



STRATEGIEPAPIER

MALWARE-SCANS SCHÜTZEN IHR UNTERNEHMEN, IHRE KUNDEN – UND IHR GESCHÄFTSERGEBNIS

INHALT

- 3 MALWARE KANN ÜBERALL LAUERN
- 3 WAS IST EIGENTLICH MALWARE?
- 3 ABLAUF EINES MALWARE-ANGRIFFS
- 5 MALWARE ALS GESCHÄFTSMODELL
- 5 VERISIGN: IHR ZUVERLÄSSIGER PARTNER FÜR ONLINE-SICHERHEIT
- 5 FAZIT
- 6 VERISIGN



MALWARE-SCANS SCHÜTZEN IHR UNTERNEHMEN, IHRE KUNDEN - UND IHR GESCHÄFTSERGEBNIS

MALWARE KANN ÜBERALL LAUERN

Dieses Strategiepapier erläutert die Bedrohungen, die von Malware ausgehen, und die Gefahr für Ihr Online-Geschäft. Sie lernen die Gründe für die Verbreitung von Malware über das Internet kennen und erfahren, wie Kriminelle als Ausgangspunkt für die Weiterverbreitung Webserver infizieren. Außerdem werden Verfahren vorgestellt, mit denen Administratoren feststellen können, wann und auf welche Weise Angreifer ihren Webserver infiziert haben.

Weitere wichtige Inhalte dieses Strategiepapiers:

- Wie Angreifer Malware über Webbrowser anstatt wie früher über infizierte E-Mail-Anhänge verbreiten
- Welchen Gewinn sich moderne Kriminelle von der Infizierung von Endbenutzer-Systemen versprechen
- Wie Malware durch die Infizierung seriöser Websites verbreitet wird
- Welche Methoden es gibt, um so viele Seiten wie möglich zu infizieren
- Die Verfahren von Internet-Kriminellen, um durch Ausnutzung von Sicherheitslücken in Websites mit einem Schlag tausende Websites mit Malware zu infizieren
- Wie Angreifer ihren Schadcode durch entsprechend programmierte Werbung verbreiten und so trotz guter Sicherung auch beliebte Websites infizieren

WAS IST EIGENTLICH MALWARE?

Der Ausdruck „Malware“ bezeichnet Schadprogramme, die in bösartiger Absicht erstellt wurden. Malware stellt ein wachsendes Problem im Internet dar. Hacker nutzen Sicherheitslücken von Webservern aus, um Malware zu installieren und darüber Zugriff auf eine Website zu erlangen. Unter der Bezeichnung Malware werden verschiedene Bedrohungen zusammengefasst: von Adware, die unerwünschte Werbe-Pop-ups anzeigt, bis hin zu Trojanern, mit denen Kriminelle vertrauliche Daten wie beispielsweise Zugangsdaten für Online-Banking stehlen können.

Malware wird immer häufiger über Webbrowser verbreitet. Diese Art der Verbreitung hat in den letzten Jahren zugenommen, da bessere E-Mail-Filter die Verbreitung von Malware über Spam-Mails zunehmend erschwerten. Und da auch Firewalls in Unternehmen und Privathaushalten immer

öfter zu finden sind, können Schadprogramme nicht mehr so leicht wie zuvor von Rechner zu Rechner über das Netzwerk verbreitet werden. Hacker haben Möglichkeiten, sich über das Internet Zugang zur Website eines Unternehmens zu verschaffen und diese als Ausgangsbasis für die Infizierung der Kunden mit Malware zu nutzen.

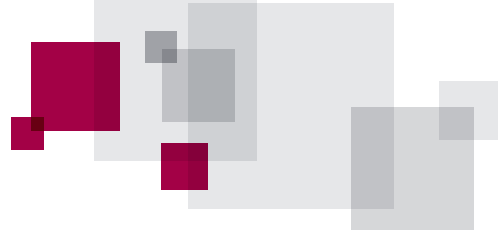
Der Code dieser Schadprogramme ist nicht so einfach festzustellen und kann die Computer von Kunden sogar infizieren, wenn sie eine Website einfach nur besuchen. Da die Infektion quasi im Vorbeigehen stattfindet, spricht man hier von „Drive-by-Malware“. In der Regel ist den Benutzern nicht im Geringsten bewusst, dass ihr Computer durch einen solchen Angriff infiziert wurde – was das Problem besonders tückisch macht. Hacker nutzen Drive-by-Malware zur Verbreitung von Viren, mit denen sie die Kontrolle über Computer erlangen oder vertrauliche Daten wie beispielsweise Kreditkartennummern stehlen.

