Dark Web 101

Was jeder Sicherheitsprofi wissen sollte

www.intsights.com

Dark Web 101:
Was jeder Sicherheitsprofi wissen sollte

Schalten Sie die Nachrichten oder Ihre Lieblings-TV-Serie ein – dann hören Sie zwangsläufig von einer riesigen kriminellen Unterwelt, in der Drogen, Sex, Waffen und Identitätsdiebstahl im Verborgenen stattfinden. Alles, was Sie brauchen, ist ein Computer oder ein mobiles Gerät, um ins Dark Web zu gelangen. Aber was ist das Dark Web wirklich?

Obwohl es sehr bekannt ist, haben weniger als ein Prozent der Internetnutzer das Dark Web je besucht. Selbst unter den IT-Sicherheitsexperten hat sich nur einer von sieben jemals in ein Dark-Web-Forum oder auf eine Dark-Web-Seite gewagt. Dieser Mangel an Erfahrung erklärt, warum so viele Fehlinformationen kursieren. Er zeigt auch, dass viele in der Security-Branche eine wichtige Informationsquelle verpassen, die ihnen helfen könnte, ihre Firma effektiver zu schützen und sich besser in die Gedankenwelt eines Hackers hineinzuversetzen.

Unser Team bei IntSights hat jahrelang im Dark Web gelebt und geforscht, für staatliche Nachrichtendienste und einige der größten Finanzinstitute der Welt gearbeitet, um dem Feind immer einen Schritt voraus zu sein. Heute nutzen wir diese Erfahrung, um Kunden auf der ganzen Welt dabei zu helfen, das Verhalten von Hackern zu überwachen und Frühwarnzeichen für bösartige Aktivitäten zu erkennen.

Dieses Whitepaper soll mit unserem Wissen dazu beitragen, die Fakten von der Fiktion zu trennen. Es soll Ihnen die Grundlagen vermitteln, die Sie als Sicherheitsexperte benötigen, um diese Informationsquelle sicher zu nutzen und Ihr Unternehmen besser zu schützen.

Was ist das Dark Web?

Die meisten Menschen greifen über Suchmaschinen wie Google, Yahoo oder Bing auf das Internet zu, aber diese Websites kratzen nur an der Oberfläche aller Internet-Inhalte. Die überwiegende Mehrheit der Inhalte befindet sich im sogenannten Deep Web, also an Orten, die über herkömmliche Suchmaschinen nicht direkt zugänglich sind. Zu dieser riesigen Sammlung von Informationen gehören beispielsweise E-Mail-Konten von Unternehmen, digitale Bezahldienste wie das Wall Street Journal oder Netflix, in der Cloud gehostete Speicherdienste wie iCloud oder Dropbox und private Online-Foren. Innerhalb des Deep Web gibt es eine Untergruppe, die als Dark Web bekannt ist – Inhalte, die absichtlich im Verborgenen schlummern. Sie sind für diejenigen, die einen gewöhnlichen Browser wie Chrome oder Firefox verwenden, nicht zugänglich.

Obwohl das Dark Web für seine Nutzung durch Kriminelle bekannt ist, gibt es an sich nichts Illegales an ihm und seinem Gebrauch auszusetzen. Vielmehr handelt es sich beim Dark Web einfach um eine Art des Zugriffs und Hostings von Webinhalten, die Anonymität bietet. Dies geschieht durch den Einsatz spezieller Software wie Tor (The Onion Router) oder I2P (Invisible Internet Project), um die Identität des Benutzers zu verschleiern. Wie jede andere Kommunikationsplattform kann auch das Dark Web sowohl für legitime Zwecke wie den Schutz der Privatsphäre und der politischen Meinungsfreiheit als auch für böswillige Aktivitäten wie den Verkauf von Drogen, Waffen oder gestohlenen Kreditkartendaten genutzt werden.

Zu den Bereichen, in denen sich die Dark-Web-Anonymität als entscheidend für die Durchsetzung positiver Veränderungen erwiesen hat, zählen die Menschenrechte und der Journalismus. Organisationen wie Amnesty International und Human Rights Watch nutzen das Dark Web, um die Arbeit von Menschenrechtsaktivisten, politischen Aktivisten und Journalisten in Ländern zu unterstützen, in denen die Internetaktivitäten stark überwacht werden. Auch strenge lokale Zensur- oder Netzkontrollgesetze wie in China, Iran und Saudi-Arabien lassen sich so umgehen.

