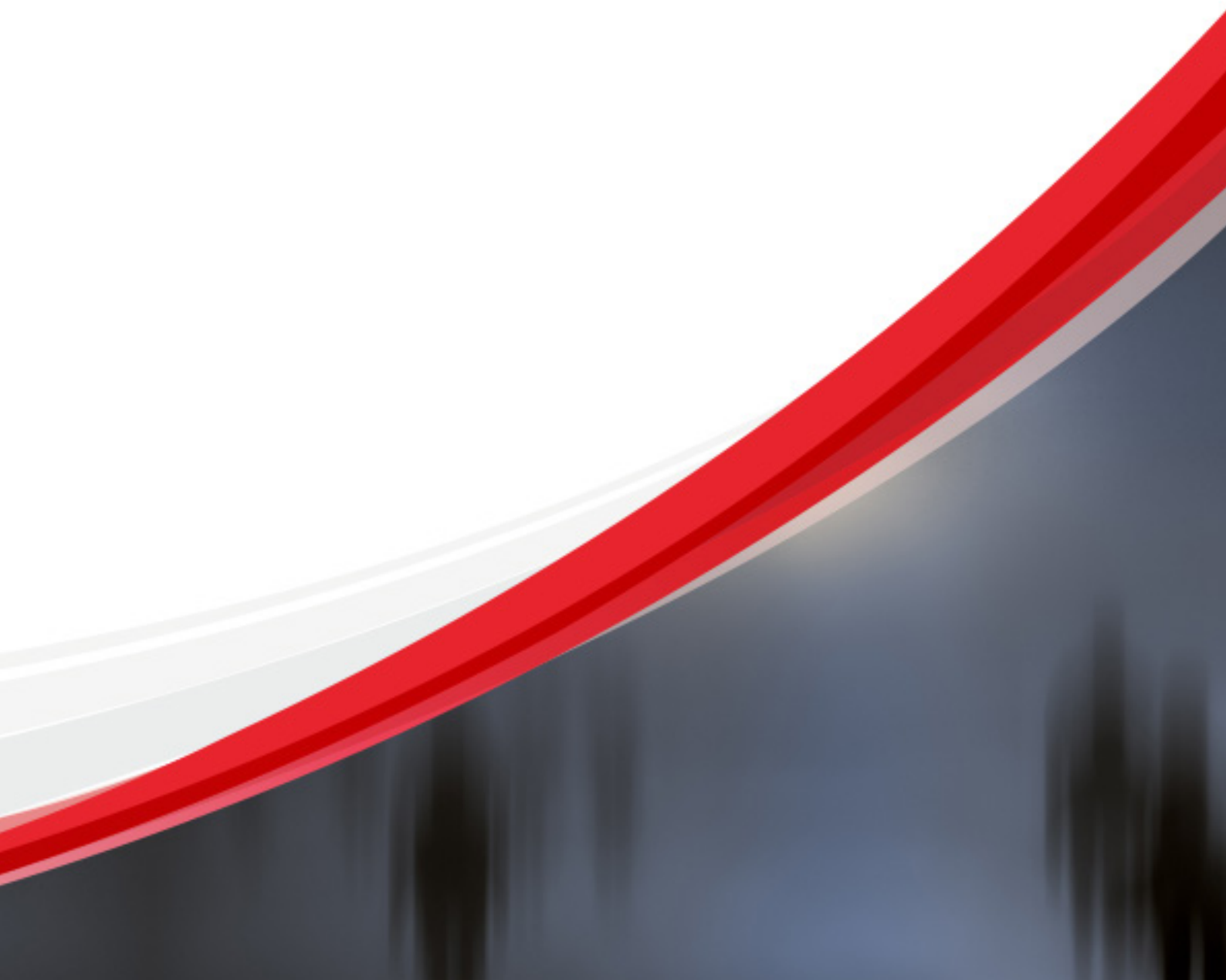
Trend Micro Research Paper

SERIE: CYBERKRIMINELLE UNTERGRUNDWIRTSCHAFT

Russischer Untergrund – Neuauflage

Max Goncharov

Forward-Looking Threat Research Team



Inhaltsverzeichnis

Serie: Cyberkriminelle Untergrundwirtschaft 4

Einleitung 5

- Methoden für die Datensammlung aus dem Untergrundmarkt 6
- Vereinheitlichen der Preise 6
- Produkt oder Service? 6

Charakteristiken des russischen Untergrundmarkts 7

Produkte 8

- Trojaner 8
- Exploits und Exploit Bundles 8
- Rootkits 10
- Verkehr 10
- Crypter 11
- Gefälschte Dokumente 12
- Gestohlene Kreditkarten- und andere Anmeldeinformationen 13

Services 13

- Dedizierte Server-Hosting-Services 13
- Proxy-Server-Hosting 14
- VPNs 14
- Pay-per-Install 14
- Denial-of-Service-Angriffe 16

Spamming....16
Flooding....17
Malware-Prüfung gegen Sicherheitssoftware....17
Social Engineering- und Account-Hacking-Services....17
Account-Hacking....18
Brute-Forcing....18
Account Hacking über Social Engineering....18
Cyberkriminelle Waren im russischen Untergrundmarkt....19
Schlussfolgerungen....22
Anhang....22
Liste der cyberkriminellen Waren, die Trend Micro nachverfolgt und überwacht....22
Produkte....22
Services....23
Glossar....24

HAFTUNGSAUSSCHLUSS

Serie: Cyberkriminelle Untergrundwirtschaft

Cyberkriminelle haben verschiedene Treffpunkte im Internet, wo sie mit Produkten und Dienstleistungen handeln. Anstatt ihre Angriffswerkzeuge von Grund auf selbst zu entwickeln, können sie diese von ihren „Kollegen“ erwerben. Wie in jedem anderen Markt diktieren auch hier Angebot und Nachfrage den Preis. In letzter Zeit sind diese Preise gefallen.

Trend Micro beobachtet seit Jahren die wichtigen Entwicklungen im cyberkriminellen Untergrund und hat sich ein beachtliches Wissen zu den Märkten und deren Angeboten erworben.

2012 erschien eine Analyse “Russian Underground 101” mit den Marktangeboten russischer Cyberkrimineller.[1] Im selben Jahr arbeitete das Team mit dem University of California Institute of Global Conflict and Cooperation gemeinsam an einer Veröffentlichung namens “Investigating China’s Online Underground Economy”, die den chinesischen Untergrund beleuchtete.[2] Im letzten Jahr schließlich beschäftigte sich Trend Micro nochmals mit dem chinesischen Untergrund und veröffentlichte dazu „Beyond Online Gaming: Revisiting the Chinese Underground Market”.[3] Jeder Untergrundmarkt hat seine eigenen Merkmale, und in diesem Jahr wird ein Bericht zum brasilianischen Markt hinzukommen.

Die Hürden für cyberkriminelle Aktivitäten sind heutzutage niedriger denn je. Toolkits sind billig zu haben, manche sogar kostenlos. Die Funktionalität ist reichhaltig und Untergrundforen für den Handel mit Produkten und Diensten florieren weltweit, vor allem in Russland, China und Brasilien. Auch nutzen die Cyberkriminellen das Deep Web, um ihre Produkte und Services außerhalb des indizierten und daher abfragbaren Webs zu vertreiben.

Infolge all dieser Entwicklungen ist das Risiko, zum Opfer der Cyberkriminellen zu werden, höher als je zuvor.

1 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf.
2 http://igcc.ucsd.edu/publications/igcc-in-the-news/news_20120731.htm.
3 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-beyond-online-gaming-cybercrime.pdf.

Einleitung

2012 veröffentlichte Trend Micro “Russian Underground 101”, ein Forschungspapier, das eine Übersicht über den cyberkriminellen Untergrund und die grundlegenden Arten von Hacker-Aktivitäten in Russland lieferte. In diesem Jahr nun untersuchten die Sicherheitsexperten die neuen Entwicklungen in diesem Untergrundmarkt. Die Informationen in dieser aktuellen Studie stammen wie schon 2012 aus Daten der von den Cyberkriminellen genutzten Online-Foren und -Diensten. Auch verwendeten die Forscher Beiträge von Hackern über deren Aktivitäten, über die von ihnen erstellten Bedrohungen und zu Informationen, die sie auf den Shopping-Sites der Foren veröffentlichen. Auch kommen grundlegende, von den Hackern befolgte Konzepte zur Sprache sowie die Informationen, die sie mit ihren „Kollegen“ austauschen. Schließlich liefert die Studie einen Vergleich der Preise von Produkten und Dienstleistungen zwischen 2011 und 2013, einschließlich der Funktionalität jedes Produkts oder Dienstes.

