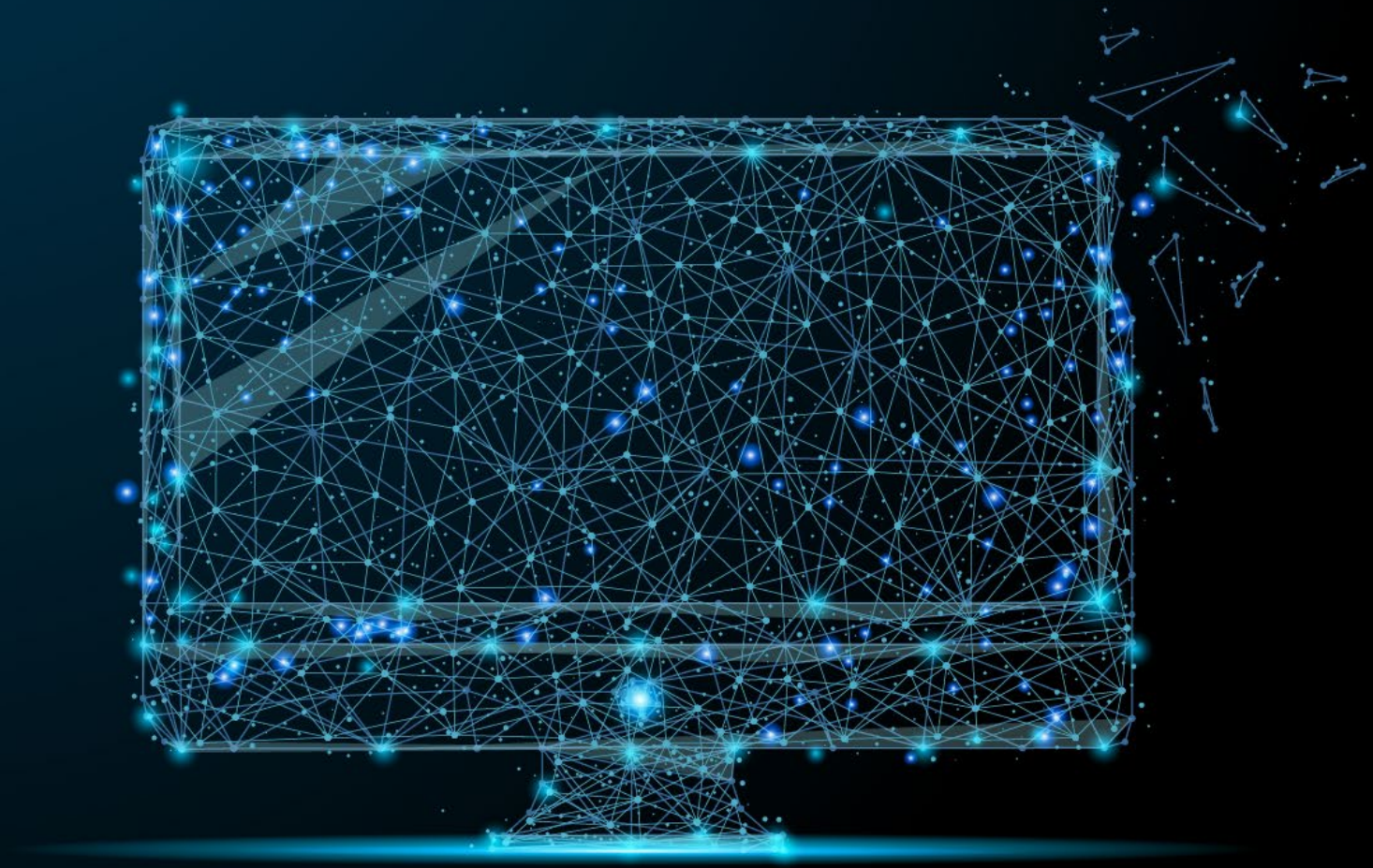
VMRAY

RÖNTGENBLICK FÜR MALWARE



Evasive Malware: Meister der Tarnung

Ein Überblick über die gängigsten Ausweich- und Verschleierungstaktiken moderner Schadsoftware

