INTSIGHTS
A RAPID7 COMPANY

Zugang zu verkaufen:

Der Handel mit Unternehmenskonten in kriminellen Foren

Vorwort

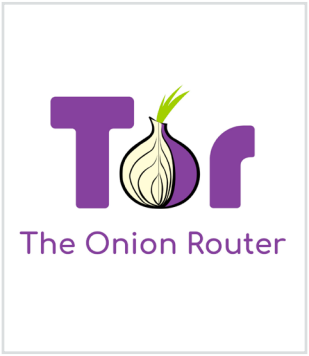
Der Verkauf und Kauf von unbefugten Zugängen zu Unternehmensnetzwerken hat sich zu einem Wegbereiter für kriminelle Cyberangriffe entwickelt, insbesondere für Ransomware-Infektionen. Einige Cyberkriminelle haben sich auf das Knacken von Netzwerken spezialisiert und verkaufen die erlangten Zugänge an Dritte, anstatt die Netzwerke selbst zu verwenden. Umgekehrt kompromittieren viele Kriminelle, die geknackte Netzwerke ausnutzen (besonders Ransomware-Betreiber) diese nicht selbst, sondern kaufen den Zugriff von anderen Angreifern.

Diese Tauschbörsen auf zwielichtigen Untergrundwebsites ermöglichen es Spezialisten mit zusätzlichen Fähigkeiten und Ressourcen, den Schweregrad und die Auswirkungen des kriminellen Ökosystems und der „Kill Chain" der Bedrohungsakteure zu erhöhen. Dieses illegale Marktangebot ist weniger bekannt als etwa der Verkauf von kompromittierten Zahlungskarten aus Einbrüchen in **Einzelhandel und Gastronomie**. Diese selten dokumentierten Angebote verdienen jedoch aufgrund ihrer potenziellen Auswirkungen eine genauere Betrachtung.

Von diesen Zugangsverkäufen sind Unternehmen in allen Branchen und Regionen betroffen. Technologie- und Telekommunikationsfirmen gehören zu den häufigsten Opfern und bringen mehr Geld. Verbrecher auf der ganzen Welt kaufen und verkaufen Netzwerkzugänge, wobei russischsprachige Akteure als Marktführer gelten. Diese Angebote beinhalten oft eine Kombination aus Fernzugriff auf ein Netzwerk und Administrator-Zugangsdaten oder andere privilegierte Konten. Durch die Verlagerung von Arbeitsplätzen an entfernte Standorte während der COVID-19-Pandemie und die daraus resultierende zunehmende Nutzung von Fernzugriffstools und -diensten haben Angreifer mehr Angriffsfläche, was den deutlichen Anstieg dieser Umsätze in den letzten 18 Monaten erheblich begünstigt hat. Dieses Phänomen gab es schon vor der Pandemie, aber es reifte und verselbstständigte sich im Jahr 2020, als einige Untergrundforen begannen, diesen speziellen Offerten eigene Unterforen einzuräumen.

Ein Überblick über den kriminellen Untergrund

Kriminelle Untergrundwebsites gelten als „kritische Infrastruktur" für das Ökosystem von Cyberbedrohungsakteuren und -betrügern. Diese Seiten bestehen aus Foren und Marktplätzen, wobei die Marktplätze wie die kriminellen Versionen von E-Commerce-Websites funktionieren. Der Verkauf von geknackten Netzwerkzugängen findet auf beiden Arten von Websites statt, aber in Foren geschieht es häufiger. Möglicherweise ist das weniger strukturierte Format von Threads, das multilaterale Diskussionen eher fördert und es den Postern ermöglicht, alte Beiträge wieder aufzufrischen, für diese Verkäufe besser geeignet als die strenger strukturierten Marktplätze. Beide Arten befinden sich meist entweder im Deep Web, das von Suchmaschinen nicht indiziert werden kann, oder im Dark Web, das die Verwendung des **Onion-Routers (Tor)** oder anderer spezieller Software erfordert, um auf sie zuzugreifen.



Diese Untergrundwebsites bilden für alle Beteiligten eine wichtige Basis. Einerseits ermöglichen sie es Käufern mit weniger Fähigkeiten oder Ressourcen, „Rohmaterial" zu erhalten, mit dem sie kriminelle Organisationen aufbauen können – Malware, andere bösartige Tools, gestohlene Daten, Konten und Zahlungskartendetails inbegriffen. Diese Möglichkeit senkt die Hürden für den Einstieg in das verbrecherische Ökosystem für Akteure, die ansonsten vielleicht nicht über die erforderlichen Fähigkeiten oder Ressourcen verfügen, aber das Geld für Investitionen haben. Auf der anderen Seite ermöglichen diese Websites Personen mit mehr Fähigkeiten und Ressourcen, die Früchte ihrer Arbeit zu monetarisieren und ihre Angriffe oder andere bösartige Aktivitäten in Profit umzuwandeln.

Diese Websites gibt es in verschiedenen Sprachen, aber die russischsprachigen Gemeinschaften sind die wichtigsten. Die russischen Foren verfügen über die ausgefeiltesten Angebote und wirken oft professioneller. In englischsprachigen Foren tummeln sich nicht nur nordamerikanische und andere englischsprachige Kriminelle, sondern auch Nicht-Muttersprachler, einschließlich der ehemaligen britischen Kolonien. Andere sprachspezifische Foren dienen geografisch konzentrierten Communitys, etwa den Rumänisch sprechenden Menschen in Rumänien und Moldawien oder den Portugiesisch sprechenden Menschen in Brasilien, die beide zu bedeutenden Zentren der Internetkriminalität zählen. Es existieren auch Foren in anderen weitverbreiteten Sprachen wie Spanisch und Deutsch.

Diese Communitys versuchen, einen Kreis des Vertrauens zu schaffen, der es Kriminellen ermöglicht, Geschäfte miteinander zu machen. Das Risiko, dass ein Käufer oder Verkäufer andere Mitglieder abzockt, bleibt stets im Hinterkopf – ebenso wie die Gefahr, sich unwissentlich mit verdeckten Strafverfolgern oder Sicherheitsforschern einzulassen. Die User können potenzielle Verkäufer oder Käufer überprüfen, indem sie ihre Geschichte und ihren Status sowie die Rückmeldungen oder Bewertungen anderer Nutzer einsehen, um Vertrauen aufzubauen. Viele Gemeinschaften verwenden Treuhandsysteme, um das Vertrauen in große Käufe weiter zu stärken, indem sie den Administratoren der Website im Laufe der Transaktion Gelder anvertrauen. Das Risiko, negatives Feedback zu erhalten oder den Administratoren gemeldet zu werden, dient als zusätzliche Abschreckung. Diese „Qualitätskontrollen" ermöglichen es Forschern auch, die Quellen menschlicher Intelligenz (HUMINT), die sie von diesen Communitys sammeln (einschließlich der Daten für diese Broschüre), zu überprüfen, indem sie die Erfolgsbilanz der Nutzer untersuchen. Ein User mit vielen zufriedenen Kunden ist eine verlässlichere Quelle als ein neuer Nutzer, da er bereits einiges in den Aufbau seines Rufs investiert hat.

Warum verkaufen Kriminelle Netzwerkzugänge?

Die Mitglieder dieser Foren und dunklen Märkte sind oft auf bestimmte Bereiche der kriminellen Untergrundgeschäfte spezialisiert. Sie führen bestimmte Funktionen innerhalb dieses Ökosystems mit Geschicklichkeit oder Leichtigkeit aus. Diese Spezialisierung und Arbeitsteilung erhöht die Auswirkungen und die Kosteneffizienz von Attacken, indem verschiedene Angriffsphasen und die daraus resultierende Ausbeutung von Daten oder Zugang an diejenigen delegiert oder ausgelagert werden, die sie am besten durchführen können.

Tatsächlich verfügen nur wenige cyberkriminelle Organisationen über eine vollständige „vertikale Integration" oder erreichen eine komplette operative Autarkie. Stattdessen bleiben die meisten von Lieferanten von „Rohstoffen" für ihre Angriffe abhängig. Möglicherweise sind sie auch auf Kunden angewiesen, die es ihnen ermöglichen, gestohlene Informationen zu verkaufen oder ihre Arbeit auf andere Weise zu Geld zu machen.

Im bekannten Fall der kompromittierten Zahlungskartenverkäufe beispielsweise haben sich bestimmte Akteure auf diese Funktion spezialisiert. Sie betreiben Point-of-Sale-Malware (PoS) oder digitale Zahlungskarten-Skimmer, die Daten von PoS-Terminals beziehungsweise E-Commerce-Websites sammeln. Diese Leute verwerten kompromittierte Karten in der Regel nicht selbst, weil die schiere Datenmenge sie daran hindern würde, die Karten zu verwenden, solange sie noch „frisch" sind. Vielleicht sind sie auch weniger geschickt im Betrug als Kartenspezialisten. Deshalb kann es für sie kosteneffizienter sein, Karten an Dritte zu verkaufen, die sowohl die Zeit als auch die Fähigkeiten besitzen, sie optimal zu nutzen.

Eine ähnliche Logik liegt dem Verkauf von geknackten Netzwerkzugängen zugrunde. Angreifer, die sich auf erste Kompromittierungen spezialisiert haben, verfügen vielleicht nicht über die Fähigkeiten, die Zeit oder die Arbeitsmoral, ihren Zugang effektiv zum Geldverdienen auszunutzen. Dies gilt besonders für die Kompromittierung spezialisierter Umgebungen mit Betriebstechnologie (etwa industrielle Kontrollsysteme) oder anderen weniger verbreiteten oder weniger konventionellen Technologien, die viele Aggressoren nicht kennen.

