Darknet als Shopping-Mall: So machen Cyberkriminelle richtig Kasse - Komplette Hackerangriffe günstiger als ein Kurzurlaub

Drogen, Waffen, Schwerstkriminalität: Das Darknet gilt zurecht als internationaler Umschlagsplatz illegaler Aktivitäten. Auch Hacker und Cyberkriminelle nutzen den digitalen Schwarzmarkt immer stärker als Kauf- und Verkaufsplattform. Zu diesem Ergebnis kommt der Security-Hersteller ESET, der das Darknet nach aktuellen Trends durchforstet hat "Malware an sich ist schon ein lukratives Geschäft", sagt Thomas Uhlemann, Sicherheitsspezialist bei ESET. "Aber jetzt kassieren Kriminelle gleicht doppelt, indem sie nach ihren Attacken die erfolgreichen Werkzeuge auch noch verkaufen oder vermieten." Selbst ungeübte Gangster sind damit in der Lage, gefährliche Angriffe durchzuführen.

Malware mit Full-Service-Dienstleistungen

Der Verkauf von Schadcode aller Art ist nicht Neues im Darknet. Mit kompletten Full-Service-Dienstleistungen von der Malware-Verbreitung über illegale Vermietung von Infrastruktur bis hin zur Finanzabwicklung bleibt neuerdings kein Hackerwunsch unerfüllt. Letztlich muss der "Kunde" nur noch entscheiden, welchen Service-Level er sich leisten kann. Selbst für den schmalen Geldbeutel gibt es genug Möglichkeiten, als Kleinstkrimineller in den Markt einzusteigen. "Die Zeiten sind endgültig vorbei, wo Teenagerstreiche das Internet bedrohten. Cyberkriminalität ist ein bestens organisiertes Geschäft - mit Service, Marketing, Werbung und detaillierten Bedienungsanleitungen agieren viele Banden professioneller als so manches legales Unternehmen", sagt Uhlemann. Dahinter stehen internationale mafiöse Grossbanden, die den Äœbergang von der analogen Welt in das Darknet erfolgreich vollzogen haben.

Ransomware dient dafür als ideales Beispiel. Eine breite Palette von Erpressersoftware-Paketen ist im Darknet erhältlich, als ob es sich um den Verkauf von legaler Software handeln würde. Updates, technischer Support, Zugriff auf Command&Control-Server und eine Reihe von Zahlungsoptionen sind nur einige der angebotenen Features. Vom simplen Einmalkauf bis hin zum Abonnement ist alles möglich. So bietet beispielsweise "Ranion" Bezugs-Pläne zu unterschiedlichen Preisen und Laufzeiten an. Sie beginnen bei 120 US-Dollar für nur einen Monat und enden im Jahres-Abo für 900 US-Dollar pro Jahr - das Luxuspaket kostet 1.900 US-Dollar.

Infrastruktur-as-a-Service: Mieten statt kaufen

Für die Malware-Verbreitung benötigen Kriminelle zwangsläufig Server, um das Business ins Rollen zu bringen. Selbstverständlich kann man sich diese auch mieten - bei Verbrechern, die den rechtmässgen Eigentümer sicher nicht um Erlaubnis gefragt haben. Es existieren verschiedene Dienste im Darknet, die Anmeldeinformationen auf Server in allen Teilen der Welt über das Remote Desktop Protocol (RDP) liefern. Die Preise liegen im moderaten Bereich von 8-15 US-Dollar pro Gerät. Bedienerfreundlich lassen sich die angebotenen Server nach Land, Betriebssystem und sogar nach Zahlungsseiten filtern, auf die Benutzer von diesem Grossrechner aus zugegriffen haben. Dem Versand von Ransomware oder Malware wie Bankingtrojaner und Spyware steht dann nichts mehr im Wege.

Ebenfalls im Angebot sind Denial-of-Service-Angriffe. Bei ihnen variiert der Preis: je nachdem, wie lange der Angriff dauern soll (zwischen ein und 24 Stunden) und wie viel Datenverkehr das Botnetz während dieser Zeit erzeugen kann. Eine dreistündige Attacke ist bei manchen Anbietern für 60 US-Dollar erhältlich.

Oldie but Goldie: Verkauf von PayPal- und Kreditkartenkonten

Cyberkriminelle, die bereits erfolgreiche Phishing-Angriffe durchführten, gehen in der Regel nicht das Risiko ein, die gestohlenen Konten selbst zu nutzen. Es ist profitabel genug und viel sicherer für sie, die Konten an andere weiterzuverkaufen. Für diesen Service berechnen sie in der Regel etwa 10 Prozent des gesamten verfügbaren Guthabens auf dem gestohlenen Konto. Einige Verkäufer zeigen obendrein gerne die Tools und gefälschten Websites, mit denen sie ihre Phishing-Aktivitäten betreiben.

"Durch die weitgehende Anonymisierung und Bezahlung per Bitcoin haben es Strafverfolgungsbehörden schwer, Cyberkriminelle festzusetzen", bilanziert Thomas Uhlemann. "Das heisst im Klartext: Wegen der neuen Möglichkeiten rechnen wir mit immer mehr Digital-Gangstern und noch mehr Angriffen. Denn der Anreiz, Porsche zu fahren ohne arbeiten zu müssen und quasi kaum erwischt zu werden, lockt sie geradezu an."