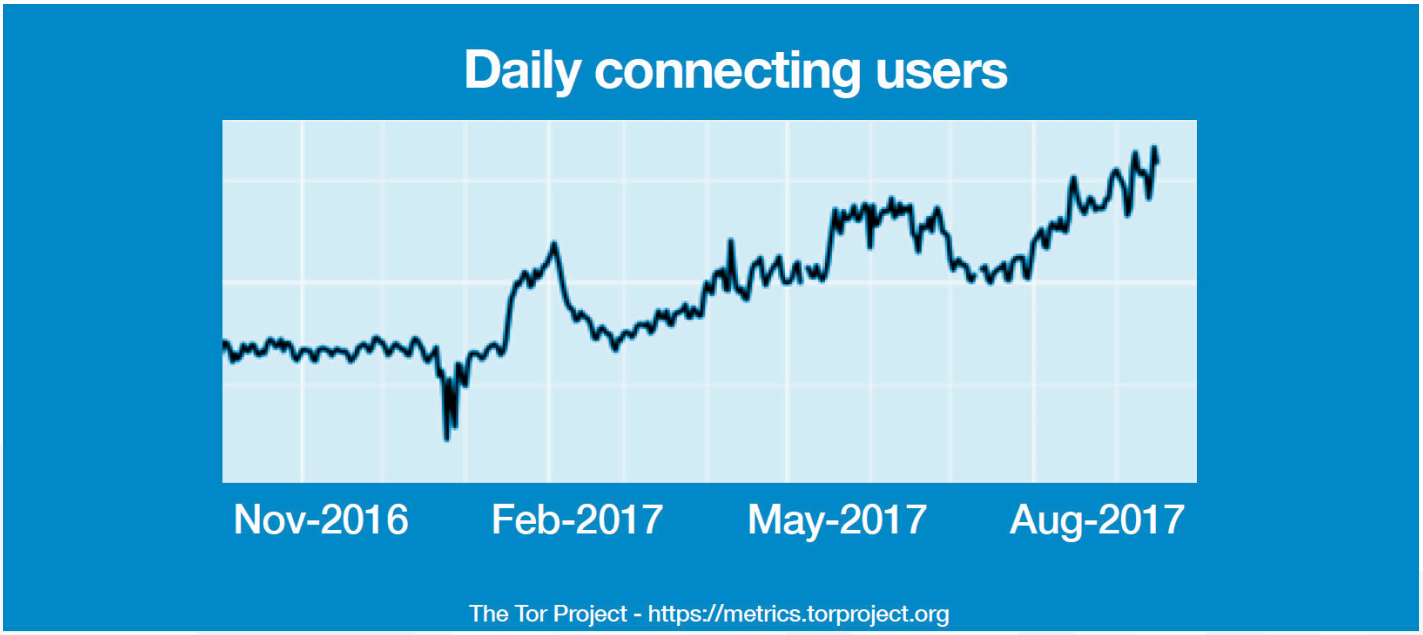
Durch die Dark-Web-Nutzung konnte die Welt mehr darüber erfahren, was in diesen Gebieten vor sich geht. Sogar Facebook hat sich auf das Dark Web eingelassen und **eine Version seiner Website erstellt, die über das Tor-Netzwerk zugänglich ist**, um Personen, die in Gebieten leben, in denen Facebook blockiert ist, den Zugang zum sozialen Netzwerk zu ermöglichen.

Jede verdeckte Website zählt zum Dark Web, aber im Gegensatz zum öffentlichen Web, das in hohem Maße miteinander verbunden und zugänglich ist, sieht das Dark Web stark fragmentiert aus. Häufig erfordert es verschiedene Technologien, um auf Websites zugreifen zu können. Aus diesem Grund sollte man sich das Dark Web weniger wie ein Netz vorstellen, sondern wie eine Reihe von dunklen Silos, die jeweils immense Mengen an Informationen und Aktivitäten enthalten, aber oft voneinander getrennt sind.

Es gibt zwar einige Technologien, die beim Zugang zum Dark Web zum Einsatz kommen (etwa I2P und Freenet) und sich immer mehr durchsetzen, aber die deutlich am weitesten verbreitete ist das Tor-Netzwerk. Mit mehr als 350.000 täglichen Usern und über 50.000 aktiven Seiten stellt Tor das größte einzelne Netzwerk von Dark-Web-Seiten im Internet dar.

Obwohl das Dark Web für seine Nutzung durch Kriminelle bekannt ist, gibt es an sich nichts Illegales an ihm und seinem Gebrauch auszusetzen.

Ironischerweise wurde Tor (auch „The Onion Router" genannt) trotz seines schlechten Rufs ursprünglich im Jahr 2002 vom US Naval Research Laboratory als anonymes Kommunikationswerkzeug für Geheimdienste entwickelt. Seitdem gilt er als bevorzugtes Werkzeug von Kriminellen, Datenschutzforschern, Akademikern und Strafverfolgern gleichermaßen. Das Netzwerk wird heute vom Tor Project, einer gemeinnützigen 501c3-Organisation mit Sitz in Massachusetts, betrieben. Viele Stiftungen, Unternehmen und Einzelpersonen unterstützen es finanziell, aber der größte Geldbetrag für das Tor-Projekt kommt weiterhin von der US-Regierung.



Wie funktioniert Tor?