So versteigerte der russischsprachige Benutzer „hardknocklife" im September 2020 einen RDP-Zugang zu einem US-Krankenhaus. Als Verkaufsargument führte er an, dass dieser RDP-Zugang zu Patientendaten führe, an denen er angeblich kein Interesse habe. US-Patientendaten von Gesundheitseinrichtungen gelten als wertvolle Ressource für Identitätsdiebe, da sie Geburtsdaten, Sozialversicherungsnummern und andere persönliche Daten enthalten, die sie für betrügerische Kreditanträge und andere Zwecke verwenden können. Der Verkäufer hätte diese Daten selbst nutzen und zu Geld machen können, zeigte aber kein Interesse daran, weil er vermutlich als Eindringling produktiver als als Betrüger sein konnte. Vielleicht fehlten ihm auch die Fähigkeiten zum Betrug. Der niedrige Preis von 500 US-Dollar, zu dem er seine Auktion startete, deutet darauf hin, dass er die Beute schnell loswerden wollte, aber sein Sofortkauf-Preis von 5.000 US-Dollar trug dem hohen Geldwert der Patientendaten Rechnung (siehe Abbildung 1).

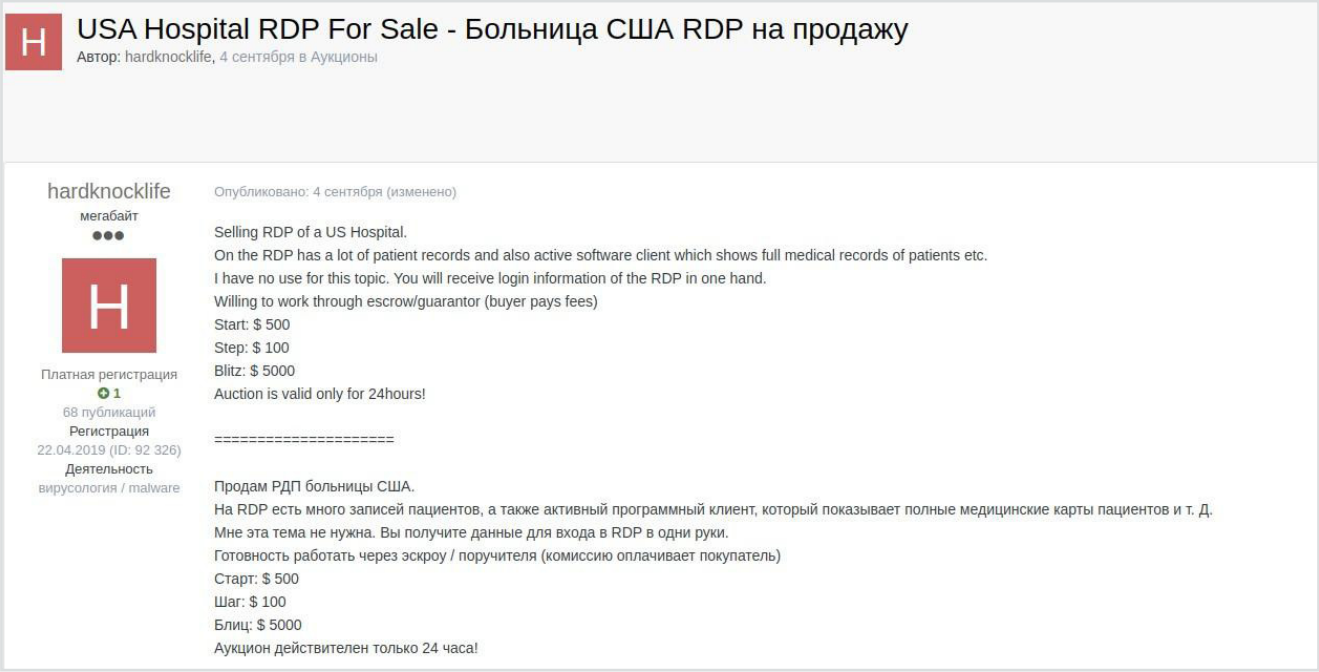


Abbildung 1

Ein weiterer Grund für Angreifer, den Zugang zu verkaufen, besteht darin, dass ihre Erkenntnisse darauf hinweisen, dass das Netzwerk nur wenige oder gar keine Daten mit einem finanziellen Wert enthält. In diesem Fall wäre es für Ransomware-Betreiber profitabler. Der Aggressor kann also den Netzwerkzugang an Ransomware-Betreiber verkaufen, die möglicherweise nicht über die Fähigkeiten verfügen, selbst in Netzwerke einzudringen. Der Handel mit kompromittierten Netzwerkzugängen bildet somit eine wichtige Voraussetzung für Ransomware-Angriffe. Solche Verkäufe an Ransomware-Betreiber ermöglichen es den ursprünglichen Eindringlingen auch, Gewinne aus Sicherheitsverletzungen zu erzielen, die andernfalls vielleicht verpufft wären und keinen Gewinn abgeworfen hätten.

Wie verkaufen Dealer ihren Netzwerkzugang?

Die gängige Art, den Verkauf eines kompromittierten Netzzugangs anzukündigen, besteht darin, einen Thread in der entsprechenden Rubrik eines kriminellen Untergrundforums zu eröffnen. Der Beitrag dort beschreibt in der Regel das Opfer, die Art und den Umfang des zu verkaufenden Zugangs sowie den Preis plus andere Transaktionsdetails.

In diesen Anzeigen werden die Opfer meist nicht namentlich genannt. Die Nutzer krimineller Foren und dunkler Märkte wissen, dass Sicherheitsforscher und Strafverfolgungsbehörden ihre Communitys überwachen. Darum nennen die Verkäufer häufig keine Namen in diesen Beiträgen, die oft von allen Usern eingesehen werden können, um die Aufdeckung ihrer Verstöße zu vermeiden. Die wenigen Dealer, die die Namen ihrer Opfer in öffentlichen Beiträgen preisgeben, sind in der Regel in englischsprachigen Foren zu finden, in denen sich manche Mitglieder weniger diskret als ihre russischen Kollegen verhalten. Es kann jedoch vorkommen, dass sie das Opfer im privaten Nachrichtenaustausch mit potenziellen Käufern, die sich nach einem Angebot erkundigen, beim Namen nennen. Einige Verkäufer zögern jedoch selbst in der privaten Kommunikation mit Interessenten, die Identität ihrer Opfer preiszugeben. Sie bieten lediglich Beweise für ihren Zugang an, die häufig in Form von Screenshots vorliegen.

Im Oktober 2020 erklärte beispielsweise der englischsprachige User „r41s3r" in einer Anzeige, warum er den Namen des Betroffenen nicht verrät. Er behauptete, dass frühere Veröffentlichungen von Namen dazu geführt hätten, dass er den Zugang zu ihren Netzwerken verloren habe, sodass er diesen Fehler nicht wiederholen werde. Möglicherweise beobachteten Sicherheitsforscher oder Behörden ältere Beiträge von ihm, in denen er einen Namen verriet. So konnten sie das Opfer vor dem unbefugten Zugriff warnen (Abbildung 2).

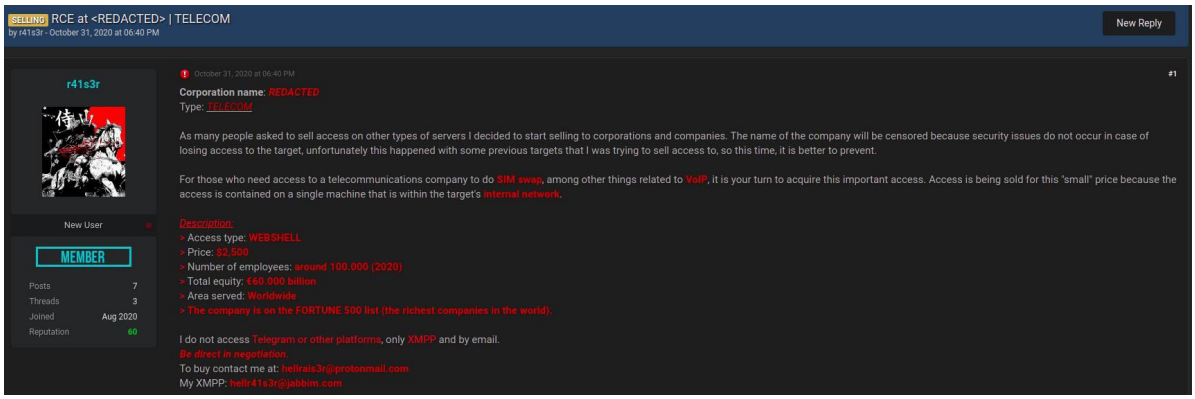


Abbildung 2

In diesen öffentlichen Anzeigen landen meist Standort, Branche und Umsatz oder Marktwert des Opfers. Häufig enthalten sie auch allgemeine Beschreibungen des kompromittierten Netzwerks, etwa die Anzahl und Art der darin befindlichen Computer und/oder die Art der darin enthaltenen Dateien und Daten. Falls der Verkäufer glaubt, dass sich das Netzwerk für eine Ransomware-Infektion eignet, schreibt er dieses Verkaufsargument in die Anzeige. Die Angabe von Umsatz- oder Marktwertzahlen ermöglicht es den Betreibern von Ransomware, die Höhe des Lösegelds einzuschätzen, das sie erpressen können. In der Annonce stehen in der Regel die Formen und Zugangspunkte zu dem kompromittierten Netzwerk, die der Käufer erhalten wird. Bei diesen Zugangspunkten handelt es sich häufig um Fernzugriffsdienste und -tools **wie RDP und VPNs**, häufig in Verbindung mit höheren Berechtigungen. Oft handelt es sich um Festpreise, aber einige Verkäufe finden auch in Form von Auktionen statt. Einige Käufer sind eher bereit, über den Preis zu verhandeln als andere – vor allem dann, wenn ein Angebot über einen längeren Zeitraum keinen Käufer findet. Typische Preise für den Verkauf eines kompromittierten Netzzugangs liegen im drei- bis fünfstelligen US-Dollar-Bereich, wobei auf den meisten Preisschildern ein vierstelliger Betrag steht.

