über 80 Jahre | Tradition & Innovation

BÜRO MAYER
IT-Systemhaus & Service

Wir überwachen, verwalten und beseitigen Ihr Digitales Risiko im Open Web, Deep Web und Darknet

digital shadows_

Mit Digital Shadows überwachen und managen Sie das digitale Risiko Ihres Unternehmens in allen erdenklichen Quellen im Open Web, Deep Web und Darknet, um Ihr Unternehmen, Ihre Marke und Ihren Ruf zu schützen.

Warum Digital Risk Management notwendig ist:

Die Industrie entwickelt sich ständig weiter, Unternehmen werden zunehmend digitaler und das „Internet der Dinge“ verändert den Produktionsprozess, wie wir ihn heute kennen.

Unternehmen generieren schon heute eine Fülle an digitalen Informationen und das Volumen der digitalen Daten wächst beständig. Experten der IT-Branche gehen von einer Verdopplung der Datenmenge in einem Turnus von etwa zwei Jahren aus.

Das fortschreitende Zusammenwachsen von mobilen und eingebetteten Informationssystemen sowie von Rohstoffen, Waren, Produktionsstätten und Zuliefer- sowie Auslieferungsketten, sorgt für diese extrem hohe Datenmenge.

Um den Schutz und die Sicherheit des Unternehmens gewährleisten zu können, müssen die externen digitalen Risiken kontinuierlich überwacht werden. Unternehmen werden mit einer Fülle von Insellösungen überschüttet, die auf den internen Schutz der Daten ausgelegt sind.

Unternehmen benötigen eine Lösung, die sowohl offene als auch geschlossene digitale Plattformen überwachen kann und Bedrohungen anzeigt, die relevant und verifiziert sind.

Digital Shadows SearchLight™:

Der SearchLight-Service von Digital Shadows kombiniert skalierbare Datenanalysen mit menschlichen Datenanalysten, um die digitalen Risiken eines Unternehmens zu verwalten, zu minimieren und mit maßgeschneiderten Bedrohungsdaten eine aktuelle Ansicht - in allen Zeitzonen und in 27 verschiedenen Sprachen - zu erstellen.

über 80 Jahre | Tradition & Innovation

BÜRO MAYER
IT-Systemhaus & Service

Wir überwachen, verwalten und beseitigen
Ihr Digitales Risiko im Open Web, Deep Web
und Darknet

digital shadows_

„Ein umfassendes Paket von Risikomanagement-Richtlinien, -Verfahren und -Technologien, die zur Kontrolle, Verwaltung, Überwachung und Reaktion auf digitale Risiken vorgesehen sind, die sich überall im Open Web, Deep Web und Darknet ergeben“

Ein strategisches Risikomanagement sollte Richtlinien und Kontrollmechanismen für folgende Szenarien bereitstellen:

• Cyber-Bedrohung: Cyber-Bedrohungen reichen von politischen Hacktivisten bis hin zu gut ausgebildeten Cyber-Bedrohungsakteuren, die nach Profit streben. Die frühzeitige Erkennung von digitalen Risiken und Datenverletzungen ist von entscheidender Bedeutung, um die Exposition und die Auswirkungen auf die Organisation zu minimieren. Digital Shadows ermöglicht Schutz mit Kontext, empfohlenen Aktionen und Korrekturen, die auf Ihre Organisation, Geografie und Branche zugeschnitten sind.

• Datenverlust: Der digitale Fußabdruck Ihres Unternehmens expandiert mit überwältigender Geschwindigkeit. Mitarbeiter, Kunden und Dritte legen unwissentlich sensible Informationen offen. Die meisten Unternehmen verfügen über Kontrollmechanismen, um Datenlecks im Unternehmensnetzwerk zu überwachen, können Webseiten aber nicht auf Ereignisse wie das Ausspionieren von Anmeldedaten und technische Lecks überwachen. Diese sensiblen Daten werden zum Beispiel häufig über den Quellcode und frühere Sites unbeabsichtigt freigegeben. Der daraus resultierende Datenverlust kann schwerwiegende Auswirkungen auf die Reputation Ihres Unternehmens haben.

• Bloßstellung einer Marke: Ihre Online-Präsenz ist für das Wachstum Ihres Unternehmens, Ihrer Marke und Ihres Ansehens von entscheidender Bedeutung, aber sie zieht auch immer mehr Bedrohungsakteure an, die Ihr Marken- und Kundenvertrauen für Profit und böswillige Absichten nutzen möchten.