Tor leitet den verschlüsselten Datenverkehr eines Users nach dem Zufallsprinzip durch eine Reihe verbundener Systeme (auch Relays genannt). Das stellt sicher, dass sich Aktivitäten nicht zum Endnutzer zurückverfolgen lassen. Tor-Nutzer können dann auf spezielle Seiten mit .onion-Domänen zugreifen, die nur über Tor-Browser zugänglich sind.

Im September 2017 wurde das Tor-Netzwerk von fast 7.000 Systemen auf der ganzen Welt unterstützt. Diese Systeme dienen als Relais, die Daten im Netzwerk weiterleiten, um den Ursprung des Datenverkehrs im Netzwerk zu verschleiern. Um zu erklären, wie das abläuft, wollen wir uns ansehen, was passiert, wenn ein Benutzer versucht, über das Tor-Netzwerk auf eine .onion-Webseite zuzugreifen.

Mit mehr als 350.000 täglichen Usern und über 50.000 aktiven Seiten stellt Tor das größte einzelne Netzwerk von Dark-Web-Seiten im Internet dar.

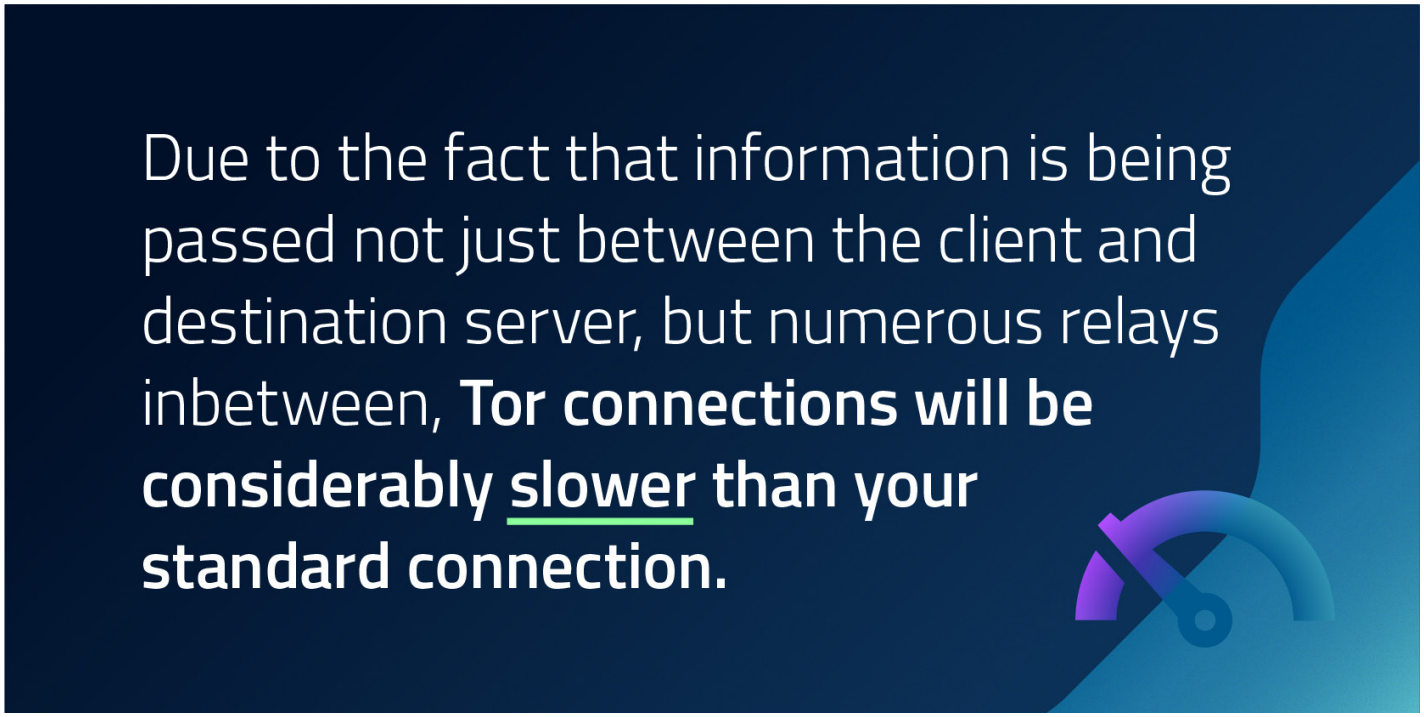
Wie sich Tor mit dem Dark Web verbindet

Zunächst einmal arbeiten .onion-Websites anders als herkömmliche Websites. Im Gegensatz zu .com oder .edu ist .onion eine spezielle Top-Level-Domain, die für den Zugang zu anonymen Seiten entwickelt wurde. Während .onion-Adressen in der Praxis ähnlich wie konventionelle Webseitenadressen in torfähigen Browsern funktionieren, sehen die meisten .onion-Adressen anders aus als herkömmliche Webseiten. Sie verwenden 16-stellige alphanumerische Identifizierungszeichen wie http://3g2upl4pq6kufc4m.onion/ und keine einprägsamen Namen oder Phrasen wie amazon.com oder yahoo.com. Um diese Tatsache zu überprüfen, kann man versuchen, den obigen Link in Chrome oder Firefox anzuklicken: Es klappt nicht, weil – wie oben erwähnt – sich .onion-Seiten nur über einen speziellen Tor-Browser aufrufen lassen.