Die Studie besteht aus fünf Hauptteilen: Der erste Teil besteht aus einer Einleitung mit den Charakteristiken des russischen Untergrundmarkts, den Produkten, Services und den cyberkriminellen Angeboten. Der zweite Teil umfasst eine Charakterisierung des russischen Untergrundmarkts und eine Abgrenzung von anderen. Der dritte und vierte Teil wiederum liefern eine detaillierte Beschreibung der im russischen Untergrund bekanntesten Produkte und Services. Im letzten Teil schließlich finden sich Preisinformationen zu diesen Produkten und Diensten.

Die cyberkriminelle Untergrundwirtschaft kennt wie jede andere Wirtschaft auch Hochs und Tiefs bei den Preisen, abhängig vom Angebot und von der Nachfrage. Im Fall des russischen Untergrunds trieb die hohe Nachfrage nach Kreditkarteninformationen die Preise in die Höhe. Doch dann ließen Sicherheitsvorkommnisse, wie die massiven Einbrüche bei beliebten Einzelhändlern vor ein paar Monaten, die Preise wieder fallen, denn es kam zu einem Überangebot an Zugangsinformationen.

Cyberkriminelle müssen ihre Identitäten geheimhalten und so gut wie möglich alle Spuren ihrer „Geschäftstransaktionen“ verwischen. Anforderungen wie diese machen Echtzeittransaktionen im Untergrundmarkt nahezu unmöglich. Damit verlaufen die Geschäfte dort viel langsamer als in der legalen Geschäftswelt.

Die gefallenen Preise der meisten im russischen Untergrund angebotenen Produkte und Dienste bedeuten aber nicht, dass die Geschäfte der Cyberkriminellen schlecht laufen. Im Gegenteil, der Markt wächst und das Angebot wird vielfältiger. Wie legale Geschäftsleute auch automatisieren die Cyberkriminellen Prozesse und senken damit die Kosten und Preise für die Produkte und Dienste. Die „Boutique“-Angebote bleiben kostspieliger, denn für ihre Entwicklung sind Spezialwissen und Kenntnisse nötig, die nur wenige böswillige Akteure haben. Es gilt zu beachten, dass solange aus den Angeboten Profit zu schlagen ist, Cyberkriminelle diese anbieten werden, um sich und ihren „Kollegen“ das Leben zu erleichtern.

Methoden für das Sammeln von Daten über den Untergrundmarkt

Trend Micro sammelt seit 2009 Daten über die Produkte und Services im Untergrundmarkt und hat diesen Prozess über den Einsatz von selbst entwickelten Werkzeugen stetig verbessert. So verläuft das Sammeln der Daten vollständig automatisiert ab, und lediglich die Nachbereitung wird per Hand durchgeführt. Beispielsweise geht es um das Vereinheitlichen von Informationen wie Produkt- oder Service-Preise. Auch sammelt das Team für mögliche forensische Ermittlungen Spitznamen, E-Mail-Adressen, ICQ-Nummern und Skype-Infos.

Die Sicherheitsforscher teilen die gesammelten Infos in 33 Gruppen (siehe Anhang) ein, die auf Ähnlichkeiten zwischen den Daten beruhen. Sie kombininieren zudem Daten, die miteinander in Beziehung stehen, weil die Kriminellen häufig Details über ihr Warenangebot in mehreren Foren gleichzeitig veröffentlichen. Einige der Waren passen in mehrere Kategorien. Beispielsweise wird bösartiger Verkehr unter Pay-per-Install (PPI)-Services, Verkehr (d.h. mit dem Ziel des Wiederverkaufs) und Blackhat Search Engine Optimization (SEO)-Dienste geführt. Diese nicht restriktive Kategorisierung bietet den Sicherheitsforschern mehr Flexibilität bezüglich der Korrelation der Daten.

Verheinheitlichen von Preisen

Das Forschungspapier zum russischen Untergrundmarkt aus dem Jahr 2012 hatte zu verschiedenen Diskussionen bezüglich der Inkonsistenz der Preise geführt. Die Erfahrung lehrt, dass die Preisspannen nicht nur aufgrund der breiten Vielfalt der vorhandenen Produkt- und Serviceoptionen entstehen, sondern auch durch die Unterschiede in der Qualität und Quantität.

Der Untergrundmarkt lässt sich beispielsweise mit dem Automobilmarkt vergleichen. Der Preis für ein Auto kann zwischen Tausenden und Millionen Dollar liegen. Die Höhe des Preises hängt zu einem guten Teil von der Qualität des Autos ab. Je seltener das Auto und je besser seine Qualität ist, desto teuerer wird es. Das gleiche gilt für die Waren im Untergrundmarkt. Liegt der preisgünstigste Virtual Private Network (VPN)-Dienst bei etwa 15 $ und der teuerste um die 135 $, so wäre der Durchschnittspreis etwa 75 $. Die in dieser Studie genannten Preise beruhen auf der Analyse der gesammelten Daten.

Produkt oder Service

Die Autoren der Studie klassifizieren eine Ware als „Produkt“, wenn der Käufer nach dem Erwerb des Werkzeugs bei einem Angriff alles selbst durchführen muss. Für einen Botnet-Angriff etwa kann er ein Botnet-Kit (d.h. ein Produkt) erwerben, das verschiedene Module, Plugins usw. umfasst. Mietet er jedoch ein Botnet, so fällt diese Transaktion unter „Services“, denn der Kunde muss sich um den Betrieb und die Wartung des Botnets nicht kümmern. Er kann einfach die Informationen vom Besitzer sammeln und diese in seinem Angriff nutzen. Im legalen Computermarkt lässt sich Microsoft™ Office® als Produkt bezeichnen, während Office 365 unter die Kategorie Service fällt. Um ersteres zu nutzen, muss der Käufer die Software installieren und eine Lizenz dafür kaufen. Letzteres hingegen kann der Käufer auf jedem Gerät nutzen, solange er Zugang zum Service hat.

Charakteristiken des russischen Untergrundmarkts

Den russischen cyberkriminellen Untergrund gibt es seit 2004, und er diente den Cyberkriminellen als Ort für den Informationsaustausch mit „Kollegen“. Zu den größten Foren gehörten zloy.org, DaMaGeLaB und XaKePoK.NeT. Als das Handelsvolumen zunahm, wurden die Untergrundforen zu idealen Geschäftsplätzen und Plattformen für das Anpreisen von kriminellen Waren. Die Plattformen dienten als Marketinginstrumente, um Crimeware zu Geld zu machen. Der Untergrundmarkt wandelte sich langsam zu einem Makrtplatz für alle Arten von Produkten und Services, die Cyberkriminellen als Hilfsmittel für die Ausführung ihrer bösartigen Vorhaben dienten.

Der russische Untergrundmarkt orientiert sich an den allgemeinen Prinzipien des Handels und Informationsaustauschs. Es war der erste Markt, der Crimeware an Cyberkriminelle lieferte und ihnen damit eine Alternative zur Erstellung von eigenen Werkzeugen für die Angriffe bot. Dieser Untergrundmarkt ist auch durch spezialisierte Angebote gekennzeichnet. Das bedeutet, dass ein Einzelner oder eine Gruppe nur Produkte oder Dienste anbietet, in deren Entwicklung beziehungsweise Ausführung sie richtig gut sind, etwa lediglich Dateiverschlüsselungsdienste, Werkzeuge für Distributed Denial-of-Service (DDoS) oder Traffic Direction Systems (TDSs).

Jeder Markt hat seine eigene Spezialität. Der russische beispielsweise ist auf den Verkauf von TDSs und Dienste für die Umleitung von Verkehr sowie für PPI spezialisiert. Insbesondere verkehrsbezogenee Produkte und Services entwickelten sich zum Eckpfeiler der gesamten russischen Schadsoftwareindustrie. Der Erwerb von Webverkehr kann nicht nur die Zahl der potenziellen Opfer erhöhen, sondern das Durchforsten des Verkehrs in den Botnet C&C-Servern kann sich auch als hilfreich erweisen, um nützliche Informationen für gezielte Angriffe zu finden.

Käufer und Verkäufer treffen einander vornehmlich in Untergrundforen. Käufer prüfen dort die Reputation der Verkäufer (falls diese Qualitätsprodukte und -dienste verkaufen), sehen sich das Angebot an und wie die Verkaufsdeals laufen. Um die Sicherheit sowohl der Verkäufer als auch der Käufer zu gewährleisten, nutzen sie Treuhänder oder „Garanten“, die das Geld der Käufer aufbewahren, bis der Einkauf abgeschlossen ist. Dieses Vorgehen schützt die Verkäufer, denn die Treuhänder stellen sicher, dass die Käufer das Geld besitzen, um die Produkte und Dienste zu bezahlen. Sie testen auch die Ware, um sicherzugehen, dass der Käufer das bekommt, wofür er bezahlt hat und nicht einer betrügerischen Werbung aufgesessen ist. Beim Handel mit gestohlenen Kreditkarteninformationen etwa prüft der Treuhänder mehrere Nummern auf ihre Legalität, bevor er dem Verkäufer das Geld aushändigt. Treuhänder erhalten für ihre Dienste üblicherweise 2 bis 15% des Verkaufspreises.

