Acronis

WHITEPAPER

Verwenden von KI zur Erkennung schädlicher Dokumente und Skripte

Zuverlässiger mehrschichtiger Schutz mithilfe von Maschinenintelligenz

Die Zahl gefährlicher Angriffe nimmt permanent zu und immer mehr Cyberkriminelle nutzen Social Engineering in E-Mails oder anderen Kommunikationskanälen als initialen Angriffsvektor. Sehr oft enthalten betrügerische E-Mails schädliche Anhänge mit Malware, die beim Öffnen ausgeführt wird und über eine Schwachstelle schädliche Aktionen durchführt. Schädliche Dokumente können auch über einen Link heruntergeladen werden, den Benutzer über andere Kommunikationskanäle erhalten.

Acronis Experten zufolge wurden bis Mitte des Jahres 2022 bei etwa einem Drittel aller Angriffe manipulierte oder schädliche Dokumente wie Microsoft Office- oder Adobe PDF-Dateien genutzt. Andere Branchenakteure zeichnen ein ähnliches Bild. In den meisten Fällen ist Malware in eine Datei eingebettet. Die Ausführung kann jedoch auf unterschiedliche Weise erfolgen. Wenn beispielsweise eine Schwachstelle das erste Mal ausgenutzt wird, werden die Berechtigungen ausgeweitet und die Malware anschließend heruntergeladen und ausgeführt. Microsoft Office- und PDF-Dateien werden seit Jahren bei Cyber-Angriffen genutzt, da sie die Einbettung von Makros, Shellcode, JavaScript und sogar ganzen Dateien ermöglichen. Doch das Problem hat sich in den letzten Jahren verschärft, da die Hacker nun Suchmaschinenoptimierung (Search Engine Optimization, SEO) nutzen, um schädliche Dateien – und insbesondere PDF-Dateien – in Suchergebnissen höher zu platzieren.

Ein ähnliches Problem betrifft schädliche Skripte, die von legitimen Tools wie PowerShell ausgeführt werden. Angriffe mit schädlichen Skripten und Dokumenten nehmen von Jahr zu Jahr kontinuierlich zu, wobei sich die Zahl laut Acronis Experten in den letzten zwei Jahren nahezu verdoppelt hat. Mit schädlichen Skripten wird das gleiche Ziel verfolgt: ein System infiltrieren, Berechtigungen ausweiten und dann den Payload herunterladen und ausführen.

Für die Cyber Security-Branche sind die oben beschriebenen Probleme gleich, da Benutzer immer zwischen harmlosen und schädlichen Dokumenten bzw. Skripten unterscheiden müssen. Die gute Nachricht ist, dass das Problem durch die Verwendung von Machine Learning (ML) und künstlicher Intelligenz (KI) – oder wie wir bei Acronis sagen: mit Maschinenintelligenz (MI) – sehr viel effektiver gelöst werden kann.

Verwenden von Maschinenintelligenz zur Bedrohungserkennung

Der Startschuss für die Verwendung von Machine Learning fiel bei Acronis im Jahr 2017, als das Unternehmen die Ransomware-Technologie Active Protection einführte. Schon bald darauf entwickelten wir ein vollständig KI-basiertes, statisches Modul für Verhaltenserkennung, das aktuell in unserem Flaggschiffprodukt Acronis Cyber Protect zum Einsatz kommt.

Das Modul wird immer auf dem neuesten Stand gehalten und mit jedem neuen Machine Learning-Modell in puncto Leistung und Erkennungsrate verbessert. Am Anfang wurde es beispielsweise zur Stapelüberwachungsanalyse von ausgeführten Prozessen genutzt. Später untersuchte es ganze Dateien und Bibliotheken auf schädliche Elemente. Heute kann es Zeichenfolgen analysieren, die aus ausführbaren Dateien extrahiert wurden, und Bilder verarbeiten. Durch zusätzliche Merkmale wie die Häufigkeit bestimmter Zeichenfolgen in einigen hundert ausgewählten Wörtern konnte die Erkennungsrate um 3 % gesteigert werden!

