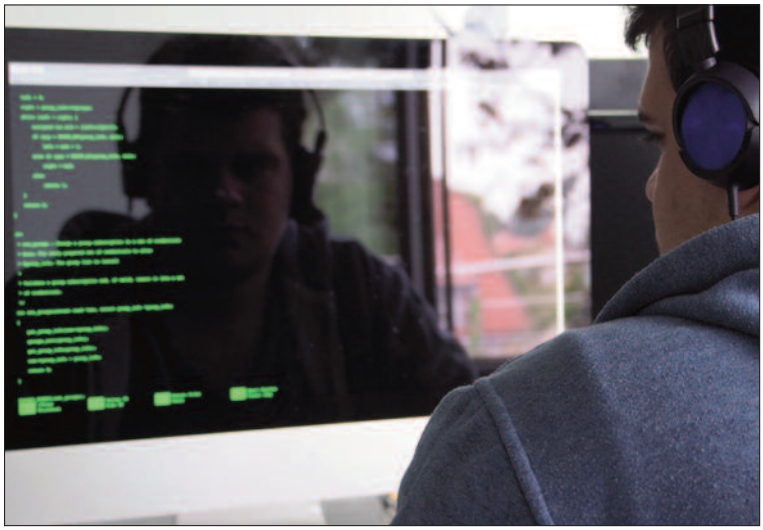
Cyberkrimineller Untergrund

Ein Großteil der Internetangriffe mit Schadsoftware auf Vermögenswerte erfolgt von Kriminellen aus dem russischen Sprachraum, wo sich ein cyberkrimineller Untergrund gebildet hat.

Experten des *Computer Incidents Investigation Departments (CIID)* von *Kaspersky Lab* analysierten 330 Cybersicherheitsvorfälle, die aus dem russischen Sprachraum gesteuert wurden. Die Ergebnisse der Studie „The Russian cybercrime underground: How it works“ bietet Einblick in die Struktur und Funktionen der Mitglieder einer Bande russischer Cyber-Krimineller. Sie beschreibt die Art der im Untergrund angebotenen „Dienstleistungen“ und beziffert die Schäden. Von 2012 bis 2015 konnten Strafverfolgungsbehörden verschiedener Länder mehr als 160 Personen aus Russland und seinen Nachbarstaaten festnehmen. Sie wurden der Cyber-Kriminalität im Finanzbereich verdächtigt. Der geschätzte Schaden beläuft sich auf 790 Millionen US-Dollar. Mit den Schäden der noch nicht festgesetzten Carbanak-Bande kommt man auf über 1,7 Milliarden US-Dollar.



Cyberkriminelle aus dem russischen Sprachraum attackieren weltweit Online-Banking-Nutzer und Finanzinstitute.

Die Experten von *Kaspersky Lab* schätzen, dass fast 1.000 Cyber-Kriminelle aus Russland und seinen Nachbarstaaten in Angriffe involviert waren. Geführt wurden sie von weniger als 20 Bandenchefs, von denen die meisten noch nicht gefasst werden konnten. Derzeit beobachtet *Kaspersky Lab* fünf größere Banden, bestehend aus 10 bis 40 Mitgliedern, die bereits 2012 und 2013 entdeckt wurden und weiter kriminelle Aktivitäten im Finanzbereich entwickeln. Mindestens zwei Gruppen greifen aktiv Organisationen im russischen Raum an, operieren aber außerdem in Deutschland, den USA, Australien, Großbritannien, Frankreich sowie in Italien.

Russischsprachige Cyber-Kriminelle gehen international vor, und diese Gefahr dürfte sich weiter vergrößern“, warnt Ruslan Stoyanov, Director des *CIID*. „Grund dafür ist die jüngste Abwertung des Rubels, was illegale Aktivitäten in anderen Währungsräumen für russische Cyber-Kriminelle attraktiver macht. Wir erwarten mehr solcher Angriffe. Sie lassen sich nur dann wirksam bekämpfen, wenn Strafverfolgungsbehörden, IT-Sicherheitsexperten und die Finanzbranche zusammenarbeiten. Unsere Experten haben bereits kriminelle Aktivitäten aufgedeckt, bevor sich diese weiter ausbreiten konnten, und sie geben ihre Erfahrungen gerne weiter im Kampf gegen die weltweite Cyberkriminalität russischen Ursprungs.“

Zum russischen cyberkriminellen Markt zählen nicht nur Bürger der Russischen Föderation, sondern auch angrenzender Staaten der ehemaligen Sowjetunion. In den meisten Fällen geht es um die Ukraine und die baltischen Länder. Unter dem „cyberkriminellen Markt“ wird die Gesamtheit der „Dienstleistungen“ und „Produkte“ verstanden, die für kriminelle Aktivitäten im Cyberspace benötigt und eingesetzt werden.