Die Zahl der russischen Untergrundforen ist jedes Jahr gestiegen. Es gibt natürlich auch eine gewisse Fluktuation, doch die bekanntesten wechseln nur gelegentlich den Hosting Service Provider und die Domänennamen, doch halten sie ihre loyalen Mitglieder. Die beliebtesten Foren wie verified.su und ploy.org zählen zwischen 20.000 und mehreren Hundert Mitgliedern.

Forumsmitglieder nutzen alle möglichen Tricks (z.B. VPNs, SOCKS-Proxies oder das TOR-Netzwerk), um ihre GeoIPs zu verschleiern, dennoch müssen sie über eindeutige Spitznamen und ICQ-Nummern identifiziert werden, um von anderen unterschieden werden zu können. So bleiben sie anonym und doch erkennbar.

Produkte

Trojaner

Ein Trojaner [Трояны], kurz für ein “trojanisches Pferd”, ist ein Stück Schadsoftware, das sich als legales Computerprogramm oder Anwendung tarnt.[4] Trojaner Spyware, eine Variante davon, stellt Malware dar, die speziell auf den Diebstahl von Nutzerdaten zugeschnitten ist. Spyware entwendet Informationen wie ICQ-Passwörter, Kontaktlisten, vertrauliche Dokumente, Bankkontodaten und so weiter. Es gibt sie auch als Keylogger, die die Tastenanschläge der Opfer aufzeichnen, um deren Online-Kontenanmeldedaten zu bekommen.[5] Zugangsdaten für Foren und soziale Netzwerke sind die am meisten nachgefragten Güter im Untergrund. Das liegt höchstwahrscheinlich daran, dass die Nutzer in sozialen Medien praktisch alles über sich preisgeben. Das bedeutet, dass der Zugang zu Konten in sozialen Medien Cyberkriminellen auch den Zugriff auf die anderen Konten der Opfer eröffnen, vor allem, wenn naive Nutzer dieselben Zugangsdaten für alle ihre Konten verwenden.

Cyberkriminelle setzen gestohlene ICQ-Nummern ein, um Spam zu verteilen oder Systeme zu “fluten”.Gestohlene File Transfer Protocol (FTP)-Konteninformationen wiederum werden für Blackhat SEO-Zwecke verkauft und genutzt.[6]

Exploits und Exploit Bundles

Exploits [Сплоиты], auch als “sploits” bekannt, sind Programme oder noch häufger Skripts, die Schwachstellen in Programmen oder Anwendungen ausnützen.[7] Die am häufigsten vorkommenden Exploits sind Browser-Exploits, die das Herunterladen von bösartigen Dateien ermöglichen. Exploits schleusen Code auf den Computer eines Opfers ein, der dann eine bösartige Datei herunterlädt und ausführt.

Beispielsweise bewirkt ein Exploit-Angriff einen Integer Buffer Overflow in der setSlice-Methode in der WebViewFolderIcon ActiveX® Komponente.[8] Mithilfe einer speziell aufgesetzten Webseite oder E-Mail kann ein Remote-Nutzer den Hauptspeicher eines Computers korrumpieren und beliebigen Code ausführen. Wenn jemand einen angreifbardn Brower benutzt, um auf eine Webseite zu gehen, in die der Exploit eingebettet ist, wird dieser Code ausgeführt.

Exploits werden üblicherweise auf Hosting Server installiert. Ein Exploit Bundle ist ein spezielles Skript, meistens in PHP geschrieben, das mehrere Exploits miteinander kombiniert. Der Einsatz eines Bundles ist effizienter als der individueller Exploits. Üblicherweise werden Bundles entweder als “intelligent” oder “nicht intelligent” klassifiziert.

4 Trend Micro Incorporated. (2014). Threat Encyclopedia. “Trojan.” Last accessed February 6, 2014, http://about-threats.trendmicro.com/us/malware/trojan.
5 Trend Micro Incorporated. (2014). Threat Encyclopedia. “Keyloggers.” Last accessed February 6, 2014, http://about-threats.trendmicro.com/us/glossary/k.
6 Ryan Flores. (November 2010). “How Blackhat SEO Became Big.” http://www.trendmicro.co.uk/media/misc/blackhat-seo-became-big-research-paper-en.pdf.
7 Trend Micro Incorporated. (2014). Threat Encyclopedia. “Exploit http://about-threats.trendmicro.com/us/glossary/e.
8 MITRE Corporation. (2014). CVE Details. “Vulnerability Details : CVE-2006-3730.” http://www.cvedetails.com/cve/CVE-2006-3730/.

Ein nicht intelligentes Exploit Bundle lädt einfach alle Exploits im Bundle gleichzeitig herunter, unabhängig davon, welchen Browser ein Opfer nutzt. Damit ist es keine sehr effiziente Lösung, denn die Ausführung mehrerer Exploits in einem Bundle kann mehr schaden als nützen. Die Routinen eines Exploits könnten sich mit anderen in die Quere kommen. Nicht intelligente Bundles sind generell billiger als intelligente.

Intelligente Bundle stellen erst fest, welche Browser- und welche Betriebssystemversion ein Opfer nutzt, bevor sie die entsprechenden Exploits herunterladen. Haben sie kein Exploit für das entsprechende Betriebssystem oder den Browser des Opfers, so laden sie nichts herunter.

In der Regel sind Exploit Bundles verschlüsselt, um der Entdeckung durch Sicherheitssoftware zu entgehen. Bundle-Entwickler versuchen auch, ihren Exploit-Quellcode zu verschleiern, damit Opfer nicht merken, dass der Code auf Websites läuft. Jedes Bundle kann sich auch normalerweise Statistiken holen (z.B. ein Mechanismus für das Aufzeichnen der Besucherzahl, ihrer Betriebssystemversionen, ihrer Browserversionen usw.).

Die Reichweite eines Exploits ist ein Kriterium für seine Effizienz – der Anteil von Nutzern, auf deren Computer der Exploit arbeitet zu der Gesamtzahl von Nutzern, die eine Seite mit dem eingebetteten Exploit besucht haben. Das heißt, wenn 1000 Nutzer eine Exploit-infizierte Seite besuchen und die Computer von 200 Nutzern werden erfolgreich mit einem Trojaner verseucht, so beträgt die Reichweite des Exploit (200 / 1.000) * 100 oder 20%.

Cross-Site Scripting (XSS)-Exploits sind im Untergrundmarkt ebenfalls verfügbar. XSS-Sicherheitslücken werden ausgenützt, wenn ein üblicherweise auf einer bösartigen Site eingebettetes Skript in der Lage ist, mit dem Inhalt auf einer anderen Site oder in einer lokalen HTML-Seite zu kommunizieren – daher auch der Name. Anders als in anderen Angriffen nutzen Hacker für XSS-Angriffe anfällige Server als Mittler, um Besucher der verseuchten Websites anzugreifen, und zwingen deren Browser bösartige Skripts auszuführen.

Danach beginnt das Skript, Befehle von einer Remote-Quelle zu empfangen, um so den Browser eines nichtsahnenden Opfers zu kontrollieren, während die erforderlichen Aktionen durchgeführt werden. Ein Skript kann lokal auf einem System aufgerufen werden oder inaktiv auf einem kompromittierten Webserver liegen, bis die betroffene Maschine einen Aufruf an die infizierte Webseite absetzt. Das Skript aktiviert sich dann auf der Maschine des Nutzers und startet die bösartigen Aktivitäten.

Um erfolgreich zu sein, müssen XSS-Angriffe mehrere Kriterien erfüllen – die Nutzung eines nicht ausreichend gesicherten Browsers, der den Ursprung eines Skripts nicht mit den von diesem geforderten Berechtigungen abgleicht, und eine nicht sorgfältig geschriebene Webseite, die Dateneingaben mangelhaft prüft. Social Engineering wird häufig dazu genutzt, um potenzielle Opfer dazu zu bringen, einen Link auf eine Seite anzuklicken, in der bösartiger Code eingebettet ist.