über 80 Jahre | Tradition & Innovation

BÜRO MAYER
IT-Systemhaus & Service

Wir überwachen, verwalten und beseitigen Ihr Digitales Risiko im Open Web, Deep Web und Darknet

digital shadows_

Globale Bedrohungen umfassen heute Marken- und Social-Media-Missbrauch sowie bösartige Web-Domains und mobile Apps, die sich auf Umsatz, Loyalität und Kundenvertrauen auswirken können.

Mit dem Schutz der Marken durch Digital Shadows SearchLight ™ registrieren Sie Ihren Markennamen, Web-Domainnamen und offizielle mobile Apps für die digitale Überwachung. Über das SearchLight-Portal erhalten Sie die relevantesten und kritischsten digitalen Risiken mit vollständiger Transparenz, Kontext und empfohlenen Maßnahmen zur Behebung des Risikos.

• Risiko durch Dritte. Digitale Risiko-Strategien müssen sich auch auf Dritte wie Geschäftspartner, Lieferanten und Kunden erstrecken, da Cyber-Angriffe sich längst auf die Kompromittierung von vertrauenswürdigen Daten über Dritte ausgestreckt haben.

Bedrohungsakteure können Ihre Lieferkette oder Lieferanten nutzen, um Zugang zu wertvollen Systemen und Ressourcen zu erhalten. Drittanbieter und Lieferketten können sehr komplex sein und sich ständig ändern. Um die Datenintegrität aufrechtzuerhalten, den sicheren Waren- und Rohstoffffluss sicherstellen und das Drittanbieterrisiko zu mindern ist es wichtig, dass Sie alle Lieferanten identifizieren, mit denen Ihr Unternehmen in Verbindung steht, da jede dieser Komponenten Ihre schwächste Sicherheitsverbindung sein kann und sich somit negativ auf Ihr Geschäft auswirken würde.

Digital Shadows SearchLight ™ verwendet eine Vielzahl von Datenquellen, um die Hauptrisiken für Ihre Lieferkette und Lieferantenbeziehungen zu identifizieren. Auf diese Weise können Sie priorisieren, welche Lieferanten am meisten gefährdet sind.

• Bloßstellung wichtiger Personen: VIPs und Führungskräfte, die für Ihr Unternehmen und Ihre Marke von entscheidender Bedeutung sind, sind oft Angriffsziele von Doxing-Kampagnen, Nachahmung oder Phishing-Attacken. Diese Angriffe dienen dem Ziel, den Ruf von Personen und Unternehmen zu schädigen oder persönliche Datenlücken, zum Erhalt von sensiblen Unternehmensinformationen, zu nutzen.

Angreifer können persönliche Informationen von Führungskräften, Vorstandsmitgliedern, wichtigen technischen Mitarbeitern und Persönlichkeiten des öffentlichen Lebens für Geldgewinne, Reputationsschäden, körperliche Schäden oder politische Erklärungen nutzen. Daher müssen Gegenmaßnahmen auf einer sorgfältigen Sammlung von Bedrohungsmustern, Analysen und Aktionen beruhen.

über 80 Jahre | Tradition & Innovation

BÜRO MAYER
IT-Systemhaus & Service

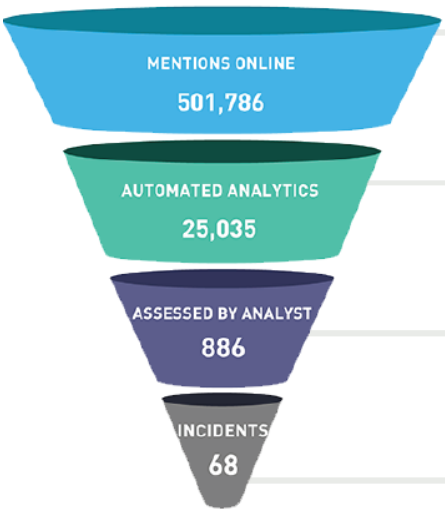
Wir überwachen, verwalten und beseitigen Ihr Digitales Risiko im Open Web, Deep Web und Darknet

digital shadows_

• Physische Bedrohungen: Zunehmend werden physische Bedrohungen in der realen Welt online organisiert, geplant und veröffentlicht. Von individuellen Bedrohungen gegen wichtige Mitarbeiter und gezielten Angriffen auf die physischen Standorte Ihres Unternehmens bis hin zu großen Protesten in den Städten, in denen Sie tätig sind, werden physische Bedrohungen häufig vor, während und nach einem Angriff online veröffentlicht oder weitergegeben.

