturen und IP-Adressen, MD5-Hash-Werte von Malware-Dateien, URLs oder Domain-Namen von Botnet-Command-and-Control-Servern (C&C). Diese Listen sind von entscheidender Bedeutung, um zu verhindern, dass neue Bedrohungen Ihre Netzwerkumgebung infiltrieren und Zugriff auf kritische Daten erlangen. Es gibt viele spezialisierte Anbieter, die solche Listen erstellen und verwalten – dafür aber hohe Beträge von ihren Kunden verlangen.
Dank Threat Detection and Response kommen nun auch kleine und mittlere Unternehmen mit schlanken Budgets in den Genuss solcher Bedrohungsanalysefunktionen. ThreatSync vergleicht die Ereignisdaten der Firebox und des Host Sensors mit den verschiedenen Threat-Feeds und kann somit umgehend feststellen, ob eine Bedrohung bereits andernorts aufgetreten ist. Wenn es sich um eine bereits bekannte Gefahr handelt, können sowohl über die Firebox als auch den Host Sensor umgehend Abwehrmaßnahmen ergriffen werden.

Malware-Erkennung am Endpunkt: Host Sensor

Threat Detection and Response vereint über den WatchGuard Host Sensor mehrere Erkennungsformen zum Aufspüren selbst raffiniertester Malware-Bedrohungen.

- Signaturen – Wie bereits erwähnt, sind Signaturen ein wichtiges Instrument zur Verteidigung gegen Malware. Die Liste der bekannten Bedrohungen muss stets aktuell sein. WatchGuard Threat Detection and Response nutzt Bedrohungsanalysen auf Enterprise-Niveau, um zu beurteilen, ob es sich bei einem verdächtigen Ereignis um eine bekannte Bedrohung handelt.
- Heuristiken – TDR verwendet ergänzend zu Signaturen sowohl statische als auch dynamische Heuristiken (Entscheidungsregeln), um anzugeben, ob sich ein Programm verdächtig verhält. Statische oder Dateiheuristiken untersuchen Struktur und Inhalt der Datei vor der Ausführung, also in inaktivem Zustand. Dynamische oder Prozessheuristiken überprüfen laufende Prozesse auf verdächtige Eigenschaften. Durch eine Kombination dieser Heuristiken lassen sich scheinbar harmlose Dateien aufspüren, die unter Umständen eine echte Bedrohung darstellen. Diese Erkennungsmethode kann in vielen Fällen eine neue oder unbekannte Bedrohung im Nu identifizieren – selbst wenn die Infektion noch gar nicht stattgefunden hat oder ein Prozess bereits läuft, aber noch keine schädlichen Vorgänge ausgeführt wurden. TDR setzt mit dem WatchGuard Host Sensor über 175 Heuristiken ein.
- Verhaltensanalyse – Da Malware-Bedrohungen bestimmten Verhaltensmustern folgen, trägt die Verfolgung dieser Schritte zuverlässig zur Erkennung komplexer, polymorpher unbekannter oder schwer fassbarer Varianten von Schadsoftware bei. Diese Erkennungsmethode geht über dynamische Heuristiken hinaus, da nicht nur die Eigenschaften laufender Prozesse überwacht, sondern auch die Prozessabläufe innerhalb des Dateisystems identifiziert werden. Beispiele für Prozessabläufe sind das Festlegen der Persistenz, Replikation, strategisches Löschen, die Nummerierung des Dateisystems, Verschlüsselung usw. Bei dieser Erkennungsform werden Verhaltensketten überwacht, und das Risikoprofil wird beim Hinweis auf zunehmend böswillige Verhaltensmuster heraufgesetzt. Das Host Ransomware Prevention-Modul beobachtet Verhaltensmuster, die traditionell mit Ransomware-Angriffen in Zusammenhang stehen, um diese Angriffe gezielt zu verhindern, bevor die Ransomware Dateien verschlüsseln kann.

Netzwerkvisualisierung: WatchGuard Firebox

Hacker greifen bei ihren Angriffen auf zahllose externe Server und Ressourcen zurück. Um Befehle zu erhalten, Informationen auszuschleusen, Verschlüsselungscodes anzufordern und Systeme zu infizieren, muss ausgeklügelte Malware beispielsweise häufig mit Command-and-Control-Servern kommunizieren. Angreifer machen sich gerne ein ganzes Inventar erfolgreich infizierter Systeme zunutze und entwickeln oft Malware, die periodisch Heartbeat-Signale an Command-and-Control-Kanäle sendet. Einblicke in den Netzwerkverkehr – hierzu zählen auch Versuche, mit Domains und IP-Adressen zu kommunizieren, die bekanntermaßen mit bösartigem Verhalten in Verbindung gebracht werden – können darauf hindeuten, dass sich eine Bedrohung in Ihrer Netzwerkumgebung eingenistet hat.