Wie übertragen Kriminelle ihren Zugang an Käufer?

Anbieter von geknackten Netzwerkzugängen verwenden gern Anmeldeinformationen als Persistenzmechanismen, um ihren Zugang zu übertragen. Es ist unklar, ob und wann diese Persistenzmechanismen auch der ursprüngliche Zugangsvektor für die Kompromittierungen waren – oder ob und wann die Angreifer den ursprünglichen Zugang auf andere Weise erlangt und dann die separaten Persistenzmechanismen eingerichtet haben, die sie verkaufen.

Eine große Lücke in der Bedrohungsanalyse bildet der anfängliche Zugriffsvektor. In den Anzeigen tauchen die ersten Zugangsträger nicht auf, da Interessenten diese Details nicht kennen müssen. Dennoch sind einige der Persistenzmechanismen, die in diesen Angeboten stehen, häufig auch als Erstzugriffsvektoren so verbreitet, dass man davon ausgehen kann, dass sie auch die Erstzugriffsvektoren gewesen sein könnten. Darüber hinaus kann in einigen Fällen eine Überprüfung der älteren Beiträge eines bestimmten Nutzers dessen zuvor verwendete Taktiken und Verfahren offenbaren, die auf die ursprünglichen Zugangsvektoren hinweisen könnten. Wenn das Angebot eines bestimmten Users beispielsweise einen RDP-Zugang beinhaltet und er früher auch RDP-Brute-Force-Tools verkauft hat, deutet das drauf hin, dass er eines dieser Tools zur Kompromittierung des Netzwerks verwendet haben könnte.

RDP-Anmeldeinformationen kommen oft bei diesen Verkäufen vor. Bei RDP handelt es sich um einen gängiges Einfallstor, insbesondere für Brute-Force-Angriffe auf Netzwerke und oft in Verbindung mit Ransomware. Viele Firmen versäumen es, nicht genutzte RDP-Dienste zu deaktivieren, was Angreifern mehr Möglichkeiten eröffnet. Selbst wenn es einen geschäftlichen Grund gibt, den RDP-Zugang zu aktivieren, verschlafen es viele Unternehmen, die RDP-Anmeldeinformationen mit einer Zwei-Faktor-Authentifizierung (2FA) oder starken Passwörtern zu schützen, was sie anfällig für Brute-Force-Attacken macht. Die verstärkte Nutzung von RDP-Diensten aufgrund der Homeoffice-Zunahme in der Pandemie hat Angreifern zudem noch größere RDP-Angriffsflächen geboten.

Auch VPN-Zugangsdaten bilden durch die verstärkte Heimarbeit in der Coronakrise eine größere Angriffsfläche. Darüber hinaus machte die plötzliche und oft groß angelegte Umstellung auf Homeoffice im März 2020 viele Unternehmen und technisch weniger versierte Mitarbeiter anfälliger für Attacken aufgrund von Fehlkonfigurationen, ungepatchten Versionen von VPN-Software, fehlender 2FA für VPN-Zugangsdaten und Social-Engineering-Angriffen mit VPN-Themen. Schon vor der Pandemie und dem Aufkommen der Fernarbeit galten VPNs als begehrte Ziele, insbesondere im Zusammenspiel mit alten, anfälligen Versionen beliebter VPN-Software.

Einige Verkäufer verwenden Webshells für die Übertragung des Zugriffs. Webshells auf einem Webserver ermöglichen böswillige Aktivitäten gegen die öffentlich zugänglichen Dienste des Servers und bieten eine Basis für zusätzliche seitliche Bewegungen in die nicht öffentlich zugänglichen Segmente eines Unternehmensnetzwerks. Der Webserver-Zugang bringt besonders viel, wenn es um die Kompromittierung von Firmen geht, deren Profit in öffentlich zugänglichen Webdiensten für Kunden liegt, etwa beim Onlinebanking oder E-Commerce. Als weitere Zugriffsoptionen auf die Webinfrastruktur gelten WordPress-Anmeldeinformationen und Anmeldedaten für SQL-Datenbanken, oft in Verbindung mit Schwachstellen bei der Remote-Code-Ausführung.

Höhere Berechtigungen sind ein häufiges Merkmal dieser Verkäufe. Viele Arten von Malware benötigen größere Rechte. Höhere Privilegien ermöglichen es Angreifern zudem, eigene Konten zu erstellen oder andere Maßnahmen zu ergreifen, die als zusätzliche Persistenzmechanismen dienen können, um Redundanz für den gekauften Zugang zu schaffen. Domänenadministrator-Anmeldedaten zählen oft zu den Verkäufen in Verbindung mit Fernzugriff. Einige Formen des Fernzugriffs, die zum Verkauf stehen, können auch mit eigenen erhöhten Rechten einhergehen.

Anwendung des MITRE-ATT&CK-Frameworks

Das MITRE-ATT&CK-Framework macht die Arbeitsteilung bei einem Einbruch zwischen den ersten Eindringlingen und den Käufern, die diesen Zugang später ausnutzen, sichtbar. Die Angreifer führen die ersten zehn Phasen einer Attacke durch: Erkundung, Ressourcenentwicklung, Erstzugang, Ausführung, Persistenz, Privilegienerweiterung, Umgehung der Verteidigung, Zugriff auf Zugangsdaten, Entdeckung und seitliche Bewegung. Die Käufer konzentrieren sich auf die letzten vier Phasen: Sammlung, Befehl und Kontrolle, Datenexfiltration und Auswirkung (siehe Abbildung 3).

Die Anzeigen in den Foren geben in unterschiedlichem Maße Aufschluss über die Taktiken, die die Eindringlinge und die Käufer in jeder Angriffsphase anwenden. So verraten die Verkäufer meist nicht ihre Taktiken für den Erstzugriff, doch die Verwendung von gültigen Konten (T1078), externen Remote-Diensten (T1133) und Exploit Public-Facing Applications (T1190) gilt als üblich. Die Forenbeiträge eröffnen einen besseren Einblick in die Taktik der Eindringlinge, da sie in den Beiträgen oft angeben, welche Mechanismen sie an die Käufer weitergeben. Gültige Konten (T1078) bilden eindeutig die Hauptform der Persistenz, da sie häufig Anmeldedaten enthalten. Viele dieser Anmeldeinformationen sind für externe Remote-Dienste (T1133) wie RDP oder VPNs. Webshells (T1505) sorgen ebenfalls für Persistenz auf Webservern. Webserver können den Zugang zu einem breiteren internen Netzwerk ermöglichen, aber sie können auch selbst von Interesse sein, da sie Dienste für die Öffentlichkeit bereitstellen.

Privilegienausdehung gilt als weitere Schlüsselphase für Erstangreifer, da diese Angebote häufig Domänen-Administrator-Konten oder andere privilegierte Anmeldeinformationen enthalten. In diesen Forenbeiträgen taucht oft auch nicht die Privilegienerweiterungstaktik des Eindringlings auf, aber angesichts der Häufigkeit, mit der diese Angebote sehr privilegierte Konten enthalten, kann man davon ausgehen, dass Valid Accounts (T1078) dazugehören. Diese und frühere Verwendungen von Valid Accounts hängen zum großen Teil von Credential-Access-Taktiken ab. Auch diese Methoden werden in den Forenbeiträgen nicht offengelegt, doch die Häufigkeit, mit der diese Angebote RDP-Anmeldeinformationen beinhalten, lässt auf die Verwendung von Brute Force (T1110) schließen. Brute Force gilt als Lieblingstaktik von Kriminellen bei RDP-Anmeldeinformationen. Wir gehen davon aus, dass Eindringlinge zunächst interne Netzwerkerkundungen in diesen Netzwerken durchführen, bevor sie diese verkaufen. IntSights hat einen Zugangsanbieter identifiziert, der Details zur internen Netzwerkerkundung in sein Angebot integriert.

Sicherheitsforscher erhalten kaum Einblick in das, was Käufer mit dem erworbenen Zugang tun, da es für sie keinen Grund gibt, diese Infos preiszugeben. Die Häufigkeit, mit der Ransomware-Betreiber diese „Produkte" kaufen, lässt jedoch darauf schließen, dass Data Encrypted for Impact (T1486) zu den gängigsten Impact-Techniken zählt. Es sieht so aus, dass die Käufer sich auch mit dem Sammeln und der Extraktion gewinnbringender Daten aus Netzwerken befassen, aber diese Techniken können sich je nach Käufer unterscheiden. Ebenso können die Command-&-Control-Techniken unterschiedlich ausfallen – je nachdem, welche Ransomware die Käufer einsetzen.

Anwendung des MITRE-ATT&CK-Frameworks

Verkäufer				Käufer
Erster Zugang	**Persistenz**	**Privilegienausdehnung**	**Zugangsberechtigung**	**Wirkung**
Gültige Konten (T1078)	Gültige Konten (T1078)	Gültige Konten (T1078)	Brute Force (T1110)	Data Encrypted For Impact (T1486)
Externe Remote-Dienste (T1133)	Externe Remote-Dienste (T1133)			
Exploit Public-Facing Application (T1190)	Webshell (T1505.003)			

Abbildung 3

Quantitative und qualitative Analyse von Underground-Netzwerkzugangsverkäufen

IntSights führte eine quantitative und qualitative Analyse einer Stichprobe von 46 Verkäufen von Netzwerkzugängen in Untergrundforen durch, über die IntSights-Kunden zwischen September 2019 und Mai 2021 informiert wurden. Diese Analyse ergab die folgenden Beobachtungen über die Quellen und Preise dieser Kompromittierungen sowie die Verteilung von Opfern und Tätern nach Branche und Region.