Ruslan Stoyanov, CIID-Direktor von Kasypersky.

Zu den„Produkten“ gehören u. a.
- Schadsoftware, die es ermöglicht, unerlaubten Zugriff auf einen Computer oder ein mobiles Gerät zu erhalten und Daten von dem infizierten Gerät und/oder Geld von dem Konto des Opfers zu stehlen (Trojaner);
- Software, mit deren Hilfe Sicherheitslücken in der auf dem Computer des Opfers installierten Software ausgenutzt werden können (Exploits);
- Datenbanken mit gestohlenen Kreditkarteninformationen oder anderen wertvollen Informationen;
- Internet-Traffic (eine bestimmte Menge von Besuchen einer Webseite, die vom Auftraggeber ausgewählt wurde, durch Anwender, die bestimmte von den Cyber-Kriminellen festgelegte Kriterien erfüllen).

Zu den „Dienstleistungen“ gehören unter anderem:
- Spam-Versand;
- Organisation von DDoS-Attacken (Überlastung von Webseiten mit Anfragen, mit dem Ziel, sie für legitime Nutzer nicht erreichbar zu machen);
- Überprüfung, ob Schadsoftware von Antiviren-Programmen erkannt wird;
- Veränderung der Schadsoftware, so dass sie nicht von Antiviren-Programmen erkannt wird;
- Vermietung von isolierten Servern und von Botnets;
- Überprüfung des Verkaufswertes gestohlener Kreditkartendaten;
- Dienstleistungen zur Verifizierung von Daten (betrügerische Anrufe, gefälschte Dokumentenscans);
- Hochpushen von schädlichen Webseiten und Werberessourcen in den Ergebnislisten von Suchmaschinen;
- Vermittlung bei Geschäften zum Erwerb von „Produkten“ und „Dienstleistungen“;
- Abschöpfen und Flüssigmachen von Mitteln.

Bezahlt wird in der Regel über ein elektronisches Bezahlsystem, wie zum Beispiel *WebMoney, Perfect Money* oder *Bitcoin*.

Fotos: Fotolia/Niko Endres, Kaspersky Lab

Die „Dienstleistungen“ der Cyber-Kriminellen werden über ein elektronisches System bezahlt, zum Beispiel mit „Bitcoin“.

Stellenanzeige der Kriminellen auf einer Website für arbeitssuchende IT-Experten: Gesucht wird ein Spezialist für Java/Flash.

Stellenangebote. Die Vielfalt der Fertigkeiten, die für die Herstellung der „Produkte“ und Bereitstellung der „Dienstleistungen“ benötigt werden, hat einen eigenen Stellenmarkt hervorgebracht, auf dem Spezialisten gesucht werden, ohne die Cyber-Kriminelle die Online-Finanzverbrechen nicht umsetzen können. Einige Berufe findet man zum größten Teil auch in jeder beliebigen Firma aus dem IT-Bereich: Programmierer/Codierer, Virenautoren (Entwicklung von Schadsoftware und Modifikation existierender Malware), Webdesigner (Erstellung von Phishing-Seiten, E-Mails), Systemadministratoren (Aufbau einer IT-Infrastruktur und deren Support), Tester (Testen der Malware), „Kryptoren“ (Änderung des Schadcodes mit dem Ziel, die Erkennung durch Antiviren-Programme zu verhindern).

„Zalivshchiki“, auf Deutsch etwa „Ausgießer“, „Vergussmeister“, werden die Bandenmitglieder genannt, die für das Abschöpfen des Geldes von den gehackten Konten zuständig sind. „Zalivshchiki“ kennen die interne Struktur der anzugreifenden Organisation oft bis ins Detail. Das kann so weit gehen, dass sie wissen, wann der Mitarbeiter Mittagspause macht, der an dem Rechner arbeitet, von dem aus die betrügerische Transaktion abgewickelt werden soll. Sie haben eine genaue Vorstellung davon, wie die automatisierten Systeme zur Betrugsabwehr funktionieren und was man tun muss, um diese Systeme zu umgehen. Sie erfüllen hochspezialisierte Aufgaben und werden nicht nach einem festen Satz bezahlt, sondern erhalten einen Prozentsatz der gestohlenen Summe.