Die Mehrheit der XSS-Angriffe zielt auf Session Cookies von Opfern – Dateien, die jedesmal, wenn der Nutzer eine Website besucht, in den Systemen gespeichert werden. Der Diebstahl von Cookies ermöglicht es Hackern, die Identität von Nutzern anzunehmen und in ihrem Namen Aktionen auszuführen. Cookies werden über die Ausführung von Befehlen im bösartigen Skript an die Angreifer übermittelt. Ein erfolgreicher XSS-Exploit kann seine Opfer daran hindern, auf wichtige Daten zuzugreifen und sie dem Identitätsdiebstahl aussetzen. Das Kapern von Sitzungen ermöglicht es dem Skript-Besitzer, jede Art von Aktivität durchzuführen, die der wahre Besitzer des Kontos auch ausführen kann, so etwa das Lesen und Löschen von E-Mails, Durchführung von Finanztransaktionen und Veröffentlichen in sozialen Medien.

XSS-Exploits lassen sich auch für den Datendiebstahl aus Formularen nutzen. Sie sind entweder „aktiv“ oder „passiv“. Ein passiver XSS-Exploit benötigt die direkte Teilnahme eines Opfers, etwa das Anklicken eines bösartigen Links. Deshalb sind Social Engineering sowie Tricksereien gefragt.

Ein aktiver XSS-Exploit wiederum benötigt keine weitere Aktion vonseiten des Opfers. Es reicht, wenn ein Opfer eine XSS-verseuchte Webseite öffnet, damit der bösartige Code automatisch ausgeführt wird. Dieser Automatisierung wegen sind aktive XSS-Exploits auch teurer.

Rootkits

Ein Rootkit [Руткиты] ist ein Programm, das bestimmte Elemente vor anderen Programmen oder dem Betriebssystem versteckt (z.B. Dateien, Prozesse, Windows® Registry-Einträge, Speicherbereiche, Netzwerkverbindungen etc.).[9] Rootkits können Prozesse, Registry Keys und andere Beweise für das Vorhandensein von bösartiger Software auf einem Computer verstecken. Unter Windows laufen alle Anwendungen in Ring 3, das System und die Treiber jedoch in Ring 0. Programme, die in Ring 0 laufen besitzen viel größere Fähigkeiten. Doch es ist nicht immer möglich, von Ring 3 zu 0 zu wechseln.[10] Aus diesem Grund gibt es zwei Rootkit-Typen – diejenigen, die auf Anwendungs-Level arbeiten und diejenigen, die auf Kernel-Level aktiv werden.

Application Programming Interface (API)-Funktionen ermöglichen die Kommunikation zwischen Programmen und einem Computer. Ein API besteht aus einer Reihe von Funktionen, die darauf zugeschnitten sind, den Nutzer auf den Kernel eines Computers auf Anwendungsebene zugreifen zu lassen. Will ein Programm eine Dateienliste in einem Verzeichnis ansehen, so muss es eine Reihe von API-Funktionen aufrufen. Schadsoftware verbirgt Dateien etwa, indem sie API-Funktionsaufrufe abfängt und ändert. Rootkits sind eine seltene Commodity im Untergrundmarkt. Doch gelegentlich gibt es Hinweise auf Rootkit-Verkäufe.

Verkehr

Verkehr [Трафф] bezieht sich auf einen Besucherstrom auf einer bestimmten Website. Das Verkehrsaufkommen bezeichnet die Zahl der Besucher (d.h. einmalig oder nicht) auf einer Site in einer bestimmten Zeitspanne. Es gibt mehrere Verkehrsquellen, einschließlich gehackter Websites, solcher auf Whitelists und Spam-Verteilern.

Um Verkehr zu erzeugen, kann eine Website gehackt werden, indem ein iframe in eine der Seiten eingefügt wird. Ein iframe, auch als „Inline Frame“ bekannt, ist versteckt, und Besucher einer gehackten Site werden ohne ihr Wissen automatisch auf die Webseiten des Hackers umgeleitet. Damit erzielen die Hacker viel Verkehr, den sie dann entweder verkaufen oder für die eigenen bösartigen Zwecke nutzen. Über den Erwerb von Vekehr können Cyberkriminelle das SEO-Ranking ihrer Sites verbessern und damit landen sie auf höheren Plätzen bei den Suchergebnissen und erreichen eine höhere Zahl an möglichen Opfern.

9 Threat Encyclopedia. “Rootkits.” http://about-threats.trendmicro.com/us/glossary/r.
10 Wikimedia Foundation, Inc. (February 14, 2014). Wikipedia. “Ring (Computer Security).” http://de.wikipedia.org/wiki/Ring_%28CPU%29

Verkehr kann inhaltlich unterschiedlich sein, abhängig von der Art der Website, von dem er kommt. Geschäftsverkehr ist am wertvollsten, denn Besucher von Geschäfts-Sites haben im allgemeinen Geld. Damit sind ihre Downloads meist profitabler für Hacker. Pornografischer Verkehr ist ebenfalls zu von Bedeutung, auch wenn er weniger wertvoll ist, doch sind die Besucherzahlen höher.

Verkehr wird häufig nach den Ländern der Besucher klassifiziert. Für Verkehr aus Australien, den Vereinigten Staaten, Großbritannien, Deutschland und Italien gibt es die höchste Nachfrage, weil es sich in erster Linie um Geschäftsverkehr handelt. Auch Verkehrsmischungen werden verkauft.

Verkehr für Blackhat SEO-Zwecke erhöht die Zahl der Besucher einer ausgewählten Website. Der Verkehr wird über ein TDS verwaltet.[11] Cyberkriminelle verwenden TDSs, um den Verkehrstypus zu bestimmen, der ihnen dabei hilft, Nutzer auf eine bestimmte bösartige Site zu leiten und die richtigen bösartigen Payloads für bestimmte Systeme zur Verfügung zu stellen.

Crypter

Dateien werden in erster Linie deshalb verschlüsselt, um verseuchte Dateien oder Schadsoftware vor Sicherheitslösungen zu verbergen. Cyberkriminelle nutzen verschiedene Verschlüsselungswerkzeuge und Techniken. Je effizienter die Verschlüsselungstechnik desto teurer ist sie. Eine der wichtigsten Komponenten eines Crypters ist der so genannte „Crypter Stub“, ein Code-Teil, das zum Entschlüsseln von bösartigem Code verwendet wird.

Crypters lassen sich in “statische” oder “polymorphe” einteilen. Ein statischer Crypter Stub wird als separates Programm verkauft, an welches die verschlüsselte Datei gebunden ist. Wird der Crypter gestartet, so wird die Datei extrahiert, entschlüsselt und ausgeführt. Einige Crypter schreiben die Datei nicht auf die Festplatte, sondern starten sie aus dem Hauptspeicher. Diese Verschlüsselungsmethode ist jedoch nicht effizient. Statische Crypter nutzen verschiedene Stubs, um jede verschlüsselte Datei einzigartig zu machen. Aus diesem Grund erstellen die Autoren normalerweise einen separaten Stub für jeden Client. Ein Stub, den eine Sicherheitssoftware entdeckt, muss geändert, oder in Hacking-Terminologie „gesäubert“ werden.

Polymorphe Crypter sind fortschrittlicher. Sie nutzen die aktuellsten Algorithmen mit Zufallsvariablen, Daten, Schlüssel, Decoder usw. Deshalb erzeugt eine Input-Quelldatei nie eine Output-Datei, die mit dem Output einer anderen Quelldatei identisch ist. Die Autoren erreichen dies, indem sie einige Algorithmen nutzen, einschließlich von Shuffling Codeblöcken, und gleichzeitig die Fähigkeit einer bösartigen Datei beibehalten, Makros auszuführen und zu erzeugen.

11 Max Goncharov. (2011). “Traffic Direction Systems as Malware Distribution Tools.” http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_malware-distribution-tools.pdf.

Gefälschte Dokumente

Anbieter von gefälschten Reisepässen und anderen Dokumenten tummeln sich ebenfalls im russischen Untergrundmarkt.