Die Stichprobe umfasst 30 Angebote aus russischsprachigen Foren (65 %) und 16 Angebote aus englischsprachigen Foren (35 %). Diese Vorherrschaft von Offerten aus russischsprachigen Foren spiegelt die führende Position russischsprachiger Krimineller in der Untergrund-Cybercrime-Szene wider. Interessant finden wir, dass es keine einheitliche englische Terminologie für diese Geschäfte gibt, weder unter Kriminellen noch unter Sicherheitsforschern, obwohl einige Forscher den Begriff „Access Broker" zur Beschreibung dieser Verkäufer verwenden. Russischsprachige Dealer setzen jedoch häufig den Ausdruck „**продам достур**" („Ich werde Zugang verkaufen") ein. Diese Wendung taucht in den russischsprachigen Anzeigen immer wieder auf, entweder in der Titelzeile oder gleich am Anfang des ersten Beitrags (siehe Abbildung 4). Durch diese einheitlichere Terminologie und Kennzeichnung lassen sich diese Anzeigen leichter mit Schlüsselwörtern suchen oder beim Überfliegen erkennen.

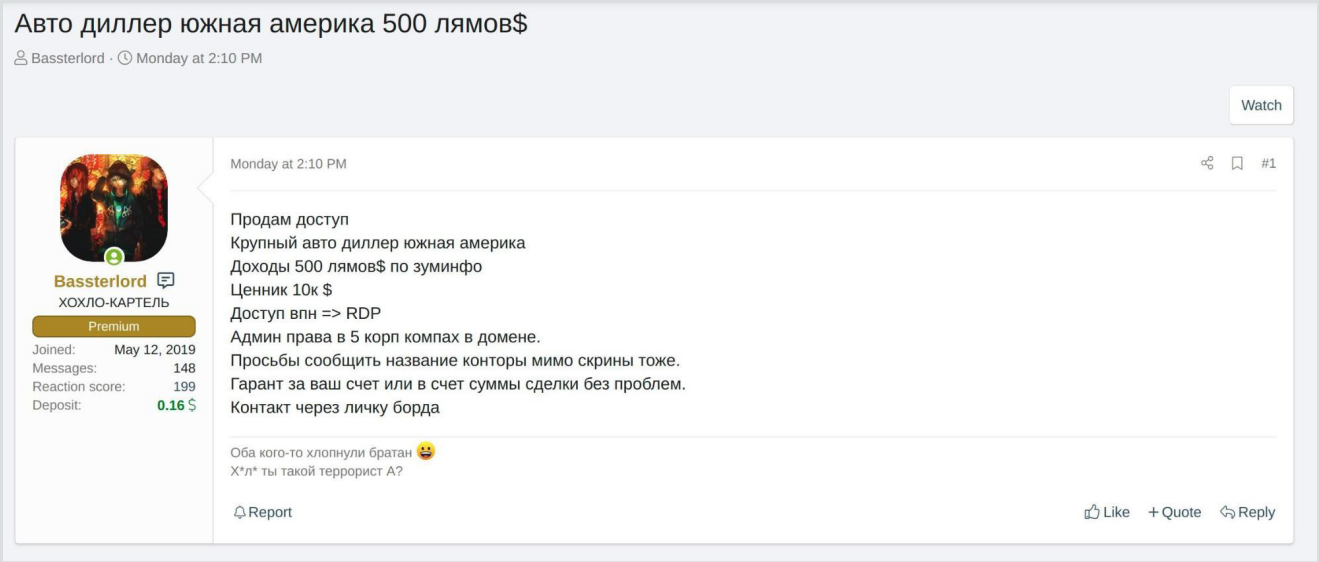


Abbildung 4

Anbieteranalyse

Ebenso deutlich zeigt sich die Dominanz einer Handvoll spezialisierter Zugangsanbieter. Nur sieben Personen waren die Quelle der meisten dieser Angebote (26 von 46 oder 56,5 %): Ihre Benutzernamen lauten „pshmm" (8), „drumrlu" (5), „7h0rf1nn" (4), „Cipher_Strike" (3), „iannker" (2), „Sheriff" (2) und „mont4na" (2). Diese Konzentration auf eine relativ kleine Anzahl spezialisierter Dealer verdeutlicht, in welchem Maße die Arbeitsteilung das Angebot an kompromittierten Netzwerken für diesen Nischenmarkt bestimmt.

Die beiden produktivsten Kriminellen verfeinern ihre Werbung stärker als ihre Konkurrenten. So erläuterte „pshmm", dass seine Standardangebote den Zugang zu Netzwerken über Fernüberwachungs- und Verwaltungssoftware (Remote Monitoring and Management, RMM) ermöglichen und nicht über die übliche Verwendung von RDP. Er stellte auch eine Liste der Funktionen zur Verfügung, die ein Käufer im Rahmen seiner Standardpakete erhält – einschließlich der Fähigkeit, Dateien zu übertragen, zu liefern und auszuführen, Befehle umzusetzen, Antivirensoftware und Firewalls zu deaktivieren und auf Active Directory und Registrierungen zuzugreifen (siehe Abbildung 5).

Der zweitaktivste Dealer („drumrlu") wählt ebenfalls ein Standardformat für seine Angebote, in diesem Fall für eine italienische E-Commerce-Firma (Abbildung 6). Die Pakete umfassen Domänenadministrator-Zugang, Zutritt zu Windows-NT-Directory-Services (für Active Directory) und vollständige Netzwerkaufklärung. Die Einbeziehung der Netzwerkerkundung fällt aus dem üblichen Rahmen, stößt aber auf Interesse. Denn diese Details erleichtern die Ausnutzung eines kompromittierten Netzwerks erheblich, indem sie den Käufer mit der Architektur und den Rechnern darin vertraut machen.

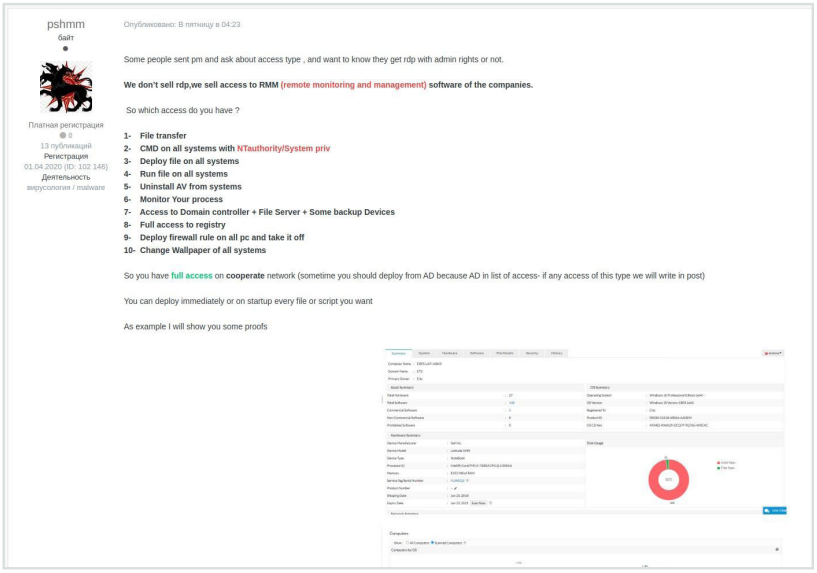


Abbildung 5

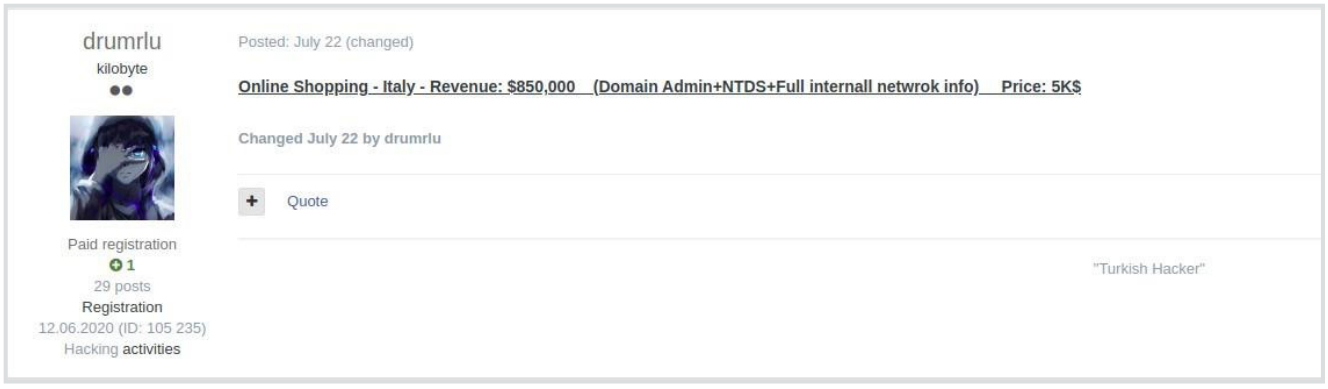


Abbildung 6

Opferregionen

Die geografische Konzentration der Opfer (Abbildung 7) entspricht den allgemeinen Trends bei kriminellen Aktivitäten im Untergrund. Fast alle (40 der 46 Angebote) in dieser Stichprobe gaben den Standort der Geschädigten an, während 15 dieser 40 Angebote (37,5 %) in Nordamerika (USA oder Kanada) lagen. Diese überproportionale Konzentration auf Nordamerika spiegelt die Vorliebe dieser Kriminellen für wohlhabende Volkswirtschaften und englischsprachige Opfer wider. Betroffene in reichen Ländern sind im Allgemeinen lukrativer, zudem sind englischsprachige Opfer oft leichter zu kompromittieren, da sie die dominierende Weltsprache Englisch sprechen.