Kuriere. Der Leiter des Kurierdienstes hat die Aufgabe, das gestohlene Geld in Empfang zu nehmen, es flüssig zu machen und der jeweiligen Gruppe ihren Anteil zu überweisen. Zu diesem Zweck baut der Kurierdienst eine eigene Infrastruktur auf, die aus juristischen und natürlichen Personen mit Bankkonten besteht, auf die das gestohlene Geld überwiesen wird und von denen es in die Taschen der Cyber-Verbrecher wandert. Der Manager eines Kurierdienstes interagiert mit dem Organisator der kriminellen Bande und stellt ihm die Nummern der Konten bereit, auf die der „Zalivshchik“ das Geld leitet. Die Kurierdienste arbeiten wie die „Zalivshchiki“ auf Provisionsbasis, wobei sie fallweise bis zur Hälfte der gesamten gestohlenen Summe erhalten.

Kuriere sind die Halter der Bezahlmittel, die auf Befehl von oben das auf dem Konto aufgetauchte Geld flüssig machen, oder es auf ein anderes, vom Manager des Kurierdienstes angegebenes Konto überweisen. Es gibt zwei Arten von Kurieren: wissentliche und unwissentliche. Unwissentliche Kuriere sind Leute, denen zumindest zu Beginn ihrer Mitarbeit nicht bewusst ist, dass sie an einer kriminellen Unternehmung beteiligt sind. In der Regel werden der Empfang und die Überweisung des Geldes einem unwissentlichen Kurier unter einem moralisch einwandfreien Vorwand übertragen. Beispielsweise kann der Leiter des Kurierdienstes eine juristische Person schaffen und für eine leitende Funktion (beispielsweise CEO oder Finanzchef) eine Person anheuern, die die Funktion eines unwissentlichen Kuriers übernimmt – das Unterschreiben von Unternehmensdokumenten, die als legale Tarnung für das Abziehen des gestohlenen Geldes dienen. Die Kurierdienste können auf eine Vielzahl von Methoden zurückgreifen, wenn es darum geht, das Geld abzuziehen. In Abhängigkeit von der Summe des gestohlenen Geldes bedienen sie sich privater Kreditkartenbesitzer, die gegen eine geringe Bezahlung bereit sind, die Eingänge auf dem Konto flüssig zu machen und sie einem Vertreter des Kurierdienstes zu überweisen. Es können auch eigens gegründete juristische Personen sein, deren Vertreter „Gehaltsprojekte“ (eine Vielzahl von Kreditkarten für die Firmenmitarbeiter für die Überweisung der Gehälter) in der Bank ausfertigen, die diese juristische Person betreut.

Eine weitere Standardmethode zum Aufbau von Kurierdiensten ist das massenhafte Eröffnen von Konten durch wissentliche Kuriere in verschiedenen Banken. Findet der Diebstahl außerhalb Russlands statt, übernimmt ein Bürger oder eine Gruppe von Bürgern aus einem osteuropäischen Land die Rolle des Kuriers, der innerhalb kurzer Zeit mehrere europäische Länder besucht, um dort jeweils Konten auf seinen Namen zu eröffnen. Daraufhin übermittelt er dem Leiter des Kurierdienstes die Zugangsdaten der Konten. In der Folge werden diese Konten benutzt, um das Geld zu „verflüssigen“.

Stuffer. Eine Variante, das gestohlene Geld abzuschöpfen, besteht im Kauf von Waren in Online-Shops mit Hilfe gestohlener Bezahlmittel, im Weiterverkauf und der Auszahlung des ihnen zustehenden Anteils an die Diebe. Mit dieser Aufgabe sind die „Stuffer“ (von „stuff“, Jargon für „Ware“) betraut.