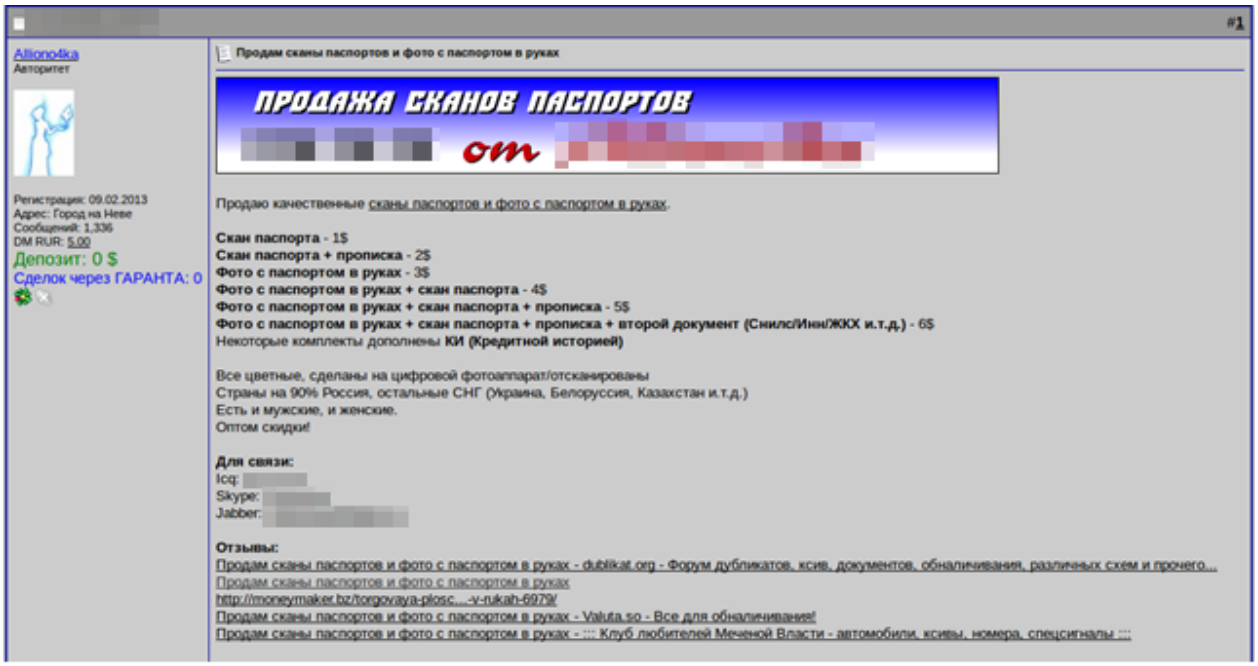


Bild 1: Sites, die gefälschte russische Reisepässe und solche aus dem Commonwealth of Independent States (CIS) verkaufen

Gestohlene Kreditkarten- und andere Zugangsinformationen

Auch diese Art von Informationen werden im Untergrundmarkt angeboten.

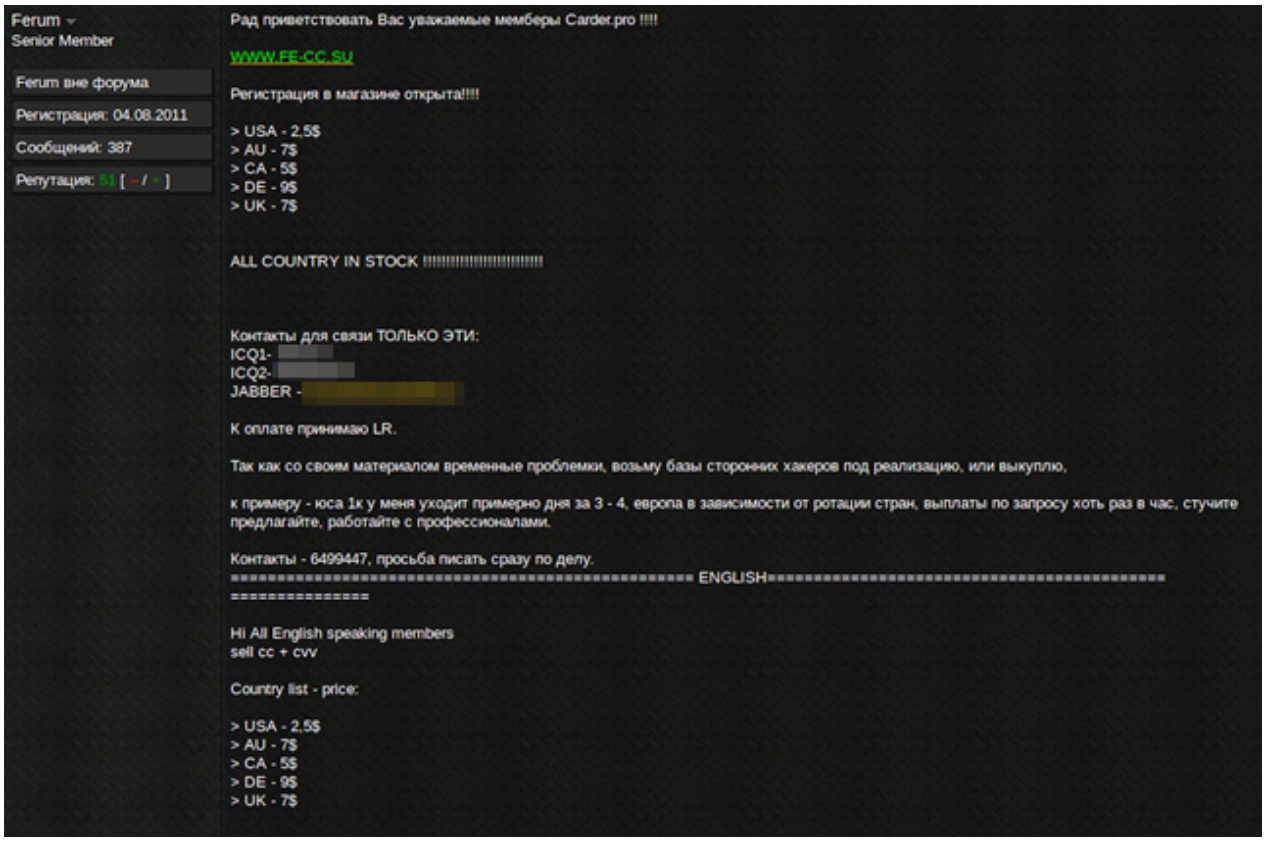


Bild 2: Site, die gestohlene Kreditkarten-Zugangsinformationen verkauft, doch lediglich an registrierte Mitglieder.

Services

Dediziertes Server-Hosting

Ein dedizierter Server [Дедики] ist einer, den ein Nutzer mietet und nicht mit anderen gemeinsam nutzt. Er lässt sich für verschiedene bösartige Aktivitäten einsetzen, von Brute Force-Angriffen bis zum Handel mit gestohlenen Geldkarten (Carding). In den meisten Fällen benutzen die Mieter ihn als C&C-Server, C&C-Proxy-Schnittstelle oder als Ablagezone für Dateien, die verseuchte Maschinen hochladen.[12] Hacker greifen normalerweise über ein VPN auf dedizierte Server zu, um über Datentransfer-Verschlüsselung ihre Anonymität zu wahren. Diese dedizierten Server-Hosting-Dienste gehören zu den gefragtesten Angeboten im Untergrundmarkt. Sie werden zu verschiedenen Preisen bezogen, abhängig vom Land, von der Geschwindigkeit, ihren Hardware-Spezifikationen und ihrer Zuverlässigkeit.

12 U.S. Department of Justice. (June 26, 2012). The FBI: Federal Bureau of Investigation. “International Cyber Crime Takedown Targets ‘Carding.’”, http://www.fbi.gov/news/news_blog/international-cyber-crime-takedown-targets-carding.

Proxy-Server-Hosting

Ein Proxy-Server [Прокся] ist ein zwischengeschalteter Computer, der als „Stellvertreter“ oder Vermittler zwischen einem Computer und dem Internet fungiert. Proxy-Server dienen verschiedenen Zwecken, etwa der Beschleunigung der Datenübermittlung und dem Filtern des Verkehrs, doch Hauptzweck ist es, Anonymität zu gewährleisten – daher auch die Beliebtheit bei Hackern. Anonymität wird in diesem Fall damit erreicht, dass der Ziel-Server die IP-Adresse des Proxy-Servers zu sehen bekommt und nicht die des Hacker-Computers. Doch haben Hacker immer wieder festgestellt, dass trotz gegenteiliger Zusicherung durch die Betreiber auch bezahlte Proxy-Server Logs vorhalten und keine vollständige Anonymität liefern können. Zu den wichtigsten Proxy-Servertypen gehören HTTP/S, SOCKS und Common Gateway Interface Proxy (CGIProxy), auch bekannt als “Anonymizer”.[13]

VPNs

VPN-Technik wird dazu verwendet, um einen sicheren, verschlüsselten Tunnel auf einem Computer zu erzeugen, wenn dieser sich mit dem Internet verbindet und Daten übermittelt werden sollen. Hacker können damit alle Arten konventioneller Programme verwenden (z.B. ICQ, Skype, E-Mail oder Website-Administrationssoftware), um sicherzustellen, dass die Daten verschlüsselt bleiben, auch wenn sie übermittelt werden. Außerdem können sie den Anschein erwecken, dass die Daten nicht von der IP-Adresse des Hackers kommen, sondern von der des VPN Service Providers.

