# La cybercriminalità «finanziaria» che parla russo: ecco come funziona

Ruslan Stoyanov, Divisione per le Indagini sugli Incidenti Informatici

Sommario

[La cybercriminalità «finanziaria» che parla russo: ecco come funziona 0](#_Toc435443087)

[Introduzione 2](#_Toc435443088)

[Il quadro della situazione 3](#_Toc435443089)

[Struttura del mercato cybercriminale russofono 6](#_Toc435443090)

[«Assortimento» 6](#_Toc435443091)

[Il «mercato» del lavoro nell’ambito del cybercrimine finanziario 7](#_Toc435443092)

[Possibili varianti riguardo all’organizzazione di gruppi cybercriminali 11](#_Toc435443093)

[La suddivisione dei ruoli all’interno di un gruppo criminale di notevoli dimensioni 14](#_Toc435443094)

[Virus writer\Programmatore 15](#_Toc435443095)

[Tester 16](#_Toc435443096)

[Webmaster e programmatori web 16](#_Toc435443097)

[Distributori 16](#_Toc435443098)

[Hacker 17](#_Toc435443099)

[Amministratori di sistema 17](#_Toc435443100)

[Call service 17](#_Toc435443101)

[Prelevatori 18](#_Toc435443102)

[Capo del “drop project” 19](#_Toc435443103)

[I “drop project” 20](#_Toc435443104)

[Stuffer 22](#_Toc435443105)

[Organizzatore 22](#_Toc435443106)

[Fasi di realizzazione degli attacchi 22](#_Toc435443107)

[Conclusioni 24](#_Toc435443108)

[Informazioni aggiuntive riguardo alla Divisione per le Indagini sugli Incidenti Informatici istituita da Kaspersky Lab 25](#_Toc435443109)

Il vasto mercato cybercriminale russofono è ben conosciuto in tutto il mondo. Gli esperti di Kaspersky Lab monitorano l’underground russo dell’hacking sin dall'inizio della sua esistenza. Nel presente articolo esploreremo, in particolar modo, le modalità operative adottate dalla cybercriminalità russa che agisce nella sfera finanziaria.

## Introduzione

Il vasto mercato cybercriminale russofono è ben conosciuto in tutto il mondo. (Per russofoni, in tal caso, si intendono non solo i cybercriminali che risultano essere cittadini della Federazione Russa, ma anche quelli che risiedono in alcuni dei paesi limitrofi, facenti precedentemente parte del territorio dell’Unione Sovietica. Nella maggior parte dei casi a tali paesi vengono collegati l’Ukraina e gli stati baltici.) Tale notorietà poggia su due fattori principali: in primo luogo, l’elevato livello di attività dimostrato dai criminali informatici di lingua russa, spesso oggetto dell’attenzione dei mass media internazionali; in secondo luogo, essa è dovuta alla facile accessibilità di un considerevole numero di risorse web che sono servite, o che servono tuttora, quale piattaforma per le comunicazioni che intercorrono tra i rappresentanti di vari ambienti cybercriminali, se non da vera e propria “piazza” virtuale per la conclusione di affari o, come minimo, per la pubblicità di “servizi” e “prodotti” di vario genere, nonché per accese discussioni riguardo alla “qualità” degli stessi e ai relativi metodi di utilizzo.

Da quando tale mercato esiste, l’assortimento dei “prodotti” e dei “servizi” offerti attraverso di esso è progressivamente cambiato, risultando sempre più orientato verso gli attacchi informatici di natura finanziaria, peraltro condotti ad un livello sempre più alto. Nel corso degli anni, una delle tipologie di crimine più diffusa è stata (e lo rimane anche al momento attuale) il giro d'affari legato alla commercializzazione dei dati sensibili sottratti dai malintenzionati, inerenti, nella fattispecie, alle carte di pagamento. Con la comparsa dei negozi Internet e di ulteriori servizi online, per i quali si ricorre all’utilizzo di forme di pagamento elettronico, hanno conosciuto una larga diffusione gli attacchi DDoS e i cybercrimini finanziari, il cui scopo è costituito dal furto dei dati confidenziali relativi alle operazioni di pagamento eseguite dagli utenti, oppure dalla sottrazione illecita di cospicue somme di denaro direttamente dai conti bancari posseduti da privati e società.

