zscaler™

E-Book

BUSTING

9 Mythen rund um dateibasierte Bedrohungen

© 2023 Zscaler, Inc. Alle Rechte vorbehalten.

Einige gängigen Meinungen zum Thema dateibasierte Bedrohungen — diese halten einer objektiven Betrachtung nicht stand.

Das Herunterladen und Übertragen von Dateien zählt im Zeitalter der digitalen Kommunikation ganz selbstverständlich zum Berufsalltag. Dennoch oder gerade deshalb lassen Mitarbeiter und andere User im Umgang mit den Risiken und Bedrohungen, die sich in Dateien verbergen können, oft nicht die gebotene Vorsicht walten. Diese Achtlosigkeit machen sich Bedrohungsakteure zunutze, um ihre Opfer mit unwiderstehlichen Tipps zu Shortcuts in Microsoft Excel und dringenden Nachrichten über überfällige Rechnungen zu ködern. Der User wird aufgefordert, eine Datei herunterzuladen oder einen Link anzuklicken, um weitere Informationen anzuzeigen.

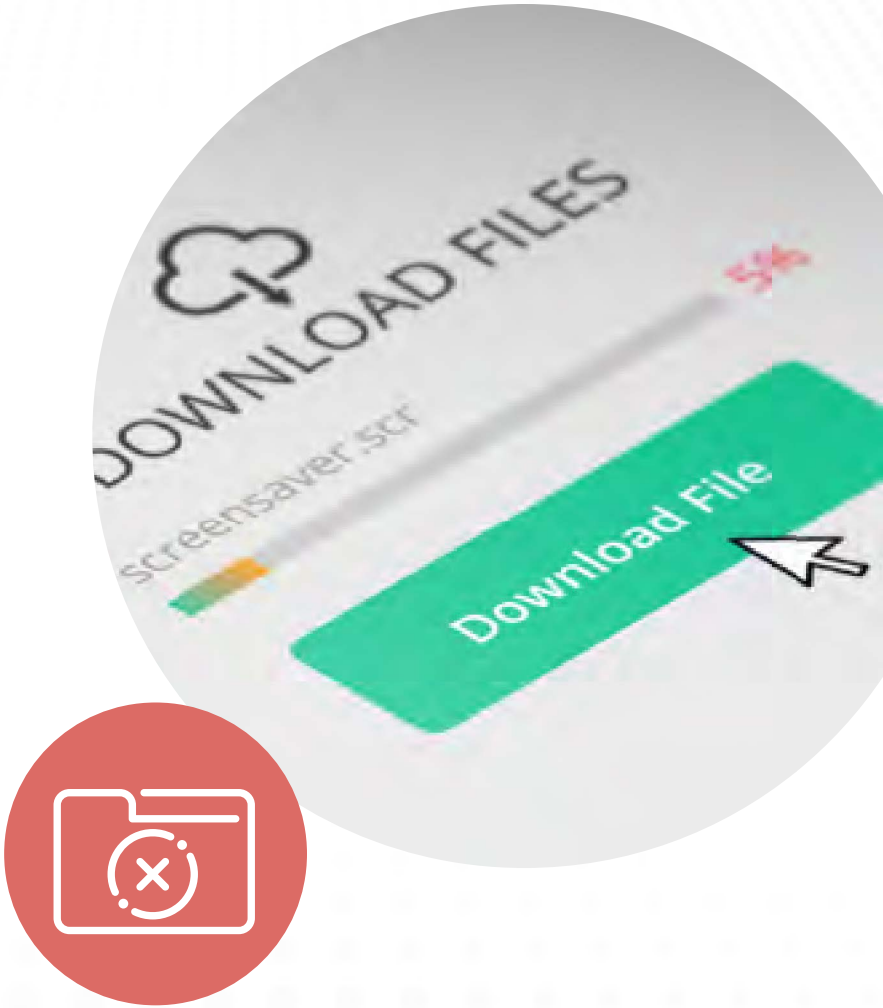
Hinzu kommt, dass User von unterwegs und direkt übers Internet auf Dateien zugreifen und dabei die Sicherheitskontrollen unterlaufen, die Ihre Administratoren eingerichtet haben. Ohne Analysefunktionen und Bedrohungsschutz für Dateien —einschließlich derjenigen, die über verschlüsselte Kanäle übermittelt werden — sind Organisationen hohem Risiko ausgesetzt und hochgradig anfällig für Patient-Zero-Infektionen.