Hochentwickelte Malware ist darauf ausgelegt, den Security-Systemen eines Unternehmens zu entgehen. So kann beispielsweise die signaturbasierte Malware-Erkennung traditioneller Anti-Virus-Lösungen ausgehebelt werden, indem die Malware zu Verschleierungsmethoden greift, die ihre identifizierbaren Merkmale verbergen oder verändern (Polymorphismus, Metamorphismus). Deshalb kommen in ausgereiften Sicherheitskonzepten stets auch Sandboxing-Technologien zum Einsatz, da diese bei der Malware-Analyse nicht auf Signaturen angewiesen sind. Ausgefeilte Malware wird jedoch auch versuchen, der Analyse in der Sandbox zu entkommen. Dieses Papier beleuchtet die als Sandbox Evasion (Umgehung der Sandbox) bekannte Fähigkeit moderner Malware und erläutert, worauf es bei der Wahl einer Sandbox mit hoher Resistenz gegenüber Evasionstechniken ankommt.

FUNKTIONSWEISE EINER SANDBOX

Das Funktionsprinzip einer Sandbox ist einfach: In einer kontrollierten, von der Produktivumgebung des Unternehmens abgeschotteten Umgebung (Sandbox) wird das Verhalten der verdächtigen Datei über einen definierten Zeitraum hinweg beobachtet und dokumentiert. Der Schadcode wird in der Sandbox also tatsächlich ausgeführt. Diese als dynamische Analyse bezeichnete Erkennungsmethode identifiziert Malware anhand des beobachteten Verhaltens. Aus den gewonnenen Erkenntnissen geht hervor, ob es sich um Malware handelt oder nicht. Während mit statischen Analysemethoden (z.B. klassische Anti-Virus-Lösungen) nur Malware erkannt werden kann, für die bereits ein digitaler „Fingerabdruck“ vorliegt, ermöglicht die dynamische Analyse auch die Erkennung neuer, bislang noch nie aufgetretener Schadsoftware, für die noch keine Identifikationsmerkmale bekannt sind.

Im Umkehrschluss gilt jedoch auch, dass die dynamische Malware-Erkennung nur funktioniert, wenn die Malware ihre schädliche Aktivität auch tatsächlich innerhalb des Analysezeitraums ausführt. Cyberkriminelle statten ihre Malware daher oft mit innovativen Evasionstechniken aus, um sie unerkannt durch die Sandbox zu bringen. Grundsätzlich lassen sich die Umgehungsmethoden in drei Hauptkategorien einteilen:

1. SANDBOX-UMGEHUNG DURCH AKTIVE ERKENNUNG DER ANALYSE-UMGEBUNG

Hier wird die Schadsoftware mit der Fähigkeit ausgestattet, eine Sandbox zu erkennen: Die Malware sucht nach kleinen, verräterischen Unterschieden zwischen einer als Produktivsystem „getarnten“ Analyse-Umgebung und den regulären Systemen eines Unternehmens. Stellt die Malware fest, dass sie sich in einer virtuellen Maschine befindet, so ist das alleingenommen noch kein sicheres Zeichen, dass es sich dabei um eine Sandbox handelt, denn viele Produktivumgebungen sind mittlerweile virtualisiert. Deshalb wird die Malware nach weiteren Hinweisen suchen, z.B. den Hersteller-spezifischen Erkennungsmerkmalen einer Sandbox oder den typischen Spuren, die einige Sandboxing-Methoden in der Analyse-Umgebung hinterlassen.

Häufig prüft die Malware, wie realitätsnah oder realitätsfern die vorgefundene Umgebung ist. Verräterische Anzeichen sind beispielsweise eine ungewöhnlich niedrige Bildschirmauflösung, das Fehlen typischer Treiber oder Anwendungen, das Fehlen von Betriebssystem-Updates, das Fehlen eingerichteter Drucker, zu geringer

Netzwerkverkehr trotz angeblicher System-Uptime von mehreren Tagen, ein zu sauberes Dateisystem ohne kürzlich verwendete Benutzerdateien, das Fehlen von Cookies, etc.
Stellt die Malware nun fest, dass sie sich in einer Sandbox befindet, wendet sie in der Regel eine der folgenden Taktiken an, um einer Entdeckung zu entgehen:

» Sie beendet sofort alle Aktivität, was jedoch verräterisch sein kann, denn es entspricht nicht dem üblichen Verhalten eines harmlosen Programms.
» Sie zeigt zur Tarnung eine Fehlermeldung im Zusammenhang mit einem fehlenden Systemmodul oder einer beschädigten Datei an.
» Sie führt einige gutartige Operationen aus, um sich als harmloses Programm darzustellen.

