SOPHOS

Wer mit Malware das große Geld macht

Wie professionelle Cyberkriminalität funktioniert und wie Sie sich dagegen schützen

Von **Chester Wisniewski**, Senior Security Advisor

Ununterbrochen steigt die Flut von schädlichem Code, die unsere Firewalls, Benutzer und Server attackiert. In den SophosLabs registrieren wir jeden Tag mehr als 200.000 schädliche Dateien. Sie werden nicht etwa von Regierungen und Spionen entwickelt, um den nächsten Cyberkrieg anzustiften. Stattdessen steckt dahinter nur eine Motivation: Geld. Inzwischen haben wir wertvolle Einblicke in die Szene der Cyberkriminellen gewonnen. Das gibt uns heute die Möglichkeit, eine effektivere Verteidigung aufzubauen und eigene Angriffe auf die Schwachpunkte der kriminellen Netzwerke zu entwickeln.

Wie professionelle Cyberkriminalität funktioniert

Bei fast jeder Malware geht es heute ums Geldverdienen. Cyberkriminelle haben dazu fantasiereiche Methoden entwickelt. Allerdings müssen bei ihnen viele Einzelfaktoren nacheinander zusammenspielen, damit der kriminelle Gesamtprozess funktioniert. Jeder einzelne Arbeitsschritt bietet uns eine Gelegenheit, die Pläne der Kriminellen zu durchkreuzen.

Im ersten Schritt suchen die Cyberkriminellen Opfer. Arglose Benutzer in ihre Netze zu locken und Computer für kriminelle Zwecke zu missbrauchen, gelingt ihnen dabei meist mit den folgenden sechs Methoden:

1. Spam: Durch E-Mail-Spam war es erstmalig möglich, mit Malware direkt Geld zu verdienen. Und das Geschäft mit fragwürdigen Tabletten, gefälschten Uhren und heiratswilligen Russinnen floriert nach wie vor. Zwar ist das Spamvolumen insgesamt zurückgegangen. Doch noch immer senden Spammer täglich Milliarden von Nachrichten in der Hoffnung, dass ein kleiner Prozentsatz die Spamfilter überwinden und einige Empfänger zum Kauf verlocken kann. Im Anhang von E-Mails kommt außerdem nach wie vor Malware ins Haus, auch wenn der größte Teil der Schadprogramme heute im Web liegt.

2. Phishing: Angreifer verwenden E-Mails nicht nur, um per Spam Produkte und Dienstleistungen anzupreisen, sie führen damit auch Phishing-Angriffe durch. Ihre E-Mails täuschen vor, von Ihrer Bank oder Ihrem E-Mail-Dienstanbieter zu stammen. Das soll Sie dazu bringen, arglos Ihre Zugangsdaten einzugeben. Auf ähnliche Weise bereiten sie auch Angriffe auf unternehmensinterne Dienste vor.

3. Soziale Medien: Viele Spammer sind inzwischen von E-Mails auf Spam-Nachrichten in sozialen Medien umgestiegen. Hat ein scheinbarer Freund oder Kollege einen Link gepostet, klicken die Nutzer in Netzwerken wie Facebook oder Twitter sorgloser darauf als sonst. Auch Sensationsberichte und beliebte Funktionen verleiten neugierige Benutzer dazu, auf unsichere Links zu klicken.

4. Blackhat SEO: Betrüger versuchen außerdem, die Suchergebnisse bei Google und Bing zu beeinflussen, was man als Blackhat SEO oder SEO Poisoning bezeichnet. Ziel ist es, die Suchergebnisse bei beliebten Themen so zu manipulieren, dass Treffer auf den ersten Suchergebnisseiten zu gefährlichen Webseiten mit Exploits, Malware oder Phishing führen. Weitere Informationen zum Thema SEO Poisoning finden Sie in unserem Fachbeitrag aus den SophosLabs (englisch).

5. Drive-by-Downloads: Viele Nutzer infizieren sich schon beim Aufruf einer Webseite, wenn diese bekannte Exploits als „Drive-by-Downloads“ enthält. Die SophosLabs spüren jeden Tag 30.000 neue Seiten im Web auf, die arglose Surfer mit Schadcode bombardieren. Sie wollen damit Schwachstellen in Betriebssystemen, Browsern, Plug-ins und Anwendungen ausbeuten.