Viele Organisationen halten nach wie vor an veralteten Sicherheitsstandards und -strategien fest, die längst keinen ausreichenden Schutz vor diesen zunehmend raffinierten Bedrohungen mehr gewährleisten. Selbst routinierte Profis mit langjähriger Erfahrung wiegen sich teilweise in falscher Sicherheit. In diesem Beitrag nehmen wir deshalb 9 gängige Mythen rund um dateibasierte Bedrohungen unter die Lupe. Außerdem haben wir einige Tipps zum Schutz vor neuartigen Angriffstechniken parat.

© 2023 Zscaler, Inc. Alle Rechte vorbehalten.

MYTHOS Nr. 1

Wer schädliche EXE- und DLL-Dateien blockiert, ist ausreichend geschützt



BUSTED

Die PE-Dateitypen (Portable Executable), die in Unternehmen am häufigsten vorkommen, sind EXE und DLL — sie sind jedoch keineswegs die einzigen PEs, die Malware übertragen können. Angreifer und Bedrohungsakteure können Bedrohungen in SYS-, OCX- und APK-Dateien einbetten — auch in so vermeintlich harmlosen Dateitypen wie SCR.

SCR-Dateien werden u. a. im Windows-Betriebssystem zum Anzeigen von Animationen, Videos und Bildern verwendet, wenn der Rechner im Leerlauf ist. Mitarbeiter nutzen gerne die Möglichkeiten zur Individualisierung ihrer Benutzeroberfläche — und achten beim Herunterladen der Dateien nicht unbedingt darauf, wie vertrauenswürdig die jeweilige Quelle ist. So kann sich hinter dem vermeintlich coolen Bildschirmschoner ein Virus oder Trojaner verbergen, der sich dann im Netzwerk verbreitet.

© 2023 Zscaler, Inc. Alle Rechte vorbehalten.

MYTHOS Nr. 2

Ein einziger User, der eine schädliche Datei öffnet, kann im gesamten Netzwerk Chaos anrichten

CONFIRMED

Cyberangriffe und Betrugsmaschen sind nicht zuletzt deshalb so lukrativ, weil es ausreicht, wenn ein einziger User auf sie hereinfällt und dem Angreifer Zugang zum Netzwerk gewährt wird bzw. ein einziges Opfer bereit ist, das geforderte Lösegeld zu zahlen.

Phishing und zielgerichtete Spear-Phishing-Kampagnen sind und bleiben eine beliebte Methode zur Übertragung von Malware. Dabei werden User dazu verleitet, eine unbekannte Datei herunterzuladen oder einen Link zu einer kompromittierten Webseite anzuklicken, die ein Exploit enthält.

Das kann zu einem Patient-Zero-Angriff führen, d. h. der betroffene Mitarbeiter oder User wird zum ersten dokumentierten Opfer einer neu entwickelten Cyberbedrohung.

Mit herkömmlichen Sandboxes, insbesondere solchen mit Passthrough-Architektur, und Antivirus-Tools, die auf Signaturen angewiesen sind, bleiben Unternehmen weiterhin anfällig für Patient-Zero-Infektionen. Neue Varianten oder Bedrohungen werden erst entdeckt, wenn mindestens ein Endgerät bereits kompromittiert ist.

Manche Bedrohungsakteure nehmen spezifische User oder Organisationen ins Visier. Sie entwickeln einzigartige Varianten von Malware für diese Entitäten, die signaturbasierte Schutzmechanismen umgehen oder sich im verschlüsselten Traffic verstecken. Durch die KI-gesteuerte Quarantäne in Zscaler Advanced Sandbox lassen sich Angriffe dieser Art verhindern.

© 2023 Zscaler, Inc. Alle Rechte vorbehalten.

MYTHOS Nr. 3

Wenn nur unbedenkliche Dateitypen (wie z. B. PDFs) zugelassen werden, haben dateibasierte Malware-Angriffe keine Chance

BUSTED

Insbesondere für Unternehmen mit geringer Risikotoleranz empfiehlt sich die Erstellung von Richtlinien für zulässige Dateitypen als effektiver erster Schritt zur Bewältigung von Bedrohungen. Jedoch sollten auch unbekannte PDF- und Microsoft-Dokumente, die direkt aus dem Internet oder aus E-Mail-Anhängen heruntergeladen werden, als verdächtig behandelt werden.