• Gefährdung der Infrastruktur. Unternehmen benötigen ein umfassendes Verständnis darüber, an welcher Stelle ihre IT-Infrastruktur gefährdet sein könnte. Dies bedeutet, dass Unternehmen Einblick in das Darknet benötigen, um Chat-Seiten von Hackern und deren Gespräche, um Themen wie Zero-Day-Schwachstellen und Exploit-Kits, wahrzunehmen.

Wie Ihnen SearchLight™ hilft:



Planen und Sammeln
SearchLight überwacht kontinuierlich das sichtbare Internet, das Deep Web und das Darknet auf Inhalte, welche eindeutige Kennzeichen aufweisen, ihren Ursprung in ihrem Unternehmen zu haben

Automatisierte Analyse
Irrelevante Erwähnungen werden mit Hilfe einer Kombination aus Data Science und maschinellem Lernen entfernt.

Manuelle Analyse
Erfahrene Analysten überprüfen maschinell ermittelte Sicherheitsvorfälle, entfernen Fehlalarme, führen weitere Untersuchungen durch, stellen einen Sinnzusammenhang her und weisen einen Sicherheitslevel zu.

Verbreitung
Relevante, priorisierte und rechtlich bedenkliche Sicherheitsvorfälle werden über unser Portal, E-Mail-Benachrichtigungen oder eine API bereitgestellt.

über 80 Jahre | Tradition & Innovation

BÜRO MAYER
IT-Systemhaus & Service

Wir überwachen, verwalten und beseitigen Ihr Digitales Risiko im Open Web, Deep Web und Darknet

digital shadows_

„Behalten Sie die Oberhand über ausgespähte Daten im Open Web, Deep Web und Darknet“

Mit SearchLight™ ermitteln Sie, wo Ihre Daten online verfügbar sind. SearchLight™ informiert Sie umfassend und zeigt, mit welchen Schritten Sie Ihr Datenrisiko verringern.

Der digitale Fußabdruck von Unternehmen wächst mit überwältigender Geschwindigkeit und die ungewollte Veröffentlichung vertraulicher Daten stellt ein erhebliches Risiko dar.

Mitarbeiter, Kunden und Dritte geben unwissentlich sensible Informationen preis. Der Verlust und die Preisgabe von Daten können gravierende Auswirkungen für das Ansehen von Unternehmen haben. Darüber hinaus nutzen Cyber-Kriminelle diese Informationen, um Sicherheitslücken auszunutzen und ihre Angriffe zu starten.

Die Häufigkeit, mit der Informationen geteilt werden, erschwert es Unternehmen nachzuverfolgen, wo diese Informationen verfügbar sind. Beispiele für ein Datendiebstahl Risiko sind Brute-Force-Attacken, Angriffe auf Zugangsdaten und der Diebstahl von geistigem Eigentum durch Cyber-Kriminelle. Digital Shadows SearchLight™ managt, überwacht und beseitigt das Risiko der Datenspionage, indem es von Analysten verifizierte Risiken mit zusätzlichen Informationen und empfohlenen Maßnahmen bereitstellt. So können Sie Ihre Zeit effizienter nutzen und müssen sich nicht von Fehlalarmen ablenken lassen.

Digital Shadows SearchLight ™ überwacht die digitalen Vermögenswerte eines Unternehmens im Open Web, Deep Web, und Darknet um ungewollt veröffentliche Daten aufzuspüren. Die Business-Intelligence-Experten von Digital Shadows überprüfen jeden Fall, um zu verifizieren, dass Sie nur über die Gefährdungen informiert werden, die für Ihr Unternehmen relevant sind.

über 80 Jahre | Tradition & Innovation

BÜRO MAYER
IT-Systemhaus & Service

Wir überwachen, verwalten und beseitigen Ihr Digitales Risiko im Open Web, Deep Web und Darknet

digital shadows_

Zu den fünf Arten von Datenrisiken, die von SearchLight™ erkannt werden, gehören:

Sensible Dokumente:

Vertrauliche, private und sensible Dokumente wie Verträge, Gehaltsabrechnungen, Entwürfe und vertrauliche Vorstandsprotokolle, die nicht für die Öffentlichkeit bestimmt sind, können Auswirkungen auf die Reputation haben und damit auch auf das Betriebsergebnis.

Kundendaten:

Ausgespähte Kundendaten können sowohl Marken- und Unternehmensrisiken als auch rechtliche Probleme verursachen. Daher ist es unerlässlich, dass personenbezogene Daten (Personally Identifiable Information, PII) erkannt werden, bevor sie an die Öffentlichkeit gelangen.

