TRUST IN GERMAN SICHERHEIT

BEAST

Grenzen traditioneller Malware-Erkennung überwinden

G DATA CyberDefense AG

Ausgeklügelte Malware in der Praxis zu erkennen, ist zu einer schwierigen Aufgabe geworden, wenn dafür nur herkömmliche signaturbasierte Erkennungsmechanismen zum Einsatz kommen.

Einschränkung Nr. 1: reaktive Erkennung

Die signaturbasierte Erkennung ist vor allem eine reaktive Methode. Ganz gleich, in welchem Umfang Automatisierung Anwendung findet: Erst nachdem eine Datei als schädlich eingestuft wurde, kann eine Signatur für diese Datei oder eine Gruppe zugehöriger Dateien (üblicherweise eine Malware-Familie) geschrieben werden.

Heute übergehen Malware-Autoren diesen reaktiven Ansatz, indem sie neue Malware immer häufiger in Umlauf bringen.

Einschränkung Nr. 2: Einzigartigkeit von Malware

Cyberkriminalität ist zu einer milliardenschweren Branche geworden. Wie herkömmliche Unternehmen steigern auch Cyberkriminelle ihre Effizienz mit Tools zur Automatisierung. Einige Malware-Autoren nutzen Automatisierungsdienste, um aktiv zu überwachen, ob Anti-Malware-Lösungen ihre Malware erkennen. Sobald eine Erkennung registriert wird, entfernen sie das erkannte Muster sofort aus ihren Samples oder verändern ihre Programme automatisch, um der Erkennung zu entgehen.

Sie verwenden extrem häufig Verschlüsselung und Packer für ihre Samples, um deren schädlichen Kern zu verschleiern. Einige Malware-Autoren bringen alle paar Minuten ein neues Malware-Sample in Umlauf. Andere generieren sogar ein individuelles Sample für jedes einzelne Opfer („serverseitige Polymorphie“).

Wenn schädliche Dateien so spezifisch sind, ist es natürlich schwierig, schädliche Muster zu finden. Solche Muster sind nötig, um eine herkömmliche Signatur zu erstellen, die es dann ermöglicht, eine ganze Malware-Familie zu identifizieren. Doch selbst wenn Muster

vorhanden sind, mit denen eine Signatur erstellt werden kann, ist dieser Aufwand praktisch nutzlos.

Einschränkung Nr. 3: Umgehung der Backend-Analyse

Ein weiteres Problem ist, dass die Identifizierung schädlicher Dateien oft auf das Analyse-Backend der Sicherheitsanbieter setzt. Jedes potenziell schädliche Sample, die den Anbietern in die Hände fällt, wird gründlich analysiert. Das passiert beispielsweise in Sandbox-Systemen, die die Samples ausführen und versuchen, alle schädlichen Aktionen zu identifizieren. Nur wenn die Samples als schädlich identifiziert werden, beginnt ein Prozess zur Identifizierung schädlicher Muster. Leider sind Malware-Samples aber oft so konzipiert, dass sie ihre Umgebung erkennen. Das bedeutet, sie erkennen, wenn sie analysiert werden. Sie zeigen ihr schädliches Verhalten womöglich erst zu einer bestimmten Zeit, an einem bestimmten Ort, nachdem sie eine bestimmte Zeit ausgeführt wurden oder nachdem eine Benutzerinteraktion erkannt wurde, die es in einem Sandbox-System normalerweise nicht gibt.

Wegen dieser Probleme müssen wir neben herkömmlichen Erkennungsmethoden auch in der Lage sein, schädliches Verhalten dort zu erkennen, wo es passiert: auf dem betroffenen System.

Die Lösung: Verhaltensanalyse

Sicherheitsanbieter haben deshalb Erkennungstechnologien implementiert, die das Verhalten von Prozessen auf einem System analysieren, um zu bestimmen, ob es schädlich oder unschädlich ist. Um sorgsam mit Hardwareressourcen umzugehen, konzentrieren sich solche Analysen auf besonders verdächtige Systembestandteile wie das Dateisystem, die Registrierungsdatenbank oder den Autostart-Ordner. So sind Sicherheitsanbieter in der Lage, völlig unbekannte Malware-Familien aufzuspüren.

Die meisten dieser Lösungen übertragen bedrohliches Verhalten in Werte, um so einen Schädlichkeitsgrad zu bestimmen. Mathematisch lässt sich ein Verlust an Genauigkeit nicht vermeiden, wenn viele dieser Werte zu einem Gesamtergebnis zusammengefasst werden. Selbst mit maschinellem Lernen bleibt bei dieser Methode eine gewisse Unschärfe, die in gewissem Umfang zu Falscheinschätzungen führt, wenn Prozesse entweder als schädlich oder unschädlich eingestuft werden.