Wird kein VPN genutzt, so werden alle Aktionen, einschließlich Öffnen von Websites, mithilfe des gewählten Internet Service Providers (ISP) durchgeführt. Die Nutzung eines VPNs als Mittler hingegen ermöglicht es Hackern, alle Anfragen ans Internet und die ankommenden Daten zu verschlüsseln. VPNs schützen die Daten und erhalten die Anonymität, indem die Anfragen für Online-Ressourcen und die Datenübermittlung unter den IP-Adressen der VPNs laufen.

Ein VPN schützt die Daten, weil es den gesamten ankommenden und nach außen gehenden Verkehr vom angeschlossenen Computer verschlüsselt. Auch können Hacker zwei IP-Adressen verwenden, sodass ein Provider den Verkehr nicht aufzeichnen kann.

Pay-per-Install

Das PPI-Service- Geschäftsmodell [Залив с отстуком] sieht vor, dass Werbetreibende demjenigen, der kostenlose Anwendungen mit Adware bündelt, jedesmal einen Betrag zahlen, wenn diese Anwendung installiert wird.[14] In einem PPI-Angriff bedeutet „installieren“, das Herunterladen und Öffnen einer Datei auf dem Computer eines Opfers. Die Downloads können als Exploit Bundle vorhanden sein oder von einem Botnet stammen. Bei einem solchen Angriff wird der Computer eines Opfers infiziert, wenn er mit einem angreifbaren Browser eine Site aufsucht, die einen Exploit hostet. Der Browser lädt dann ein bösartiges Skript herunter und führt dieses aus. Dies ist eine der beliebtesten Methoden, um Schadsoftware zu verteilen (am häufigsten Trojaner).

13 Wikimedia Foundation, Inc. (February 12, 2014). Wikipedia. “Proxy Server” http://de.wikipedia.org/wiki/Proxy_%28Rechnernetz%29

14 Kyle Wilhoit. (February 19, 2013). TrendLabs Security Intelligence Blog. “Business Models Behind Information Theft” http://blog.trendmicro.com/trendlabs-security-intelligence/business-models-behind-information-theft/

Download-Dienstleistung ist ein häufiges Angebot. Im Fall des PPI-Geschäftsmodells liefert ein Kunde die bösartige Datei, die der Service Provider dann verteilt. Diese Dienstleistung wird üblicherweise auf der Basis des Ziellands angeboten. Das bedeutet, die PII-Bewertung eines Landes wird von der Wahrscheinlichkeit bestimmt, dass eine bösartige Datei von einem Bürger dieses Staats oder einem Unternehmen heruntergeladen und geöffnet wird. Cyberkriminelle können auf diese Weise an eine Vielfalt von vertraulichen Informationen (etwa Kreditkartennummern) kommen und unter Umständen sogar Root-Zugriff auf Unternehmens-Sites oder –Netzwerke erlangen.

Zwei grundlegende Arten von Aktivitäten gibt es im Markt der Download Services: Entweder übergibt der Kunde dem Service Provider eine bösartige Datei zur Verteilung oder ein Provider bietet entsprechende Dienste für Interessierte. Auch existieren Partnerprogramme für beide Arten.[15]

Ein Verkehrs-Converter wandelt diesen in Downloads um. Downloads werden mittlerweile pro 1.000 Installationen verkauft. Die Packages umfassen üblicherweise zwei Komponenten – Verkehr und ein Exploit Bundle. Der Verkehr an sich ist wertlos. Er muss erst in Downloads umgewandelt werden, um von Nutzen zu sein. Beispielsweise können 1.000 einzigartige Besucher in 24 Stunden bis zu 50 Downloads generieren.

Um Downloads zu erhalten, nutzen Hacker Exploits [сплоиты] oder Skripts, mit denen sie über eine Sicherheitslücke in einem Programm (z.B. in einem Browser) eine gewünschte Aktion durchführen können, sowie Exploit Bundles oder Exploit-Sammlungen, die durch ein einziges Skript zusammengehalten werden. Die Reichweite eines Exploit Bundles ist gleich der Verkehrsmenge, die in Downloads umgewandelt wird. Doch ist es unmöglich, die genaue Reichweite aufgrund des Verkehrs von nur 1.000 Hosts zu bestimmen. Es bedarf zumindest 20.000 Hosts, um eine genauere Messung durchzuführen.

Bild 3: Funktionsweise von TDSs

Die Verwaltung eines Exploit Bundles bedarf auch eines Hosts. Dafür nutzen Hacker zumeist dedizierte Server [дедики] oder bulletproofe Hosting Services [абузоустойчивый], um den Verkehr [залить] auf eine mit einem Exploit versehene Webseite zu lenken und Downloads zu erhalten. Die "Zutaten" für Downloads (Verkehr, Exploits und Hosts) werden einzeln verkauft.

Gemischter Download-Verkehr (z.B. europäischer, asiatischer oder ein globaler Mix) wird ebenfalls häufig angeboten.

15 Paul Ferguson. (October 27, 2009). TrendLabs Security Intelligence Blog. "'What the Experts Still Don't Know' - The Thriving Cybercrime Underground." http://blog.trendmicro.com/trendlabs-security-intelligence/what-the-experts-still-dont-know-the-thriving-cyber-crime-underground/.

Die Bedeutung des Eigners bestimmt maßgeblich den Wert des Verkehrs. Je größer die Organisation, zu der er gehört, desto teuerer ist er. Der verkaufte Geschäftsverkehr kommt hauptsächlich aus den USA und Australien. Da der meiste US-Verkehr pornografischer Natur ist, gilt der australische qualitativ höherwertig und wird häufiger für Carding-Zwecke genutzt.

Denial-of-Service-Angriffe

Denial-of-Service (DoS)- [ДДоС] und DDoS-Angriffe gehören zu den Hacking-Attacken auf Computer. Dabei erzeugen sie Bedingungen, in denen legalen Computernutzern der Zugriff auf ihre eigenen Systemressourcen verweigert wird. Die Hacker dahinter versuchen nicht, illegal in geschützte Computer einzubrechen oder Daten zu stehlen bzw. zu zerstören, sie wollen lediglich Websites oder Computer lahmlegen.

Ein DDoS-Angriff erzeugt eine Riesenzahl unechter Anfragen von einer Unmenge von Computern weltweit, die einen Zielserver überfluten. Als Ergebnis wendet der Server alle seine Ressourcen darauf auf, die Anfragen zu erledigen, und ist damit nicht länger erreichbar. Die Nutzer der Computer, die gefälschte Anfragen schicken, sind meist ahnungslos. DDoS-Software wurde ursprünglich nicht für bösartige Zwecke entwickelt, sondern etwa dafür, um die Durchsatzkapazität von Netzwerken und ihre Toleranz gegenüber externer Last zu erforschen. In einem solchen Fall ist ein falsch strukturiertes Internet Control Message Protocol (ICMP)-Paket am effizientesten, denn es erfordert eine Menge Verarbeitungsleistung. Nachdem festgestellt wurde, was an diesem Paket fehlerhaft ist, wird ein entsprechendes Antwortpaket an den Absender geschickt. Somit ist das Ziel, nämlich ein Netzwerk zum Stottern zu bringen, erreicht.

DDoS-Angriffe benötigen die Nutzung von speziell aufgesetzten Bots und Botnetzen. Um einen DDoS-Angriff anzustoßen, muss ein Hakcer erst auf einen Zielcomputer zugreifen. Dann installiert er dort einen Dienst mit seinem DDoS Botkit und wiederholt dies auf mehreren anderen Maschinen, die er damit zu Zombies macht. Dann startet er das Masterprogramm, das auch von einem DDoS-Botkit kommt auf seiner oder einer Remote-Maschine und initiiert so einen Angriff von einer ausgewählten IP-Adresse. Das Masterprogramm befiehlt allen Daemons, das ausgewählte Opfer anzugreifen, etwa um eine bestimmte Website lahmzulegen.

Spamming

Spamming [Спам] bezieht sich auf die Massenverteilung von E-Mails. Spam kann ein Thema haben oder auch nicht. Spam mit Thema zielt auf eine bestimmte Gruppe (etwa Interessenten für Dating, für Jobsuche oder pornografische Websites). Eine Schlüsselrolle dabei übernimmt eine Datenabank mit entsprechenden Empfängern.

Spam ohne Thema wiederum wird an praktisch jedermann versendet. Es gibt kein bestimmtes Ziel. Wichtig ist die Menge der Empfänger.

Spam lässt sich auch nach dem Verteilermedium kategorisieren – E-Mail, Instant Messaging, soziale Netzwerek oder SMS. Jedes Medium erfordert seinen eigenen Satz von Empfängern und Ressourcen zur Verteilung.