Wie Sie sich sicherlich vorstellen können, lassen sich mit einem ähnlichen Ansatz schädliche Dokumente und Skripte erkennen. Widmen wir uns zunächst den Microsoft Office-Dokumenten. Obwohl Microsoft kürzlich angekündigt hat, Makros in Dokumenten, die über das Internet verbreitet werden, standardmäßig zu deaktivieren, löst dies nicht alle Probleme. Windows fügt Dateien aus nicht vertrauenswürdigen Speicherorten (z. B. dem Internet oder eingeschränkten Zonen) das Attribut „Mark of the Web“ (MOTW, engl. für „Zeichen des Webs“) hinzu. Dies erfolgt beispielsweise bei Browser-Downloads oder E-Mail-Anhängen. Allerdings erhalten dies nur Dateien, die auf einem NTFS-Dateisystem gespeichert werden. Bei Geräten mit FAT32-Dateisystem ist dies nicht möglich. Und was passiert, wenn die Datei aus einer legitimen E-Mail stammt? Außerdem kann dieses Vorgehen in einem Bereich, in dem Makros sehr häufig genutzt werden (z. B. in der Buchhaltung), zu Problemen führen. Dennoch wird die Sicherheit von Umgebungen durch solche Richtlinien verbessert. Zudem können in einigen Fällen typische Phishing-Angriffe wie die Emotet-Kampagne erfolgreich abgewehrt werden. Doch wie bereits erwähnt, ist diese Maßnahme nicht ausreichend und führt in vielen Unternehmen zu weiteren Komplikationen. Deshalb haben unsere Acronis KI-Spezialisten das Erkennungsmodul so verbessert, dass es per Machine Learning schädliche Dokumente erkennen kann.

Makro-Skripte könnten als schädlich eingestuft werden, wenn sie eine oder mehrere der folgenden Aktionen ausführen:

- Erstellung von Prozessen
- Ausführung von Skripten in PowerShell, VBA usw.
- Herunterladen von Dateien von Remote-Servern
- Einbettung in andere Office-Dateien oder Office-Vorlagen-Dateien

Selbstverständlich ist die Erkennung in der Praxis schwieriger, da viele weitere Parameter berücksichtigt werden müssen. Das Machine Learning-Modell von Acronis prüft daher beispielsweise folgende Attribute von DOCX-Dateien:

- Verschiedene Merkmale zum Text und zu VBA-Funktionen
- Verhältnis-Merkmale wie Kommentare, Code usw.
- Die Entropie eines Makros selbst, des enthaltenen Codes und der Kommentare
- Eventuell präsente Verschleierungen und was verschleiert wird
- Bekannte Parameter von Kompromittierungsindikatoren wie URLs, ausführbare Dateien usw.

Diese Liste ist natürlich nicht vollständig, sie zeigt jedoch, dass viele Aspekte anhand eines großen Datensatzes analysiert werden, der kontinuierlich überarbeitet und aktualisiert wird. Mit dieser Methode erreichen wir eine hervorragende Erkennungsrate bei einer komprimierten Modellgröße von weniger als einem Megabyte. Ohne KI und ML wären solche Ergebnisse unmöglich. Zudem sollte beachtet werden, dass dies nur ein Teil eines robusten mehrschichtigen Schutzkonzepts ist und nur ausgelöst wird, wenn die Bedrohung nicht vorher von anderen Technologien wie E-Mail-Sicherheitsscans und Sandboxes oder URL-Filterung erkannt wird.