Drive-by-Malware: Wie funktioniert sie? Sind auch kleine Websites bedroht?

Drive-by-Malware lädt sich ohne Zustimmung des Benutzers selbsttätig auf seinen Computer herunter. Cyberkriminelle nutzen Sicherheitslücken in Browsern bzw. Plugins zur Verbreitung von Malware aus: Der Schadcode wird als unsichtbares Element auf einer Website verborgen (z. B. als iframe oder Javascript-Code mit verschleierter Funktionsweise) oder in einem Bild eingebettet (z. B. in einer Flash- oder PDF-Datei). Von hier aus kann er dann ohne Wissen des Besuchers auf seinen Rechner geladen werden. Hiervon ist jede Website bedroht. Kleine Websites können anfälliger sein, weil ihre Betreiber mit höherer Wahrscheinlichkeit weder die Ressourcen noch die Fachkenntnisse haben, um Angriffe zu erkennen und zügig zu bekämpfen.

Ein Besuch auf einer infizierten Website reicht aus, um den Computer des Besuchers mit Malware zu infizieren. Indem Hacker gezielt Websites mit geringen Besucherzahlen angreifen, bleiben sie länger unerkannt und können mehr Schaden anrichten.





ABLAUF EINES MALWARE-ANGRIFFS

In zwei Schritten infiziert ein Angreifer einen Computer über den Webbrowser. Zunächst benötigt er eine Möglichkeit, zum Opfer eine Verbindung herzustellen. Anschließend muss der Angreifer die Malware auf dem Computer des Opfers installieren. Beide Schritte können schnell und, je nach Angriffsstrategie, ohne Zutun des Opfers durchgeführt werden.

Eine Möglichkeit, den Browser eines Opfers dazu zu bringen, Schadcode auszuführen, besteht ganz einfach darin, das Opfer zum Besuch einer Website, die mit Malware infiziert ist, aufzufordern. Wer weiß, dass eine Website infiziert ist, wird diese natürlich aller Wahrscheinlichkeit nach nicht besuchen, und daher muss der Angreifer den wahren Zweck der Website verschleiern. Gewiefte Angreifer gehen bei der Verbreitung von Schadcode mit der Zeit: Häufig werden mit Malware infizierte Nachrichten über soziale Netzwerke wie Facebook oder über Instant-Messaging-Systeme verbreitet. Diese Methoden haben zwar einen gewissen Erfolg, funktionieren allerdings nur, wenn es gelingt, ein Opfer zum Besuch einer bestimmten Website zu verleiten.

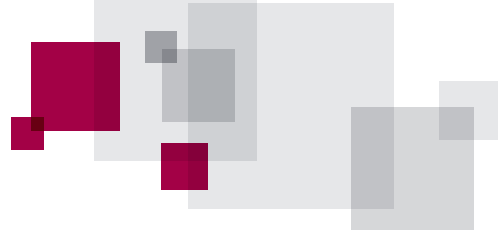
Eine andere Strategie nimmt Websites ins Visier, die von den potenziellen Opfern aus eigenem Antrieb besucht werden. Hier verschafft sich der Angreifer Zugriff auf die gewählte Website und fügt einen kurzen Abschnitt HTML-Code ein, der einen Link zum eigenen Server enthält. Dieser Code kann von jedem beliebigen Ort aus geladen werden, selbst von ganz anderen Websites. Jedes Mal, wenn ein Benutzer eine solchermaßen präparierte Website besucht, besteht die Möglichkeit, dass der Code des Angreifers den Computer des Besuchers mit Malware infiziert.

