Sophos-Studie: Wachsende Bedrohung durch Dropper-as-a-Service

Als raubkopierte Software getarnt liefern sogenannte Dropper ganze Malwarebündel aus, darunter Programme für Informationsdiebstahl, Klickbetrug und vieles mehr.

Sophos hat eine neue Studie mit dem Titel „Fake Pirated Software Serves Up Malware Droppers as a Service“ veröffentlicht. Die Studie beschreibt, wie Cyberkriminelle Dropper, also als Trojanisches Pferd für Schadsoftware dienende Programme, nutzen, um Personen, die auf der Suche nach gehackten Versionen beliebter Geschäfts- und Consumer-Anwendungen sind mit vielfältigen schädlichen und unerwünschten Inhalten zu beliefern.

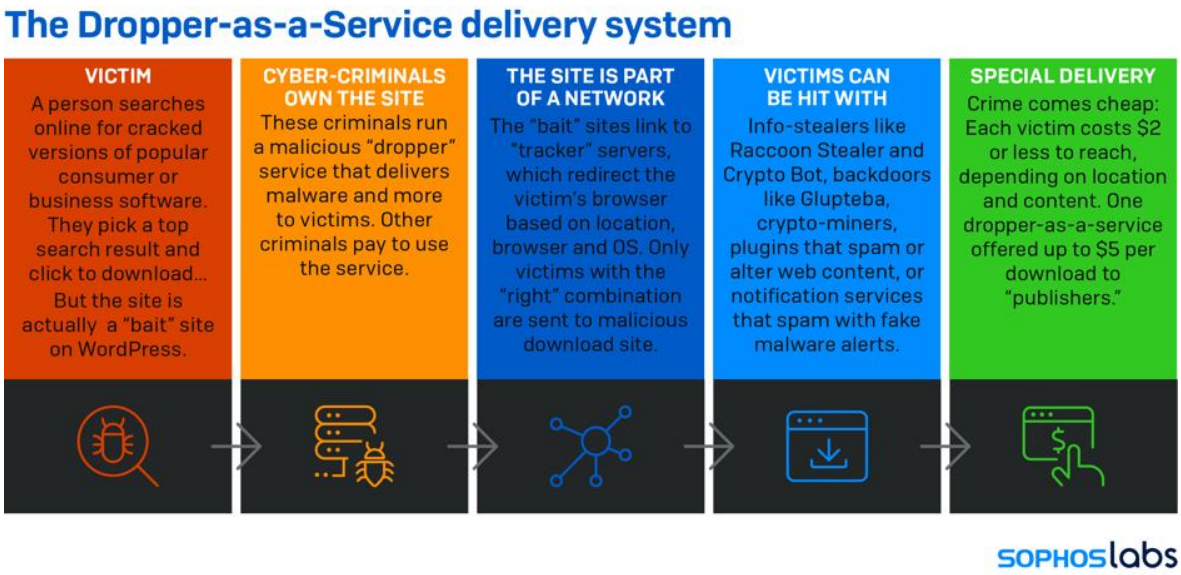
Bezahlte Download- bzw. Dropper-Dienste gibt es schon seit längerer Zeit und die kriminellen Betreiber verdienen damit gutes Geld. Die jüngsten Untersuchungen von Sophos deuten darauf hin, dass dieser Erfolg zum Teil auf die immer noch hohe Nachfrage nach raubkopierten Anwendungen zurückzuführen ist. Zudem ermöglichen es die kostenpflichtigen Dienste dieser Art auch weniger qualifizierten Cyberkriminellen, massenhaften Datendiebstahl oder sogar Kryptowährungsbetrug zu minimalen Kosten durchzuführen. Dropper-as-a-Service-Anbieter betreiben effektive Gewinnmaximierung, indem sie eine Reihe bösartiger oder unerwünschter Inhalte in Droppern bündeln und die Opfer gleich mit einer Reihe von schädlichen Anwendungen in einem einzigen Download überschütten.

Home-Office erhöht das Risiko zusätzlich

In den letzten 18 Monaten haben Millionen von Menschen im Home-Office gearbeitet und dabei oft private Geräte benutzt, was das Risiko bösartiger Dropper-Downloads für Unternehmen zusätzlich verstärkt hat. Gleichzeitig sind die weitaus lukrativeren Unternehmensziele damit auch für Cyberkriminelle in Reichweite, die normalerweise nicht die Kompetenz für komplexe Angriffe haben. Bei den Untersuchungen der SophosLabs wurden beispielsweise Dropper entdeckt, die Backdoors wie Glupteba sowie Diebstahl-Malware wie Raccoon Stealer und Crypto Bot enthalten. Hinsichtlich der Sicherheit ist Malware, die von Droppern geliefert wird, glücklicherweise entweder aufgrund ihrer Signatur oder ihres Verhaltens leicht von sicherer Software zu unterscheiden. Allerdings sind schädliche Pakete oft in verschlüsselten Archiven enthalten. Die meisten Sicherheitstechnologien erkennen die schädlichen Dateien erst dann, wenn sie entpackt werden.

Wie Dropper-as-a-Service arbeitet

Die SophosLabs haben vor kurzem eine Studie über den Raccoon Stealer veröffentlicht, der als Teil eines Schadcode-Pakets von einem Dropper-as-a-Service verteilt wurde. Im Anschluss an diese Untersuchung haben die Forscher analysiert, wie diese Dropper-Dienste ihre verschiedenen Daten übermitteln. Das folgende Diagramm zeigt, was passiert, wenn auf den Download einer vermeintlichen Raubkopie geklickt wird, die in Wirklichkeit aber ein getarnter Malware-Dropper ist:



Schutz vor Dropper Malware
Sophos empfiehlt Unternehmen, ihre Sicherheitssoftware sowie die Einstellungen und Richtlinien zu überprüfen und sicherzustellen, dass schädliche und unerwünschte Downloads erkannt und blockiert werden. Dazu gehört auch ein robuster Ansatz zur Web-Filterung. Die in einem Dropper-Paket versteckte Malware kann möglicherweise erst beim Entpacken entdeckt werden. Zu diesem Zeitpunkt kann sie sich allerdings bereits im Netzwerk befinden. Ein guter Webfilter überprüft nicht nur reguläre Downloads, sondern auch den verschlüsselten Netzwerkverkehr. Denn laut einer Sophos-Studie verwendet mehr als die Hälfte der Malware mittlerweile Transport Layer Security (TLS) Verschlüsselung für die Kommunikation. Webfilter schützen Unternehmen und ihre Mitarbeiter auch davor, sich mit gefährlichen oder nicht vertrauenswürdigen Servern zu verbinden, indem sie schädliche Domains und URLs blockieren.

Unternehmen sollten die Netzwerksicherheit zudem durch einen aktuellen Endpoint-Schutz ergänzen, der über Funktionen zur Verhaltenserkennung auf allen von den Mitarbeitern für den Fernzugriff verwendeten Geräten verfügt. Sophos Firewall und Intercept X for Endpoints bieten beispielsweise all diese Funktionen und mehr, einschließlich Schutz vor Ransomware.

Zudem sollten private Anwender eine Sicherheitslösung wie Sophos Home auf ihre Geräte installieren, um vor Malware und Cyberbedrohungen geschützt zu sein. Eine weitere bewährte Sicherheitspraxis besteht darin, das Herunterladen und Installieren von nicht lizenzierter Software zu vermeiden. Anwender sollten sich immer vergewissern, dass die Software rechtmäßig ist.

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de