6. Malware: Auch Würmer, Viren und andere Malware-Dateien sind noch immer zahlreich im Umlauf. Sie sind heute zwar seltener als noch vor zehn Jahren, doch zur Infektion ungeschützter Systeme und um Computer zu missbrauchen bleiben Sie für die Täter ein wichtiges Mittel.

Wer mit Malware das große Geld macht

Hat ein Krimineller sein Opfer am Haken oder dessen Computer unter seiner Kontrolle, stehen ihm viele Verdienstmöglichkeiten offen. Die folgenden acht Methoden sind sehr verbreitet:

Verkauf von Produkten

Die einfachste Art, um mit Malware, Spam oder manipulierten Webseiten Geld zu machen, ist der simple Verkauf von Produkten. Die Betrüger richten einfach einen Online-Shop ein. Dann verwenden sie infizierte Webseiten, Spam und Werbeaktionen, um potenzielle Kunden auf ihr Angebot zu locken.

Einige Shops sind nur Attrappen. Andere verkaufen wirklich etwas, nämlich Produktfälschungen. Die Palette reicht von Viagra, Rolex-Uhren und Gucci-Handtaschen bis hin zu raubkopierten Software-Paketen.

Stehlen von Anmeldeinformationen

Phishing-E-Mails sehen absichtlich so aus, als hätte sie jemand geschrieben, den Sie kennen und dem Sie vertrauen. Kriminelle setzen dabei auf Social Engineering, um Benutzernamen und Kennwörter für Webseiten mit hohem Ertragswert zu ergaunern. Typisch sind PayPal, Online-Banking, Facebook, Twitter, Yahoo und webbasierte E-Mail-Dienste.

Betrüger können solche Unternehmen problemlos imitieren, da im Online-Bereich alles digital ist. Sie stehlen einfach die Nachrichten von den legitimen Firmen und leiten die Links auf gefälschte Webseiten weiter. Und der prozentuale Anteil von Phishing-E-Mails wächst weiter. Die Methode ist vor allem deshalb so erfolgreich, weil die wenigsten Nutzer die Gefahren kennen.

Pay-per-Click-Betrug

Ist ein Computer erst einmal kompromittiert, kann er spezielle Malware nachladen, die den Datenverkehr mit dem Internet manipuliert. Solche Schadprogramme leiten zum Beispiel die Mausklicks der Opfer heimlich auf Anzeigen um, die die Kriminellen vorher auf ihren eigenen Webseiten platziert haben. Auf diese Weise verdienen sie Geld mit eigentlich normalen Werbenetzwerken.

Gefälschte Sicherheitssoftware

Die meiste Malware verhält sich unauffällig. Die gefälschte Virenschutzsoftware hingegen will ganz im Gegenteil auffallen, nervt und blinkt. Sie wird von manipulierten Webseiten auf den Computer geschmuggelt. Ist sie installiert, versucht sie den Benutzer mit allen Mitteln zu überzeugen, er habe seinen Computer mit Malware infiziert.

Die gefälschte Virenschutzsoftware zeigt dazu zahlreiche erfundene Bedrohungen an – doch bevor es diese „entfernt", verlangt es etwa 80 EUR für die Reinigungsfunktion. Die gefälschte Virenschutzsoftware schützt also nicht vor Bedrohungen – sie ist selbst eine! Die Betrüger können ihre Opfer sogar um noch mehr Geld bringen, indem sie erweiterten Support und mehrjährige Verträge anbieten. Gefälschte Security-Suites gibt es für Windows, Mac und sogar Android.

Ransomware

Mit Ransomware verschlüsseln Cyberkriminelle Ihre Dokumente, den Bootsektor oder andere wichtige Komponenten Ihres PCs, und halten diese solange als „Geiseln", bis Sie das geforderte Lösegeld bezahlen. Ransomware verwendet moderne Verschlüsselungsalgorithmen, und nur ihre Urheber verfügen über den Code zur Entschlüsselung Ihrer Dateien. Wenn Sie wieder auf sie zugreifen wollen, müssen Sie also bezahlen.

In der Vergangenheit war Ransomware vor allem in Russland verbreitet. In letzter Zeit sind auch Nordamerika, Europa und Australien betroffen. Im Jahr 2012 war eine Variante sehr verbreitet, die sich als Nachricht einer Regierungsbehörde ausgab und behauptete, man habe kinderpornografisches Material auf dem Computer gefunden. Der Rechner sei deswegen gesperrt worden, hieß es weiter, und könne nur gegen Zahlung einer Strafe in Höhe von 100 Euro wieder entsperrt werden.