Die .onion-Adressen sehen anders aus als herkömmliche Websites, da sie 16-stellige alphanumerische Zeichenfolgen verwenden.

Um auf diesen und andere Links im Onion-Web zuzugreifen, muss man den Tor-Browser von https://www.torproject.org/projects/torbrowser.html.de herunterladen. Das gilt auch für den Zugriff auf Seiten von I2P (https://geti2p.net/en/), wo eine andere Technologie zum Einsatz kommt, um ein anderes Netzwerk von Dark-Web-Seiten zu hosten. Unabhängig davon, welchen Dienst jemand nutzen möchte, gilt das Herunterladen und Installieren der richtigen Software als wichtiger erster Schritt für den Zugriff auf das Dark Web. Hier konzentrieren sich unsere Beispiele ausschließlich auf .onion-Seiten, die über das Tor-Netzwerk verfügbar sind, aber der Prozess ähnelt auch I2P und anderen verwandten Technologien.

Sobald der Tor-Browser installiert ist, werden die gesendeten Daten in eine Reihe von verschlüsselten Paketen zerlegt. Außerdem löscht Tor zu diesem Zeitpunkt automatisch einige Header-Informationen, die Rückschlüsse auf den Absender zulassen könnten.



Sobald die Kopfzeile und die Daten-Nutzlast verschlüsselt sind, wählt Tor einen zufälligen Weg unter Nutzung von mindestens drei Relays zum Zielserver. Anschließend beginnt die Übertragung der Daten. Um zu ihrem Ziel zu gelangen, müssen sie zunächst mehrere Schichten durchlaufen, weshalb Tor auch oft als Zwiebelnetzwerk bezeichnet wird.

Sobald eine Verbindung steht, verwendet Tor für eine kurze Zeit dieselbe Route. Dann generiert das System einen neuen Pfad, um die Möglichkeit für andere zu begrenzen, vergangene Online-Aktivitäten mit aktuellen Sitzungen zu verbinden. Da die Informationen nicht nur zwischen dem Client und dem Zielserver übertragen werden, sondern auch zwischen zahlreichen Relays, laufen Tor-Verbindungen deutlich langsamer als konventionelle Kontakte ab.

Sieht man von der Langsamkeit ab, macht es die Kombination aus Multi-Hop-Verbindung und Verschlüsselung möglich, dass Tor ein so hohes Maß an Anonymität im Internet garantiert. Man kann sich diesen Prozess ähnlich wie die langen, verschlungenen Wege vorstellen, die Mafiosi in Hollywood-Filmen benutzen, um die Polizei abzuschütteln.

Informationsarten für die Dark-Web-Überwachung

Malware und Exploit-Kits
Postings, in denen neue Exploits oder Malware für Ihr Unternehmen oder Ihre Branche angefordert oder verkauft werden, können eine frühe Warnung sein, dass Kriminelle eine Attacke planen. Die Postings können auch Hinweise enthalten, welche Software die Angreifer verwenden oder welche Zugangspunkte sie ins Visier nehmen.

Kreditkarten
Gestohlene Kreditkartendaten sind ein großes Geschäft: Millionen von Konten stehen zum Verkauf, einige Anbieter bieten sogar eine Geld-zurück-Garantie für deaktivierte Konten an. Das Angebot reicht von einfachen Spur-1- und Spur-2-Daten bis hin zu professionell hergestellten Klonkarten.

Anmeldedaten
Auflistungen mit Anmeldedaten oder andere Zugangsinformationen zu Ihren Unternehmens- oder Partnersystemen.

Dateienverkauf
Dokumente und Entwürfe Ihrer Organisation oder einer Partnerfirma, die im Dark Web zum Verkauf stehen, deuten auf eine Sicherheitsverletzung hin. Diese kann sensible Informationen preisgeben, die ein Angreifer nutzen könnte, um Mitarbeiter zu erpressen, eine Phishing-Kampagne zu starten oder Zugang zu weiteren vertraulichen Informationen zu erhalten.

Betrugswerkzeuge
Betrugs-Tools sind schlüsselfertige Pakete, die für die Durchführung von Phishing- oder anderen Kampagnen zum Einsatz kommen. Es befinden sich verschiedene Arten im Angebot, zum Beispiel Scam-Seiten, also vorgefertigte Phishing-Websites, die sofort mit dem Phishing loslegen können. Viele Anbieter passen die Tools an die Wünsche des Käufers an, beispielsweise durch das Kopieren der Website einer großen Bank.