Der Markt für Spamming-Dienste ist bunt gemischt. Die Nachfrage nach Datenbank-, Forums- sowie soziale Netzwerkkonten ist am höchsten. Sie werden nach Interessen, Alter, sozialem Status usw. gefiltert, um möglichst viele Informationen zu den Personen in

den Datenbanken zu erhalten. Damit können die Spammer einfacher die für sie relevanten Ziele für die Aussendungen aussuchen. Datenbanken werden normalerweise nach Abschnitten verkauft, abhängig von der anvisierten Zielgruppe (z.B. Jobsuchende).

Auch E-Mail-Anmeldedaten, die für die Spamverteilung benötigt werden, sind erhältlich. Zusätzlich können Spammer Verteilungs-Tools und/oder Programme für Instant Messaging- und SMS-Verteilung erwerben. Werkzeuge für das Spamming von Foren und sozialen Netzwerken gibt es seltener. Die Preise hängen von der Funktionalität, Verteilungsgeschwindigkeit und anderen Kriterien ab.

Private Spamming-Services, die für die Verteilung von Nachrichten über eine Kunden- oder private Datenbank genutzt werden, sind teurer.

Flooding

Flooding stellt eine einfache Routing-Technik in Computernetzwerken dar, wobei eine Quelle oder ein Knoten Pakete über jeden nach außen gehenden Link schickt. Die Technik wird in DDoS-Angriffen angewendet, um einen Netzwerkdienst unerreichbar zu machen. Der Service wird mit einer Menge unvollständiger Server-Verbindungsanfragen geflutet. Aufgrund der vielen Anfragen ist der Server oder Host nicht mehr in der Lage, echte Anfragen gleichzeitig zu verarbeiten. Ein Flooding-Angriff füllt den Hauptspeicher-Buffer des Servers oder Hosts, und sobald dieser voll ist, können keine weiteren Verbindungen erstellt werden. Das Ergebnis ist ein DoS. Im Angebot sind einige Flooding-Services, vor allem für Anrufe und SMS, doch sind diese Offerten seltener. Ihr Hauptziel ist die Belästigung des Opfers.

Prüfen von Schadsoftware gegen Sicherheitsprogramme

Malware-Checking-Dienste dienen Cyberkriminellen dazu zu prüfen, ob ihre bösartigen Dateien von bekannten Sicherheitsprodukten entdeckt werden. Sie nutzen keine kostenlosen oder öffentlich erhältlichen Dienste wie VirusTotal oder VirSCAN, denn diese haben Verbindung zu den Sicherheitsanbietern. Trend Micro etwa bekommt von diesen Service Providern Muster der hochgeladenen Schadsoftware. Die Muster werden dann zu neuen Pattern verarbeitet.

Einer der beliebten Untergrund Checking Service Provider, Scan4You.net, prahlt auf seiner Website damit, dass man völlig sicher sein kann, dass die zur Prüfung eingereichten Dateien nicht an Antivirus-Datenbanken geschickt werden. „Alle Reporting-Systeme in unserer Version der Antivirus-Engines wurden deaktiviiert.“

Social Engineering und Account Hacking

Hacking bezieht sich auf den nicht autorisierten Zugriff auf Informationen, ohne die Nutzung von Software. Cyberkriminelle setzen Social Engineering ein, um die Nutzer dazu zu verführen, ihre Passwörter oder andere vertrauliche Informationen preiszugeben. Zu den klassischen Taktiken gehören Anrufe bei einem Unternehmen, um sicherzustellen, wer die erforderlichen Informationen hat, und dann den Administrator unter der Identität eines Mitarbeiters wegen eines „dringenden Zugriffsproblems“ anzurufen.

Reine Social Engineering-Services sind nicht sehr gefragt. Social Engineering erlaubt es Betrügern vor allem die E-Mail- und social Media-Konten von Opfern zu hacken oder Ahnungslose auf Phishing-Site zu locken.

Es werden mittlerweile drei Arten von Hacking-Diensten im russischen Untergrund angeboten:

Konten-Hacking-Services

Konten-Hacking [Взлом акков] ist eine weit verbreitete Fertigkeit unter Cyberkriminellen. Die Nachfrage nach dieser Art von Dienstleistung ist ebenfalls enorm, abzulesen an den Anzeigen dafür im Untergrund. Die am häufigsten vorkommenden Hacking-Ziele sind E-Mail-Konten und solche in sozialen Medien. Site- und Foren-Konten-Hacking wird seltener angeboten. Tatsächlich werden konkrete Aufträge üblicherweise separat in privaten Gesprächen ausgehandelt.

Brute-Forcing Services

Brute Forcing [Брут] stellt eine der ältesten Methoden dar, die Cyberkriminelle nutzen, um E-Mail- oder andere Konten (z.B. FTP, Telnet und ICQ) zu hacken. Sie erfordert einfach “das Erraten des Passworts“. Der Untergrund bietet dafür spezielle Programme an, die den Prozess automatisieren. Es bedarf lediglich der Compilierung und eines guten Wörterbuch-Feeds.

Die bekanntesten Programme sind Brutus und Hydra. Es ist sehr schwer, Konten über Brute Forcing zu hacken, weil das benötigte Passwort nicht unbedingt im genutzten Wörterbuch vorhanden ist. Auch kann der Vorgang ziemlich viel Zeit in Anspruch nehmen. Doch mit steigender Verarbeitungs-Power steigt die Nachfrage nach diesen Diensten wieder. Je schneller der Computer, desto mehr Passwörter kann das Programm prüfen. Einige Cyberkriminelle bieten auch Dienste für die Entschlüsselung von Hashes an.

Account Hacking über Social Engineering

Das Erraten von Antworten auf die so genannten “geheimen Fragen” ist ebenfalls relevant für das Hacken von E-Mail-Konten. Doch weil viele Fragen wie „Wo lebe ich?” oder “Was ist mein Lieblingsessen” als Prompt setzen, sollten sie ihr Passwort vergessen, ist die Aufgabe, die Antworten zu erraten, nicht sehr schwierig.

Cyberkriminelle Waren im russischen Untergrundmarkt

Die Tabelle zeigt die verschiedenen Produkte und Services, die im russischen Untergrundmarkt verkauft werden.

Produktangebote im russischen cyberkriminellen Untergrundmarkt			
Produkt	**Preise 2011**	**Preise 2012**	**Preise 2013**
Trojaner: • Phoenix • Adrenalin • Limbo • ZeuS (von Trend Micro als "ZBOT" erkannt) • SpyEye	 500 US$ 790 US$ 350 US$ 120 US$ 500 US$	 150 US$ Keine Daten Keine Daten 0 US$ 0 US$	 0 – 35 US$ Keine Daten Keine Daten 0 US$ 0 US$
Exploit Kit: • Eleonore Browser Exploit Kit • Phoenix Exploit Kit • eCore Exploit Pack	 700 US$ 600 US$ 1.000 US$	 Keine Daten 250 US$ Keine Daten	 Keine Daten 0 US$ Keine Daten
Verkehr: • PPI/1.000 Installationen USA • PPI/1.000 Installationen Europa • PPI/1.000 Installationen Asien	 190 – 400 US$ 240 – 340 US$ 220 – 400 US$	 120 – 340 US$ 100 – 400 US$ 120 – 190 US$	 50 – 130 US$ 40 – 170 US$ 90 – 200 US$
Crypter: • hauptsächlich statisch • Statisch mit Stub und Add-ons • Polymorph	 10 – 30 US$ 30 – 80 US$ 100 US$	 4 – 10 US$ 15 – 25 US$ 80 US$	 Keine Daten 10 – 30 US$ 65 US$
Proxy Server Host-Liste pro 300 IP-Adressen	3 US$	4 US$	6 US$
Gescannte gefälschte Dokumente: • Europäischer Pass • Russischer und andere CIS-Pässe	 2,50 US$ 2 – 5 US$	 1 US$ 1 – 5 US$	 1 US$ 1 – 2 US$

Produktangebote im russischen cyberkriminellen Untergrundmarkt			
Produkt	**Preise 2011**	**Preise 2012**	**Preise 2013**
Kreditkarten Zugangsdaten (pro Karte):			
• Amerikanisch	2,50 US$	1 US$	1 US$
• Australisch	7 US$	5 US$	4 US$
• Kanadisch	5 US$	5 US$	4 US$
• Deutsch	9 US$	7 US$	6 US$
• Britisch	7 US$	6 – 8 US$	5 US$

* Proxy Server Host-Listen wurden mit der Zeit immer teurer, weil die Proxy Hosting-Dienste von weniger VPN-Hosting-Services geliefert wurden