Mitarbeiterdaten:

Mitarbeiter können durch ausgespähte Anmeldeinformationen ausspioniert werden. Dies erlaubt Angreifern, Account-Übernahmen durchzuführen oder Spearphishing-E-Mails zu erstellen.

Technische Informationen:

Angreifer können den offengelegten Firmen-Code, Konfigurationsdateien und andere technische Details wie Software- und Systeminformationen dafür nutzen, um gezielte Angriffe auszuführen und somit Zugang zu Ihrem Netzwerk zu erhalten.

Geistiges Eigentum:

Ausgespähtes geistiges Eigentum, beispielsweise Produktdesigns, Patente uvm. macht Sie anfällig für Wirtschaftsspionage und eine Gefährdung des Wettbewerbs.

Die ungewollte Veröffentlichung vertraulicher Daten

Unternehmen und Organisationen bieten oft Daten von Mitarbeitern, Partnern, Zulieferern und Kunden öffentlich zugänglich an. Dies geschieht in den meisten Fällen unbeabsichtigt und häufig auf Grund kleiner Fehler.

Niemand möchte Fehler machen. Dennoch passieren diese ganz offensichtlich und täglich mit sensiblen Daten.

über 80 Jahre | Tradition & Innovation

BÜRO MAYER
IT-Systemhaus & Service

Wir überwachen, verwalten und beseitigen
Ihr Digitales Risiko im Open Web, Deep Web
und Darknet

digital shadows_

Allein in den ersten drei Monaten dieses Jahres fanden **die Threat Intelligence Experten von Digital Shadows** über 1,5 Milliarden Unternehmens- und Kundendokumente im Netz – frei zugänglich über offene Amazon Simple Storage Service (S3), rsync, SMB bzw. FTPserver, falsch konfigurierte Websites und Network Attached Storage (NAS)-Laufwerke.

Die gefundenen Dokumente (in über **12.000 Terabyte** an Daten) beinhalteten Login-Daten, Passwörter, Datenbank-Backups, Konfigurations-Files, Programmquellcode, Gehaltsabrechnungen, Steuererklärungen, Kreditkarteninformationen und sogar Krankenakten einzelner Personen.

In einem konkreten Fall entdeckte Digital Shadows eine große Menge an Point-of-Sales-Terminaldaten, also Kundendaten, die an einer bargeldlosen Verkaufsstelle in einem Supermarkt oder in einer Filiale erfasst werden. Dazu zählen auch Transaktionsdaten, Uhrzeit, Ort und sogar Kredit- und Geldkarteninformationen.

Auf Unternehmensseite stellen öffentlich zugängliche Intellectual-Property-Dateien, also geistiges Eigentum ein erhebliches Risiko dar. Zu den brisanten Fundstücken zählt u. a. die Zusammenfassung eines Patents einer Lösung für erneuerbare Energien – ironischerweise mit dem Vermerk »streng vertraulich«. Ein weiteres Beispiel ist proprietärer Quellcode, der im Rahmen einer Copyright-Anmeldung eingereicht wurde und Details zum Design und dem Workflow einer Website für Software Electronic Medical Records (EMR) enthält.

Ein Albtraum für Datenschützer - persönlicher kann es kaum werden.

Den vollständigen Report von Digital Shadows »Too Much Information: Misconfigured FTP, SMB, rsync, and S3 Buckets Exposing 1.5 Billion Files« finden Sie nach Registrierung hier:

Gerade im Hinblick auf die neue Datenschutzgrundverordnung der EU und den damit verbundenen regulatorischen Auflagen sollte die große Menge an exponierter Daten, die online zu finden sind, jedem Unternehmen und jeder Organisation zu denken geben.

über 80 Jahre | Tradition & Innovation

BÜRO MAYER
IT-Systemhaus & Service

Wir überwachen, verwalten und beseitigen Ihr Digitales Risiko im Open Web, Deep Web und Darknet

digital shadows_

Open Web, Deep Web und Darknet – was steckt dahinter

Der Begriff Deep Web bezeichnet den Teil des Internets, der nicht über die gängigen Suchmaschinen wie Google, Yahoo und Co. (Open Web) angesteuert werden kann.

Zu einem großen Teil besteht das Deep Web aus spezifischen Datenbanken und Webseiten, die keinen freien Zugang haben. Beispiele dafür sind Inhalte, die nur gegen Bezahlung geöffnet werden können, oder Firmen- und Regierungsdaten.

Eine Metapher für das Verhältnis von Deep Web zum Open Web ist ein Eisberg. Die Spitze des Eisbergs stellt dabei das Open Web dar, wohingegen der gesamte Wasserinhalt das Deep Web repräsentiert.