Die meisten Verbraucher werden davon nichts zu spüren bekommen. Unternehmen verwenden jedoch oft bewusst hochspezialisierte Softwaretools und Prozesse auf eine Art und Weise, die zwar unschädlich, in den meisten anderen Umgebungen jedoch ungewöhnlich ist. Ist die Schwelle des Tools zur Verhaltensanalyse zu hoch eingestellt, blockiert es diese Prozesse. Ist sie zu niedrig eingestellt, wird Malware eventuell nicht erkannt. In der Praxis versuchen Sicherheitsanbieter, Fehler in der Erkennung zu vermeiden, indem sie Benutzer auffordern, die Ausführung von Prozessen zu bestätigen. Passiert dies zu oft, schalten die Benutzer entweder die Technologie aus oder ignorieren Warnungen. In beiden Fällen steigt das Risiko von Infektionen.

Die richtige Lösung: BEAST

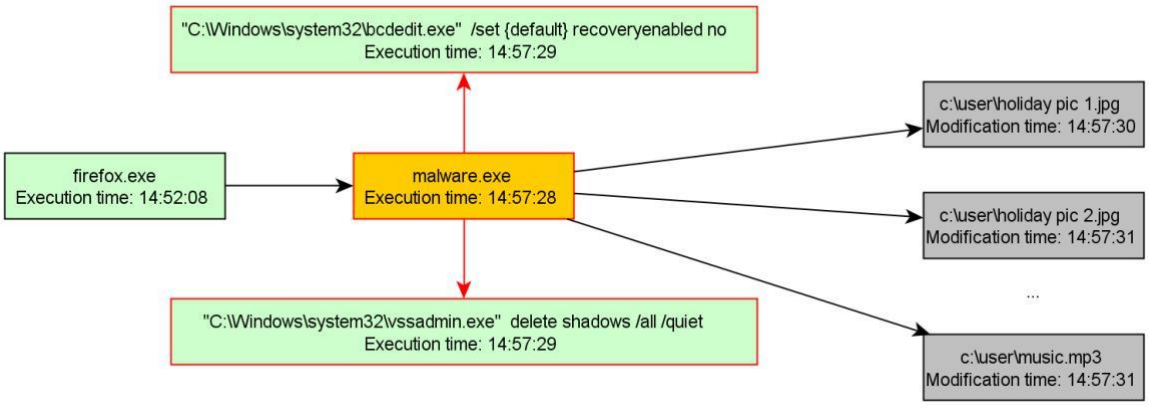
BEAST ist eine von GDATA entwickelte verhaltensbasierte Erkennungstechnologie, die Verhalten überwacht und jede beobachtete Aktion in einer lokalen, schlanken

Graphdatenbank speichert. BEAST setzt nicht auf die Erkennung der Malware selbst, sondern auf die Beobachtung des generischen schädlichen Verhaltens. Dies ist besonders nützlich bei seltener Malware und seltenen Malware-Familien.

Funktionsweise von BEAST: graphenbasierte Regelzuordnung

Auf einem geschützten System überwacht BEAST das Verhalten und speichert jede Aktion. Dazu zählen Zugriffe auf das Dateisystem, auf die Registrierung, Netzwerkverbindungen und die Kommunikation zwischen Prozessen. Jedes Mal, wenn etwas zur Graphdatenbank hinzugefügt wird, wird der Graph nach schädlichen Verhaltensmustern durchsucht.

Der folgende Graph zeigt beispielhaft diese Art von regelbasierten Vergleichen:



Dieser Beispielbenutzer wurde wahrscheinlich von einer Website dazu verleitet, die Schaddatei „malware.exe“ im Firefox-Browser aus dem Internet herunterzuladen. In

diesem Fall handelt es sich konkret um eine Infektion mit Ransomware. Ransomware verschlüsselt die Dateien des Benutzers und fordert ihn anschließend zur Zahlung eines bestimmten Geldbetrags auf, um die Dateien wieder zu entschlüsseln.

Der schädliche Prozess startet hier sofort eine Instanz des Systemtools „bcedit“, um die Windows Startup-Reparaturfunktion zu deaktivieren. Danach startet er eine Instanz des Systemtools „vssadmin“, um sogenannte Schattenkopien zu löschen, mit denen sich versehentlich überschriebene Dateien wiederherstellen lassen. Anschließend beginnt er, mehrere Dateien im Verzeichnis „C:\user“ zu verschlüsseln.

Da es sich beim Start der beiden vorhin erwähnten Systemtools um typische Vorbereitungsmaßnahmen handelt, die Ransomware vor dem Verschlüsseln von Dateien durchführt (um den Benutzer daran zu hindern, sein System wiederherzustellen), kann dieses Verhalten (rot gekennzeichnet) eindeutig als schädlich gewertet werden. Aus diesem Grund würde der Prozess „malware.exe“ gestoppt und die Binärdatei in die Quarantäne verschoben. Da die Binärdateien „vssadmin.exe“ und „bcdedit.exe“ unschädliche Systemtools sind, die von der Ransomware nur missbräuchlich verwendet werden, blieben sie auf dem System erhalten.