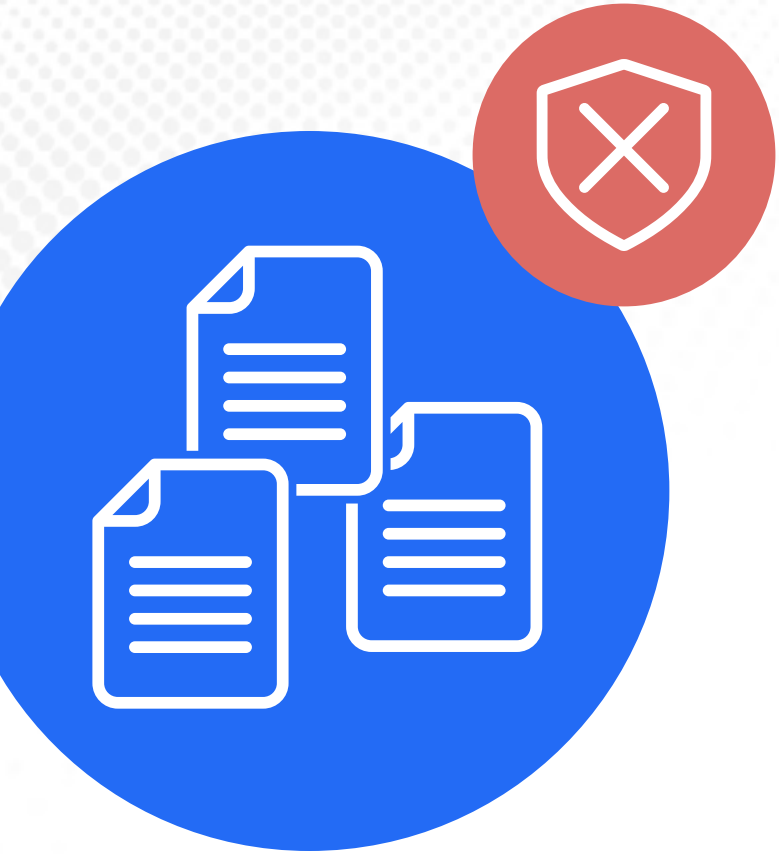
PDF-Dateien lassen sich nämlich hervorragend für Angriffe ausnutzen, indem z. B. JavaScripts eingebettet werden, die beim Öffnen des Dokuments ausgeführt werden. Außerdem haben Sicherheitsexperten bereits mehrmals Sicherheitslücken in den Adobe-Programmen Reader und Acrobat nachgewiesen.

Gewitzte Bedrohungsakteure können Kontrollmechanismen unterlaufen, indem sie kontinuierlich neue PDFs generieren, deren Überprüfung hardwarebasierte Sandbox-Lösungen überfordert. Alternativ werden User mit Social-Engineering-Techniken dazu verleitet, einen Link in einer ansonsten harmlosen PDF-Datei anzuklicken, der sie zu einer kompromittierten oder schädlichen Webseite weiterleitet.

Auch Microsoft-Dokumente können eingebettete Ransomware, Malware, Spyware, Grayware oder Adware enthalten. Zudem setzen Bedrohungsakteure schädliche Makros zum Ausführen von Befehlen ein.

Unglücklicherweise können Legacy-Sandboxes, die zwischen Leistung und Sicherheit abwägen müssen, möglicherweise nicht alle Seiten und eingebetteten Objekte überprüfen.

© 2023 Zscaler, Inc. Alle Rechte vorbehalten.



Ab Dezember 2022 werden Makros aus dem Internet in Office 365 standardmäßig blockiert.

MYTHOS Nr. 4

Makros in Microsoft-Office-Dokumenten müssen blockiert werden

PLAUSIBLE

Makros sind Befehle und Anweisungen, die Aufgaben automatisieren und benutzerdefinierte Funktionen erstellen, um bei der Erledigung von Routinearbeiten Zeit zu sparen und die Produktivität zu steigern.

Bedrohungsakteure verwenden Makros jedoch zur Verbreitung von Malware und Ausführung von Schadcode, um sich unbefugten Zugang zu einem System oder Netzwerk zu verschaffen bzw. eine Backdoor zu erstellen. Zum Abrufen schädlicher Makros kommt u. a. die Technik der Remote-Vorlageninjektion zum Einsatz, d. h. eine Vorlage wird von einem Server geladen, den die Angreifer kontrollieren.