2. SANDBOX-UMGEHUNG DURCH AUSNUTZUNG VON SANDBOX-SCHWÄCHEN

Die aktive Suche nach Sandbox-Merkmalen kann aber auch als suspekte Aktivität ins Auge fallen, wenn sie bei der Analyse registriert wird. Eine subtilere Methode ist daher die Ausnutzung von Schwächen und Lücken, die in manchen Sandboxing-Technologien vorhanden sind. Zu diesen Umgehungstechniken zählen:

» **Monitoring ausschalten:** die Malware versucht der Analyse zu entgehen, indem die Überwachungsmethoden der Sandbox ausgehebelt werden, z.B. durch die Entfernung oder Umgehung von Hooks (bei Hooking-basierten Sandboxes), durch die Verwendung von Dateiformaten, die in der Sandbox nicht ausgeführt werden können (beispielsweise .ps1, .hta, .dzip) oder durch die Nutzung von Technologien, die bei der Analyse unentdeckt bleiben (z.B. COM, Ruby, ActiveX, Java).
» **Analyse-Umgebung lahmlegen:** ein primitiver, aber gelegentlich sehr effektiver Ansatz besteht darin, die Analyse-Umgebung mit Formaten zu überwältigen, die von der Sandbox nicht unterstütz werden, so z.B. Dateigrößen mit mehr als 10 MB oder mehrfach komprimierten Dateien.

3. SANDBOX-UMGEHUNG DURCH KONTEXT-SENSITIVES VERHALTEN

Bei diesem Ansatz versucht die Malware weder das Vorhandensein einer Sandbox festzustellen, noch sucht sie nach Lücken oder Schwächen in der Sandbox-Architektur. Stattdessen verzögert sie die Ausführung der bösartigen Nutzlast, bis ein bestimmter Auslöser (Trigger) eintritt. Der Trigger ist so gewählt, dass die Auslösung während des Aufenthalts in der Sandbox unwahrscheinlich ist. Auch auf diese Weise kann Malware in der Analyse-Umgebung unentdeckt bleiben. Die Trigger lassen sich in vier Kategorien einteilen:

» **Time Bombs:** Sandboxes analysieren suspekte Dateien in der Regel nur wenige Minuten. Malware, die einen zeitbasierten Trigger enthält, bleibt inaktiv („schläft“), bis der im Trigger festgelegte Zeitpunkt erreicht ist. Der Trigger könnte z.B. so gesetzt sein, dass die Aktivität erst an einem bestimmten Tag oder nur zu einer bestimmten Uhrzeit beginnt (nur am 12. März oder nur montags um 13 Uhr).
» **System-Ereignisse:** In diesem Fall ist der auslösende Trigger an den Eintritt eines System-Ereignisses gekoppelt, wie Herunterfahren, Neustart, Einloggen oder Ausloggen eines Benutzers. Konkret könnte es so aussehen, dass die Malware im ersten Schritt eine ausführbare Datei installiert, die nach einem System-Neustart aktiv wird und die zweite, schädliche Nutzlast herunterlädt.
» **Nutzerinteraktion:** Hierbei wartet die Malware auf bestimmte Benutzeraktionen, bevor sie aktiv wird. Beispiele hierfür sind: Mausbewegungen, Tastatureingaben oder Interaktion mit bestimmten Anwendungen, wie zum Beispiel Browser, E-Mail oder einer Online-Banking-Anwendung oder das Anklicken mehrerer Schaltflächen und Kontrollkästchen, beispielsweise im Rahmen von bösartigen Installationsprogrammen.
» **Spezifisches Zielsystem:** Hochentwickelte zielgerichtete Angriffe (Targeted Malware) funktioniert nur auf den für sie vorgesehenen Zielsystemen, auf anderen Systemen bleiben sie inaktiv. Die Identifizierung des korrekten Ziels basiert hierbei häufig auf dem aktuellen Benutzernamen, der Zeitzone, dem Tastaturlayout, der IP-Adresse sowie anderen Eigenschaften, die nur in der anvisierten Zielumgebung anzutreffen sind.

EVASIONSTECHNIKEN EINEN STRICH DURCH DIE RECHNUNG MACHEN: WORAUF KOMMT ES BEI DER WAHL EINER SANDBOX AN?

Sandbox ist nicht gleich Sandbox – bei den ausgefeilten Täuschungsmanövern moderner Malware muss die gewählte Technologie einen hohen Schutz vor Sandbox Evasion zu bieten. Ältere Technologien oder Sandboxes mit Basis-Funktionalität haben nicht die benötigte Resistenz. Aber auch Sandboxing-Technologien der neueren Generation sollten auf architekturelle Schwächen geprüft werden.