Le “scorribande” che hanno preso di mira i portafogli elettronici degli utenti domestici e degli utenti corporate hanno avuto inizio con il trojan ibank (2006); sono in seguito comparsi, sulla scena del malware bancario, ZeuS (2007) e SpyEye (2009). Si sono poi aggiunti al famigerato gruppo di software nocivi Carberp (2010) e Carbanak (2013). E non è di certo questo l’elenco completo dei programmi Trojan mediante i quali i malfattori realizzano il furto del denaro e dei dati sensibili degli utenti.

Quanto più si diffondono le transazioni finanziarie online, tanto più divengono attraenti, per i cybercriminali, le organizzazioni che praticano costantemente tali operazioni. Nel corso di questi ultimi anni, i criminali informatici hanno sempre più spesso attaccato non solo i clienti delle banche e dei negozi online, ma anche, in maniera diretta, le organizzazioni finanziarie: istituti bancari e sistemi di pagamento. [La storia del gruppo APT Carbanak](https://securelist.ru/blog/issledovaniya/25106/bolshoe-bankovskoe-ograblenie-apt-kampaniya-carbanak/), specializzato nella conduzione di attacchi informatici nei confronti delle banche, e scoperto da Kaspersky Lab, rappresenta una chiara conferma di tale tendenza.

Gli esperti di Kaspersky Lab monitorano l’underground russo dell’hacking sin dall'inizio della sua esistenza. Kaspersky Lab pubblica regolarmente dettagliati [report sul panorama delle cyber-minacce finanziarie](https://securelist.ru/analysis/ksb/25094/finansovye-kiberugrozy-v-2014-godu-vremya-peremen/), i quali riflettono i cambiamenti che progressivamente intervengono, in un determinato periodo di tempo, riguardo al volume degli attacchi condotti dai malintenzionati attraverso il dispiegamento dei cosiddetti malware “finanziari”.

Le informazioni relative al numero degli attacchi eseguiti evidenziano la vasta portata del problema, ma non rivelano nulla riguardo a chi organizza gli stessi e alle modalità con cui tali attacchi informatici vengono allestiti e condotti. Ci auguriamo che questo nostro articolo possa contribuire a far luce su tali oscuri aspetti della criminalità informatica legata alla sfera finanziaria.

I dati qui di seguito riportati sono stati ottenuti grazie allo svolgimento di decine di indagini - alle quali, nel corso di questi ultimi anni, hanno partecipato gli esperti di Kaspersky Lab - e a seguito delle ripetute osservazioni eseguite, nell’arco di vari anni, dagli analisti che operano presso la nostra società, relativamente al mercato del cybercrimine russo.

## Il quadro della situazione

Secondo le stime di Kaspersky Lab, nel periodo intercorrente tra il 2012 e il 2015, le forze dell'ordine di numerosi paesi (tra cui Stati Uniti, Russia, Bielorussia, Ukraina e vari paesi dell’Unione Europea) hanno complessivamente arrestato oltre 160 cybercriminali russofoni, facenti parte di gruppi criminali di piccole, medie e grandi dimensioni, i quali si sono indebitamente appropriati di cospicue risorse finanziarie, in tutto il mondo, mediante l’utilizzo di appositi programmi malware. Il danno complessivo derivante dalle attività illecite da essi condotte supera i 790 milioni di dollari USA. (Tale stima si basa sull’analisi delle informazioni pubbliche riguardanti gli arresti di persone sospettate di aver compiuto cybercrimini di natura finanziaria nel periodo 2012-2015, e sui dati elaborati per conto proprio da Kaspersky Lab). Di questo colossale importo, circa 509 milioni di dollari sono stati rubati, dai criminali informatici in questione, al di fuori dei confini dei paesi situati nello spazio geografico precedentemente occupato dalle repubbliche dell’Unione Sovietica. Naturalmente, le cifre sopra indicate prendono in considerazione solo le perdite finanziarie effettivamente confermate; i dati relativi ai danni economici ufficialmente comprovati sono stati ottenuti dalle forze dell’ordine nel corso delle attività investigative svolte. In realtà, i cybercriminali hanno potuto sottrarre, in maniera illecita, somme di denaro significativamente superiori.