Fotos: Fotolia/Ulchik74, Kaspersky Lab

Das sind Mitglieder einer Cybercrime-Bande, die das Geld, das sich auf gehackten Konten befindet, für den Kauf von Waren in Internet-Shops ausgeben. Der Stuffer ist eine Spielart des „Zalivshchiks“, allerdings wird das Geld nur auf diese Weise von den Konten abgezogen, wenn die gestohlenen Summen relativ gering sind. Stuffer arbeiten eng mit den Hehlern zusammen. Diese „Synergie“ beinhaltet häufig, dass der Hehler Waren eines bestimmten Typs bestellt, bis hin zu einem bestimmten Hersteller oder Modell, und dieser Auftrag dann ausgeführt wird.

Der Organisator ist der Topmanager in der kriminellen Hierarchie. In seine Verantwortung fallen die Finanzierung des Vorbereitungsstadiums, die Zusammenstellung der Aufgaben der ausführenden Elemente, die Kontrolle über ihre Erfüllung und die Kommunikation und Interaktion mit externen Akteuren, etwa Kurierdiensten und Call-Services (wenn es keine eigenen gibt). Der Organisator bestimmt das Angriffsziel, wählt die benötigten „Spezialisten“ aus und regelt das Finanzielle mit ihnen.

Foto: Fotolia/Svort

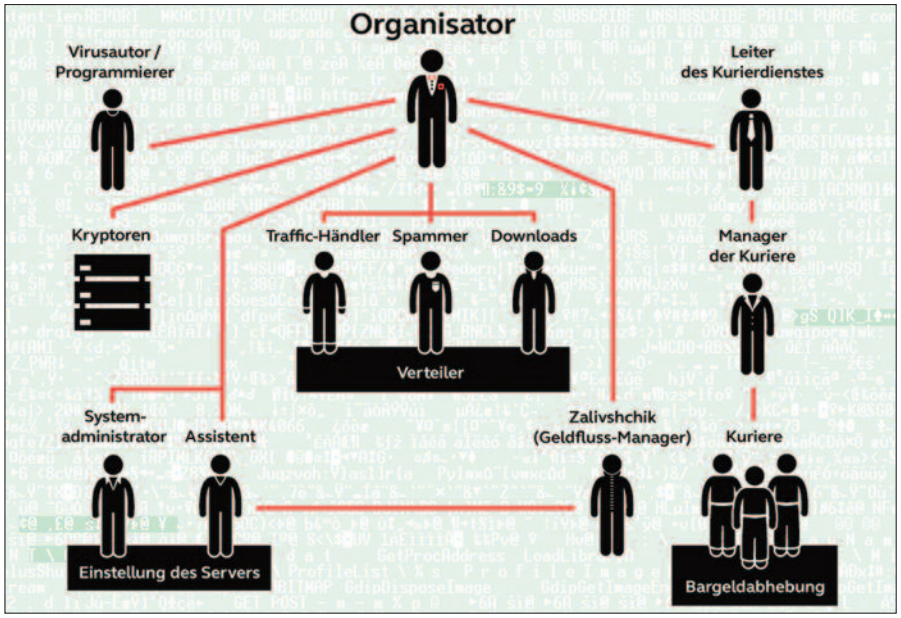
Gestohlene Kreditkarteninformationen: „Angebot“ der Cyber-Kriminellen.

Das Anwerben von „Mitarbeitern“ in einer Organisation erfolgt entweder auf Webseiten oder auf Ressourcen für Leute, die an unkonventionellen Verdienstmöglichkeiten im Internet interessiert sind. In anderen Fällen werden die Anzeigen auf gewöhnlichen Jobsuche-Webseiten veröffentlicht oder bei Jobbörsen für entfernte Mitarbeiter. Die auf dem Cybercrime-Markt angeworbenen Arbeitskräfte lassen sich in zwei Typen einteilen:

• In jene, die sich der Illegalität des Projekts bewusst sind, an dem ihnen eine Mitarbeit angeboten wird, und in

• jene, denen das – zumindest im Anfangsstadium – nicht bewusst ist. Im letzten Fall geht es in der Regel um Leute, die für vergleichsweise einfache Arbeiten benötigt werden, beispielsweise die Nachbildung der Benutzeroberfläche von Online-Banking-Systemen oder von Webseiten. Veröffentlichen sie „gefälschte“ Stellenangebote, setzen die Cyber-Kriminellen häufig darauf, dass sich Leute aus der russischen Provinz oder aus an Russland grenzenden Ländern (meist aus der Ukraine) melden, wo es häufig schwierig für einen IT-Spezialisten ist, einen Job mit angemessener Bezahlung zu finden. Einem Mitarbeiter aus der Provinz muss man weniger zahlen als Angestellten aus Großstädten.