Die Blockierung sämtlicher Makros — inklusive solcher in vertrauenswürdigen Dateien — würde leider zu erheblichen Störungen der Arbeitsabläufe führen. Das hätte wiederum zur Folge, dass User nach Möglichkeiten suchen würden, eine entsprechende Richtlinie zu umgehen. Im Ergebnis kommt es zu beeinträchtigter Transparenz für Administratoren und womöglich zu zusätzlichen Risiken für das Unternehmen.

Stattdessen sollten Systemadministratoren Makros aus dem Internet sowie in nicht vertrauenswürdigen Dateien blockieren und User schulen, Aufforderungen zum Aktivieren von Makros zu ignorieren.

© 2023 Zscaler, Inc. Alle Rechte vorbehalten.

MYTHOS Nr. 5

Dateien mit mehreren verschachtelten Archivdateien müssen automatisch blockiert werden

PLAUSIBLE

Archivdateien dienen zur Gruppierung mehrerer Dateien in einer einzigen Datei. Dadurch wird die Portabilität verbessert, zudem lässt sich durch Dateikomprimierung Speicherplatz sparen.

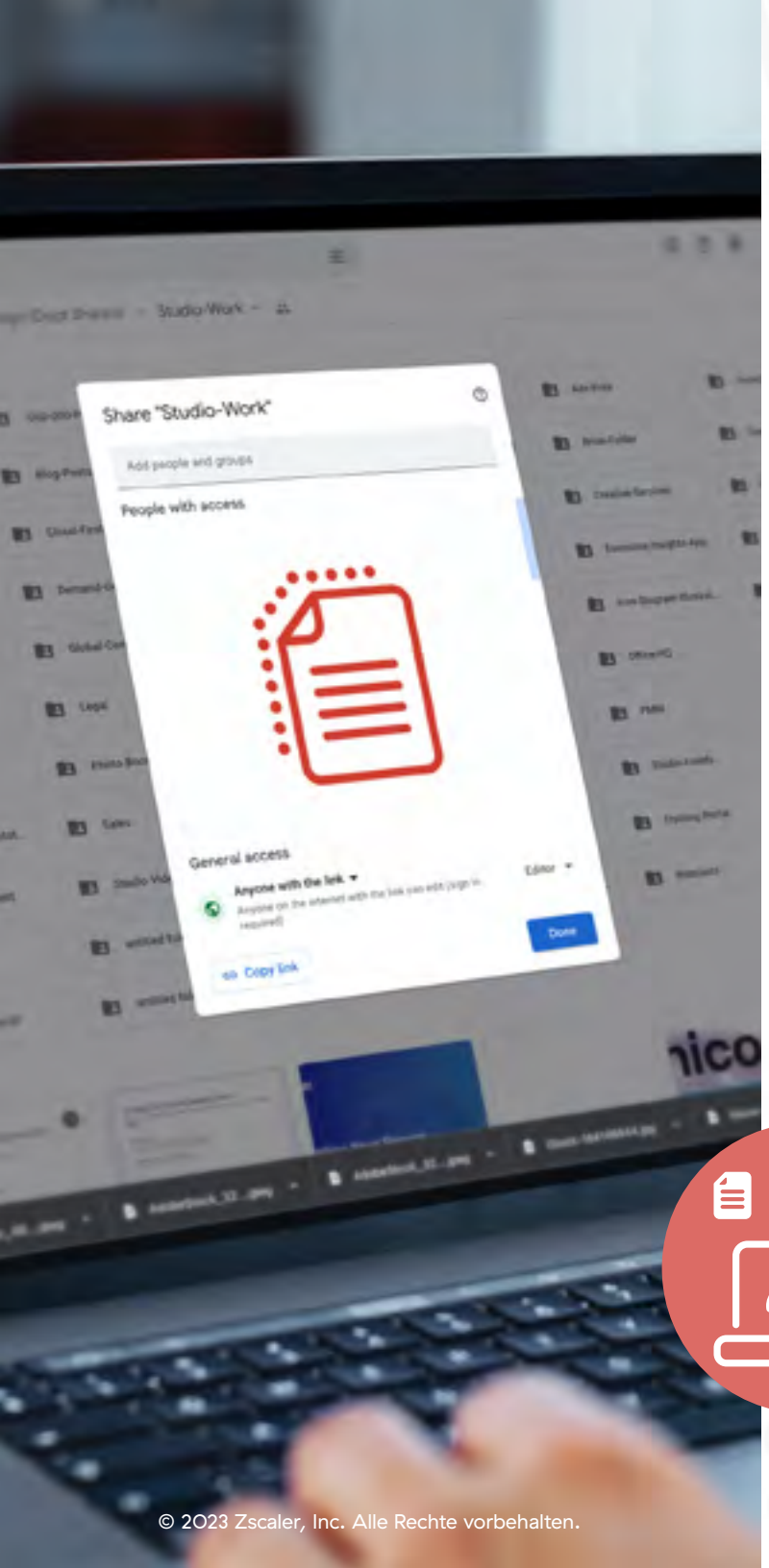
ZIP-Dateien unterstützen beispielsweise eine verlustfreie Datenkomprimierung. Beim Dekomprimieren der Datei werden die Daten in ihrer ursprünglichen Fassung wiederhergestellt.