Häufige Verfahren zur Verbreitung von Malware:

- **Software-Updates:** Malware veröffentlicht in sozialen Netzwerken Links zum Anschauen eines Videos. Beim Versuch, das Video abzuspielen, wird der Benutzer aufgefordert, seine angeblich veraltete Videosoftware zu aktualisieren. Die als Update angebotene Software enthält Schadcode.

- **Banner-Werbung:** Auch als „Malvertising“ bekannt. Benutzer klicken im guten Glauben auf ein Werbebanner, woraufhin versucht wird, Schadcode auf dem Computer des Benutzers zu installieren. Es kommt auch vor, dass die Werbung den Benutzer zu einer Website umleitet, die zum Herunterladen einer PDF-Datei mit gut verborgenem Schadcode auffordert, oder dass vom Benutzer die Eingabe von Zahlungsdaten verlangt wird, um ein PDF fehlerfrei herunterzuladen.
- **Dokumente zum Herunterladen:** Benutzer werden dazu verleitet, eine Datei, die einem bekannten Programm wie Microsoft Word oder Excel zugeordnet ist, zu öffnen – und diese Datei installiert dann einen Trojaner.
- **Man-in-the-Middle-Angriff:** Hierbei ist der Benutzer überzeugt, mit einer vertrauenswürdigen Website Daten auszutauschen. Tatsächlich werden diese Daten, z. B. Benutzername und Passwort, allerdings an einen Cyber-Kriminellen gesendet. Ebenfalls möglich: Der Kriminelle übernimmt die Kontrolle über die Verbindung zwischen Benutzer und Website und lässt die Sitzung weiterhin offen, nachdem der Benutzer sie vermeintlich geschlossen hat. Nun kann der Kriminelle den offiziellen Zugang missbrauchen: Hat sich der Benutzer bei seinem Bankkonto angemeldet, kann der Kriminelle Geldbeträge überweisen. Hat der Benutzer etwas gekauft, kann der Kriminelle die beim Kauf verwendete Kreditkartennummer aufrufen und stehlen.
- **Keylogger:** Mit einer der oben vorgestellten Methoden werden Benutzer dazu gebracht, Keylogger-Software herunterzuladen. Das Keylogger-Programm protokolliert dann bestimmte Aktionen, beispielsweise Mausklicks oder Tastenanschläge, und erstellt Screenshots, um Zugangsdaten für Online-Banking oder Kreditkartendaten auszuspäionieren.





MALWARE ALS GESCHÄFTSMODELL

Wie ziehen Angreifer Gewinn aus Malware? Mit infizierten Computern lässt sich auf vielfältige Weise Geld machen. Am einfachsten durch Werbung: Ebenso, wie sich zahlreiche Websites durch Werbung finanzieren, kann Malware Werbung anzeigen, die Zahlungen an den Kriminellen generiert.

Auch Erpressung ist möglich. Die Kontrolle über ein großes Netzwerk infizierter Computer, ein sogenanntes „Botnetz“, gibt einem Angreifer Macht, die er dazu benutzen kann, mit der Drohung mit einem Denial-of-Service-Angriff (DoS) von Website-Betreibern Geld zu erpressen. Bei einem DoS senden die an das Botnetz angeschlossenen Computer eine solche Flut von Anfragen an die betreffende Website, dass diese überlastet zusammenbricht. Der Angreifer bietet dem Website-Betreiber an, den Angriff gegen eine Geldzahlung einzustellen.

Kriminelle nutzen infizierte Computer auch häufig zum Ausspähen wertvoller Benutzerdaten, beispielsweise Zugangsdaten zum Online-Banking. Dies ist eine der ausgefeiltesten und am besten verborgenen Formen von Malware. Die Kriminellen können die erbeuteten Daten selbst für ihre eigenen Zwecke nutzen oder sie an Dritte verkaufen, die dann Gewinn daraus schlagen.

