Neu erkannte Domänen-Sicherheitskategorie in Umbrella aktivieren

Inhalt

Einleitung

In diesem Dokument wird die Sicherheitskategorie "Neu erkannte Domänen" (NSD) unter Cisco Umbrella beschrieben.

Hintergrundinformationen

Newly Seen Domains (NSD) ist eine Sicherheitskategorie, die Domänen identifiziert, die zum ersten Mal innerhalb der letzten 24 Stunden von einem Benutzer des Cisco Umbrella DNS Service abgefragt wurden (einschließlich des kostenlosen OpenDNS Service für Privatanwender). Diese Sicherheitskategorie funktioniert wie jede andere Sicherheitskategorie und kann als Teil einer bestehenden oder einer neuen Sicherheitseinstellung aktiviert werden. Domänen bleiben für einen Zeitraum von 24 Stunden in der Liste.

Definition von Domänen durch Cisco Umbrella als "neu erkannt"

Neue Domänen werden häufig als Teil neuer Malware-Kampagnen erstellt. Cyberkriminelle nutzen neue Domänen, da sie bei herkömmlichen signaturbasierten Methoden nicht erkennen, dass sie bekannte schädliche Websites blockieren. Eine Phishing-Kampagne kann beispielsweise eine neue Domäne erstellen, die eine große Spam-Kampagne begleitet und Benutzer dazu anhält, auf einen Link zu klicken. Der Link ist noch nicht als Teil dieser Kampagne bekannt und wird nicht von Standardlisten mit schädlichen Domänen blockiert. Bevor der Link zu diesen Listen hinzugefügt wird, haben Kriminelle genügend Zeit, um Daten auszuschleusen, Malware zu installieren und sich Zugriff auf das Netzwerk zu verschaffen.

Die Sicherheitskategorie "Neu erkannte Domänen (NSD)" wird aktiviert, indem DNS-Protokolle auf Domains überprüft werden, die noch nie zuvor gesehen wurden. Aufgrund des Umfangs ungültiger Abfragen muss die Clientabfrage eine korrekte Antwort erhalten, damit eine Domäne als neu erkannt gekennzeichnet werden kann. Sobald eine Domäne zum ersten Mal angezeigt wird, wird

sie 24 Stunden lang zu einer Liste hinzugefügt. Nach diesem Zeitraum wird die Domäne nicht mehr neu angezeigt und aus der Liste entfernt.

Ein Bericht zeichnet die Kategorie auf, unter der sich eine Domäne zum Zeitpunkt der Abfrage befand. Wenn eine Domäne daher bei einer Abfrage als neu erkannt kategorisiert wurde, wird sie als solche im Bericht über die Aktivitätssuche oder die Sicherheitsaktivität gemeldet. Sobald jedoch die Domäne aus der Liste abläuft, wird sie beim Schwenken auf diese Domäne im Vergleich zu aktuellen Daten über sie (insbesondere unter Verwendung der neuen Berichte über Ziele oder Identitäten, der Investigate Console oder der Investigate API) nicht mehr als neu erkannt angezeigt. Kurz gesagt, wenn Sie eine Domain einige Tage später erneut besuchen, können Sie sie nicht mehr als neu in Umbrella gesehen anzeigen. Dies ist beabsichtigt, kann jedoch zu einer anfänglichen Verwirrung führen.

Die einzige Definition einer neu erkannten Domäne ist genau diese: es ist neu gesehen. Daher ist ein erheblicher Teil der Domänen, die als neu erkannte Domänen kategorisiert wurden, nicht schädlich. Daher wird erwartet, dass bei dieser Sicherheitskategorie legitime Domänen erkannt werden. Vorsichtsmaßnahmen gegen dieses Auftreten wurden implementiert, insbesondere für bestimmte Services und CDNs wie Akamai und Cloudfront, die randomisierte Subdomänen generieren, um Inhalte zu liefern. Herkömmliche Zusicherungen gegen beliebte Domains wie Facebook und Google wurden ebenfalls verwendet, um sicherzustellen, dass diese nicht enthalten sind.

Darüber hinaus werden nur vollständig qualifizierte Domänennamen (Domäne der zweiten Ebene oder eine Unterdomäne einer Domäne der zweiten Ebene) als Domänen betrachtet, die neu eingesehen werden. Domänen oberster Ebene und Domänen oberster Ebene mit Ländercode sind in den neu erkannten Domänen nicht enthalten, um die Blockierung großer Domänengruppen zu vermeiden.