Dinamiche inerenti al numero di arresti di cybercriminali russofoni resi pubblicamente noti nel periodo 2012-2015

Un altro parametro atto a fornire valide indicazioni sull’effettiva portata del problema relativo alla cybercriminalità russofona è rappresentato dal numero di persone condannate, in questi ultimi anni, in riferimento ad articoli di legge inerenti alla criminalità informatica. Soltanto in territorio russo, dall’anno 2013 al primo semestre del 2015 compreso, sono state condannate 459 persone, ai sensi degli articoli 272 (accesso illegale a dati informatici) e 273 (creazione e distribuzione di software nocivo) del codice penale della Federazione Russa. Di queste, tuttavia, solo 21 sono state condannate ad una pena detentiva. Desideriamo far notare che la differenza esistente tra il numero degli individui arrestati e il numero delle persone condannate può essere facilmente spiegata dal fatto che gli arresti dei cybercriminali non vengono sempre resi noti dai mass media. Spesso, inoltre, all’eclatante arresto del capo di una gang cybercriminale, segue una serie di arresti di altri membri del gruppo; ne consegue che il numero finale degli imputati risulta decisamente superiore al numero delle persone sospettate, diramato inizialmente.

Dall’anno 2013 in poi, il team che compone la Divisione per le Indagini sugli Incidenti Informatici, operante presso Kaspersky Lab, ha preso parte alle investigazioni condotte riguardo ad oltre 330 incidenti legati alla cyber-sicurezza. Più del 95% di tali incidenti informatici è risultato collegato al furto di denaro o di informazioni sensibili di natura finanziaria.

Sebbene nel 2015 il numero degli arresti di cybercriminali russofoni, in relazione a casi riguardanti crimini informatici commessi in ambito finanziario, sia sensibilmente aumentato rispetto all’anno precedente, il mercato del cybercrimine si presenta ancora decisamente “affollato”. Secondo le stime degli esperti di Kaspersky Lab, nel corso degli ultimi tre anni, nel mondo della cybercriminalità che si esprime in lingua russa è risultato complessivamente coinvolto fino ad un migliaio di persone, considerando tutti coloro che hanno partecipato alla creazione delle infrastrutture, quelli che hanno sviluppato e distribuito programmi malware adibiti al furto delle risorse finanziarie degli utenti, i criminali che hanno direttamente compiuto il furto di ingenti somme di denaro o hanno provveduto a trasformare in contanti ed incassare le somme illecitamente sottratte. La maggior parte di tali malfattori è ancora in libertà.

È invece possibile calcolare con più precisione il numero delle persone che fanno parte della composizione essenziale, ovvero della struttura di base dei gruppi criminali in attività (gli organizzatori; i cosiddetti “prelevatori”, ovvero coloro che si occupano del trasferimento delle somme di denaro sottratte dai conti bancari compromessi; gli hacker professionisti, specializzati nel violare i computer altrui): tale numero non supera le 20 persone. Si tratta, nella circostanza, degli abituali visitatori dei forum underground, riguardo ai quali gli esperti di Kaspersky Lab hanno raccolto, nel corso degli ultimi tre anni, una considerevole quantità di informazioni, le quali indicano il loro potenziale coinvolgimento, nel ruolo di partecipanti e attori chiave, in attività di stampo criminoso, legate al furto di denaro.

Risulta difficile stabilire il numero esatto dei gruppi che operano dal territorio della Russia e dei paesi limitrofi; molti dei raggruppamenti coinvolti in attività criminali prendono magari parte ad alcune cyber-rapine, per poi interrompere in maniera inattesa, per un motivo o per l’altro, la propria attività. Inoltre, alcuni dei membri di gruppi ormai smascherati, e in pratica scomparsi dalla scena, proseguono la loro attività nell’ambito di nuove gang cybercriminali.

La Divisione per le Indagini sugli Incidenti Informatici, allestita da Kaspersky Lab, può attualmente affermare, con certezza, che esistono almeno cinque grandi gruppi cybercriminali all’opera, specializzati nel commettere crimini di natura finanziaria. Si tratta di gruppi le cui attività, nel corso di questi ultimi anni, sono state costantemente monitorate dai nostri esperti.

Tutti e cinque i gruppi, ancora attivi, hanno iniziato ad essere osservati dagli esperti di Kaspersky Lab sin dal periodo 2012-2013. Il numero delle persone che li compongono è compreso tra le 10 e le 40 unità. Almeno due di tali raggruppamenti attaccano attivamente obiettivi situati non soltanto sul territorio della Federazione Russa, ma anche al di fuori dei confini di quest’ultima: negli Stati Uniti, in Gran Bretagna, Australia, Francia, Italia e Germania.