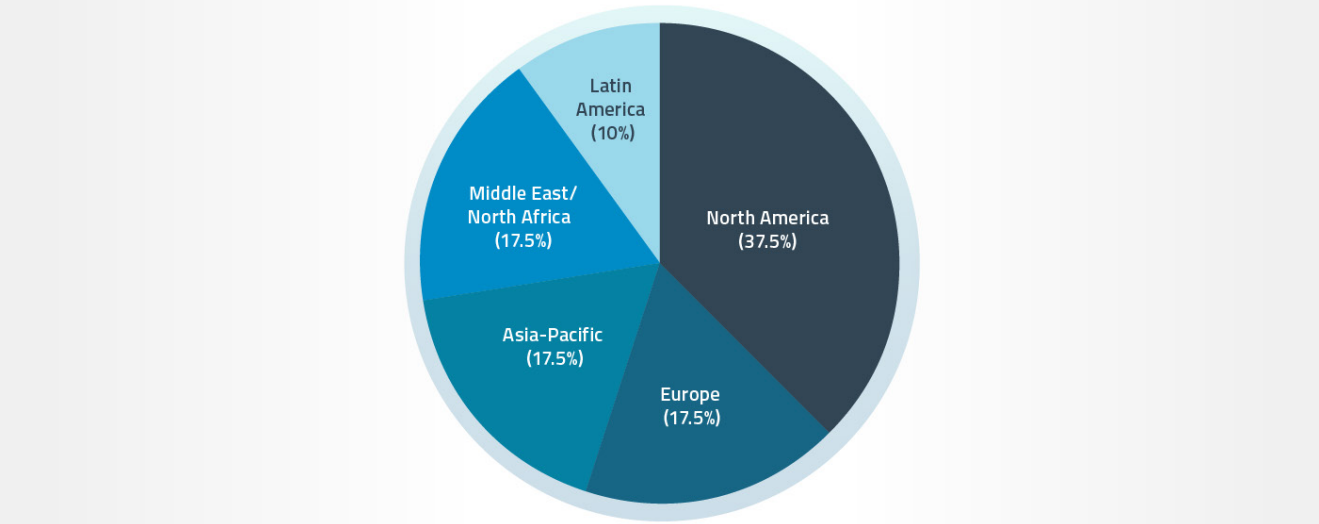


Abbildung 7

Abgesehen von der überproportionalen Betonung Nordamerikas existiert kein klarer geografischer Schwerpunkt. Es gab jeweils sieben Opfer (17,5 %) in Europa, im asiatisch-pazifischen Raum sowie im Nahen Osten und Nordafrika. Europäische Firmen zählen auch wegen des Wohlstands der europäischen Volkswirtschaften zu begehrten Opfern. Der asiatisch-pazifische Raum weist ebenfalls große und wohlhabende Volkswirtschaften auf, aber vier der sieben Geschädigten in dieser Region saßen in Indien. Indische Firmen sind aufgrund der weiten Verbreitung der englischen Sprache in Indien und der Auslagerung vieler westlicher Geschäftsvorgänge nach Indien ein begehrtes Ziel.

Auch der Nahe Osten zieht Gangster an, da Saudi-Arabien, die Vereinigten Arabischen Emirate und andere wohlhabende Monarchien über einen großen Reichtum an Kohlenwasserstoffen verfügen. Fünf der sieben Opfer befanden sich in diesen reichen Ländern, aber überraschenderweise war keines von ihnen ein Öl- oder Gasunternehmen. Die einzige Energiefirma war ein Stromversorger in Jordanien, also weder ein reicher Staat noch ein großer Energieproduzent. Bei den anderen sechs Geschädigten handelte es sich entweder um Unternehmen aus dem Gesundheitswesen oder aus dem Bereich Technologie/Telekommunikation. Mit einer Ausnahme befanden sich alle anderen Öl- und Gas- oder Energieopfer entweder in Nordamerika oder in Europa. „Gabrie1" versteigerte etwa den Zugang zu einem amerikanischen Öl- und Gasunternehmen (Abbildung 8). Die USA sind auch ein führender Öl- und Gasproduzent.

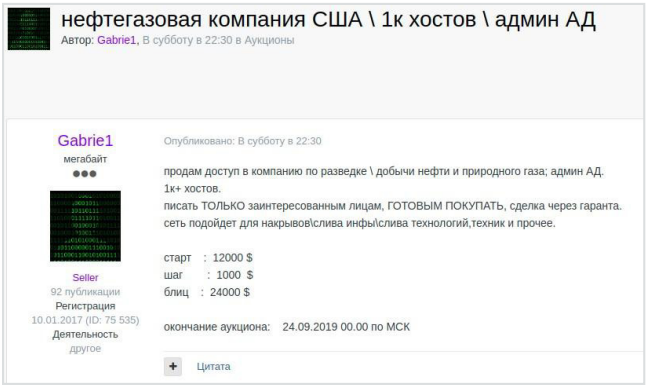


Abbildung 8

In unserer Stichprobe wies Lateinamerika mit nur vier zum Verkauf stehenden Netzzugängen die geringste Opferzahl auf. Dieses geringere Interesse an den Entwicklungsländern steht im Einklang mit den allgemeinen Trends in diesen Untergrund-Communitys. Dennoch hielt diese geringere Beachtung einige Zugangsanbieter nicht davon ab, hohe Preise für den Zutritt zu lateinamerikanischen Zielen zu verlangen. So wollte beispielsweise „annker" im Dezember 2020 umgerechnet etwa 27.000 US-Dollar in Bitcoin als Gegenleistung für eine Webshell mit Root-Rechten auf einer in Argentinien ansässigen Zahlungsplattform, die in elf Ländern tätig ist (siehe Abbildung 9). In diesem Fall scheint die potenziell lukrative Möglichkeit, ein Finanzdienstleistungsunternehmen zu kompromittieren, die wichtigste Rolle bei der Preisgestaltung gespielt zu haben – und nicht die geografische Lage.

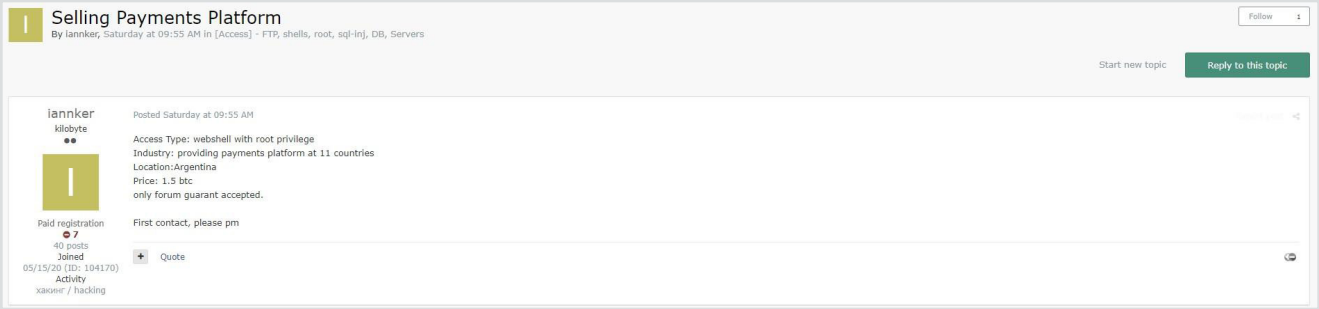


Abbildung 9

Branchenanalyse

Der Handel mit Netzzugängen erweist sich als branchenübergreifendes Phänomen. In der Stichprobe war der Technologie- und Telekommunikationszweig mit 10 der 46 Opfer (22 %) die am häufigsten betroffene Branche. Drei weitere lagen mit jeweils neun Opfern dicht beieinander: Finanzdienstleistungen, Gesundheitswesen/Pharmazeutik sowie Energie und Industrie (jeweils 19,5 %). Weitere betroffene Bereiche waren die Automobilindustrie, der Einzelhandel und das Gastgewerbe sowie freiberufliche Dienstleistungen (siehe Abbildung 10).