Wichtige Hinweise zur Implementierung

Da einige unerwünschte Erkennungen zu erwarten sind, empfiehlt Cisco Umbrella dringend, diesen Bericht im Audit-Modus zu verwenden oder nur den Modus zu erkennen, ohne zu blockieren oder Maßnahmen zu ergreifen. Standardmäßig werden neu erkannte Domänen von allen Benutzern, die in ihren Sicherheitseinstellungen über diese Kategorie verfügen, in den Berichten als entdeckt angezeigt. Dies bedeutet, dass die Funktion standardmäßig ohne Blockierung aktiviert ist. In den meisten Fällen müssen die Benutzer anhand von Berichten ermitteln, welcher Datenverkehr zu der Kategorie passt, und diese Informationen nutzen, um diese Domänen genauer zu untersuchen, um festzustellen, ob sie möglicherweise ein Sicherheitsrisiko darstellen, anstatt sie automatisch zu blockieren.

Ein weiterer wichtiger Vorbehalt besteht darin, dass die erste Abfrage an die Domäne zulässig ist. Dies liegt daran, dass Cisco Umbrella bisher noch keine Abfrage für diese Domäne erhalten hat und daher nicht von den Protokollierungssystemen verarbeitet wurde, um in die Kategorie "Neu erkannte Domänen" aufgenommen zu werden. Die Zeitspanne zwischen der ersten Abfrage einer Domäne und ihrer Anzeige in der Liste der Domänen, die mit der Kategorie übereinstimmen,

beträgt etwa fünf Minuten, kann jedoch darüber hinausgehen, da Cisco Umbrella (aufgrund von Verarbeitungszeit und -volumen) nicht unbedingt 100 % der DNS-Abfrageprotokolle verarbeitet.

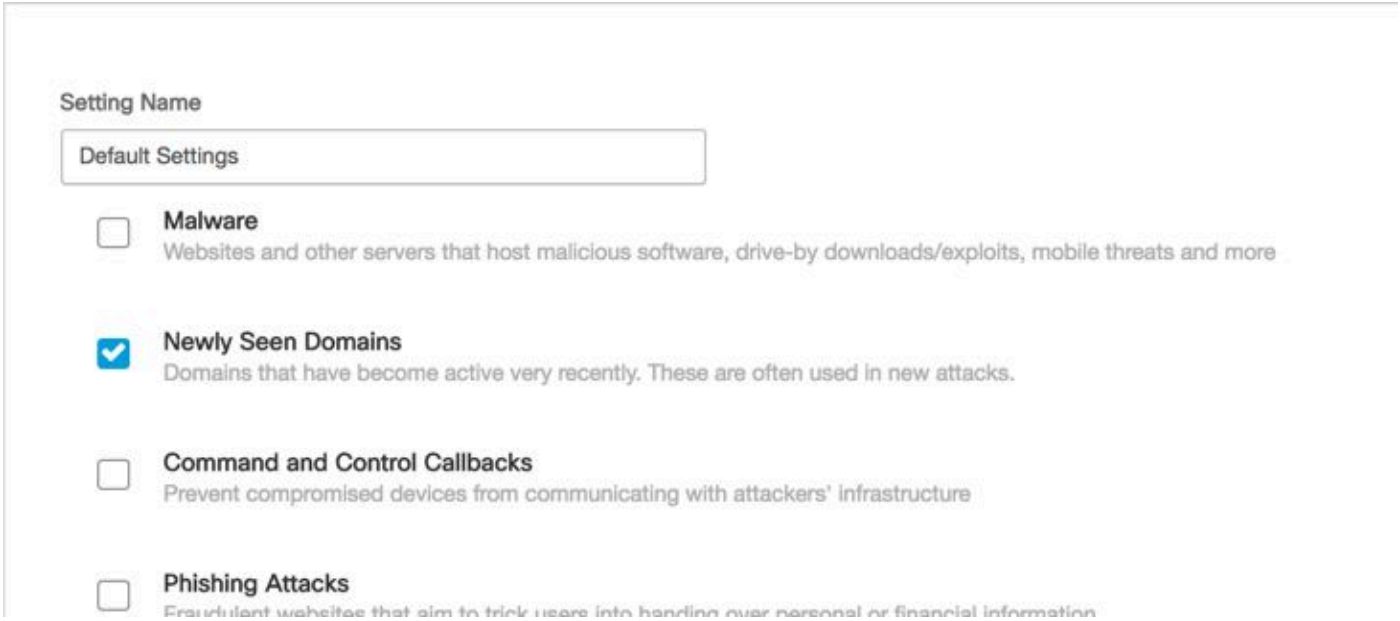
Neuen erkannten Domänen Proxying

Kunden, die den Umbrella Intelligent Proxy verwenden, beobachten auch, dass einige Domänen in der NSD-Kategorie Proxys sind. Das ist Absicht. Das Team von Umbrella Labs ermittelt anhand der gesammelten Daten, ob diese neuen Domänen umgehend in die Malware-Kategorien aufgenommen werden können. Ein Nebeneffekt davon ist, dass nicht standardmäßiger Datenverkehr, der an eine neu erkannte Domäne gesendet wird, die ebenfalls als Proxy verwendet wird, auf Proxyebene verworfen wird. Der intelligente Proxy stellt lediglich die Proxys der Ports 80 und 443 bereit, die normalerweise für den Web-Datenverkehr verwendet werden. Dies geschieht automatisch, wenn der Proxy aktiviert ist, unabhängig davon, ob die Kategorie gesperrt ist oder nicht. Um zu verhindern, dass ein Proxy für eine einzelne neu erkannte Domäne erstellt wird, fügen Sie diese der entsprechenden Zulassungsliste hinzu.