Poiché le indagini non sono state ancora completate, non risulta per il momento possibile pubblicare informazioni più dettagliate riguardo alle attività condotte dai suddetti gruppi cybercriminali. Kaspersky Lab, da parte sua, continua le proprie investigazioni relativamente all’attività di questi gruppi, e collabora attivamente con le forze dell’ordine della Federazione Russa e di altri paesi, allo scopo di neutralizzare le temibili attività svolte dai criminali informatici in questione.

Le indagini condotte riguardo all’attività di tali gruppi hanno permesso agli esperti di Kaspersky Lab di acquisire interessanti informazioni sui metodi operativi adottati dai malfattori, e sulla struttura che caratterizza l’attuale mercato della cybercriminalità russa.

## Struttura del mercato cybercriminale russofono

### «Assortimento»

Per mercato cybercriminale si intende, abitualmente, l’insieme dei “servizi” e dei “prodotti” utilizzati per compiere azioni illegali di vario genere nell’ambito del cyberspazio. Questi “prodotti” e “servizi” vengono offerti per il relativo acquisto da parte di utenti o gruppi di utenti riconducibili a community Internet dedicate, la maggior parte delle quali è di tipo “chiuso”.

Con il termine “prodotti” si intendono i seguenti elementi:

* Software appositamente sviluppati per ottenere l’accesso non autorizzato a computer o dispositivi mobili, allo scopo di realizzare il furto di dati sensibili dai dispositivi infetti e/o sottrarre risorse finanziarie dai conti bancari delle vittime (trojan);
* Software appositamente progettati per sfruttare le vulnerabilità individuate nei programmi installati sui computer degli utenti-vittima (exploit);
* Database relativi ai dati sensibili, illecitamente carpiti, contenuti nelle carte di pagamento, e ad altre informazioni “preziose”;
* Traffico Internet (una determinata quantità di visite ad un sito web, prescelto dal committente, da parte di utenti che presentano una serie di caratteristiche specifiche).

Alla categoria dei “servizi” vengono associati:

* Conduzione di campagne di spam;
* Organizzazione di attacchi DDoS (allo scopo di sovraccaricare di richieste determinati siti web, con il preciso intento di rendere gli stessi inaccessibili agli utenti legittimi);
* Apposite verifiche condotte sui programmi malware che i cybercriminali intendono utilizzare, per determinare se tali software nocivi vengono di fatto rilevati, o meno, dai programmi antivirus;
* “Ricodifica” del malware (tramite apposite modifiche del software dannoso, per far sì che quest’ultimo non venga rilevato dagli antivirus);
* Concessione in affitto di exploit pack;
* Locazione di server dedicati;
* Servizi VPN (fornitura di accesso anonimo alle risorse web, protezione dello scambio di dati):
* Affitto di hosting di tipo abuse-proof (servizi di hosting che non reagiscono ad eventuali reclami o denunce per contenuti nocivi e, di conseguenza, non disattivano i server);
* Concessione in affitto di botnet;
* Verifica del “valore” dei dati sensibili illecitamente carpiti, relativi a carte di pagamento;
* Appositi servizi di conferma dei dati (false telefonate, false scansioni di documenti);
* Innalzamento del ranking di siti dannosi e siti pubblicitari nell’ambito dei risultati restituiti dai motori di ricerca;
* Servizi di intermediazione nelle transazioni relative all’acquisto di “prodotti” e “servizi”;
* Prelievo e incasso di mezzi finanziari.

Il pagamento dei “prodotti” e dei “servizi”, nel mercato cybercriminale, viene in genere effettuato mediante l’utilizzo di uno dei sistemi di pagamento elettronico esistenti, quali WebMoney, Perfect Money, Bitсoin, etc.

In varie combinazioni, tutti questi "prodotti" e "servizi” vengono venduti ed acquistati per l’allestimento di cinque tipologie principali di cybercrimine, le quali possono essere ugualmente combinate in maniera diversa, a seconda dello specifico gruppo che ne fa uso:

* Attacchi DDoS (commissionati o a scopo di estorsione);
* Furto di dati personali e dei dati confidenziali necessari per accedere al denaro elettronico (per la successiva rivendita degli stessi o per sottrarre illecitamente risorse finanziarie);
* Furto del denaro custodito nei conti bancari o negli account di altre organizzazioni;
* Spionaggio domestico o aziendale;
* Blocco dell’accesso ai dati presenti nel computer infettato dal malware, a fini di estorsione.