Ransomware sperrt Computer oder verschlüsselt Dateien, bis das Opfer ein Lösegeld an den Cyberkriminellen bezahlt.

Spam in sozialen Medien

Es war noch nie so schwer wie heute, uns eine E-Mail zu schicken. Spamfilter blockieren 99 % der unerwünschten Nachrichten, der Empfänger bekommt sie gar nicht erst zu Gesicht. Schafft es doch mal eine Spam-Mail in den Posteingang, erkennen die meisten Benutzer sie oft schon am gefälschten Absender. Spammer weichen daher immer häufiger auf die Webseiten sozialer Medien aus, allen voran Facebook und Twitter.

Die Kriminellen erwerben gestohlene Benutzerdaten oder bringen Benutzer indirekt dazu, ihre betrügerischen Nachrichten zu verbreiten. Die Betrüger profitieren dabei direkt von Ihrem sozialen Kapital: Je mehr Freunde und Verfolger Sie haben, desto mehr Spam lässt sich über Ihr Konto verbreiten. iPad-Gewinnspiele oder Diätversprechen klickt man nun mal mit viel größerer Wahrscheinlichkeit an, wenn sie von jemandem stammen, den man kennt und dem man vertraut.

Online-Banking-Malware

Zahlreiche Kriminelle haben sich aufs Online-Banking spezialisiert. Was mit einer simplen Keylogging-Software zum Stehlen von Benutzernamen und Kennwörtern begann, hat sich zu einem ausgefeilten Katz-und-Maus-Spiel zwischen Betrügern und Banken entwickelt.

Moderne Banking-Trojaner gibt es auf Systemen mit BlackBerry, Windows, Android und anderen. Sie können SMS-Nachrichten abfangen und Ihre Benutzeranmeldung vom Bildschirm weg als Video aufzeichnen und an die Betrüger senden. Das FBI fasste 2010 eine Bande, die ihre Opfer beinahe um fast 175 Mio. EUR erleichtert hätte.[1]

Betrügerische SMS-Mehrwertdienste

Anstatt nach Ihrer Kreditkarte zu fragen oder zu versuchen, direkt von Ihrem Bankkonto Geld abzuheben, greifen Malware-Autoren und Spammer in sozialen Netzen heute oft auf SMS-Dienste zurück. Beispielsweise nehmen Sie auf Facebook an einer Umfrage teil und geben für die erhoffte Gewinnmitteilung Ihre Handynummer an. Mit dieser Nummer melden die Betrüger Sie für einen SMS-Mehrwertdienst an. Raubkopierte Anwendungen für Android-Handys kommen mitunter mit einem unerwünschten Zusatzprogramm, das auf Ihre Kosten SMS an Mehrwertdienstnummern sendet.

Das Netzwerk der Cyberkriminellen

Es sind sehr viele Arbeitsschritte nötig, bis das Geld aus Online-Betrügereien in kriminelle Kassen fließt. Daher müssen sich die Täter spezialisieren. Sie brauchen daher Erfahrung und Fachwissen, um dauerhaft unseren Schutzsystemen und der Strafverfolgung zu entgehen. In diesem Abschnitt erklären wir die unterschiedlichen Rollen in einem erfolgreichen kriminellen Netzwerk.

Exploit-Schreiber

Einige Hacker spezialisieren sich darauf, Sicherheitslücken in Software aufzuspüren und in sogenannten „Exploit Packs“ zu sammeln. Die Exploit-Schreiber verkaufen ihre Exploit Packs an technisch weniger versierte Betrüger. Diese wiederum verwenden sie auf Webseiten und in E-Mail-Anhängen, um Malware auf ungepatchten Computern zu installieren.

Übersetzer

Die sprachliche Qualität vieler Spam-E-Mails, Lockmittel und Social-Engineering-Angriffe hat sich in den vergangenen Jahren deutlich verbessert. Die hinter solchen Angriffen stehenden Banden investieren offenbar in professionelle Übersetzungsdienste. So können sie noch mehr Opfer hinters Licht führen.