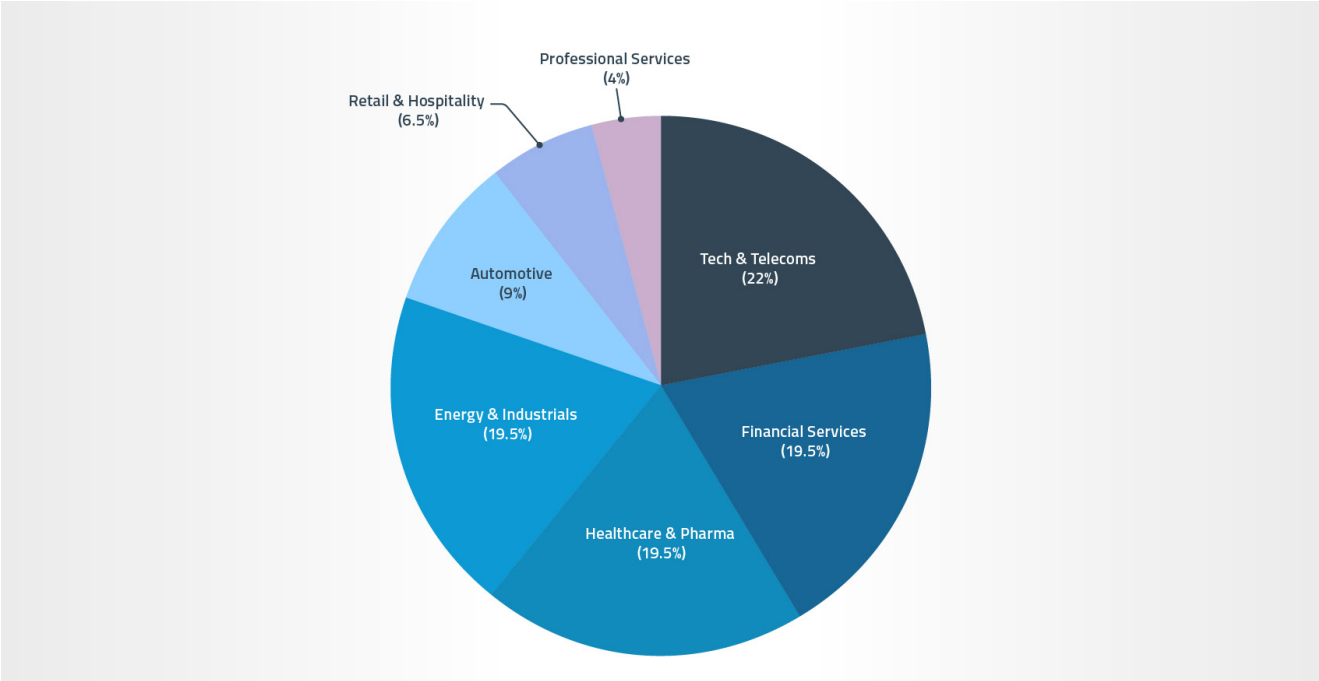


Abbildung 10

Der Anteil der Opfer aus dem Einzelhandel und dem Gastgewerbe fällt überraschend gering aus, wenn man bedenkt, wie beliebt dieser Geschäftszweig als Ziel krimineller Untergrundbanden ist. Ransomware-Betreiber gehören zu den Hauptkunden dieser Zugangsvermittler, aber eine Ransomware-Infektion ist möglicherweise nicht der optimale Weg, um den Zugang zu einem Einzelhandels- und Gaststättengeschäft zu monetarisieren. Der Einsatz von PoS-Malware auf physischen Zahlungsterminals oder von digitalen Zahlungskarten-Skimmern auf E-Commerce-Websites und Online-Zahlungsformularen könnte mehr Geld einbringen. Der Einsatz von Ransomware während des Einzugs von Zahlungskarten wäre kontraproduktiv, er würde den Fluss der Zahlungskartendaten unterbrechen und das Opfer auf die Anwesenheit eines Eindringlings aufmerksam machen.

Trotz der wenigen Geschädigten im Einzelhandel und Gastgewerbe betraf das zweitteuerste Angebot in dieser Stichprobe mit einer Bitcoin-Preisvorstellung im Wert von rund 66.000 US-Dollar den Zugang zu einer Organisation, die Hunderte von Einzelhandels- und Gastgewerbeunternehmen unterstützt. Bei dem Leidtragenden handelte es sich um einen Drittanbieter von Kundenbindungs- und Belohnungsprogrammen. Der Verkäufer wies auf die Möglichkeiten hin, wie dieser Zugang Geld abwerfen könnte: Quellcode-Überprüfung und -Manipulation, Zugriff auf die Konten und Punkte von Mitgliedern von Treueprogrammen sowie Spam- und Phishing-Angriffe, einschließlich Ransomware-Kampagnen gegen Mitglieder dieser Programme. Kundenbindungsmaßnahmen (etwa Vielfliegerprogramme von Fluggesellschaften) empfinden viele Verbrecher als attraktive Ziele.

Preisgestaltung

Die Preisgestaltung unterscheidet sich deutlich. Zu den Faktoren, die den Preis beeinflussen können, gehören der Umfang und die Zugriffsprivilegien, die Größe und der Wert des Opfers als Quelle krimineller Einkünfte, die Branche und der Standort des Opfers sowie die Verkaufsstrategien der verschiedenen Verkäufer. Sechs der 46 Angebote trugen kein Preisschild, sodass die Interessenten ihre eigenen Angebote machen konnten. Weitere sechs dieser Deals erfolgten in Form von Auktionen; für diese statistische Analyse verwendete IntSights einen Durchschnitt aus dem Eröffnungsgebot und dem „Sofort kaufen"-Preis und behandelte diesen Durchschnitt wie einen Festpreis.

Der Durchschnittspreis für diese 40 Deals betrug etwa 9.640 US-Dollar, der Medianpreis lag bei 3.000 Dollar. Die große Diskrepanz zwischen Durchschnitts- und Medianpreis ist zu einem großen Teil auf einige ungewöhnlich hohe Preise bei den teuersten Angeboten zurückzuführen. IntSights-Forscher sehen den Durchschnittspreis von 3.000 Dollar als repräsentativeres Beispiel für die typischen Offerten. Tatsächlich waren 3.000 Dollar nicht nur der Medianpreis, sondern auch der gängigste Einzelpreis: Fünf der 40 Angebote (12,5 %) mit einem Preisschild entsprachen genau diesem Betrag. IntSights-Forscher sehen den Durchschnittspreis von 9.640 Dollar als besseren Indikator für das obere Ende der Preisspanne. In aufsteigender Reihenfolge geordnet, erreichte oder übertraf die Liste dieser 40 Preise nur den Durchschnitt von 9.640 Dollar im obersten Viertel oder unter den zehn höchsten Preisen dieser 40. Dieses obere Ende begann bei exakt 10.000 Dollar. Im untersten Viertel (die zehn niedrigsten Preise unter diesen 40 Angeboten) lagen alle außer dem höchsten lediglich im dreistelligen Bereich.

Diese Zahlen bestätigen die folgenden Beobachtungen der IntSights-Forscher: Der größte Teil dieser Offerten bewegt sich im vierstelligen US-Dollar-Bereich, die teureren Angebote stoßen in fünfstellige Regionen vor, während die billigsten Offerten dreistellige Preise in US-Dollar aufweisen.

Eine Untersuchung der höheren und niedrigeren Preise beleuchtet die Faktoren, welche die Preise beeinflussen. Der niedrigste Preis von 240 Dollar galt dem Zugang zu einer Gesundheitseinrichtung in Kolumbien. Gangster bevorzugen Opfer in reichen Ländern, da diese lukrativer sind. Die Preise für das Gesundheitswesen fallen auch deshalb niedriger aus, weil man glaubt, dass sie leichter zu kompromittieren sind, was durchaus stimmen kann. Zudem besteht ein

Gleichgewicht oder Ungleichgewicht zwischen Angebot und Nachfrage. Gesundheitseinrichtungen waren die Opfer von neun der 46 Angebote (19,5 %). Die Preise im Gesundheitssektor mit einem Durchschnitt von 4.860 Dollar und einem Medianpreis von 700 Dollar fallen in dieser Stichprobe auch deutlich niedriger als in anderen Branchen aus. Organisationen des Gesundheitswesens gelten seit Langem als beliebtes Ziel von Ransomware-Betreibern. Die geringeren Zugangskosten zu Betrieben des Gesundheitswesens haben sie wahrscheinlich zu einem noch begehrteren Ziel für Ransomware-Betreiber gemacht, die von diesen Verkäufern abhängig sind.

Eine Annonce des Nutzers „TrueFighter" vom Juli 2020 lässt sich als Lehrbuchbeispiel für den Verkauf von Netzzugängen anführen. Der Beitrag weist sowohl im Titel als auch zu Beginn des Textes die russische Botschaft „Ich werde Zugang verkaufen" auf. Bei dem ungenannten Opfer handelte es sich um ein regionales Krankenhausnetz in den USA mit einem Umsatz von 60 Millionen US-Dollar. Krankenhäuser gelten als beliebte Ziele für Ransomware-Angriffe. Der Verkäufer bot eine Kombination aus RDP-Zugang und Domänenadministrator-Anmeldedaten für 3.000 US-Dollar an. RDP ist eine gängige Form des Fernzugriffs bei diesen Verkäufen, und die Domänenadministrator-Anmeldedaten räumen den Käufern hohe Privilegien ein, mit denen sie Ransomware-Nutzdaten ausführen oder andere bösartige Ziele erreichen können. Besonders gründliche Kriminelle würden vermutlich auch Patientendaten klauen, bevor sie Ransomware einsetzen, da Patientendaten vor allem für Identitätsdiebe wertvoll sind. Der Wert von 3.000 US-Dollar für dieses Angebot ist der Medianpreis für diese Stichprobe (siehe Abbildung 11).

Der zweitniedrigste Preis (300 Dollar) wurde für den Zugang zu einem Automobilhersteller in Indien gezahlt. Wie im Beispiel weiter oben drückt ein Standort in einem Entwicklungsland oft den Preis nach unten. Das Angebot umfasst nur lokale Verwaltungsrechte innerhalb der Domäne und keine Domänencontroller-Rechte, was viele Akteure bevorzugen. Das Netzwerk hat eine relativ kleine Anzahl von Hosts. Die Vielfalt der Möglichkeiten, den Zugang zu Industrie- oder Produktionsfirmen zu Geld zu machen, ist für Kriminelle weniger offensichtlich als bei Zielen in den Bereichen Finanzdienstleistungen, Einzelhandel, Gastgewerbe und Gesundheitswesen. Ransomware wäre eine logische Wahl, besonders nach dem Vorfall mit der Colonial Pipeline im Mai 2021, aber die Monetarisierung von geistigem Eigentum oder Kundendaten dieser Firmen ist für viele Kriminelle nicht so klar ersichtlich (siehe Abbildung 12). Einen Überblick über die Bedrohungen für Industriefirmen finden Sie im **IntSights-Bericht zur Bedrohungslage im Energie-, Versorgungs- und Industriebereich.**

Abbildung 11

Abbildung 12

Ein weiteres günstiges Angebote (700 Dollar) betrifft ebenfalls ein Produktionsunternehmen: Eine in Texas ansässige Firma, die sich auf den Bau und die Reparatur von oberirdischen Lagertanks für Öl- und Gas-, Energie-, Chemie- sowie Agrarunternehmen spezialisiert hat. Dieses Angebot kostet etwas mehr als das des oben genannten Autoherstellers, da die Firma in den USA sitzt, eine größere Anzahl von Hosts im Netzwerk hat und höhere

Domänencontroller-Privilegien aufweist. Dennoch ist das Unternehmen möglicherweise ein weniger begehrtes Ziel und erzielt deshalb aufgrund der Art seines Geschäfts einen niedrigeren Preis. Viele Verbrecher interessieren sich nur für Ransomware (siehe Abbildung 13) beim Geldverdienen.