Secondo le osservazioni effettuate dagli esperti di Kaspersky Lab, le azioni criminali collegate al furto del denaro sono le più diffuse, nel corso di questi ultimi anni. Pertanto, tutte le informazioni fornite in seguito riguarderanno in primo luogo proprio tale segmento del mercato cybercriminale russofono.

### Il «mercato» del lavoro nell’ambito del cybercrimine finanziario

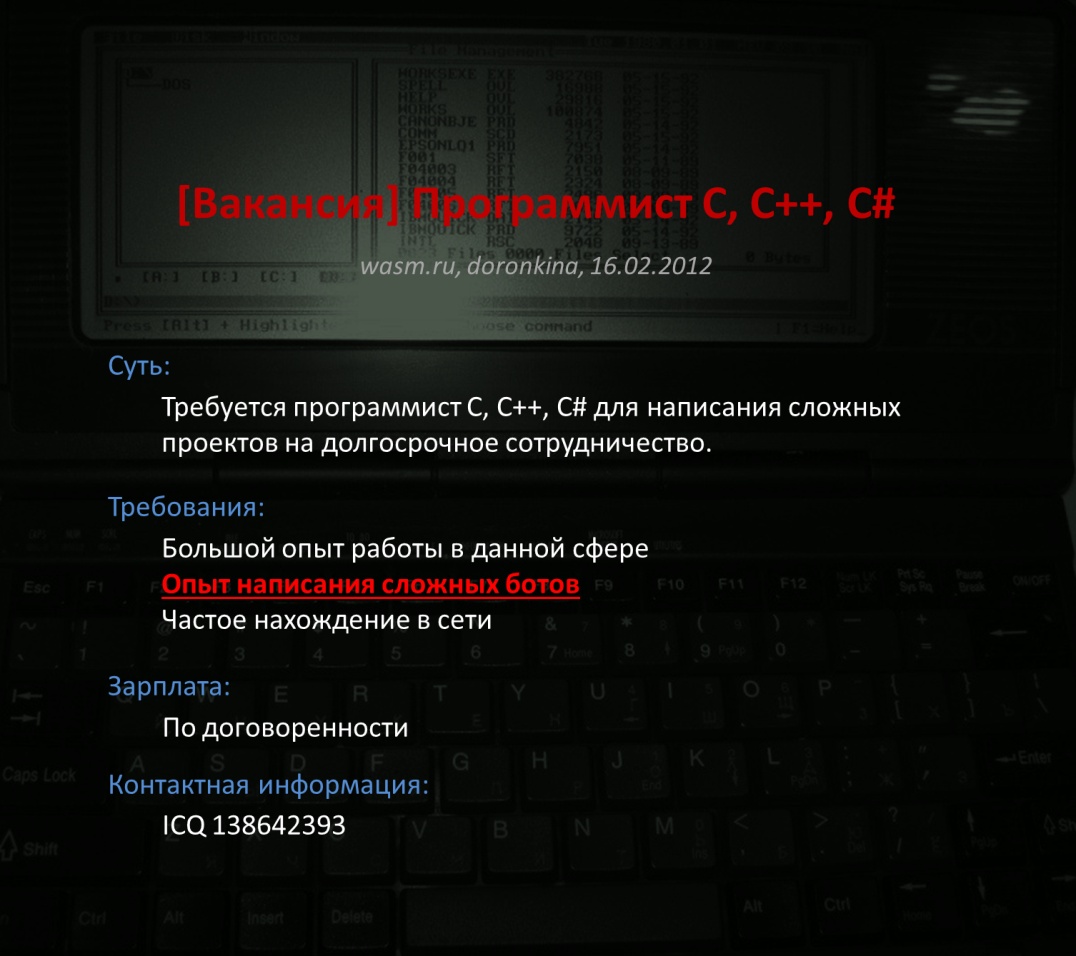
La grande varietà di competenze necessarie per la realizzazione dei “prodotti” e la prestazione dei “servizi” in precedenza elencati, ha dato vita ad un vero e proprio mercato del lavoro, attraverso il quale il cybercriminale ricerca gli specialisti e i “professionisti” in grado di compiere crimini informatici connessi alla sfera finanziaria.

