Thema: **Gauner-Marktplatz Darknet – So übel ist die dunkle Seite des World Wide Web tatsächlich**

Beitrag: 2:18 Minuten

Anmoderationsvorschlag: Phishing, Bot-Angriffe, Datenklau: Dass das Internet praktisch unendliche Möglichkeiten für Cyberkriminelle bietet, weiß man ja. Relativ neu ist aber, dass die jetzt aber gar keine Hackergenies sein müssen, die selbst die Angriffe programmieren, sondern die Malware ganz einfach kaufen oder sogar mieten können. Die ideale Plattform dafür bietet das Darknet – was es damit genau auf sich hat, verrät jetzt meine Kollegin Jessica Martin.

Sprecherin: Das Darknet ist ein bestimmter Teil des Internets, in den man nur reinkommt, wenn man den Eingang kennt – und der führt meist über den Torbrowser. Dann steht einem eine ganz neue, anonymisierte Welt und ein riesiger digitaler Schwarzmarkt offen. Natürlich geht es hier oft um Drogen, Waffen und andere üble kriminelle Energie.

O-Ton 1 (Thomas Uhlemann, 17 Sek.): „Mittlerweile sind die ganzen Marktplätze da auch ziemlich professionalisiert, das heißt, es gibt mafiöse Großbanden, die ihre Geschäfte jetzt natürlich auch im Netz abwickeln und auf den ersten Blick wirkt das Ganze auch stellenweise sehr seriös. Und seit ner geraumen Zeit ist das Darknet auch ein Marktplatz für Schadsoftware, also Malware, Viren, Trojaner und Co."

Sprecherin: Also das Handwerkszeug für einen Angriff auf digitale Daten.

O-Ton 2 (Thomas Uhlemann, 26 Sek.): „Und zwar dann ganz im Full-Service-Paket – das heißt, es gibt also ausführliche Bedienungsanleitungen, es gibt technischen Support und es gibt Updates, die dann installiert werden können, also Software-Pflege. Und das Besondere ist hier, dass die Cyberkriminellen dabei doppelt abkassieren, indem sie zum Beispiel ihre eigenen Bot-Netze selbst nutzen, um Daten abzugreifen und die geschaffene Infrastruktur dann nach getaner Arbeit quasi an Dritte weiterverkaufen oder vermieten, die dann wieder ihre eigenen Angriffe starten können."

Sprecherin: Die Cyberkriminellen lassen sich da selbstverständlich laufend Neues einfallen.

O-Ton 3 (Thomas Uhlemann, 21 Sek.): „Für uns besonders relevant sind natürlich die Angebote, bei denen komplette Infrastrukturen auch stellenweise stundenweise vermietet oder komplett verkauft werden. So kann man, wenn man zum Beispiel einen sogenannten DDos-Angriff fahren will, also Server in der Welt angreifen möchte, für ein paar Stunden die entsprechende Infrastruktur – also, die ganzen Server und Rechner, die diese Anfragen starten – dort mieten."

Sprecherin: Natürlich sind auch Kreditkartendaten nach wie vor ein gutes Geschäft:
Die Cyber-Gangster bieten die – bei früheren Phishing-Angriffen geklauten – Daten zum Teil schon für eine Provision in Höhe von 10 Prozent des auf dem Konto zu ergaunernden Guthabens an und verdienen selbst daran ordentlich. Nichts ist also sicher.

O-Ton 4 (Thomas Uhlemann, 26 Sek.): „Und deshalb ist es ganz entscheidend, immer auch für Schutz am eigenen Rechner zu sorgen, das heißt also Malware-Schutzlösungen zu installieren und eben nicht nur einen Virenscanner, sondern auch für Firewalls und Spamfilter da zu sorgen und die eigenen Daten sicher zu halten, das heißt also, alles, was ich ins Internet bewege, zu verschlüsseln und dann natürlich auch sichere Passwörter verwende, am besten einen Passwortsafe, wo ich mir einmal ein großes Masterpasswort merken muss. Und dann schafft man es auch, ein bisschen sicherer zu bleiben."

Abmoderationsvorschlag: Sie haben es gehört: Die Gefahr, Opfer von einem Cyberangriff zu werden, steigt immer weiter. Wenn Sie sich jetzt mal ausführlich mit dem Thema beschäftigen wollen, finden Sie alles rund ums Thema Daten-Sicherheit natürlich im Internet – zum Beispiel unter eset.de.

Thema: **Gauner-Marktplatz Darknet – So übel ist die dunkle Seite des World Wide Web tatsächlich**

Interview: 3:12 Minuten

Anmoderationsvorschlag: Phishing, Bot-Angriffe, Datenklau: Dass das Internet praktisch unendliche Möglichkeiten für Cyberkriminelle bietet, weiß man ja. Relativ neu ist aber, dass die jetzt aber gar keine Hackergenies sein müssen, die selbst die Angriffe programmieren, sondern die Malware ganz einfach kaufen oder sogar mieten können. Die ideale Plattform dafür bietet das Darknet – was es damit genau auf sich hat, weiß Thomas Uhlemann vom Internet-Sicherheitsanbieter ESET, hallo!