Neue Möglichkeiten: nachträgliche Bereinigung

G DATA nutzt automatisierte Backend-Systeme oder manuelle Analytik und identifiziert so täglich zahlreiche Indikatoren für Kompromittierung bzw. IOC (Indicators of Compromise). Ein IOC kann ein Command&Control-Server (C&C) sein, mit dem ein Botnet betrieben wird, oder eine bestimmte Datei, die als schädlich identifiziert wurde.

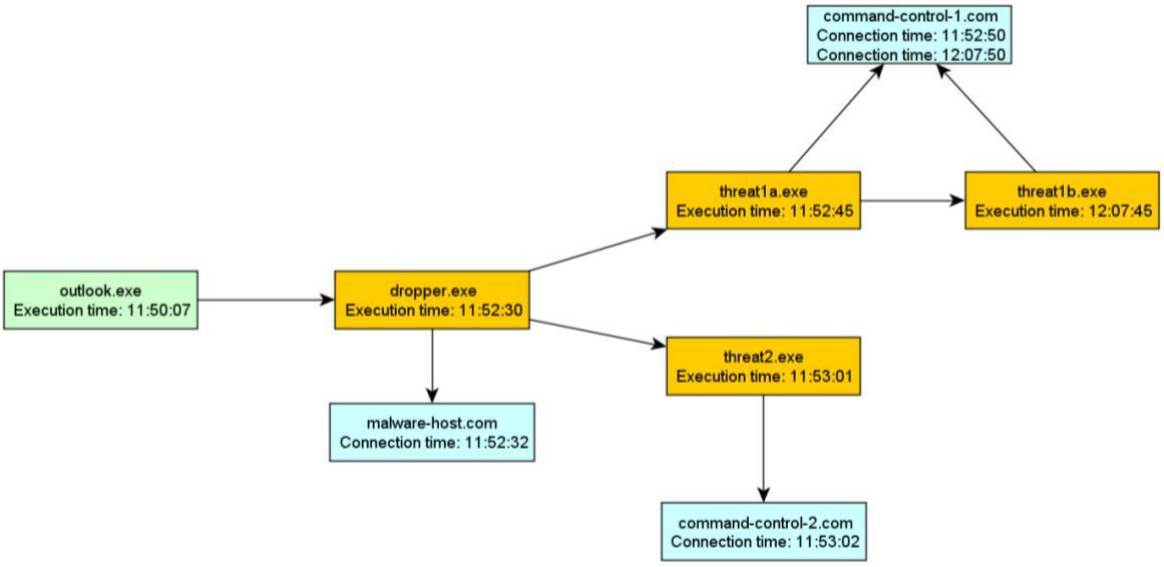
Bei herkömmlicher Endpoint-Sicherheitssoftware werden Aktionen nur dann mit IOC-Listen verglichen, wenn die Aktion gerade stattfindet. Bevor eine Datei ausgeführt wird, wird sie beispielsweise mit einer Liste bekannter schädlicher Dateien verglichen. Oder wenn sich ein Prozess mit einem Host verbindet, wird der Host anhand einer Liste bekannter C&C überprüft. Wird der Host als schädlich identifiziert, wird der gesamte Prozess als schädlich erkannt.

Das zentrale Problem ist jedoch, dass die IOC-Identifizierungsprozesse des Sicherheitsanbieters eben reaktiv sind. Sie beginnen, nachdem die Anbieter mit der Analyse der Bedrohung begonnen haben. Das ist aber erst möglich, nachdem eine Bedrohung aufgetaucht ist. Selbst wenn dies automatisiert und sehr kurzfristig erfolgt, ist die zeitliche Lücke im Kontext der Malware-Erkennung immer noch bedeutungsvoll. Einfach ausgedrückt: Sicherheitsanbieter kommen oft zu spät und können nichts dagegen tun, wenn sie auf herkömmliche Methoden setzen.

In BEAST sind die Aktionen (Verhalten) in einer lokalen Graphdatenbank gespeichert. Deshalb kann alles in dieser Datenbank mit von G DATA identifizierten IOCs verglichen werden, selbst nachdem sie aufgetreten sind. Und da die Graphdatenbank auch alle Aktionen in Verbindung mit dem IOC enthält, können alle diese Aktionen rückgängig gemacht werden. Das ermöglicht de facto eine nachträgliche Malware-Entfernung.

Dies ist besonders wichtig, wenn ein System kompromittiert ist, aber noch keine schädlichen Aktionen ausgelöst wurden, die die allgemeine Verhaltenserkennung auslösen könnten.