Schätzungen nach enthält das Deep Web 550 Mal so viele Daten wie das Open Web. Wird das Deep Web nur von Kriminellen genutzt?

Das Deep Web kann mit gewöhnlichen Browsern angewählt und genutzt werden. Ob kriminell oder nicht, spielt dabei, im ersten Schritt, keine Rolle. Zwar sind die Inhalte des Deep Webs nicht mit einem Klick per Suchmaschine zu finden, jedoch können sie mit ein paar weiteren Klicks verhältnismäßig schnell erreicht werden. Somit sind die größten Teile des Deep Webs völlig frei zugänglich, beziehungsweise können über ein Abonnement freigeschaltet werden.

Ein Unterschied dazu stellt der Bereich des Darknet dar.

Das Darknet ist ein Bereich des Deep Web, der grundsätzlich ein anonymes Surfen ermöglicht. Da es im Open Web zu Aufzeichnungen der Surfaktivitäten von Anwendern kommt, haben Entwickler mit der Erfindung des Darknet eine neue Möglichkeit geschaffen. Durch die Nutzung eines bestimmten Browsers (Tor Browser) ist es möglich anonym zu surfen und so die Privatsphäre zu schützen.

Dieser Vorteil wird auch von Kriminellen genutzt, die so illegale Handlungen planen und ausführen können, ohne dass sie dabei beobachtet werden. Jüngste Festnahmen haben jedoch gezeigt, dass es den Polizeibehörden möglich war, illegale Handelsplätze zu schließen und Kriminelle, die im Darknet unerlaubten Handel trieben, zu verhaften.

Die Geschlossenheit dieser Seiten erfordert einen spezifischen Ansatz, um Zugang zu bestimmten Bereichen des Darknet zu erhalten und damit einen vollständigen Überblick über das digitale Risiko.

über 80 Jahre | Tradition & Innovation

BÜRO MAYER
IT-Systemhaus & Service

Wir überwachen, verwalten und beseitigen Ihr Digitales Risiko im Open Web, Deep Web und Darknet

digital shadows_

Wer nutzt das Deep Web & Darknet?

Anonymität ist vor allem für zwei Gruppen interessant:

Auf der einen Seite stehen Menschen, die den Schutz des Deep Web für Ihre Kommunikation benötigen. Sie teilen sensible Daten und Informationen und müssen zum Teil um ihr eigenes Leben oder das ihrer Informanten fürchten, wenn sie sich nicht im Schutz des Deep Web austauschen.

Zu dieser Gruppe gehören politisch Unterdrückte oder Dissidenten, Oppositionelle aus diktaturgeführten Ländern oder Journalisten und Whistleblower. Über das Deep Web können sie auch auf Inhalte zugreifen, die ihnen im sichtbaren Netz durch politische Restriktionen nicht zur Verfügung stehen, die zensiert sind oder die Sie in Lebensgefahr bringen würden.

Die Anonymisierung hilft Journalisten dabei, Ihre Quellen zu schützen. So konnten beispielsweise die Aktivisten des Arabischen Frühlings über das TOR-Netzwerk auf „Social Media Kanäle“ zugreifen und ihre Informationen über die Revolution verbreiten. Und auch Whistleblower wie „Edward Snowden“ nutzen das Deep Web, um brisante Informationen an die Öffentlichkeit zu bringen. Diese erste Gruppe schützt sich mit der Flucht ins Deep Web somit vor negativen Konsequenzen und Verfolgung.

Die zweite Gruppe nutzt die Anonymität des Deep Web, um negativen Konsequenzen zu entgehen und sich einer Strafverfolgung zu entziehen. Diese Gruppe setzt sich aus Menschen zusammen, deren Aktivitäten im sichtbaren Internet (Open Web) sehr schnell zu einer Anzeige sowie Geld- und Haftstrafen führen würden. Im Darknet finden sich Foren, Webshops und Handelsplattformen für Dienstleistungen und Waren, die sonst entweder illegal oder strengen gesetzlichen Regelungen unterworfen sind.

Welche Möglichkeiten haben Kriminelle im Darknet?

Im Darknet gibt es alles, was es nach dem geltenden Gesetz gar nicht geben dürfte. Nicht registrierte Waffen, Drogen, gefälschte und gestohlene Dokumente, Kreditkarten, uvm. Zunehmend bieten auch IT-Experten mit kriminellen Ambitionen ihre Dienste im Darknet an. Von Überlastangriffen (DDoS-Attacken), die gezielt Websites und Internetdienste lahmlegen sollen über Viren-Baukästen bis zu Spam-Kampagnen – das Darknet ist ein Einkaufsparadies für Cyberkriminelle. Bezahlt wird meist in einer der zahlreichen elektronischen Crypto-Währungen, die ebenfalls auf Anonymität ausgelegt sind.