Begrüßung: „Hallo!“

1. ***Herr Uhlemann, was ist das Darknet eigentlich ganz konkret – für alle, die noch nicht damit zu tun hatten?***

O-Ton 1 (Thomas Uhlemann, 39 Sek.): „Als Darknet oder auch Darkweb bezeichnen wir einen Teilbereich des Internets, der durch spezielle Zugänge, wie zum Beispiel den Torbrowser, abgesichert ist und in dem die Teilnehmer untereinander kommunizieren können und zwar anonym. Es ist aber nicht jedem klar, wer da tatsächlich miteinander zu tun hat, und die Bezahlung erfolgt auch anonym mit sogenannten Kryptowährungen wie Bitcoin zum Beispiel. Und mittlerweile sind die ganzen Marktplätze da auch ziemlich professionalisiert, das heißt, es gibt da mafiöse Großbanden, die ihre Geschäfte jetzt natürlich auch im Netz abwickeln und auf den ersten Blick wirkt das Ganze auch stellenweise sehr seriös. Und seit ner geraumen Zeit ist das Darknet auch ein Marktplatz für Schadsoftware, also Malware, Viren, Trojaner und Co.“

2. ***Wie habe ich mir das vorzustellen?***

O-Ton 2 (Thomas Uhlemann, 34 Sek.): „Also, im Grunde kann man dort im Schadsoftwarebereich so gut wie alles kaufen. Das geht bei einzelner Malware los, bis hin zu ganzen Infrastrukturen für Angriffe. Und zwar dann ganz im Full-Service-Paket – das heißt, es gibt also ausführliche Bedienungsanleitungen, es gibt technischen Support und es gibt Updates, die dann installiert werden können, also Software-Pflege. Und das Besondere ist hier, dass die Cyberkriminellen dabei doppelt abkassieren, indem sie zum Beispiel ihre eigenen Bot-Netze selbst nutzen, um Daten abzugreifen und die geschaffene Infrastruktur dann nach getaner Arbeit quasi an Dritte weiterverkaufen oder vermieten, die dann wieder ihre eigenen Angriffe starten können.“

3. ***Aber das sind doch wahrscheinlich ziemlich teure Programme, die sich kaum ein Kleinkrimineller leisten kann, oder?***

O-Ton 3 (Thomas Uhlemann, 25 Sek.): „Ja, das ist die Krux dabei, es ist nämlich das ganze Gegenteil: Im Darkweb herrscht ein ziemlicher Preiskampf, da gibt es viele Anbieter, und die wollen sich alle gegenseitig unterbieten. Deshalb sind Hackerangriffe mittlerweile sehr günstig zu bekommen, kosten zum Teil sogar tatsächlich weniger als eine Städtereise.

Und auch im Bereich Ransomware – also Erpressersoftware, die fremde Computer kapern und dann Lösegeld fordern zum Beispiel oder die Daten verschlüsseln – gibt es mittlerweile für ein paar wenige Hundert Dollar."

4. ***Womit wird denn sonst noch so am digitalen Schwarzmarkt gehandelt?***

O-Ton 4 (Thomas Uhlemann, 35 Sek.): „Ja, es gibt da praktisch nichts, was es nicht gibt. Für uns besonders relevant sind natürlich die Angebote, bei denen komplette Infrastrukturen auch stellenweise stundenweise vermietet oder komplett verkauft werden. So kann man, wenn man zum Beispiel einen sogenannten DDos-Angriff fahren will, also Server in der Welt angreifen möchte, für ein paar Stunden die entsprechende Infrastruktur – also, die ganzen Server und Rechner, die diese Anfragen starten – dort mieten. Und natürlich sind auch Kreditkartendaten, die bei früheren Phishing-Angriffen ergaunert wurden, ein großes Geschäft: Die verscherbeln die Anbieter manchmal sogar schon für Provisionen in Höhe von zehn Prozent des Guthabens auf dem geklauten Konto."

5. ***Was heißt das jetzt für uns User, die gar nichts mit dem Darknet zu tun haben und ganz harmlos im World Wide Web unterwegs sind?***

O-Ton 5 (Thomas Uhlemann, 43 Sek.): „Dadurch, dass Profi-Kriminelle oder Leute mit kriminellen Absichten sich ins Darkweb einfach so bewegen können, und tatsächlich für einen schmalen Geldbeutel dort Schadsoftware und vieles mehr kaufen können, ist damit zu rechnen, dass wir vermehrt Hacker-Angriffe sehen, und die auch natürlich den Durchschnittsnutzer treffen können. Und deshalb ist es ganz entscheidend, immer auch für Schutz am eigenen Rechner zu sorgen, das heißt also Malware-Schutzlösungen zu installieren und eben nicht nur einen Virenscanner, sondern auch für Firewalls und Spamfilter da zu sorgen und die eigenen Daten sicher zu halten, das heißt also, alles, was ich ins Internet bewege, zu verschlüsseln und dann natürlich auch sichere Passwörter verwende, am besten einen Passwortsafe, wo ich mir einmal ein großes Masterpasswort merken muss. Und dann schafft man es auch, ein bisschen sicherer zu bleiben."

Thomas Uhlemann von ESET über das Darknet – den digitalen Schwarzmarkt für Cyberkriminelle und solche, die es werden wollen! Danke für das Gespräch!

Verabschiedung: „Ich danke auch!"

Abmoderationsvorschlag: Sie haben es gehört: Die Gefahr, Opfer von einem Cyberangriff zu werden, steigt immer weiter. Wenn Sie sich jetzt mal ausführlich mit dem Thema beschäftigen wollen, finden Sie alles rund ums Thema Daten-Sicherheit natürlich im Internet – zum Beispiel unter eset.de.

Hinweis an Interviewpartner: Länge pro Antwort maximal 30 Sekunden!