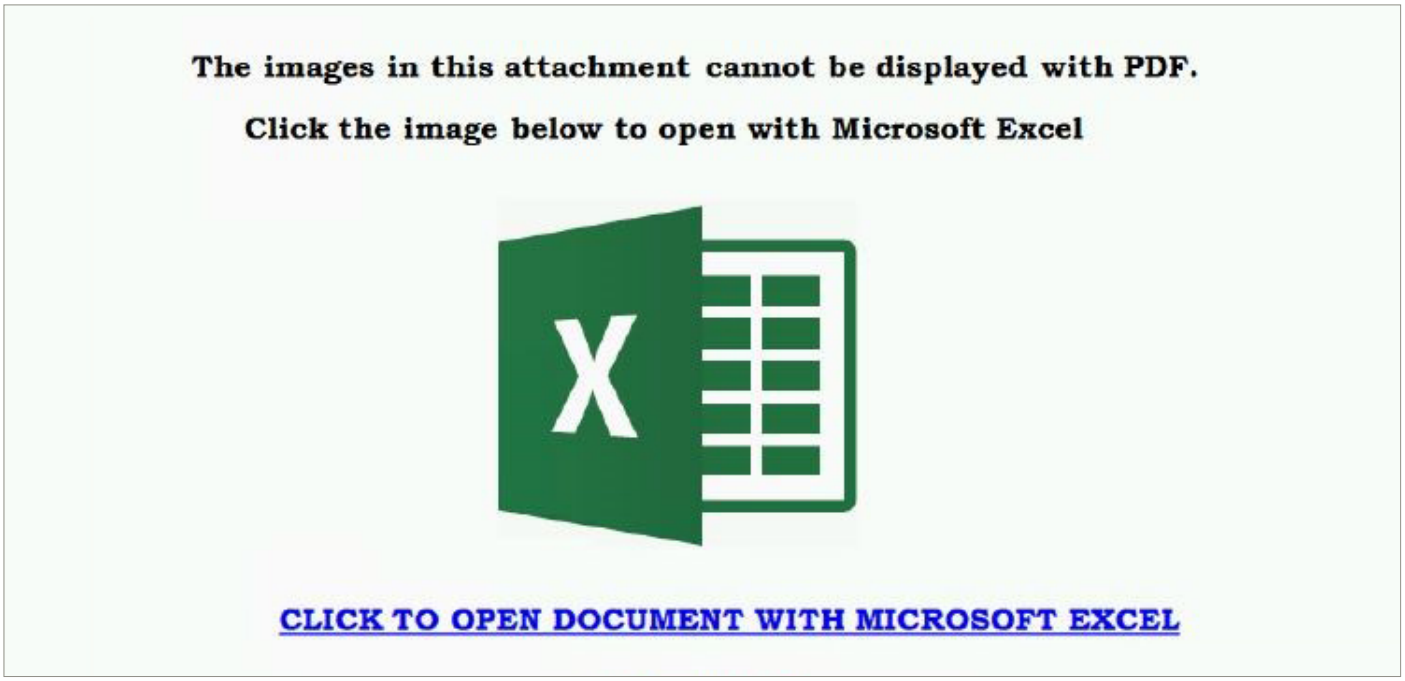
Ein ähnlicher Ansatz wurde von den Acronis Experten vor Kurzem zur Erkennung schädlicher AutoIT-Skripte eingesetzt, die häufig bei Service Providern genutzt werden. Mit einem winzigen Modell, das eine Größe von etwa 0,6 MB hat, erzielen wir bereits eine Erkennungsrate von 92 %. Das gleiche gilt für DOCX-Dateien, deren Erkennungsmodell ständig verbessert wird.

Beseitigen der Bedrohung durch manipulierte PDF-Dateien

Neben Word-Dokumenten für Microsoft Office ist für Cyberkriminelle auch das Portable Document Format (PDF) von Adobe ein äußerst beliebtes Tool, um Systeme zu kompromittieren oder Malware in den Rechner eines Benutzers einzuschleusen. PDF-Dateien basieren auf der Sprache PostScript und enthalten sehr viele Informationen wie Text, Hyperlinks, Multimedia, Bilder, Anhänge, Metadaten usw., die es zu einem vielseitigen Format machen. Das PDF-Format hat eine „Aktionen"-Funktion, die es ermöglicht, Links oder Dateien zu öffnen und JavaScript-Code sowie andere Operationen auszuführen, die – wie Sie sich vorstellen können – auch zu böswilligen Zwecken missbraucht werden können.