Wir überwachen, verwalten und beseitigen Ihr Digitales Risiko im Open Web, Deep Web und Darknet

digital shadows_

Da sich die User im Darknet nahezu spurlos bewegen, können Ermittler die Täter hinter den kriminellen Angeboten, Online-Shops oder Forums im Darknet nur nach langwieriger Recherche aufspüren. Ermittlungsbehörden haben aus diesem Grund Spezialeinheiten gegründet, deren Aufgabe es ist, in die illegalen Bereiche des Darknet einzudringen.

Auch klassische Überwachungsarbeit gehört zu den eingesetzten Werkzeugen, um die Täter zu fassen: Oft werden zum Beispiel Drogengeschäfte über Packstationen abgewickelt. Dass für derartige Transaktionen häufig gestohlene und im Darknet verkaufte Zugangskarten für die Packstation genutzt werden, macht das kriminelle Geflecht des Darknet deutlich.

Welche Märkte gibt es im Darknet?

Ein kurzer Einblick auf bekannte Märkte

Dream Market: Dieser Marktplatz beschäftigt sich mit allen Arten von Produkten und Dienstleistungen aus den Bereichen: Drogen, gehackte Kreditkarten, geknackte Software, Betrug, Fälschung, Elektronik, Verteidigung, Schmuck, Software, Erotika, Datenlecks uvm.

Dream Market gilt, nach der Schließung von AlphaBay, als einer der vertrauenswürdigsten Markplätze im Darknet.

1A Quality Cards: Dieser Marktplatz zählt als einer der vertrauenswürdigsten Kartenhändler, mit einer etablierten Reputation und einem „fairen“ Preis von ungefähr $ 100 USD je Karte. Die Karten sind real (physisch) und können per Post empfangen und in Geldautomaten oder Online-Käufen verwendet werden.

rsClub Market: Dieser Marktplatz bietet Drogen, "Betrugsbezogenen" Artikel sowie Guides und Tutorials an. Im Bereich Drogen: Cannabis, Haschisch, Stimulanzien, Opioide und Benzos. Im Bereich der „Betrugsbezogenen" Artikel: Accounts and Bank Drop (Hacked Accounts für Banken, Social Media , Erotik-Websites etc.), CVV und Karten (Gehackte Kreditkarten), Dumps und Tracks (gehackte Kreditkarten-Dumps, Passwort-Datei-Dumps usw.), Persönliche Informationen und Scans (gescannte Kopien gefälschter Reisepässe, Führerscheine , geänderte persönliche Daten), Sonstiges (gehackte Geschenkkarten, Adult Accounts, E-Books , uvm.)

über 80 Jahre | Tradition & Innovation

BÜRO MAYER
IT-Systemhaus & Service

Wir überwachen, verwalten und beseitigen Ihr Digitales Risiko im Open Web, Deep Web und Darknet

digital shadows_

Welche Dienstleister findet man in Darknet Foren?

Malware- / Exploit-Entwickler: Diese Personen sind die Entwickler der bösartigen Tools und Exploits, mit denen Cyberkriminelle Aktivitäten ausführen. Zu den entwickelten Tools gehören Remote Access Trojaner / Remote Administration Tools (RATs), Exploit Kits (EKs), Crypter, Keylogger und Information Stealers (InfoStealers). High-End-Entwickler sind technisch versierte Personen, die ihr Wissen und ihre Fähigkeiten einsetzen, um Softwaretools und Exploits zu erstellen, die in der Lage sind, gängige Sicherheitskontrollen zuverlässig zu umgehen, um Angreiferziele zu erreichen.

Obwohl die Entwickler die Köpfe hinter assoziierten Produkten sind, verwenden sie sie normalerweise nicht, um Opfer direkt anzugreifen. Stattdessen verkaufen sie diese Angebote in den Untergrundforen nach Profit. Die meisten Entwickler vermarkten ihr Angebot mit dem Haftungsausschluss, dass das Produkt ausschließlich für Bildungszwecke gedacht ist und nicht für illegale Aktivitäten verwendet werden sollte. Diese Sprache ist typisch für Malware-Autoren, die versuchen, sich von der wahrscheinlichen (und oft zweckbestimmten) illegalen Verwendung ihrer entwickelten Software zu distanzieren.