Tutorials
Bildungsmaterialien stehen nicht ganz oben auf der Liste der Bestseller im Dark Web, aber Tutorials bringen trotzdem Geld im Dark Web. Diese Anleitungen für kriminelles Verhalten gibt es in vielen Formen, sie bieten wertvolle Einblicke in die Verfahren und Techniken, die sowohl Amateur- als auch Profihacker einsetzen.

Insider-Bedrohungen
Ein wachsendes Risiko für Unternehmen geht von Mitarbeitern oder Partnern aus, die Zugänge verkaufen oder Informationen klauen. Aktivitäten dieser Art machen auf die Anwesenheit eines böswilligen Insiders aufmerksam und können helfen, seinen genauen Ort innerhalb der Organisation zu ermitteln.

Wenn Sie lernen, das Dark Web effektiv zu überwachen, können Sie Angriffe erkennen, bevor sie stattfinden, Insider-Bedrohungen aufspüren und sehen, wann Ihre Daten oder die wichtiger Partner kompromittiert worden sind.
Die Schaffung dieser Fähigkeit oder die Sicherstellung, dass Ihre Firma die Hilfe von Experten oder Diensten wie IntSights in Anspruch nimmt, spielt eine immer wichtigere Rolle. Denn die Systeme werden anfälliger für Datendiebstahl und Insider-Bedrohungen, zudem eröffnet die Nutzung von SaaS-Drittanbietern neue Angriffsflächen.

Tipps für den Einstieg in die Dark-Web-Überwachung

Tor und ähnliche Systeme zielen darauf ab, sichere und anonyme Kommunikation zu ermöglichen, aber das macht sie nicht unantastbar. Im Folgenden stellen wir einige Tipps und Tricks vor, die wir Ihnen empfehlen, wenn Sie zum ersten Mal das Dark Web für die Überwachung von Sicherheitsrisiken in Unternehmen nutzen.

1. JavaScript, Flash and Java deaktivieren

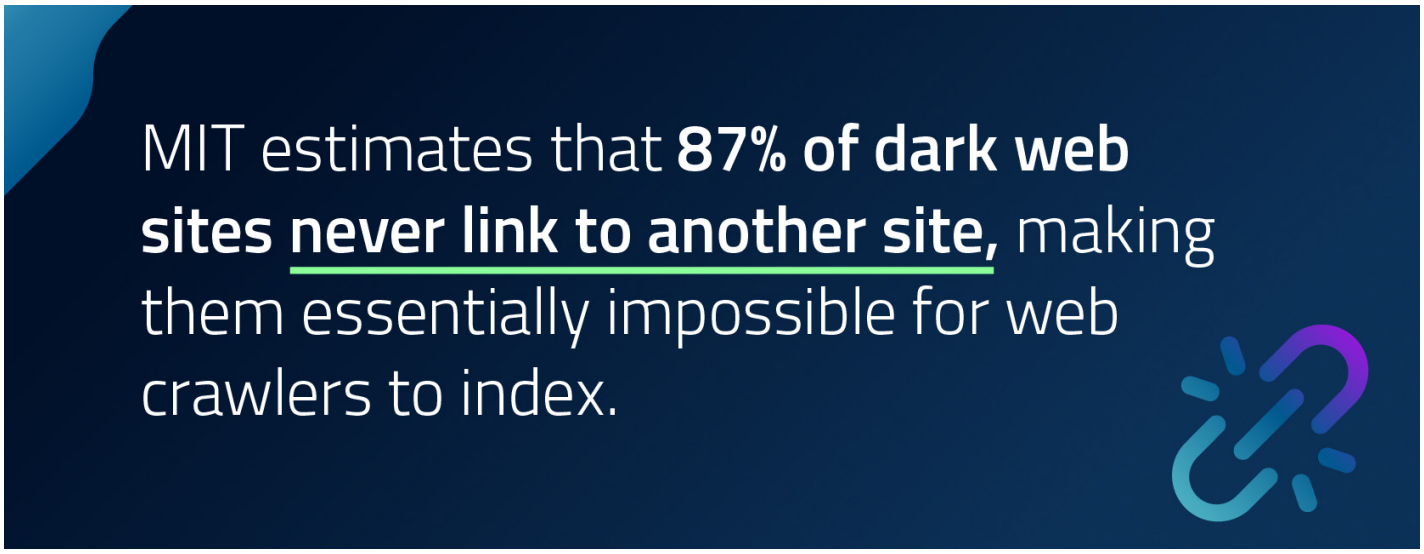
Das ist wichtig, da Tor nicht vor aktiven Inhalten schützt und die Aktivierung dieser Dienste von Angreifern ausgenutzt werden kann, um Identitäten zu kompromittieren oder Infos von Computern zu stehlen.

2. Virtuelle Machinen verwenden

Als Experte für Informationssicherheit kennen Sie die Risiken, die mit Online-Aktivitäten einhergehen. Anstatt Ihr System diesen Risiken auszusetzen, empfehlen wir Ihnen, nur innerhalb einer virtuellen Linux-Maschine auf das Dark Web zuzugreifen. Dadurch bleiben Ihre Aktivitäten auf die virtuelle Maschine beschränkt, was das Risiko verringert, dass ein Angreifer auf den Rechner zugreifen kann.