Für bestimmte Branchen, etwa im Rechts- und Finanzwesen, kann es sinnvoll sein, Informationen in einem oder mehreren Verzeichnissen oder zusätzlichen verschachtelten Archivdateien zu speichern, um den Zugriff darauf einzuschränken.

Angreifer können Schutzmechanismen umgehen, indem sie ihre schädliche Payload hinter mehreren archivierten Dateien verschachteln. Möglicherweise führen sie auch weiteres Unheil im Schilde. Zip-Bomben zum Beispiel sind darauf ausgelegt, den Betrieb eines Programms oder Systems zu überfordern, indem sie übermäßig viel Rechenleistung oder Speicherplatz beanspruchen. Dadurch können Bedrohungsakteure Antivirensoftware deaktivieren und Malware übertragen.

Archivdateien mit mehr als sechs verschachtelten Verzeichnissen werden von Zscaler Sandbox automatisch blockiert.

© 2023 Zscaler, Inc. Alle Rechte vorbehalten.



MYTHOS Nr. 6

Schädliche Dateien können in Google Drive und OneDrive frei- bzw. weitergegeben werden

CONFIRMED

Vertrauenswürdige Filesharing-Websites vermitteln die Illusion von Sicherheit, da sie oft über integrierte Virensuchprogramme verfügen. Trotzdem hat das ThreatLabz-Team von Zscaler schon mehrmals Fälle von Malware-Übertragungen aus Google Drive, AWS, Dropbox und OneDrive nachgewiesen. Angreifer nutzen diese Tools gerade wegen ihrer Vertrauenswürdigkeit, um sich den Anschein von Legitimität zu verschaffen und Sicherheitskontrollen zu umgehen.

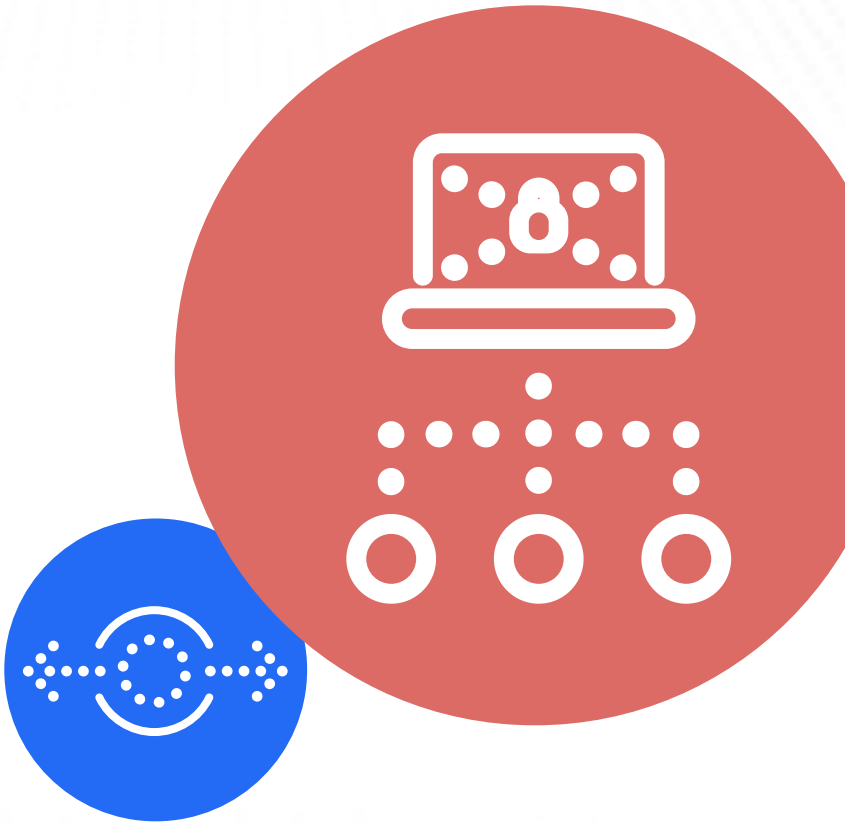
Deswegen müssen Unternehmen unbedingt ihren gesamten Web- und FTP-Traffic nach Bedrohungen durchsuchen, und zwar auch SSL/TLS-verschlüsselte Dateien. Dadurch wird Transparenz gewährleistet und verhindert, dass Angreifer sich unbefugten Zugang zum Netzwerk verschaffen.