Achten Sie dabei auf diese drei Kriterien:

1. ARTEFAKTE IN DER ANALYSE-UMGEBUNG VERMEIDEN.

Die Analyse-Umgebung sollte nichts enthalten, das auf Monitoring und Instrumentierung hinweist. Bei Hooking-basierten Sandboxing-Methoden ist es nahezu unmöglich, die Hooks komplett zu verbergen (d.h. die injizierten User-Mode- oder Kernel-Level-Treiber, die die API-Aufrufe und andere Malware-Aktivitäten überwachen und abfangen). Die Sandbox-Technologie sollte stattdessen einen Ansatz verfolgen, bei dem das Verhalten der Schadsoftware von außerhalb der Analyse-Umgebung stattfindet. Eine in den Hypervisor eingebettete Monitoring-Methode in Verbindung mit Virtual Machine Introspection (VMI) macht das möglich.

2. ANALYSE-UMGEBUNG REALITÄTSNAH GESTALTEN.

Generische Sandboxes mit identischen Standard-Umgebungen reichen nicht mehr aus. Um nicht erkannt zu werden, sollte die Sandbox die Produktivsysteme des Unternehmens möglichst detailgetreu nachbilden und pseudozufällige Attribute in die Analyse-Umgebung einsetzen. Sehr wirksam ist der Einsatz von Golden Images in der Sandbox-Umgebung, d.h. die Verwendung der standardmäßigen Betriebssysteme und Anwendungskonfigurationen, die das Unternehmen nutzt. Damit lassen sich auch zielgerichtete Angriffe identifizieren, die nur auf den Systemen des anvisierten Unternehmens aktiv werden. Die Sandbox sollte simulierte Benutzer-Interaktionen, wie beispielsweise automatisiertes Klicken auf Links oder Schaltflächen sowie automatisierte Reboots unterstützen.

3. MALWARE-VERHALTEN UMFASSEND SICHTBAR MACHEN:

Eine Sandbox muss detaillierten Einblick in die komplexe Struktur eines Malware-Angriffs geben und jede Interaktion der Malware mit der Systemumgebung registrieren und sichtbar machen. Dazu muss sie eine möglichst breite Palette verschiedener Datei-Formate und Programm-Typen ausführen können, da Malware in unterschiedlichsten Formen auftreten kann. Sleep-Funktionen der Malware müssen erkannt und ausgeschaltet werden, sodass der Schadcode noch innerhalb des Analysezeitraums zur Ausführung kommt. Die Qualität des Reportings ist ebenfalls von großer Bedeutung: manche Analyse-Reports sind zu oberflächlich und es fehlen wesentliche Details zum Malware-Verhalten; andere Reports enthalten zu viele irrelevante Informationen, sodass die wichtigen Signale durch Rauschen verwässert werden. Gute Reports zeichnen sich durch große Detailtiefe bei gleichzeitiger Rauschfreiheit aus, damit Angriffsvektoren rasch aufgedeckt werden können.

ÜBER VMRAY

VMRay bietet die branchenweit präziseste Lösung zur automatisierten Erkennung und Analyse moderner Malware-Bedrohungen. Weltweit vertrauen Unternehmen und Organisationen mit hohen Cybersicherheitsanforderungen auf VMRay Technologien.

Zum Kundenkreis zählen global agierende Finanz- und Versicherungsunternehmen, Industrie- und Technologiekonzerne, führende Wirtschaftsprüfungsunternehmen, sowie Behörden, Regierungs- und Forschungseinrichtungen.

Die VMRay Plattform umfasst drei Lösungen, die auf spezifische Incident Response- und SOC-Anforderungen ausgerichtet sind:

VMRAY ANALYZER

Der Gold Standard für die dynamische Analyse moderner Malware liefert Bedrohungsinformationen in großer Detailtiefe und unterstützt IR-Teams bei der Erkennung komplexer Angriffe.

VMRAY ETD

Ergänzt vorhandene Email-Security-Lösungen und identifiziert Email-basierte Angriffe, die von anderen Systemen nicht erkannt und abgefangen werden.

VMRAY DETECTOR

Skaliert die automatisierte Erkennung von Malware über das gesamte Unternehmen hinweg und stellt schnelle, präzise Verdikte zum Schadpotenzial der untersuchten Malware-Samples bereit.

VMRAY

VMRAY