3. Wissen, wonach man sucht

Das Dark Web ist ein großer und gefährlicher Ort. Wir raten Ihnen dringend, die Art der Daten und Informationen, nach denen Sie suchen, klar zu definieren, bevor Sie sich ins Dark Web wagen. Oben haben wir einige der Arten von Informationen definiert, die Sie im Dark Web finden können. Wenn Sie sich jedoch auf die spezifischen Informationen konzentrieren, die Sie überwachen möchten, fällt es Ihnen leichter, das zu finden, wonach Sie suchen. Das bewahrt sie davor, Dinge zu entdecken, die Sie nicht sehen wollen.



4. Dark-Web-Suchmaschinen meiden

Es gibt zwar Dark-Web-Suchmaschinen, aber viele der Informationen, die Sie suchen, sind nicht indexiert oder lassen sich nicht per Suchmaschine finden. Nach Schätzungen von MIT-Forschern sind 87 Prozent der Dark-Web-Seiten nie mit einer anderen Seite verlinkt, sodass sie im Grunde nicht greifbar sind. Darüber hinaus dienen viele dieser Dienste als Honigtöpfe für Leute, die Nutzeraktivitäten im Dark Web identifizieren, verfolgen und diese Informationen dann online veröffentlichen. Deshalb verwenden wir von IntSights bei unseren Recherchen niemals Suchmaschinen für das Dark Web.

5. Lieber mit Indizes starten

Indizes sind Websites mit Links zu verschiedenen Dark-Web-Seiten, die oft nach Kategorien geordnet sind. Dabei handelt es sich – ähnlich wie bei Reddit – oft um von der Gemeinschaft organisierte Seiten, die Google meistens leicht findet. Im Gegensatz zu Suchmaschinen gelten sie als zuverlässiger und sicherer, da Sie keine Suchanfrage stellen, sondern einfach Links aus Quellen kopieren. Eine kostengünstige Methode, um Websites im Tor-Netzwerk zu finden. Einen guten Index für den Anfang stellt https://thehiddenwiki.org dar.

6. Ein eindeutiges, im Dark Web einzigartiges Pseudonym benutzen

Tor ermöglicht einen anonymen Zugang zum Dark Web, mischt sich aber nicht ein, welche Informationen oder Entscheidungen man dort trifft. Zu den häufigsten Anfängerfehlern zählt die Verwendung eines Pseudonyms oder anderer Identifikationsdaten, die anderen Online-Identitäten ähneln oder mit ihnen verbunden sind. Wenn diese Informationen nicht korrekt verwendet werden, können Hacker Ihre Aktivitäten im Dark Web mit anderen Online-Handlungen von Ihnen in Verbindung bringen und sie schließlich zu Ihrer Identität oder Ihrem Unternehmen zurückverfolgen.

7. Klartext reden

Wie jede andere Gemeinschaft oder Nachbarschaft besitzt auch das Dark Web seine eigene Sprache, um Dinge zu beschreiben, Geschäfte zu tätigen und Menschen zu bezeichnen. Die falsche Sprache kann verraten, dass Sie ein Dark-Web-Neuling sind, was die Leute dort misstrauisch macht. Bevor Sie sich in ein Forum stürzen, sollten Sie sich für die Fachsprache Zeit nehmen und sich auf den Gesprächsstil einstellen. Es folgen Beispiele für einige gängige Begriffe, die russische Hacker in Dark-Web-Foren verwenden.

Begriff	Aussprache	Definition
Взлом	Vzlom	hacken
Взломщик	Vzlomshik	Hacker
Вбив	Vbiv	Carding
Залив	Zaliv	Geldwäschemethode, bei der sowohl Karteninhaber als auch Absender strafrechtlich verantwortlich sind
Нал	Nal	Bargeld
обнал/обналичка	Obnal	unerlaubte Auszahlung
Безнал	Beznal	bargeldlose Zahlung
Акки	Akki	Accounts
Дедик	Dedik	Server
Прозвон	Prozvon	Autorisierung
Контора	Kontora	Marktplatz
Бабки/Бабло	Babki/Bablo	Geld
Транза	Tranza	Transaktion
Локает	Lokae	Lockdown
Карж	Karj	Hehlerware
Захолдит	Zacholdit	auf Eis legen
Ася	Asya	ICQ Messenger