Serviceangebote im russischen cyberkriminellen Untergrundmarkt			
Produkt	**Preise 2011**	**Preise 2012**	**Preise 2013**
Dediziertes wasserdichtes Server-Hosting			
• Low-end	160 US$	100 US$	50 US$
• High-end	450 US$	160 US$	190 US$
• Virtual Private Server (VPS)	70 US$	40 US$	12+ US$
Proxy-Server-Hosting (pro Tag):			
• HTTP/S	2 US$	1 US$	1 US$
• SOCKS	2 US$	2 US$	2 US$
VPN:			
• Mit einem Ausgangspunkt	8 – 12 US$	Keine Daten	Keine Daten
• Mit unbegrenzten Ausgangspunkten und Verkehr	40 US$	38 US$	24 US$
• Durchschnittspreis	22 US$	20 US$	15 US$
Umwandlung (PPI pro 1.000 Installationen):			
• Australischer Verkehr	300 – 500 US$	200 – 500 US$	120 – 600 US$
• U.K.-Verkehr	220 – 300 US$	No data	150 – 400 US$
• US-Verkehr	100 – 150 US$	100 – 250 US$	120 – 200 US$
• Europäischer Verkehr	90 – 250 US$	75 – 90 US$	50 – 110 US$
• Gemischter weltweiter	12 – 15 US$	10 – 17 US$	10 – 12 US$
• Russischer Verkehr	100 – 500 US$	100 – 190 US$	140 – 400 US$

Serviceangebote im russischen cyberkriminellen Untergrundmarkt			
Produkt	**Preise 2011**	**Preise 2012**	**Preise 2013**
DDoS Angriff: • Dauert 1 Stunde • Dauert 24 Stunden	 4 – 10 US$ 30 – 70 US$	 2 – 25 US$ 15 – 60 US$	 2 – 60 US$ 13 – 200 US$
Spamming (pro 10.000 Nachrichten): • Generisch (nutzt eine öffentliche Datenbank) • Beruht auf externer Mail- Datenbank • SMS • ICQ • Skype	 13 US$ 17 US$ 600 US$ 55 US$ Keine Daten	 8 US$ 14 US$ 300 US$ 15 US$ 110 US$	 4 – 5 US$ 13 US$ 100 US$ 4 – 9 US$ 86 US$
Flooding: • E-Mail (pro 10.000 Nachrichten) • Festnetzanschluss • SMS (pro 1.000 Nachrichten)	 30 US$ 32 US$ 15 US$	 3 US$ 23 US$ 10 US$	 2 US$ 25 US$ 8 US$
Malware-Prüfung gegen Sicherheits-software: • Tägliche Prüfung • Automatisches Re-Uploading, falls eine Malware entdeckt wurde • Prüfen gegen bösartige URL-Blacklists	 50 US$ 50 US$ 50 US$	 30 US$ 30 US$ 30 US$	 30 US$ 30 US$ 30 US$
Hacking: • Facebook-Konto • VK-Konto • Odnoklassniki-Konto • Twitter-Konto • Gmail-Konto • Mail.ru-Konto • Yandex.ru-Konto • Hotmail-Konto	 200 US$ 120 – 140 US$ 94 US$ 167 US$ 117 US$ 74 US$ 74 US$ 107 US$	 160 US$ 100 US$ 90 US$ 40 US$ 120 US$ 70 US$ 70 US$ 100 US$	 100 US$ 76 US$ 94 US$ Keine Daten 100 US$ 50 US$ 50 US$ 100 US$
Nachbesserung gefälschte Dokumente	15 – 20 US$	10 – 20 US$	5 – 28 US$

Schlussfolgerungen

Der russische Untergrund wechselt ständig die Ziele und erlangt Zugang zu besseren und moderneren Technologien. Deshalb müssen Sicherheitsanbieter auch immer effizientere und bessere Lösungen zum Schutz der Kunden und deren Assets zur Verfügung stellen.

Das Forschungspapier hat gezeigt, dass die cyberkriminelle Wirtschaft genauso funktioniert wie jede andere legale. Es gibt Preisschwankungen, abhängig vom Angebot und von der Nachfrage. Der Unterschied zu legalen Geschäftsleuten jedoch besteht darin, dass die Cyberkriminellen ihre Identitäten geheim halten und soweit wie möglich auch die Spuren ihrer „Geschäftstransaktionen" beseitigen müssen.

Die Geschäfte im russischen Untergrund laufen gut, auch wenn die Preise der meisten Produkte und Dienstleistungen gefallen sind. Das kann sogar bedeuten, dass der Markt wächst, denn es kommen immer mehr Warenangebote hinzu. Cyberkriminelle automatisieren ihre Prozesse und können daher ihre Preise senken. Allein die „Boutique"-Angebote bleiben hochpreisig, weil darin viel Spezialwissen und Fertigkeiten stecken.

Diese Studie behandelt lediglich die grundlegenden Tools und Technologien, die Cyberkriminelle erzeugen und für die Verbesserung ihrer Geschäfte einsetzen. Auch liefert das Forschungspapier nur Preis-Momentaufnahmen aus den Untergrundforen, um ein allgemeines Bild der russischen Untergrunds zu zeichnen und den Vergleich zur wirklichen Geschäftswelt zu ziehen.

Wichtig ist es, im Hinterkopf zu haben, dass Cyberkriminelle so lange ihre Produkte und Dienste anbietern werden, solange sie daraus Profit ziehen können.

Anhang

Liste von cyberkriminellen Untergrundwaren, die Trend Micro nachverfolgt und überwacht

Produkte

- Datenbanken
- Exploits
- Fälschungen (z.B. Währungen etc.)
- Zugangsdaten für FTP-Konten
- Zugangsdaten für Online Gaming-Konten
- Ransomware
- Remote Access Trojaner (RAT)
- Rootkits

- Gescannte Dokumente
- Seriennummern
- Verkehr
- Trojaner
- Webshells

Services

- Missbrauch-Services
- Konten-Hacking
- Blackhat SEO
- Aktivitätsbezogene C&C-Server
- Carding
- Verschlüsselung
- DDoS
- Dediziertes Server-Hosting
- Electronische Bezahlung
- Geldwäsche
- Malware-Prüfung gegen Sicherheitssoftware
- Geldwäsche und Geldkurierdienste
- Verschleierung
- PPI
- Programmierdienste
- SMS-Betrug
- Social Engineering
- SOCKS Proxy-Server-Hosting
- Spamming
- VPN

Glossar

- **Account:** Акки [aki]
- **Botnet:** Ботнет [botnet]
- **Brute forcing:** Брут [brootforce or brutforce]
- **Cryptor:** Криптор [kriptor]
- **Dedicated server:** Дедики [Dediki]
- **DoS:** ДДоС [DDoS]
- **Exploit:** Сплоиты [sploiti]
- **Fraud:** Фрод [fraud] (i.e., any fraud kind: email, SMS, banking, etc.)
- **Joiner:** Склейка [skleyka]
- **Password brute forcing:** Подбор Паролей [podbor paroley]
- **PPI:** Залив [zaliv] or Пробив [probiv]
- **Proxy server:** Прокся [proksya]
- **Rootkit:** Руткиты [rootkit]
- **SOCKS 5:** Соксы [SOCKS 5]
- **Spam:** Спам [spam]
- **Traffic:** Траф [traf]
- **Trojan:** Трояны [Trojan]
- **Web inject:** Инжекты [inzhekti]

Über TREND MICRO

Trend Micro, der international führende Anbieter für Cloud-Security, ermöglicht Unternehmen und Endanwendern den sicheren Austausch digitaler Informationen. Als Vorreiter bei Server-Security mit mehr als zwanzigjähriger Erfahrung bietet Trend Micro client-, server- und cloud-basierte Sicherheitslösungen an. Diese Lösungen für Internet-Content-Security und Threat-Management erkennen neue Bedrohungen schneller und sichern Daten in physischen, virtualisierten und Cloud-Umgebungen umfassend ab. Die auf der Cloud-Computing-Infrastruktur des Trend Micro Smart Protection Network basierenden Technologien, Lösungen und Dienstleistungen wehren Bedrohungen dort ab, wo sie entstehen: im Internet. Unterstützt werden sie dabei von mehr als 1.000 weltweit tätigen Sicherheits-Experten. Trend Micro ist ein transnationales Unternehmen mit Hauptsitz in Tokio und bietet seine Sicherheitslösungen über Vertriebspartner weltweit an.

http://www.trendmicro.de/
http://blog.trendmicro.de/
http://www.twitter.com/TrendMicroDE

Securing Your Journey
to the Cloud

TREND MICRO DEUTSCHLAND GMBH

Central & Eastern Europe
Zeppelinstraße 1
85399 Hallbergmoos
Tel: +49 811 88990-700
Fax: +49 811 88990-799
www.trendmicro.com