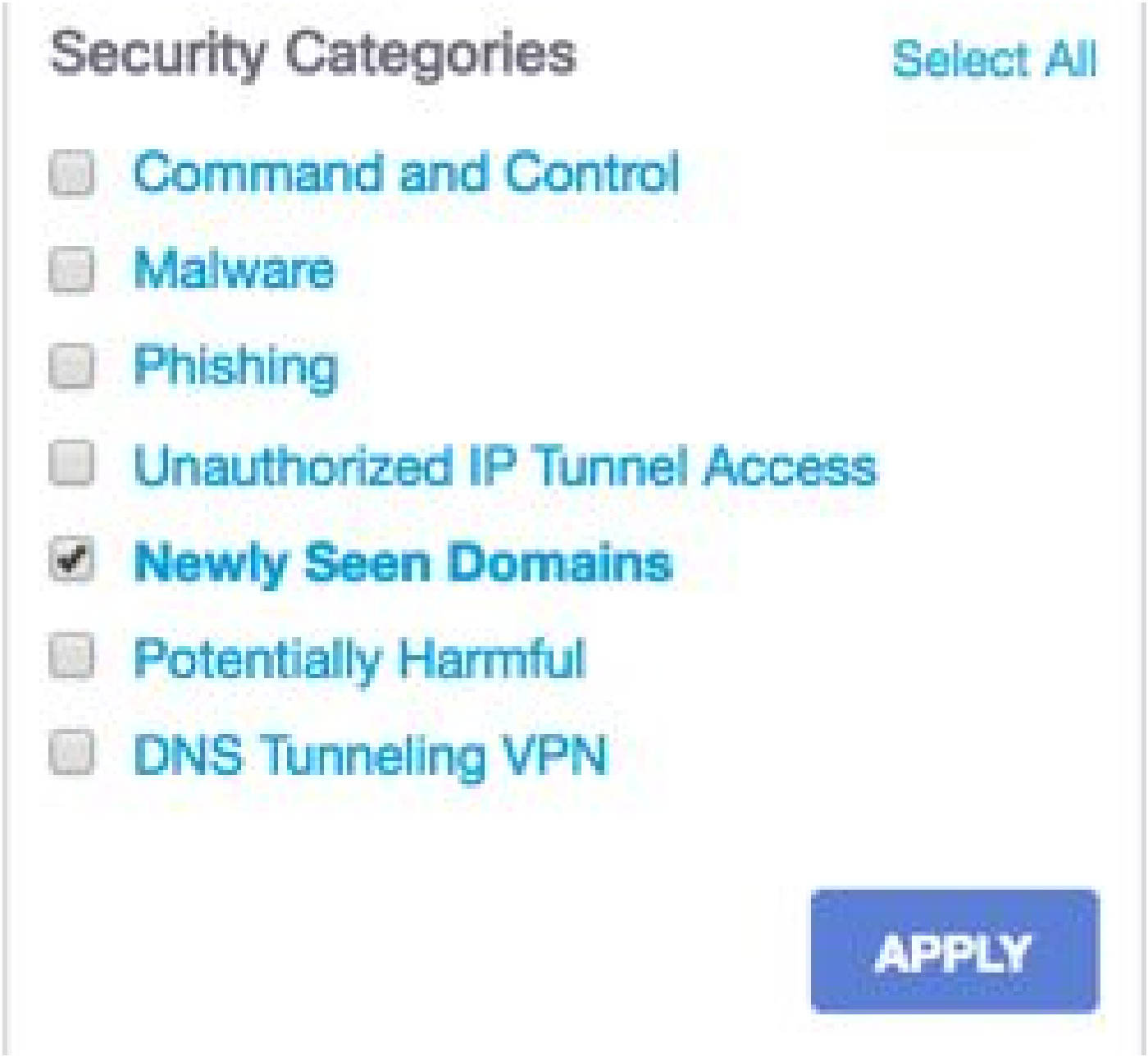
Weitere Informationen zum Intelligent Proxy finden Sie in unserer Dokumentation Enable the Intelligent Proxy.

Neu erkannte Domänen aktivieren

Die Sicherheitskategorie Neu erkannte Domäne kann wie jede andere Kategorie unter Richtlinien > Sicherheitseinstellungen aktiviert und anschließend eine vorhandene Sicherheitseinstellung bearbeitet werden. Alternativ dazu kann sie im Richtlinienkonfigurations-Assistenten selbst ausgeführt werden.



Neu erkannte Domänen können auch in bestimmten Berichten, z. B. bei der Aktivitätssuche, gefiltert werden.



115015007423

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.