L’elenco delle possibili “professioni” risulta in pratica analogo a quello che caratterizza qualsiasi società operante nel settore IT:

* Programmatori / coder / virus writer (creazione di software nocivi e modifica di quelli già esistenti);
* Web designer (creazione di pagine di phishing, e-mail, etc.);
* Amministratori di sistema (allestimento delle infrastrutture IT e relativo supporto);
* Tester (testing del software dannoso);
* “Cryptor” (adibiti alle operazioni di ricodifica dei codici maligni, allo scopo di eludere il rilevamento da parte dei programmi antivirus).

Non fanno parte dell’elenco né i capi delle gang cybercriminali, né i cosiddetti “prelevatori”, ovvero quelli che si occupano del trasferimento del denaro illegalmente sottratto dai conti bancari violati - e nemmeno coloro che sono alla testa dei “drop project”, gli schemi preposti al processo di trasformazione in contanti ed incasso, attraverso i “money mules”, o “muli del denaro”, delle somme rubate; in effetti, i rapporti che intercorrono tra questi elementi dei gruppi criminali possono essere piuttosto ricondotti all’ambito del partenariato, e non risultano quindi classificabili alla stregua di “ordinari” rapporti datore di lavoro-candidato al posto di lavoro.

A seconda del tipo e delle dimensioni dell’impresa criminale, i capi dei vari gruppi possono procedere ad una vera e propria “assunzione” dei collaboratori nell’organico del raggruppamento, sulla base di uno stipendio prestabilito; in alternativa, la collaborazione può avvenire in modalità freelance: in questo caso, il lavoro svolto viene retribuito sulla base dei parametri relativi al progetto effettivamente realizzato.



Testo di un annuncio di “lavoro” relativo all’assunzione di un programmatore da parte di uno dei gruppi cybercriminali, collocato all’interno di un forum semichiuso. Tra i requisiti richiesti ai candidati spicca l’esperienza nella scrittura di bot complessi.

I gruppi dediti al cybercrimine effettuano il reclutamento dei loro “collaboratori” sia nei siti dove tradizionalmente si riuniscono gli utenti della Rete coinvolti in attività criminose, sia tramite risorse web frequentate da coloro che si interessano a metodi “non standard” per realizzare guadagni in Internet. Negli altri casi, gli annunci vengono collocati all’interno di siti specializzati per la ricerca di lavoro e collaboratori, o negli appositi uffici di collocamento online dedicati ai collaboratori da remoto.

In generale, tutti i “dipendenti” assunti nell’organico dei vari gruppi, e in tal modo coinvolti nel cybercrimine, possono essere suddivisi in due tipologie ben distinte: coloro che sono consapevoli dell’illegittimità del progetto di lavoro che viene loro proposto, e quelli che, invece, perlomeno nella fase iniziale, non sono a conoscenza di tale circostanza. In quest'ultimo caso si tratta, di solito, di persone necessarie per lo svolgimento di compiti relativamente semplici, come il realizzare specifiche copie dell’interfaccia relativa a sistemi e siti web utilizzati da vari istituti bancari.