Firebox-Appliances verbessern die Erkennung zusätzlich, da sie dem TDR-Modul die Korrelation des Netzwerkverhaltens und der von den WatchGuard-Sicherheitsdiensten erfassten Ereignisse ermöglichen. APT Blocker, Reputation Enabled Defense (RED), Gateway AntiVirus und WebBlocker sind Sicherheitsdienste auf Enterprise-Niveau, die auf die Abwehr der neuesten Bedrohungen ausgelegt sind und jeweils Informationen bereitstellen, die auf das Vorhandensein einer Bedrohung hinweisen. Jeder einzelne Sicherheitsdienst erfasst Sicherheitsereignisse und überträgt diese zwecks Korrelation und Bewertung an das ThreatSync-Modul, das ein umfassenderes Bild der Gefahren vermittelt. Bösartige ausgehende Verbindungen, die blockiert wurden, werden korreliert. Dies gibt Aufschluss über den auslösenden Endpunkt und Prozess. Letzterer kann daraufhin beendet werden.

WebBlocker
Dieser Sicherheitsdienst ist mit einer Cloud-Datenbank verbunden, die Informationen zu über 50 Millionen bekannten bösartigen Websites auf der ganzen Welt enthält. Hierzu zählen englische, deutsche, spanische, französische, italienische, niederländische, japanische und chinesische Websites sowie Websites in vereinfachtem Chinesisch.

- **Sicherheitsereignis:** Herstellen einer Verbindung zu einer Website mit blockierten Inhalten.

Reputation Enabled Defense
Reputation Enabled Defense (RED) identifiziert die Bedrohung mittels eines Reputations-Suchdienstes, der URLs entweder als gut, schlecht oder unbekannt einstuft. Der Suchdienst nutzt eine leistungsstarke, cloudbasierte Reputationsdatenbank, die Daten aus unterschiedlichen Feeds, beispielsweise von branchenführenden Antivirus-Modulen, miteinander vereint.

- **Sicherheitsereignis**: Versuch, eine Website mit schlechter Reputation aufzurufen.
- **Sicherheitsereignis:** Versuchte Kommunikation mit einem Botnet-Command-and-Control-Server

Gateway Antivirus
Gateway AntiVirus (GAV) prüft den Datenverkehr in allen gängigen Protokollen (HTTP, HTTPS, FTP, TCP, UDP, SMTP und POP3) und verwendet dazu laufend aktualisierte Signaturen und Heuristiken zur Erkennung und Abwehr von Malware aller Art.

- **Sicherheitsereignis**: Gateway AntiVirus hat einen Virus im Webdatenverkehr entdeckt.
- **Sicherheitsereignis:** Gateway AntiVirus hat einen Virus im E-Mail-Datenverkehr entdeckt.

IntelligentAV
Intelligent AV nutzt künstliche Intelligenz, um besseren Schutz vor immer weiter verbreiteter Zero-Day-Malware zu gewährleisten. Während signaturbasierte AV-Lösungen nur bekannte Bedrohungen erkennen können, macht es IntelligentAV möglich, Bedrohungen vorherzusagen und aus aktiven Angriffen auf Ihr Netzwerk zu lernen.

- **Sicherheitsereignis:** IntelligentAV hat einen Virus im Webdatenverkehr entdeckt.
- **Sicherheitsereignis:** IntelligentAV hat einen Virus im E-Mail-Datenverkehr entdeckt.

APT Blocker
WatchGuard APT Blocker nutzt das Prinzip der Verhaltensanalyse, um festzustellen, ob eine Datei bösartig ist. APT Blocker identifiziert verdächtige Dateien und übergibt diese an eine fortschrittliche, cloudbasierte Sandbox-Lösung. Dabei handelt es sich um eine virtuelle Umgebung, in der Code analysiert, emuliert und ausgeführt wird, um dessen Bedrohungspotenzial zu bestimmen.

- **Sicherheitsereignis:** APT Blocker erkennt/blockiert eine Bedrohung im Webdatenverkehr.
- **Sicherheitsereignis:** APT Blocker erkennt/blockiert eine Bedrohung im E-Mail-Datenverkehr.