1 „Zbot suspects arrested in Ukraine“, Naked Security Blog, http://nakedsecurity.sophos.com/2010/10/01/zbot-suspects-arrested-ukraine

Bot-Hirten

Ein Bot-Hirte infiziert die Zombie-Computer in einem Botnet, damit Kriminelle es zur Verbreitung von Spam, für DDoS-Angriffe, zum Proxying und für andere kriminelle Cloud-Computing-Anwendungen verwenden können. Bot-Hirten verkaufen oder vermieten die Computerkontrolle, je nach Käufer aufgeteilt z.B. nach Ort der Zombie-Computer oder nach Typ der Bots.

Money Mules und Mule Manager

Wirtschaftskriminelle brauchen willige Helfer, die für sie zu Banken gehen, Gelder überweisen oder Schecks einlösen. Mule Manager sind auf die Rekrutierung solcher Personen spezialisiert. Sie suchen Menschen, denen es finanziell schlecht geht oder die gewillt sind, bei einem Finanzbetrug mitzumachen. Diese Money Mules werden sehr häufig mit angeblichen Home-Office-Jobangeboten geködert.

Partnyo'rka-Besitzer

„Partnyo'rka" lässt sich frei mit „Partnernetzwerk" übersetzen. In der Art legitimer Affiliate-Netzwerke richten sich Partnyo'rkas an Kleinkriminelle, um für Versandapotheken, gefälschte Luxusartikel und andere Waren und Dienstleistungen zu werben. Die Partnyo'rka-Betreiber bezahlen ihren Helfern für jeden Verkauf eine Provision. Partnyo'rka-Besitzer suchen über Spam-E-Mails, Foren, Chats, Blog-Kommentare und soziale Medien nach Helfern. Darüber hinaus manipulieren sie Webseiten und verwenden Blackhat-SEO-Methoden.

Tool-Provider

Software zu entwickeln, ist an sich nicht kriminell. Allerdings schreiben einige Mitmenschen ausschließlich Tools, die der Verbreitung von Spam und Malware dienen. Cyberkriminelle können für Beträge zwischen 20 und mehreren Tausend Euros zahlreiche Tools kaufen, darunter Exploits, Toolkits, CAPTCHA-Löser und Spam-Werkzeuge.

Malware-Schreiber

Wie Microsoft-CEO Steve Ballmer es einmal ausdrückte, sind „Entwickler, Entwickler, Entwickler" das Herzstück der Cyberkriminalität. Dabei verbreiten die meisten Malware-Entwickler ihre Produkte offenbar nicht direkt, sondern verkaufen ihre Dienste an Netzwerke organisierter Cyberkriminalität.

Wie wir gewinnen können

Solange sich damit Geld verdienen lässt, werden Kriminelle weiterhin jede Gelegenheit nutzen, uns zu betrügen. So erscheint der Kampf gegen die Cyberkriminalität reichlich zermürbend. Und doch ist es ein Kampf, den wir gewinnen können. Auf dem Weg zum Geld müssen unsere Gegner stets eine ganze Reihe von Arbeitsschritten hinter sich bringen. Indem wir nur ein einziges Glied in dieser Abfolge durchbrechen, können wir ihnen bereits das Handwerk legen. Wer stets möglichst sofort alle Updates installiert, unnötige Anwendungen deinstalliert und bei normalen Benutzern auf Administratorrechte verzichtet, der vereitelt bereits über 90 % dieser Angriffe.

Und die gelingen oft nur, weil die Benutzer arglos und unvorbereitet sind. Machen Sie daher Ihren Mitarbeitern anhand von Beispielen die Gefahren bewusst. Geschulte Benutzer sind weit weniger geneigt, schädliche Anhänge zu öffnen oder aus Neugier auf irgendwelche Links zu klicken. Die Benutzer müssen außerdem verstehen, dass Security-Tools zwar die Netzwerksicherheit erhöhen, der wichtigste Verteidigungsmechanismus zum Schutz vertraulicher Unternehmensdaten jedoch der Benutzer selbst ist.

Um uns erfolgreich zu verteidigen, müssen wir uns unsere Schwachstellen klarmachen, gemeinschaftlich an ihnen arbeiten und unser Wissen darüber weitergeben. Wenn wir weniger Anwendungen installieren, unsere Benutzer schulen und die Administratorrechte einschränken, können wir Betrügern ihre Aufgabe so schwer machen, dass sie sich lieber ein anderes Opfer suchen.

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0
+49 721 255 16 0
E-Mail: sales@sophos.de

Boston, USA | Oxford, UK

Sophos White Paper 06.12v1.dNA

SOPHOS