© 2023 Zscaler, Inc. Alle Rechte vorbehalten.

MYTHOS Nr. 7

Durch Eindämmen einer Infektion auf einem Endgerät mit einem EDR werden weitere Kompromittierungen verhindert

BUSTED



Die Eindämmung der Infektion ist eine wichtige Strategie bei der Orchestrierung der Behebungsmaßnahmen für ein infiziertes Endgerät. Sie kann sich jedoch als unwirksam erweisen, wenn sich der Angreifer bereits lateral im Netzwerk ausgebreitet oder Malware oder Ransomware installiert hat. Malware-Entwickler machen sich mit Vorliebe Schwachstellen oder Lücken in EDRs und anderen gängigen Sicherheitstools zunutze. Beispielsweise erstellen sie Binärdateien, die Kontrollmechanismen unterlaufen und die Reaktionsstrategie manipulieren können.

Zudem gewährleisten EDRs nur Schutz vor Bedrohungen, die direkt vom Endgerät ausgehen. Gegen andere Angriffsarten, z. B. die Ausnutzung von Cloud-Anwendungen zur Übertragung von Malware, können sie nichts ausrichten. Deswegen ist Netzwerkschutz ein unverzichtbares Muss.

Sobald eine Bedrohung erkannt wird, beginnt für die zuständigen Sicherheits- und IT-Teams ein Wettlauf gegen die Zeit: Die Bedrohung muss möglichst schnell für sämtliche User, Geräte und Anwendungen blockiert und die Zugriffsrichtlinien entsprechend angepasst werden, um den laufenden Angriff zu stoppen.

Zscaler Sandbox verhindert, dass dateibasierte Bedrohungen über Web- und Dateiübertragungsprotokolle (einschließlich SSL/TLS) an User ausgeliefert werden.

© 2023 Zscaler, Inc. Alle Rechte vorbehalten.

MYTHOS Nr. 8

Legacy-Sandbox-Appliances gewährleisten effektiven Schutz vor Malware

BUSTED

Über **85 % aller Angriffe werden inzwischen im verschlüsselten Traffic übertragen**. Herkömmliche Sandbox-Appliances sind mit der Entschlüsselung hoher Traffic-Volumen überfordert und gewährleisten keine lückenlose Überprüfung auf versteckte Bedrohungen. Appliances mit Passthrough-Architekturen und Richtlinien, die unbekannte Dateien erst zulassen und dann scannen, können Patient-Zero-Infektionen nicht zuverlässig verhindern.

Cloud-basierte Sandbox-Lösungen gewährleisten höhere Analysekapazitäten. Dabei ist jedoch zu bedenken, dass Out-of-Band-Architekturen sich nur bedingt zur Bedrohungsprävention eignen. Schutzmaßnahmen können nämlich erst nachträglich auf sämtliche User angewendet werden, wenn das ursprüngliche Opfer bereits kompromittiert ist.

Zscaler Sandbox gewährleistet Inline-Schutz mit sofortiger Bereitstellung sicherer Dateien, Abwehr von Patient-Zero-Angriffen und granularen Policy-Controls. Durch einen skalierbaren SSMA-Ansatz (Single-Scan, Multi-Action™) verhindert der Cloud-basierte Service die Ausbreitung unbekannter Malware mithilfe von Dateien.

© 2023 Zscaler, Inc. Alle Rechte vorbehalten.