Back Office Support – Marketing: Werkzeuge, die in den Untergrundforen verkauft werden, werden zunehmend durch attraktive, professionell aussehende Marketing-Layouts beworben. Eine solche Werbung enthält Elemente wie Merkmale und Fähigkeiten des jeweiligen Werkzeugs oder Dienstes. Die Designs und Layouts werden häufig von Grafik- und Designspezialisten erstellt, die selbst ihre Dienste in Foren bewerben.

Das funktioniert für die Toolentwickler gut, da sie keine Zeit für die Erstellung von Marketingmaterial aufwenden müssen.

Stattdessen lagern die Entwickler diese Arbeit an diese Spezialisten aus. Ein attraktives Layout für die im Darknet verkauften Werkzeuge und Dienstleistungen ist für die Gewinnung von Käufern unerlässlich geworden. Ähnlich einer traditionellen Unternehmenswerbung / Marketingstrategie beeinflussen solide Designs und Branding die Verkaufszahlen.

Back Office Support - Anbieter von ressourcenbasierten Diensten*:* Diese Kategorie böswilliger Akteure bietet verschiedene Arten von Diensten an, z. B. Bullet Proof Hosting Service (BPHS), Distributed Denial of Service (DDoS) und andere. Solche Angebote werden zu vorher vereinbarten Tarifen vermietet, oft mit Garantien für Verfügbarkeit und Leistung.

Back Office Support - Bösartiger Trainingsanbieter: Diese Personen bieten Schulungsdienste an, darunter Aspekte wie Angriffstechniken, Malware-Infektion und Verbreitungsmethoden sowie Hosting und Verwaltung der Botnet-Infrastruktur. Diese Angebote umfassen gut dokumentierte, leicht verständliche und schrittweise Anleitungen für alle, die mehr über die Tipps und Tricks erfolgreicher Cybercrime-Operationen erfahren möchten.

Welche Werkzeuge bietet das Darknet?

Einige der gebräuchlichsten Werkzeuge, die in den Marktplätzen und Foren verkauft werden, sind RATs, Crypter und Infostealer. Einige dieser Tools werden als Malware-Erstellungs-Kits verkauft, die eine flexible Integration von Funktionen in eigenständige „Builds“ für die Bereitstellung ermöglichen, einschließlich Sicherheitsumgehung und Betriebsfunktionen.

In den folgenden Abschnitt beschreiben wir einige der wichtigsten Tools, die im Cybercrime-Ökosystem beobachtet wurden.

RATs*:* Remoteverwaltungstools oder alternativ Remotezugriffstrojaner ermöglichen es einem böswilligen Akteur, die Kontrolle über den Computer eines Opfers zu übernehmen. Moderne RATs sind eine zuverlässige und vielseitige Klasse von Werkzeugen, die von Akteuren für eine Reihe von Motivationen genutzt werden.

InfoStealer: InfoStealer sind eine Unterklasse von Überwachungs-Malware, die Elemente wie Tastenanschläge, den Bildschirmstatus und Dateien oder Datenspeicher von Interesse vom Computer eines Opfers erfasst und an einen Angreifer sendet. Diese Malware-Klasse bietet unmittelbare Vorteile für einen Angriff und kann auch als Input für integrierte, progressive gegnerische Operationen dienen.

Crypter: Crypter spielen eine wichtige Rolle im gesamten Malware-Erstellungszyklus. Sie ermöglichen es Cyberkriminellen, Malware zu entwickeln, die Legacy-Sicherheitslösungen umgehen kann, ohne Alarme auszulösen.

Beim „Krypten“ handelt es sich um Software, die eine Kombination aus Verschleierung, Verschlüsselung und Code-Manipulation verwendet, um Malware FUD (Fully Undetectable) zu erzeugen.

Nachdem die Malware-Binärdateien erstellt wurden, können sie durch einen Crypter geleitet werden, um die Wahrscheinlichkeit zu erhöhen, dass Sicherheitsmaßnahmen, die ihr Ziel schützen, erfolgreich umgangen werden können.

Malware-Spreading: Malware-Spreading-Dienste bieten Schritt-für-Schritt-Anleitungen zur Durchführung schädlicher Kampagnen. Sie bieten in der Regel Anleitungen und Verfahren zur Durchführung von Kampagnen, um Computersysteme mit Malware zu infizieren und Informationen mithilfe verschiedener Tools, Techniken und Verfahren zu extrahieren.