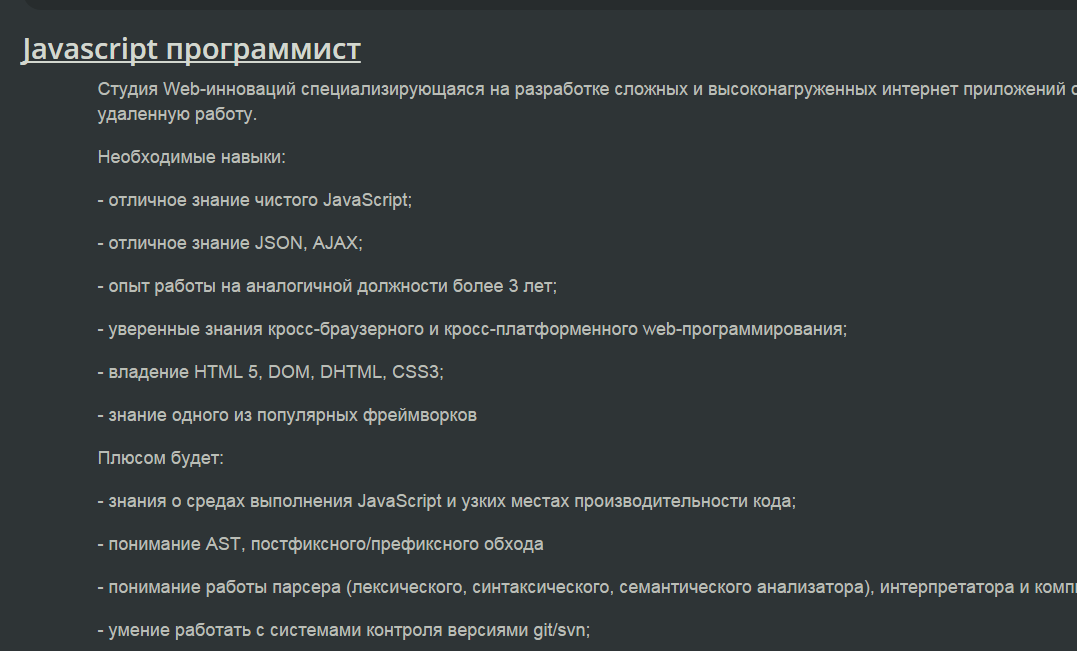
Comunicando la disponibilità di “veri” posti vacanti, i cybercriminali si attendono spesso di trovare collaboratori provenienti da remote regioni della Russia e dai paesi ad essa limitrofi (per lo più dall’Ukraina), dove esistono frequenti problemi a livello di occupazione lavorativa e di salari dignitosi per gli specialisti dell’informatica.



*Un malintenzionato comunica la disponibilità di un impiego in qualità di esperto di java/flash, su un popolare sito web ukraino dedicato alle offerte/ricerche di lavoro per gli specialisti dell’informatica. Tra i requisiti richiesti: buone conoscenze a livello di programmazione in Java e Flash, conoscenza delle specifiche JVM/AVM ed altro. Per $2.500, l’organizzatore offre un lavoro da remoto su base permanente e piena occupazione.*

Il motivo della ricerca di “collaboratori” ubicati in regioni periferiche è ben evidente: esso è dettato dalla possibilità di risparmiare, visto che il personale proveniente da regioni geografiche remote può essere pagato di meno rispetto ai “dipendenti” situati nelle grandi città. I malfattori, inoltre, danno spesso la preferenza a quei candidati che non sono stati ancora coinvolti in attività di natura cybercriminale.

Di frequente, impieghi del genere vengono presentati come proposte di lavoro del tutto legittime; soltanto dopo aver ricevuto l’incarico diviene chiaro il vero scopo del lavoro assegnato.



*In questo esempio, l’organizzatore del gruppo criminale offre un lavoro ad un programmatore javascript, e maschera la sua proposta di impiego presentandosi in veste di “studio per l’innovazione Web, specializzato nello sviluppo di complesse e sofisticate applicazioni Internet”*

Nel caso dei siti legittimi dedicati alle offerte/ricerche di lavoro, il pubblico al quale sono rivolti tali annunci è costituito da specialisti IT dotati di minore esperienza nel settore.



*In questo caso l’impiego offerto, ovvero quello di sviluppatore specializzato nel linguaggio di programmazione С++, riguarda l’elaborazione di software "custom". Per software "custom” si sottintende, naturalmente, il software dannoso.*

Il secondo motivo che sta alla base della ricerca di “collaboratori” da remoto, è rappresentato dal desiderio, da parte dell’organizzatore del raggruppamento cybercriminale, di rendere il più possibile anonima l’attività della gang che egli capeggia, e di creare condizioni tali per cui la persona “assunta” non potrà disporre di informazioni complete riguardo alla vera identità del “datore di lavoro”.