Dabei bevorzugen Cyber-Kriminelle häufig Bewerber, die noch keine kriminelle Vorgeschichte haben. Oft werden solche Stellenanzeigen als legitime Arbeitsangebote dargestellt. Erst nachdem die neuen Mitarbeiter ihre Aufgaben erhalten haben, wird die wahre Natur dieser Arbeit offenbart. Der zweite Grund für die Suche nach entfernten „Mitarbeitern“ ist das Bestreben der Organisatoren, die Aktivität der Gruppe weitestgehend zu anonymisieren



Aufgabenverteilung einer Finanz-Cybercrime-Gruppe.

und Bedingungen zu schaffen, in denen der Auftragnehmer keine vollständigen Informationen über die Person des Auftraggebers hat.

Call Services. Für den Erfolg des cyberkriminellen Unternehmens ist Social Engineering entscheidend, besonders wenn es um Angriffe auf Organisationen geht, um große Summen zu stehlen. Selbst wenn es den Online-Verbrechern gelungen ist, die Kontrolle über den Computer zu erlangen, von dem die Transaktion ausgeführt werden kann, kann diese nur erfolgreich abgeschlossen werden, wenn ihre Legitimität bestätigt wird. Genau diese Aufgabe übernimmt der „Call Service". Im richtigen Moment schlüpft einer seiner „Mitarbeiter" entweder in die Rolle eines Mitarbeiters der angegriffenen Organisation oder in die eines Mitarbeiters der Bank, mit der die Organisation zusammenarbeitet, und bestätigt die Legitimität des Zahlungsvorgangs.

Angriffsetappen. Bei Attacken auf ein Unternehmen bestellt der Organisator bei einem Zulieferer Informationen über das Unternehmen. Mit deren Hilfe kann ein glaubhaftes Social-Engineering-Schema ausgearbeitet werden. Geht es um einen Angriff auf individuelle Anwender, entfällt die vorbereitende Aufklärung oder sie beschränkt sich auf die Auswahl der „Zielgruppe" der Attacke (beispielsweise Online-Banking-Anwender bestimmter Banken) und die Erstellung von Phishing-Mails und Phishing-Seiten.

Infektion. Das Eindringen in das interne Netz wird mit Hilfe von zielgerichteten (Spear-Phishing) oder massenhaften Versendungen von Phishing-Mails umgesetzt, die einen schädlichen Link auf eine Drittressource oder ein speziell aufbereitetes Dokument in Form eines Anhangs enthalten. Das Öffnen des angehängten Dokuments oder der Klick auf den mitgeschickten Link führt zur Infektion des Systems mit einem Schadprogramm. Häufig erfolgt die Infektion automatisch, ohne Kenntnis und Beteiligung des Nutzers. Nach dem Aufruf des Links wird automatisch ein Schadprogramm auf seinen Computer geladen (Drive by Download) und dort gestartet.

In anderen Fällen erfolgt die Infektion über gehackte Webseiten, über die der Nutzer verdeckt auf eine Drittressource mit einer Exploit-Sammlung geleitet wird. Landet der Anwender auf einer solchen Seite, wird sein System mit Malware verseucht.

Im weiteren Verlauf wenden die Cyber-Kriminellen eine Reihe von schädlichen Tools an, die für die Festsetzung der Schadsoftware im System sorgen. Beispielsweise hacken und infizieren sie interne Seiten der Organisation mit Schadsoftware, um eine Neuinstallation des Schädlings für den Fall zu gewährleisten, dass die Schutzlösung auf den angegriffenen Computern die vorherige Malware-Version gelöscht hat. Außerdem installieren Cyber-Kriminelle nicht selten Software in einer angegriffenen Infrastruktur, die den ungehinderten Zugriff auf die internen Netze der Organisation von außen ermöglicht. Auf die gehackten Computer werden verborgene Fernsteuerungstools geladen, mit Hilfe derer die Verbrecher versuchen, sich die Accounts der Systemadministratoren anzueignen. Großflächig legale Fernwartungs-Programme werden eingesetzt, deren Funktionalität vielen Nutzern bekannt ist. Auf der letzten Etappe wird auf die Finanzsysteme zugegriffen und das Geld von den Konten der angegriffenen Organisationen auf die Konten der Kurierdienste überwiesen, oder das Geld wird direkt von Geldautomaten abgehoben.