8. Um Hilfe bitten

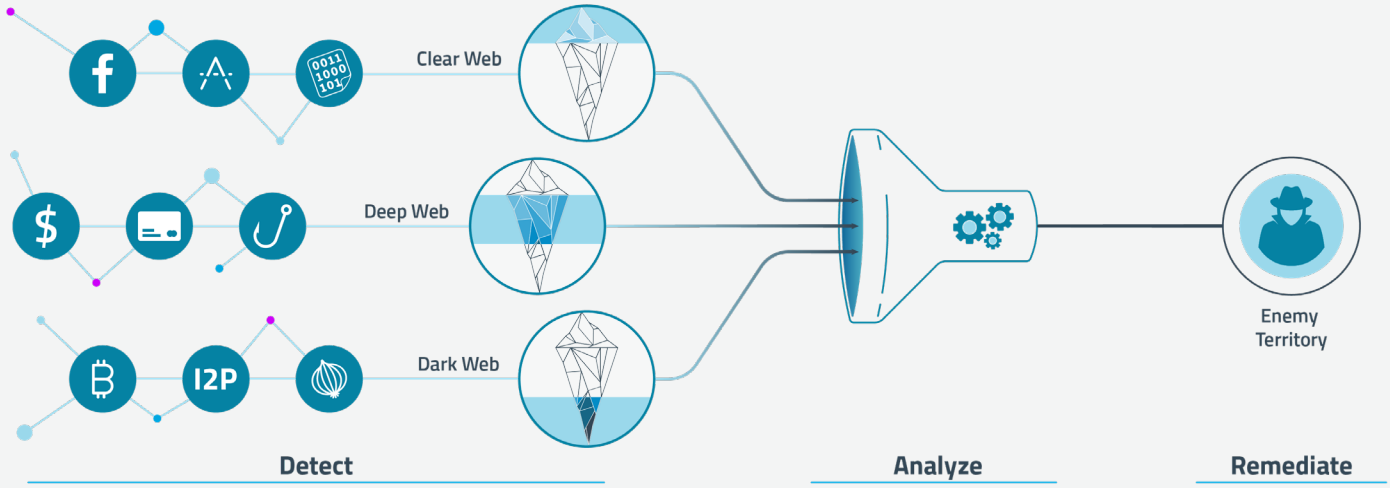
Scheuen Sie sich nicht, um Hilfe zu bitten. So wie Hacker ihre Taktiken austauschen und zusammenarbeiten, um sich einen Vorteil zu verschaffen, müssen auch die Verteidiger lernen, dasselbe zu tun. Die Geheimdienste, große Unternehmen und Bedrohungsanalysefirmen nutzen seit Jahren das Dark Web, um Informationen über Bedrohungen zu erhalten. Fachleute aus diesen Gruppen tauschen bewährte Verfahren in ihren Blogs, auf Konferenzen und bei lokalen Treffen aus. Bei IntSights veröffentlichen wir regelmäßig bewährte Vorgehensweisen und Informationen über die neuesten Trends in unserem Blog und ermutigen die Teilnehmer, sich mit Kommentaren oder Fragen zu melden.

Das Dark Web und verwertbare Bedrohungsdaten

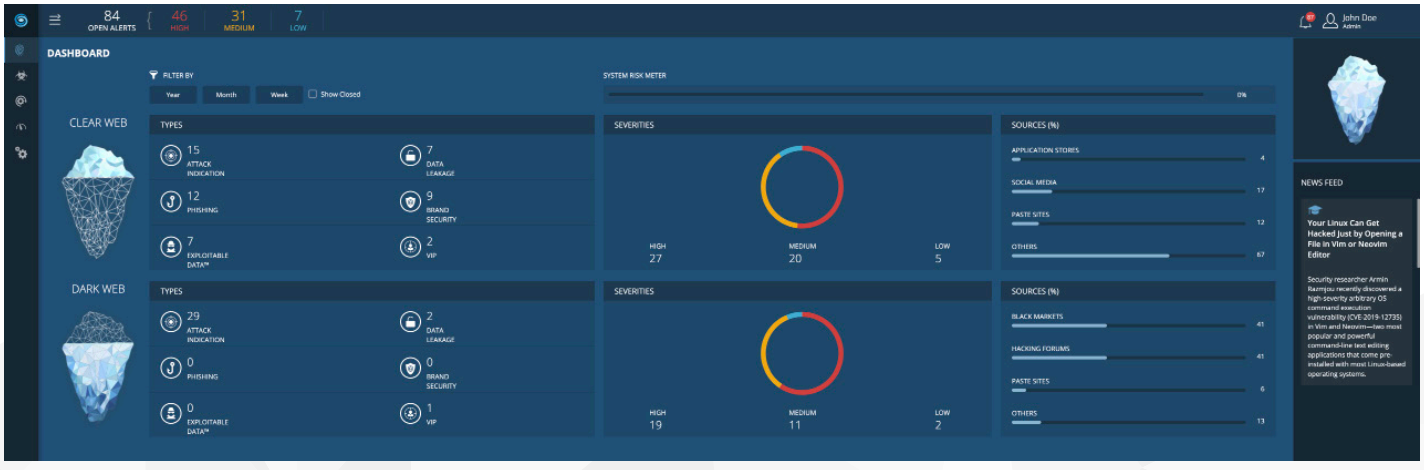
Einige Unternehmen verfügen zwar über die internen Kapazitäten, um die Vorteile des Dark Web komplett zu nutzen. Die Realität sieht jedoch so aus, dass viele Firmen nicht über die Zeit, die Ressourcen oder das Fachwissen verfügen, um das Deep- und Dark Web manuell auf Frühwarnungen vor Angriffen zu überwachen. Selbst diejenigen, die die entsprechenden Ressourcen besitzen, haben oft Schwierigkeiten, die gesammelten Informationen so zu kanalisieren, dass sie das Netzwerk rechtzeitig aktualisieren und somit schützen.