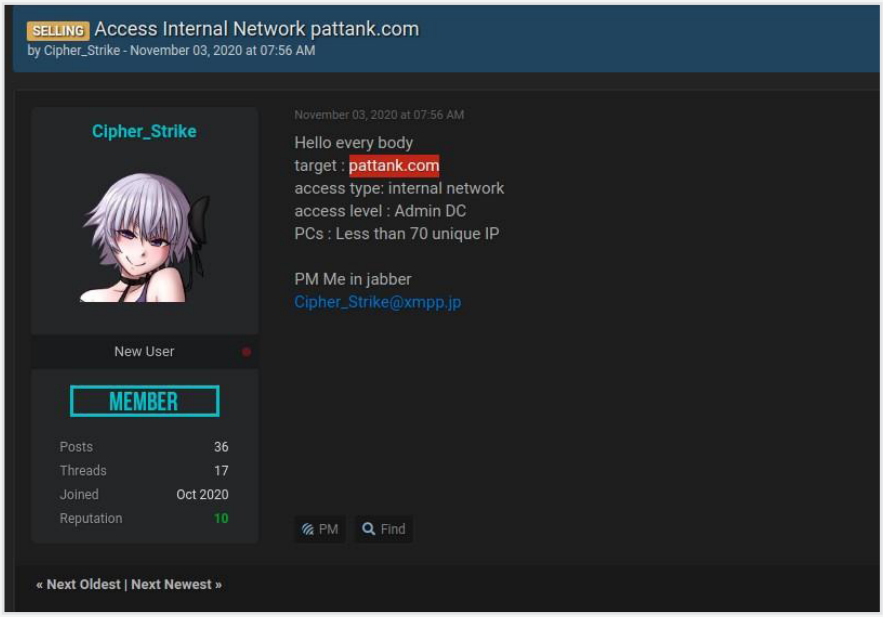


Abbildung 13

Am anderen Ende der Preisskala sticht die Technologie- und Telekommunikationsbranche als beliebtestes Ziel heraus. Von den zehn teuersten Angeboten in dieser Stichprobe betrafen vier Telekommunikations- oder Technologieunternehmen. Zudem gab es in dieser Stichprobe nur zwei Angebote aus dem Bereich Technologie und Telekommunikation, deren Preise unter 10.000 Dollar lagen, was unserer Grenze für höhere Preisregionen entspricht. Die mit Abstand teuerste Offerte in dieser Stichprobe mit einem Preis von Bitcoin im Wert von circa 95.000 US-Dollar (zu den damals gültigen Wechselkursen) galt einem Telekommunikationsdienstleister. Der Verkäufer beschrieb ihn als den größten Anbieter von Mobilfunkdiensten in einem nicht näher bezeichneten asiatischen Land mit einem Umsatz von über einer Milliarde US-Dollar (siehe Abbildung 14).

IntSights-Forscher glauben, dass sowohl der hohe Wert als auch die große Zahl von Technologie- und Telekommunikationsunternehmen als Opfer von Einbrüchen auf deren Nützlichkeit für weitere Angriffe auf andere Ziele zurückzuführen ist. Wie IntSights in seinem **Bericht über die Cyber-Bedrohungslandschaft in der Telekommunikationsbranche** hervorhebt, versuchen Kriminelle beispielsweise, Zugang zu Mobilfunkanbietern zu erhalten, um SIM-Swapping-Angriffe auf Online-Banking-Kunden durchzuführen, die eine Zwei-Faktor-Authentifizierung (2FA) per SMS verwenden. Ihr Ziel ist es, diese Telefonnummern auf SIM-Karten umzuleiten, die sie kontrollieren, um 2FA-Codes für ihre Online-Banking-Anmeldedaten zu erhalten und so diese Konten zu kompromittieren. Viele Cybergangster führen diese

Abbildung 14

Attacken über Netzwerke von Insidern durch, die für ihre Dienste in kriminellen Foren Werbung machen. Einige dieser Verbrecher verlangen zwischen 200 und 400 US-Dollar pro Telefonnummer, was sehr teuer ist. Der Kauf des Zugangs zu einem Mobilfunkanbieter mag zwar erst etwas kostspielig erscheinen, könnte aber langfristig Geld sparen.

Ebenso kann der unbefugte Zugang zu Technologieunternehmen Angriffe auf die Lieferkette der Kunden dieser Firmen ermöglichen, wie IntSights in seinem **Bericht zur Cyber-Bedrohungslandschaft der Technologiebranche 2021** betont. Aggressoren können Software-Updates kompromittieren oder den Quellcode verändern, um den Software-Nutzern bösartigen Code unterzujubeln. Auch ohne den Quellcode zu verändern, können ihn Gangster auf unbekannte Schwachstellen untersuchen, die sie dann ausnutzen. Code-Signatur-Zertifikate von Technologiefirmen sind wertvolle Zusätze zu Malware-Nutzdaten, die die Chancen erhöhen, einer Entdeckung zu entgehen.

Die einzige andere Branche mit mehr als einem Vertreter unter den zehn teuersten Angeboten in dieser Stichprobe ist die Finanzdienstleistungsbranche. Banken und andere Finanzdienstleistungsunternehmen bilden ein Topziel für Cyberkriminelle, da sie zu den direkt anzapfbaren Geldquellen für sie zählen, wie IntSights in seinem **Cyber Threat Landscape Report 2021 für die Banken- und Finanzdienstleistungsbranche** feststellt.

Deshalb zählen Banken auch zu den kniffligsten Zielen, da sie oft über umfangreiche Sicherheitsmaßnahmen verfügen. In der Tat scheinen die Finanzdienstleistungsangebote in dieser Stichprobe die Verbrecher vor größere Schwierigkeiten zu stellen. Keine einzige Annonce erwähnte einen Domänenadministrator oder andere Anmeldeinformationen mit ähnlich hohen Privilegien in einem Netzwerk. In vielen Fällen bleibt unklar, ob oder inwieweit der zum Verkauf stehende unbefugte Zugang über die öffentlich zugängliche Webserver-Infrastruktur hinausgeht. Die Persistenzmechanismen für die Finanzdienstleistungsangebote umfassen eine unverhältnismäßig hohe Anzahl von Webshells und WordPress-Anmeldeinformationen. Die Webshells verfügen häufig über Root-Rechte und die WordPress-Zugangsdaten oft über administrative Rechte, doch es wird nicht klar, ob und bis zu welchem Grad sie einen seitlichen Zugriff auf die Backend-Infrastruktur ermöglichen. Nur ein Verkäufer („7h0rf1nn") gab an, dass solche Querbewegungen zusätzliche Kosten verursachen (Abbildung 15). Die Preise für diesen eingeschränkten Zugang zu Banken sind viel höher als bei Angeboten mit ähnlich eingeschränktem Zugriff zu anderen Branchen.

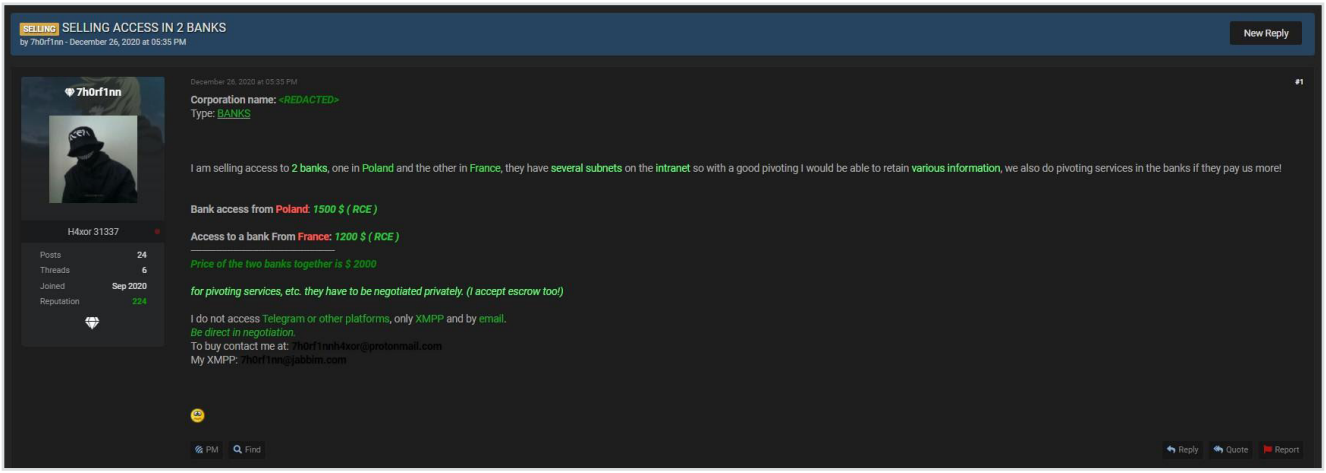


Abbildung 15

So verlangte der User „iannker" im Oktober 2020 einen Preis von 10.000 Dollar für eine Webshell mit Root-Rechten bei einer US-amerikanischen Onlinebank. Es blieb unklar, ob das Angebot auch das Eindringen in das interne Netzwerk der Bank oder nur den Zugriff auf öffentliche Webserver umfasst. Ein solcher Webserver-Zugang könnte Betrug oder andere böswillige Handlungen gegen die Kunden dieser Bank ermöglichen, was diesen Zugang auch ohne seitliche Bewegung über das Netzwerk zu einer lukrativen Investition machen würde (siehe Abbildung 16).