MYTHOS Nr. 9

Cybersicherheitsschulungen sind ein Garant dafür, dass User keine unbekannten Dateien öffnen

PLAUSIBLE

Es wäre ein Fehler, die Mitarbeiter und User lediglich als schwächstes Glied im Sicherheitsprogramm Ihrer Organisation anzusehen. In Wirklichkeit stellen sie einen Angriffsvektor dar und müssen als solcher behandelt werden. Sicherheitsschulungen für Ihre User gehören ebenso zu einer effektiven Bedrohungsabwehrstrategie wie Maßnahmen zur Verkleinerung der Angriffsfläche und Behebung von Fehlkonfigurationen. Nur so können Sie Ihr Geschäftsrisiko minimieren und verhindern, dass schädliche Dateien heruntergeladen werden.

Mit Mitarbeiterschulungen ist es jedoch nicht getan. Daneben müssen Unternehmen zukunftsfähige Sicherheitstools einsetzen, die Funktionen zur dynamischen Erkennung von Angriffstechniken wie Domain-Squatting und Spoofing sowie zur Blockierung der entsprechenden Websites bereitstellen. Diese Phishing-Websites sind nur schwer als Fälschungen zu identifizieren. Oft verwenden sie legitime Webhosting-Services und verfügen sogar über Google-Trust-Zertifikate. Es sind Fälle bekannt, bei denen selbst erfahrene Sicherheitsexperten auf die Täuschung hereingefallen sind und sich dazu verleiten ließen, Dateien von diesen Websites herunterzuladen.

© 2023 Zscaler, Inc. Alle Rechte vorbehalten.

Zscaler Sandbox gewährleistet zuverlässigen Schutz vor dateibasierten Angriffen

Mit Inline-Überprüfung und der branchenweit ersten KI-gesteuerten Engine zur Malware-Prävention, die auf einer skalierbaren, Proxy-basierten Architektur basiert, kann Zscaler Sandbox unbekannte Bedrohungen und verdächtige Dateien automatisch erkennen, blockieren und dynamisch isolieren.

Schädliche Dateien und Codeausführungen werden in allen Web- und Dateiübertragungsprotokollen (FTP), einschließlich SSL/TLS, analysiert und blockiert.

Sie erhalten verwertbare Erkenntnisse und Kontextinformationen zu dateibasierten Bedrohungen mit einem detaillierten Report zu Angriffszyklus, Killchain, Verhalten der Malware und Payload Intent. Alle Daten werden direkt aus den Code-Binärdateien bezogen und anhand des Frameworks MITRE ATT&CK ausgewertet.

Weitere Informationen zur Zscaler Sandbox finden Sie auf unserer **entsprechenden Webseite** sowie im **Datenblatt**.

	Erweiterte Funktionen* **In ZIA Transformation und Unlimited inbegriffen**
Inline-Blockierung	✓
Dateitypen	EXE, DLL, SCR, OCX, SYS, CLASS, JAR, PDF, SWF, DOC(X), XLX(X), PPT(X), APK, ZIP, RAR, 7Z, BZ, BZ2, TAR, TGZ, GTAR, RTF, PS1, HTA, VBS, Skriptdateien in ZIP-Dateien
KI-basierte Quarantäne	✓
Policy-Control	✓ Granulare quarantänebasierte Richtlinien
Reporting	✓
Alle URL-Kategorien	✓
API-Integrationen	✓

*Erweiterte Funktionen für Zscaler Sandbox sind als Add-on-Modul für ZIA Essentials- und Business-Editionen erhältlich

© 2023 Zscaler, Inc. Alle Rechte vorbehalten.

zscaler™ | Experience your world, secured.™

Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Zscaler Zero Trust Exchange schützt Tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlust. Die SASE-basierte Zero Trust Exchange ist in über 150 Rechenzentren auf der ganzen Welt verfügbar und die weltweit größte Inline-Cloud-Sicherheitsplattform. Weitere Informationen finden Sie auf **zscaler.de** oder auf Twitter unter **@zscaler**.

© 2023 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™ und ZPA™, Zscaler Digital Experience und ZDX™ sowie weitere unter **zscaler.de/legal/trademarks** aufgeführte Marken sind entweder (i) eingetragene Marken bzw. Dienstleistungsmarken oder (ii) Marken bzw. Dienstleistungsmarken von Zscaler, Inc. in den USA und/oder anderen Ländern. Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber.

+1 408 533 0288

Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA

zscaler.de