Bullet Proof Hosting-Dienstanbieter: Bullet Proof Hosting Service (BPHS) -Dienstanbieter ermöglichen es Cyber-Kriminellen, bösartige Inhalte zu hosten, ohne dass das Risiko besteht, dass sie außer Gefecht gesetzt werden. Es gibt mehrere BPHS-Anbieter, die Dienste unter dem Banner legitimer Geschäftsdienste anbieten. Es gibt jedoch auch einige BPHS-Anbieter, die ihre Dienste offen für böswillige Akteure anbieten, indem sie die auf ihren Servern gehosteten Inhaltstypen und dedizierte Pakete für das Hosting verschiedener Arten bösartiger Hosting-Dienste hervorheben.

DDoS-Dienste: Distributed Denial of Service (DDoS), auch als Booter oder Stresstest bezeichnet, sind Online-Ressourcen, die hauptsächlich zum Testen der Belastbarkeit von Websites verwendet werden. Böswillige Akteure nutzen diese Dienste, um Websites und einzelne Online-Internetnutzer zu Fall zu bringen.

In der Regel bieten diese Dienste volumetrische Layer-4- (Transport) - und Layer-7- (Anwendungs-) Angriffe, bei denen die Ressourcen des Ziels verbraucht werden und es nicht mehr auf legitime Anforderungen reagiert, wodurch der Dienst letztendlich zum Erliegen kommt.

Fazit

Viele Artikel und Forschungsarbeiten, die von der Informationssicherheitsindustrie veröffentlicht wurden, diskutieren, wie Cyber-Angriffe in Phasen aufgeteilt werden können, die weithin als das „**cyber kill-chain Modell**“ bekannt sind.

Darknet-Märkte spielen dabei wichtige Rollen ("*Bewaffnungs-* und *Ausbeutungsphase*" & "*Maßnahmen zu Zielen")* in der gesamten Angriffskette.

über 80 Jahre | Tradition & Innovation

BÜRO MAYER
IT-Systemhaus & Service

Wir überwachen, verwalten und beseitigen Ihr Digitales Risiko im Open Web, Deep Web und Darknet

digital shadows_

Cyberkriminelle können mit Darknet-Märkten ihr Ziel erreichen und durch den Verkauf der Daten, die aus den Computersystemen der Opfer gestohlen wurden, Geld verdienen und damit das Unternehmen und seinen Ruf schädigen.

Neben dem Verkauf erbeuteter Daten von Angriffen auf Firmen, ist Insiderdatendiebstahl ein erfolgreiches Verkaufsmodell auf den Darknet-Märkten, da Insider mit dem Wissen und Know-how dazu beitragen, authentische, gefälschte Produkte zu schaffen.

Digital Shadows - zum Schutz Ihres Unternehmens

Digital Shadows - SearchLight ™ vereint eine der umfassendsten und skalierbarsten Datenanalysen der Branche mit dem Wissen und der Expertise von Datensicherheits-Experten. SearchLight ™ bietet Ihnen einen maßgeschneiderten, Cloud-basierten Abonnement-Service, der kontinuierlich mehr als 100 Millionen Datenquellen - in 27 Sprachen - im Open Web, Deep Web und Dark Net (Online-Quellen, Social Media, IRC-Chat-Rooms, kriminellen Foren, technischen Foren, offene FTP Server, Code Sharing Plattformen, Amazon S3-Buckets, App Stores uvm.) überwacht, um die spezifischen Risiken eines Unternehmens zu identifizieren und dieses vor **Cyber-Bedrohungen**, **Preisgabe von Daten**, **Bloßstellung der Marke**, **Risiko durch Dritte**, **Bloßstellung wichtiger Personen**, **Physischer Bedrohungen** und **Gefährdung der Infrastruktur** zu schützen.

Warum sich Digital Shadows lohnt

Umfangreiche Berichterstattung

Wir überwachen alle erdenklichen Quellen im sichtbaren Internet, im Deep Web und im Darknet. Unsere Lösung identifiziert eine Vielzahl von digitalen Risiken, einschließlich Cyber-Bedrohungen, Datenverlust und Reputationsrisiken.

Relevante Threat Intelligence

Ein Verzeichnis der inviduellen Faktoren eines Unternehmens, dessen Tochtergesellschaften und Partner, welches diese eindeutig definieren, ermöglicht uns, nur die individuell relevanten Sicherheitsrisiken bereitzustellen.

Menschliche Wahrnehmung

Unsere Analysten filtern das Signal aus dem Rauschen, entfernen Fehlalarme und übermitteln nur die relevanten Sicherheitsrisiken. So sparen Sie Zeit und Geld.

Kontaktieren Sie uns

Alexander.Porschen@bueromayer.de

0951 96 24 150
0171 97 88 499

Für weitere Informationen besuchen Sie www.digitalshadows.com