Schwarze Listen und ihre Folgen

Wegen der Schäden, die Malware anrichten kann, setzen Google, Yahoo, Bing und andere Suchmaschinen Websites, bei denen Malware festgestellt wurde, auf eine Sperrliste, die sogenannte schwarze Liste. Bei Websites auf der schwarzen Liste warnt die Suchmaschine potenzielle Besucher, dass die Website nicht sicher ist – oder sie nimmt die Website gar nicht erst in die Suchergebnisse auf.

Wenn Ihre Website einmal auf die schwarze Liste geraten ist, sind die möglichen Folgen für Ihr Unternehmen verheerend, da nützt auch die beste Suchmaschinenoptimierung nichts. Eine Website kann ohne Warnung und ohne Wissen der Betreiber auf die schwarze Liste gesetzt werden – und sie wieder von der schwarzen Liste entfernen zu lassen, gestaltet sich äußerst schwierig. Für den langfristigen Erfolg jeder Website ist es daher unverzichtbar, Maßnahmen zu ergreifen, die dafür sorgen, dass die Website erst gar nicht auf die schwarzen Listen der Suchmaschinen gerät.

VERISIGN: IHR ZUVERLÄSSIGER PARTNER FÜR ONLINE-SICHERHEIT

VeriSign brachte Mitte der 1990er Jahre als erstes Unternehmen ein kommerzielles SSL-Produkt auf den Markt und ist auch heute noch führender Anbieter von SSL-Zertifikaten und zudem die weltweit anerkannteste Marke für Internetsicherheit. Dieses Ansehen bei Privat- und Firmenkunden hat sich VeriSign über viele Jahre durch seine innovativen Spitzenleistungen und die Einbindung modernster Verfahren in seine hochwertigen SSL-Lösungen erarbeitet.



VeriSign bietet seinen Kunden mit den bewährten SSL-Zertifikaten Gewissheit in puncto Online-Sicherheit, bleibt dort aber nicht stehen: Damit stets der optimale Schutz gewährleistet ist, werden die SSL-Produkte permanent durch die Unterstützung der neuesten Standards und die Einbindung von ergänzenden Verfahren und Lösungen optimiert. Im Zuge dieser Optimierung bietet VeriSign als Teil seiner SSL-Lösungen die tägliche Durchsuchung von Websites nach Malware an, damit Ihre Website, Ihr guter Name und die vertraulichen Daten Ihrer Kunden vor den immer wieder neuen Angriffsversuchen aus dem Internet geschützt bleiben.



FAZIT

Der Markt für Online-Käufe und -Dienstleistungen ist in den letzten zehn Jahren enorm gewachsen. In dem Maße, wie das Internet im Alltagsleben Einzug gehalten hat, haben allerdings auch kriminelle Aktivitäten zugenommen. Malware ist immer häufiger zu finden und gefährdet das weitere Wachstum des Online-Handels durch die Gefahr des Missbrauchs vertraulicher Daten. So führt Malware zu Ängsten und zu Umsatzeinbußen für Unternehmen. Soll das Potenzial des Online-Handels also voll ausgeschöpft werden, wird ein wirksames Mittel zur Bekämpfung von Malware benötigt.

VeriSign hat eine umfassende Lösung für Vertrauen und Sicherheit im Angebot. Diese kombiniert Premium SSL-Zertifikate mit innovativen Funktionen, die gewährleisten, dass die öffentlich zugänglichen Bereiche Ihrer Websites regelmäßig auf Malware überprüft werden. Als sichtbares Zeichen dafür dient das VeriSign-Siegel, die weltweite Vertrauensmarke Nr. 1. Gemeinsam mit VeriSign bauen Sie so bei Ihren Kunden das Vertrauen auf, das für Online-Transaktionen erforderlich ist. Wenn Sie möchten, dass Ihre Kunden für ihren Online-Einkauf voller Vertrauen zu Ihnen kommen, entscheiden Sie sich für SSL-Zertifikate von VeriSign.

VERISIGN

VeriSign ist führender Anbieter von Internetinfrastrukturdiensten für die digitale Welt. Milliardenfach pro Tag verlassen sich Unternehmen und Kunden bei vertrauensvoller Kommunikation und sicherem Handel auf unsere Internetinfrastruktur.

Weitere Informationen erhalten Sie unter www.Verisign.de.