Stellen Sie sich zur Veranschaulichung den folgenden vereinfachten Verhaltensgraphen vor:



Zunächst wird im E-Mail-Programm Outlook ein infizierter Anhang geöffnet. Dadurch wird eine Datei namens „dropper.exe“ erstellt und vom Prozess „outlook.exe“ ausgeführt. Der

neue Prozess verbindet sich dann mit „malware-host.com“, um weitere schädliche ausführbare Dateien („threat1a.exe“, „threat2.exe“) herunterzuladen und auszuführen. Beide verbinden sich mit ihren jeweiligen C&C-Servern („command-control-1.com“, „command-control-2.com“). Nach ungefähr 15 Minuten empfängt „threat1a.exe“ einen Befehl, die ausführbare Datei auf „threat1b.exe“ zu aktualisieren, die nachfolgend eine Verbindung zum gleichen C&C-Server herstellt.

Wenn beispielsweise G DATA den Server „command-control-2.com“ oder die ausführbare Datei „dropper.exe“ als IOC identifiziert, kann BEAST – selbst Stunden nach der Infektion – einfach den Graphen durchlaufen und jede einzelne Binärdatei in Verbindung mit der Infektion finden und entfernen.

Dazu zwei Anmerkungen: Auch jede Änderung an der Windows-Registrierung und somit der Systemkonfiguration wird erfasst und kann rückgängig gemacht werden (hier aus Gründen der Übersichtlichkeit weggelassen). „outlook.exe“ als bekanntermaßen unschädliche ausführbare Datei würde nicht entfernt werden.

Was ist der Unterschied zur vorhandenen Verhaltensanalyse?

Die vorhandene Verhaltensanalyse empfängt im Wesentlichen einen Datenstrom aller von einem Prozess durchgeführten Aktionen. Sie weist jeder einzelnen Aktion einen bestimmten numerischen Wert zu, der die Schädlichkeit bezeichnet. Danach summiert er alle diese Werte. Wird dadurch ein bestimmter Schwellenwert überschritten, wird der Prozess als schädlich eingestuft.

Im Wesentlichen ist die Verhaltensanalyse somit auf Prozesse fokussiert, während BEAST einen Überblick über das gesamte System hat. Und weil die Verhaltensanalyse lediglich die in Zahlen ausgrdrückte Schädlichkeit von Aktionen zusammenfasst, ist es nicht möglich, bestimmte Kombinationen von Aktionen als schädlich zu erkennen. Das macht es schwierig, schädliche Verhaltensmuster konkret zu erkennen. Immer, wenn einer Aktion ein neuer oder höherer Schädlichkeitswert zugewiesen wird, kann dies zu falsch-positiven Erkennungen der Verhaltensanalyse führen. Das hat es in der Vergangenheit schwierig

gemacht, schnell auf neue Bedrohungen zu reagieren. Und selbst bei aller Sorgfalt: Falls einer Aktion ein neuer oder höherer Schädlichkeitswert zugewiesen wird, besteht immer ein hohes Risiko, falsch-positive Erkennungen auszulösen. Bei BEAST wiederum basieren die Erkennungen auf sehr spezifischen Kombinationen schädlicher Aktionen. Deshalb ist es einfacher, neue Regeln hinzuzufügen und gleichzeitig generell wesentlich weniger für Fehlalarme anfällig zu sein.

Außerdem ist die Möglichkeit eines rückblickenden Vergleichs von IOCs und eine nachträgliche Bereinigung nur mit BEAST möglich.

Wozu brauchen wir BEAST, wenn wir doch DeepRay haben?

Die Stärke von DeepRay ist, durch Packer zu schauen. Das ermöglicht es uns, schädliche Malware-Kerne zu identifizieren. Die initiale Identifizierung von Malware-Kernen ist allerdings ein manueller Vorgang. Für die meisten Crimeware-Familien stellt dies kein Problem dar. Doch selbst hier trägt BEAST dazu bei, die zeitliche Lücke bis zu einer DeepRay-Erkennung zu schließen, für den Fall, dass die Malware im Kern verändert wird. Aber neben den am weitesten verbreiteten Crimeware-Familien gibt es auch eine große Zahl von Malware-Familien, die einzeln zwar nicht sehr verbreitet, in der Summe aber für eine Vielzahl von Infektionen verantwortlich sind. Der Grund, warum sie nicht so verbreitet sind, besteht darin, dass sie für gezielte Angriffe eingesetzt werden. Dies macht sie besonders gefährlich. Da BEAST nicht auf die Identifizierung eines bestimmten Malware-Kerns setzt, sondern auf die allgemeine Beobachtung schädlichen Verhaltens, trägt es dazu bei, diese Bedrohungen einzudämmenund somit eine weitere Schutzschicht hinzufügt.