PDF-Dokumente lassen sich mit Browsern und einer Vielzahl an Programmen öffnen. Diese haben alle potenzielle Schwachstellen, die von Bedrohungsakteuren ausgenutzt werden können. Dazu zählen beispielsweise die Ausführung von beliebigem Code, Pufferüberlauf, Speicherfehler, Out-of-Bounds-Zugriff und viele mehr. Aktuell existieren hunderte CVEs (Common Vulnerabilities and Exposures) für PDF-Reader und fast 300 bekannte Schwachstellen allein für Adobe Acrobat Reader. Sicherheitsforscher und Bedrohungsakteure finden praktisch jeden Tag neue PDF-bezogene Exploits.

Hier ist ein Beispiel für die Ausnutzung der Schwachstelle CVE-2021-28550 in der Praxis: Folgende Versionen von Acrobat Reader DC sind von einer Use-After-Free-Schwachstelle betroffen: 2021.001.20150 (und älter), 2020.001.30020 (und älter), und 2017.011.30194 (und älter). Nicht autorisierte Angreifer könnten die Schwachstelle für die Ausführung von beliebigem Code unter dem aktuellen Benutzer ausnutzen. Dazu muss ein Benutzereingriff erfolgen, d. h. das Opfer muss eine schädliche Datei öffnen.



Beispiel für Phishing mit einem schädlichen Link in einer PDF-Datei

Wie bereits beschrieben, prüft das Acronis Machine Learning-Modell zur Erkennung schädlicher PDF-Dateien eine Vielzahl an Parametern, um zu einem korrekten Urteil zu kommen:

- Entropie
- Gesamtanzahl der Zeichen
- Anzahl besonderer Schlüsselwörter
- Zahl der Zeilen und speziellen Zuweisungszeilen
- sowie weitere Parameter

Dies führt zu einer identischen und äußerst hohen Erkennungsrate.

Cyber Security-Schulungen zur deutlichen Risikoreduzierung

Natürlich muss ein solches Erkennungsmodell in eine gute Cyber Protection-Lösung integriert sein. Dennoch lässt sich die Sicherheit einzelner Personen und eines gesamten Unternehmens erheblich verbessern, wenn die Benutzer darin geschult werden, welche Bedrohungen es gibt und wie sie damit umgehen sollten. Schließlich erfordern schädliche Dokumente oder Skripte in den meisten Fällen einen Benutzereingriff – und ohne diesen Benutzereingriff gibt es keine Bedrohung.

Diese Sensibilisierungsschulungen müssen grundlegende Sicherheitsregeln abdecken:

- Prüfen Sie stets die Quelle von E-Mails und Links. Kennen Sie diese Person? Erwarten Sie diese Datei? Überprüfen Sie auf jeden Fall die tatsächliche E-Mail-Adresse des Absenders, nicht nur den Namen oder Alias.
- Haben Sie bereits auf eine Datei geklickt und es erscheint eine Inkompatibilitätsmeldung, Sie werden um eine Aktion gebeten, es erscheinen mehrere Links oder ein gefälschtes Captcha oder Ähnliches, sollten Sie sofort alles schließen und löschen und das Sicherheitsteam informieren.
- Wenn Sie auf eine Datei geklickt haben, ohne dass danach etwas passiert ist, könnte dies ebenfalls ein schlechtes Zeichen sein. Wenn eine Datei geöffnet wurde und nicht das geschah, was Sie erwartet haben, sind Sie möglicherweise Opfer eines Angriffs geworden und sollten sofort das Sicherheitsteam benachrichtigen.

Die beste Regel ist also, keine Anhänge zu öffnen und nicht sofort auf Links zu klicken. Überprüfen Sie alles zwei Mal. Falls Sie sich dann immer noch nicht sicher sind, kontaktieren Sie das Sicherheitsteam. Bleiben Sie wachsam und geschützt!

Acronis

Weitere Informationen unter
www.acronis.com