Die Fehler, die diesen Cyber-Kriminellen nicht selten unterlaufen, führen zu ihrer Identifizierung und Festnahme. Doch der verhältnismäßig geringe Preis, den sie für den Einstieg in das Cybercrime-Milieu auf dieser „Amateurebene" zu zahlen haben (ab 200 US-Dollar) und die Möglichkeit, wesentlich mehr zu verdienen, ziehen immer neue Einzeltäter an. Zwei Männer wurden 2012 von einem russischen Gericht wegen des Diebstahls von mehr als 13 Millionen Rubel (damals etwa 422.000 US-Dollar) von Onlinebanking-Nutzern einer russischen Bank zu Freiheitsstrafen von viereinhalb Jahren auf Bewährung verurteilt. Die beiden Verurteilten setzen aber ihre Cybercrime-Aktivitäten fort und ergaunerten weiter Geldsummen. Im Mai 2015 wurden sie erneut verhaftet.

Die Gründe für die Ausbreitung der Finanzkriminalität mit russischsprachigem Hintergrund in den letzten Jahren sind laut Kaspersky-Experten unter anderem

- der Mangel an qualifiziertem Personal bei den Strafverfolgungsbehörden,
- Mängel in der Gesetzgebung, die es Cyber-Kriminellen in den meisten Fällen ermöglichen, sich der Verantwortung zu entziehen oder mit einer milden Strafe davonzukommen, und
- die mangelnde internationale Zusammenarbeit zwischen Strafverfolgungsbehörden und Expertenorganisationen verschiedener Länder.

Im Gegensatz zu der realen Welt laufen Überfälle im Cyberspace unbemerkt ab und digitale Beweise können nur innerhalb kurzer Zeit nach der Tat sichergestellt werden. Dabei besteht für die Kriminellen keine Notwendigkeit, sich in dem Land aufzuhalten, in dem

FOTO: KASPERSKY LAB

Das ergaunerte Geld wird überwiesen oder von Geldautomaten abgehoben.

das Verbrechen begangen wird. Die sich den russischsprachigen Cyber-Kriminellen bietenden Bedingungen sind günstig – ein geringes Risiko, strafrechtlich verfolgt zu werden und hohe Gewinne. Das hat zur Folge, dass die Zahl der Verbrechen und die kriminellen Umsätze steigen.

Kaspersky Lab ruft andere Unternehmen sowie die Strafverfolgungsbehörden aller Länder zur Zusammenarbeit auf, um die Aktivität cyberkrimineller Gruppen zu unterbinden. Die von *Kaspersky Lab* initiierte internationale Ermittlung der Aktivität der Carbanak-Gruppe ist das erste Beispiel für eine erfolgreiche internationale Kooperation. Mitglieder der Carbanak-Bande erleichterten 100 Banken, E-Payment-Systeme und andere Finanzinstitute aus 30 Ländern um insgesamt eine Milliarde US-Dollar.

Die Attacken gehen weiter. Österreichische Banken und Finanzinstitute waren bisher nicht betroffen. Die Cyber-Kriminellen verschafften sich über Spear-Phishing-Attacken Zugang zu einem Angestellten-Computer, der mit dem Carbanak-Schadprogramm infiziert wurde. Anschließend waren sie in der Lage, sich im internen Netzwerk einer Bank zu bewegen und die für die Videoüberwachung zuständigen Computer der Administratoren aufzuspüren und zu übernehmen. Die Angreifer konnten nun alles, was sich auf den Bildschirmen der für die Betreuung der Geldtransfersysteme verantwortlichen Mitarbeiter abspielte, einsehen und aufnehmen. So kannten sie jedes Detail über die Arbeit der Angestellten und konnten die Aktivitäten imitieren, um Geld zu überweisen oder bar auszuzahlen. *Siegbert Lattacher*

Kaspersky-Studie „The Russian cybercrime underground: How it works“: https://de.securelist

FOTO: FOTOLIA/ANDREY POPOV