IntSights hat es sich zum Ziel gesetzt, Unternehmen dabei zu helfen, das Dark Web voll auszuschöpfen. Dafür haben wir eine Plattform für das Bedrohungsmanagement entwickelt, die das externe Risikoprofil einer Firma kontinuierlich überwacht, Zehntausende von Bedrohungsquellen analysiert und aggregiert sowie den Lebenszyklus der Risikobeseitigung automatisiert, indem sie Daten in verwertbare Informationen umwandelt. Dazu durchforsten wir kontinuierlich das Dark Web, indexieren die gesammelten Daten und analysieren sie, um potenzielle Bedrohungen für Kunden zu identifizieren.

Unsere bahnbrechenden Data-Mining-Algorithmen und einzigartigen maschinellen Lernfähigkeiten scannen kontinuierlich das Clear-, Deep- und Dark Web, um maßgeschneiderte, kontextbezogene Erkenntnisse über potenzielle Bedrohungen für Ihr Unternehmen zu liefern. Sie lassen sich nahtlos in Ihre bestehenden Sicherheitslösungen integrieren, um operative Schwachstellen zu beseitigen, Daten zu sichern und Ressourcen zu schützen.



Die IntSights-Plattform überwacht Zehntausende Quellen im freien, tiefen und dunklen Internet, um maßgeschneiderte Bedrohungsdaten zu erzeugen, die speziell auf Ihre Marke, Ihre Vermögenswerte und Ihre Mitarbeiter zugeschnitten sind. Im Gegensatz zu IOCs oder anderen rein maschinenlesbaren Informationen durchbricht IntSights das Durcheinander und liefert den Kontext, der zur Überwachung externer, von Menschen verursachter Risiken erforderlich ist.



Mit unseren maßgeschneiderten, intelligenten Fähigkeiten überwachen und analysieren wir kontinuierlich die Domänen, IP-Adressen, DLP-Indikatoren, mobilen Anwendungen, Social-Media-Seiten, geheimen Projekte, Technologien, BINs, VIP-Namen und E-Mails Ihres Unternehmens. So erkennen wir Risiken für Ihre Firma. Wir beobachten Hunderte von kriminellen Akteuren genau und untersuchen aktiv die neuesten Kampagnen, Malware-Entwicklungen und Taktiken. Alle Daten landen in einer umfassenden Bibliothek mit bekannten Bedrohungsindikatoren, kriminellen Elementen und untersuchten TTPs.

Mithilfe dieser Daten kann IntSights Gefahren zusammenfassen und IOCs sowie qualitative Informationen über Akteure in einer einzigen Bedrohungsmanagement-Plattform priorisieren, um die Reaktion und Behebung zu beschleunigen. Wir klassifizieren jeden IOC und jeden Angriffspunkt nach Kontext, Schweregrad und Relevanz, um eine individuelle Risikobewertung für Ihr Unternehmen zu entwickeln.

So gelingt es unserem Team, Gefahren präzise zu kategorisieren und Sie auf potenzielle Angriffe, Datenlecks, Markenimitationen, Phishing-Angriffe, externe Systemschwachstellen und VIP-Warnungen aufmerksam zu machen.

Über IntSights

IntSights, ein Unternehmen von Rapid7, ermöglicht es Unternehmen jeder Art und Größe, den vollen Nutzen aus externen Bedrohungsdaten zu ziehen, unabhängig vom Umfang oder dem Entwicklungsstand ihrer Threat-Intelligence-Programme. Im Gegensatz zu allen anderen Lösungen auf dem Markt reduziert IntSights die Komplexität von Threat Intelligence und liefert sofortigen Nutzen – ohne den großen Aufwand oder die beträchtliche Ressourcenzuweisung, die herkömmliche Threat-Intelligence-Lösungen erfordern. IntSights ist skalierbar und eignet sich für jede Firma, und die reibungslose Integration unserer Echtzeit-Cyber-Bedrohungsdaten in die bestehende Sicherheitsinfrastruktur unterstützt Betriebe dabei, ihre Investitionsrendite zu maximieren.

IntSights verfügt über Niederlassungen in Amsterdam, Boston, Dallas, New York, Singapur Tel Aviv und Tokio. Wenn Sie mehr erfahren möchten, besuchen Sie bitte intsights.com oder treten Sie in Kontakt mit uns über LinkedIn, Twitter oder Facebook.