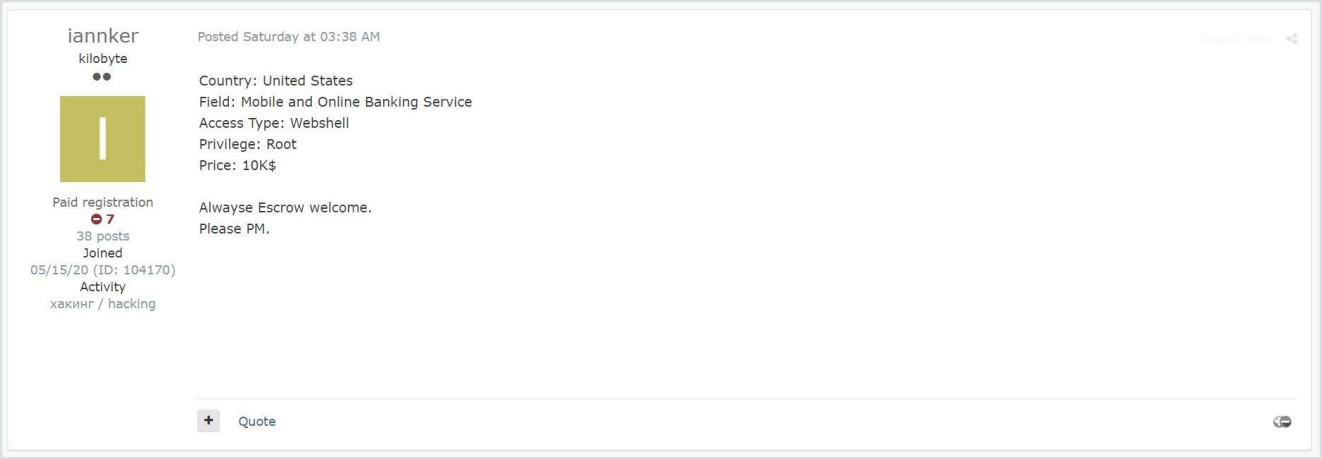


Abbildung 16

Die Daten dieser Annoncen stimmen mit den Beobachtungen von Sicherheitsforschern überein, wonach die COVID-19-Pandemie mit ihren zahlreichen Homeoffice-Arbeitskräften zum Anstieg dieser Verkäufe beigetragen hat. Die plötzliche und weitverbreitete Einführung von Fernzugriffsdiensten wie RDP und VPN war eine wichtige Voraussetzung für Sicherheitsverletzungen – auch für solche, die Angreifer an andere Kriminelle verkauften. Im Juli 2020 kam es zu einem dramatischen Anstieg dieser Angebote, nachdem sich die Schließungen und die Verlagerung der Arbeit auf Fernzugriffsdienste längerfristig auf Firmen ausgewirkt hatten. Die Gangster brauchten zudem selbst ein bisschen Zeit, um sich auf die neue Situation einzustellen. Im Oktober, November und Dezember 2020, als in den USA und Europa weitere Infektionswellen auftraten, gab es einen stetigen Strom an neuen Offerten.

Wie können wir Infos nutzen, um Kompromittierungen zu erkennen und auf sie zu reagieren?

Diese Verkäufe ebnen den Weg für skrupellose Bedrohungen, aber sie bieten Sicherheitsexperten auch die Möglichkeit, Attacken zu erkennen und zu vereiteln. Die Arten von Zugangsdaten und Persistenzmechanismen, die von diesen Verkäufern am häufigsten weitergegeben werden, zählen für Sicherheitsteams zu den vorrangigen Zielen. Beispielsweise könnten Audits oder andere Überprüfungen dieser Anmeldeinformationen und Persistenzmechanismen für Bedrohungsjäger nützlich sein. Umgekehrt sollten Firmen, die in diesen Foren Meldungen über den Verkauf von unbefugtem Zugang zu ihren Netzwerken erhalten, zunächst damit beginnen, die Protokolle auf die Arten von Anmeldeinformationen und Persistenzmechanismen zu überprüfen, die in der Verkaufsanzeige stehen.

Andere Infos aus diesen Annoncen sollten auch den Eingreifgruppen für Zwischenfälle zur Verfügung stehen. Viele Reaktionsteams und Sicherheitsexperten gehen davon aus, dass in allen Phasen eines Einbruchs – vom ersten Zugriff bis zum Datendiebstahl – Kontinuität herrscht. Allein die Existenz dieser Deals in kriminellen Foren zeigt, dass diese Annahme oft nicht stimmt und zu falschen Schlussfolgerungen verleiten kann. Die Tools und Taktiken der Ersteindringlinge können sich erheblich von denen der späteren Käufer unterscheiden, die diesen Zugang ausnutzen. Veränderungen oder Diskontinuitäten bei den Kompromittierungsindikatoren (IOCs) und den Taktiken, Techniken und Verfahren (TTPs) können diese Übertragungen des Zugangs widerspiegeln und daraus resultieren. Untersuchungen deuten darauf hin, dass die Ersteindringlinge IP-Adressen verwendeten, die zu einem bestimmten Internetdienstanbieter oder geografischen Gebiet führten. Das Verschwinden dieser IOCs aus den Netzwerkprotokollen könnte zu der falschen Schlussfolgerung verleiten, dass die Attacke beendet ist, obwohl sie in Wirklichkeit nur den Besitzer gewechselt hat, der eine andere Infrastruktur verwendet.

Der für den Verkauf des Netzwerkzugangs nötige Zeitraum kann der Security mehr Zeit verschaffen, eine Sicherheitsverletzung zu entdecken, bevor ein Käufer sie zu Geld oder etwas anderes damit macht. Die Zeit zum Finden eines Käufers variiert beträchtlich und reicht von Stunden bis zu Monaten. Meist dauert es Tage oder Wochen. Wenn Sicherheitsteams einen Eindringling entdecken, der schon länger Zugang hat, aber noch nicht damit begonnen hat, ihn zu Geld zu machen (etwa durch Abzug profitabler Dateien oder Einsatz von Ransomware), dann könnte diese Verzögerung darauf hindeuten, dass der ursprüngliche Eindringling noch einen Interessenten sucht.

Sicherheitsexperten können die Opfer dieser Verkäufe oft identifizieren, indem sie sich als potenzielle Käufer ausgeben, um ihnen weitere Informationen zu entlocken. Verkäufer geben in ihren öffentlichen Anzeigen in der Regel keine Namen von Opfern an, aber sie verraten Interessenten, die sie für glaub- und vertrauenswürdig halten, manchmal die Namen der Geschädigten. Selbst wenn ein Dealer keine Namen nennen will, kann er bereit sein, Screenshots oder andere Details weiterzugeben, die eine Identifizierung des Unternehmens ermöglichen.

Empfehlungen

Vorbeugung

Die Einhaltung der folgenden Best-Practice-Checkliste kann Netzwerk-Kompromittierungen verhindern, die zu Zugangsverkäufen im kriminellen Untergrund führen:

- Einsatz starker, eindeutiger und sich häufig ändernder Passwörter.
- Verwendung von 2FA, insbesondere für RDP, VPNs und andere Fernzugriffsdienste.
- Mobile Authentifizierungs-Apps für die 2FA und keine SMS.
- Ratenbegrenzung zur Abwehr von Brute-Force-Angriffen, insbesondere bei RDP.
- Anmeldedaten-Überwachung auf E-Mail-Adressen aus der Domäne Ihres Unternehmens.
- Aktualisieren Sie die VPN-Software, um die neuesten Sicherheits-Patches zu erhalten.
- Deaktivieren Sie Fernzugriffsdienste, die Mitarbeiter nicht mehr benötigen, wenn sie ins Büro zurückkehren.
- Fordern Sie Heimarbeiter auf, ihre Passwörter zu ändern und die Firmware ihrer Router zu aktualisieren.
- Statten Sie Geräte mit Endpunkt- und Netzwerksicherheitsüberwachung für Mitarbeiter aus, die langfristig an einem anderen Ort arbeiten. Sorgen Sie dafür, dass sie regelmäßig Sicherheitsupdates erhalten.
- Richten Sie ein System mit häufigen, segmentierten und redundanten Back-ups ein, um verschlüsselte Dateien im Falle einer Ransomware-Infektion wiederherstellen zu können.

Schadensbegrenzung

Hier finden Sie Methoden zur Schadensbegrenzung, falls Sie feststellen, dass Ihr Zugang zum Verkauf steht:

- Falls Sie bemerken, dass Ihr Netzwerkzugang in einem kriminellen Forum gelandet ist, nehmen Sie Kontakt mit dem Sicherheitsforscher auf, der die Meldung gemacht hat. Dieser ist möglicherweise in der Lage, dem Verkäufer Details über die Sicherheitsverletzung zu entlocken, indem er sich als potenzieller Käufer ausgibt.
- Wenn die Annonce für den Zugriff auf Ihr Netzwerk den Persistenzmechanismus oder privilegierte Konten angibt, dann führen Sie eine Prüfung dieser Konten auf verdächtige Aktivitäten durch.
- Lassen Sie sich von einem Anwalt beraten, bevor Sie die Möglichkeit in Betracht ziehen, den unbefugten Zugang zum Netzwerk Ihres Unternehmens zurückzukaufen, da dies rechtliche Folgen haben kann.
- Im Falle einer Ransomware-Infektion sollte das Sicherheitsteam das gesamte Ausmaß der Verletzung ermitteln, die in der Verschlüsselung von Dateien gipfelt. Ransomware-Betreiber führen oft vor der Verschlüsselung von Dateien andere Aktivitäten durch, etwa den Diebstahl gewinnbringender Daten.
- Zahlen Sie kein Lösegeld. Viele Lösegeldzahlungen führen aufgrund von technischen Fehlern oder betrügerischen Ransomware-Betreibern nicht zur Wiederherstellung der Dateien. Zahlungen ermutigen zu weiteren Erpressungsversuchen und verschaffen Kriminellen mehr Ressourcen für zukünftige Attacken.

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**.