Bedrohungssichtung mit APT Blocker und KI

Ein Bedrohungsindex ist für eine leistungsstarke Bedrohungsabwehr äußerst hilfreich. Indikatoren, die auf verdächtige Dateien hindeuten, können angesichts der ständig weiterentwickelten Malware-Programme erste Hinweise auf eine bislang unbekannte Schadsoftware liefern. Dank der engen Verflechtung mit WatchGuard APT Blocker können verdächtige Dateien nun für eine umfassende Analyse und Neubewertung an eine fortschrittliche Cloud-Sandbox gesendet werden. Da ThreatSync auf KI aufbaut, wird die Engine regelmäßig auf Tausende bösartiger und gutartiger Dateien trainiert. Dadurch kann ThreatSync zutreffendere Bedrohungsbewertungen zuweisen, die Klassifizierung verdächtiger Dateien automatisieren und bestimmen, welche davon an APT Blocker gesendet werden sollen. Zur automatisierten Gefahrenabwehr sendet APT Blocker die Ergebnisse automatisch zurück an ThreatSync.

APT Blocker emuliert ein komplettes System (CPU und Speicher), um detaillierte Einblicke in die Ausführung von Malware-Programmen zu erhalten. Dateien durchlaufen zuerst weitere Sicherheitsdienste wie Gateway AntiVirus und Intrusion Prevention. Im Anschluss wird ein Fingerprint der Dateien erstellt und mit einer Datenbank verglichen. Liegen keine Informationen zu einer Datei vor, wird sie mithilfe des Systememulators analysiert, der die Ausführung aller Befehle überwacht.

APT Blocker analysiert das gesamte Verhalten der Malware, von ausgeführten CPU-Anweisungen und angeforderten Netzwerkverbindungen bis hin zu Dateien, Speicher und Geräten, auf die die Schadsoftware möglicherweise zugegriffen hat. APT Blocker kann darüber hinaus Ausweichmanöver erkennen, die anderen Sandbox-Lösungen verborgen bleiben. Hierzu zählen Zeitverzögerungen, das Warten auf Benutzereingaben, bösartige Eingriffe in das Betriebssystem, die verschlüsselte Datenübertragung an Command-and-Control-Infrastrukturen sowie die Fragmentierung von Dateien, deren Ausführung erst nach dem erneuten Zusammensetzen erfolgt.

Die von APT Blocker zu prüfenden Dateien werden während der Analyse aktiv am betroffenen Endpunkt überwacht. Stellt sich die Datei als bösartig heraus, identifiziert ThreatSync die Datei sofort an allen geschützten Endpunkten und beginnt mit der Problembehebung.

Schlussfolgerung

In diesem White Paper wurden die Funktionen der Threat Detection and Response-Plattform (TDR) beschrieben, die unternehmensrelevante bekannte, unbekannte und schwer fassbare Malware-Bedrohungen erkennt, überprüft und eine zeitnahe Reaktion ermöglicht, um Ihnen einen besseren Überblick über TDR zu vermitteln:

- TDR erkennt bekannte, unbekannte und schwer fassbare Malware, die den meisten Antivirus-Produkten entgeht, und nutzt hierfür Sensoren im Netzwerk und an Endpunkten.
- TDR spürt nicht nur Malware auf, die von vorhandenen Sicherheitstechnologien nicht erkannt wird, sondern reagiert umgehend, um die Infektion einzudämmen, und wehrt die Bedrohungen ab.
- Die TDR-Korrelation im Netzwerk und an den Endpunkten in Verbindung mit externen Feeds zur Bedrohungslage gestattet eine bessere Gefahrenvisualisierung und -verifizierung.
- ThreatSync reduziert die Zahl der Fehleinschätzungen (False Positives) durch eine Kombination von Bedrohungsindizes und -analysen.
- TDR reagiert dank der automatisierten, richtlinienbasierten Gefahrenabwehr schneller und effizienter auf Bedrohungen und entschärft dabei gezielt nicht nur Einzelprozesse, sondern berücksichtigt das gesamte Spektrum der Prozessabläufe.
- Die enge Verflechtung mit APT Blocker sorgt für eine wirksame, mehrschichtige Bedrohungsbewertung und eine umfassende Analyse verdächtiger Dateien.

Weitere Informationen finden Sie unter www.watchguard.com/tdr.

Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den weltweit führenden Anbietern im Bereich Netzwerksicherheit und hat sich insbesondere bei Best-in-Class Unified Threat Management, Firewalls der nächsten Generation, sicherem WLAN sowie Netzwerkprodukten und -services einen Namen gemacht. Mehr als 80.000 Unternehmen weltweit vertrauen auf die ausgeklügelten Schutzmechanismen auf Enterprise-Niveau, wobei dank der einfachen Handhabung insbesondere kleine bis mittlere sowie dezentral aufgestellte Unternehmen von WatchGuard profitieren. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält WatchGuard Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter WatchGuard.de.

Deutschland, Österreich, Schweiz: +49 700 92229333 INTERNATIONALER VERTRIEB +1.206.613.0895 www.watchguard.de