### Possibili varianti riguardo all’organizzazione di gruppi cybercriminali

Le gang criminali specializzate nel furto di cospicue somme di denaro, o nel carpire informazioni sensibili relative all’ambito finanziario (le quali consentono, poi, di ottenere l’accesso al denaro posseduto dagli utenti-vittima), si differenziano tra di loro sia per il numero di persone che partecipano alle stesse, sia per l’effettiva portata delle attività criminose svolte. Di fatto, possono essere individuate tre forme principali di coinvolgimento nella sfera della criminalità informatica:

* Programmi di partenariato
* Singoli “imprenditori”, gruppi di piccole e medie dimensioni (fino a dieci partecipanti)
* Gruppi organizzati di grandi dimensioni (dieci o più partecipanti)

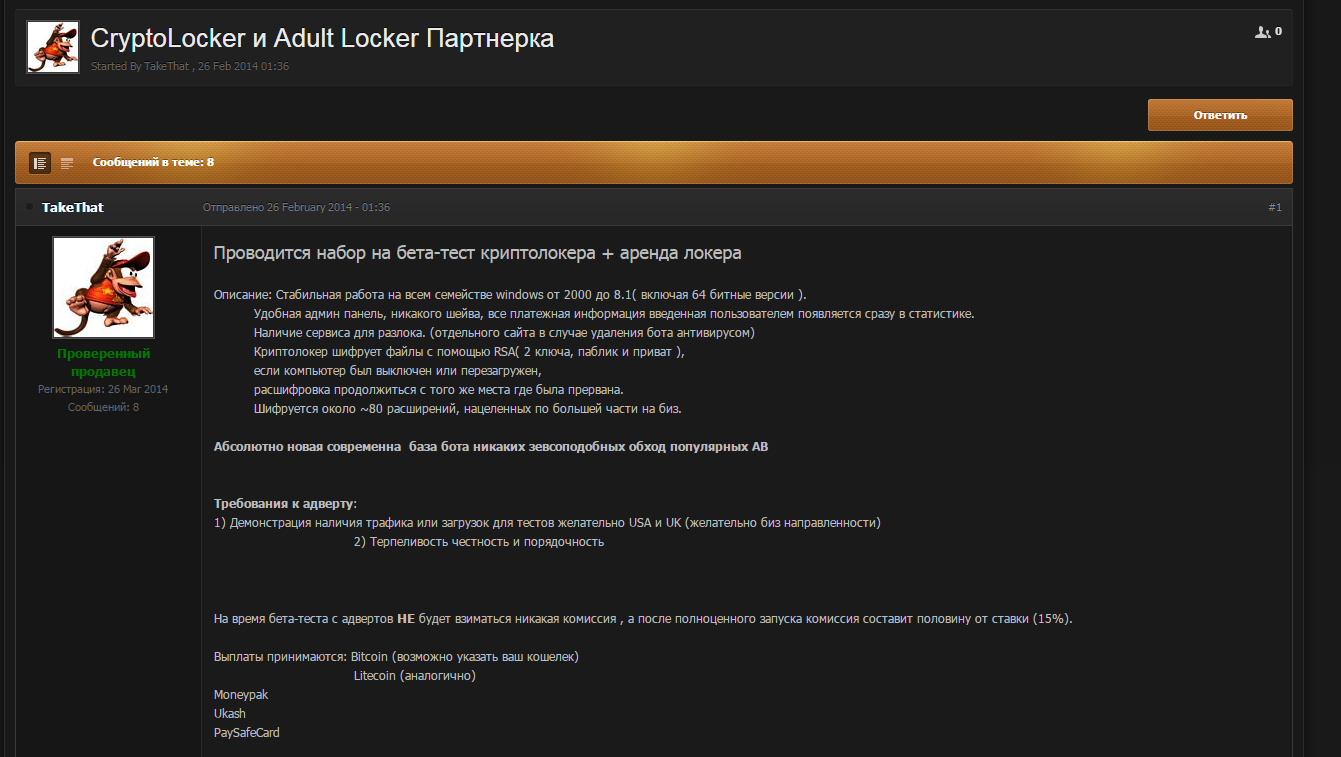
Si tratta, ad ogni caso, di una suddivisione convenzionale. L’entità delle attività condotte dal gruppo dipende, in effetti, dal grado di esperienza delle persone che vi prendono parte, dalle loro ambizioni, dal livello delle capacità organizzative di cui le stesse fanno prova. In alcuni casi, gli esperti di Kaspersky Lab hanno ad esempio osservato dei raggruppamenti cybercriminali relativamente piccoli in grado di svolgere compiti che, di solito, richiedono gli sforzi e il coinvolgimento di un numero di persone significativamente superiore.

#### Programmi di partenariato

I programmi di partenariato (o programmi di affiliazione) costituiscono il metodo più semplice e in assoluto meno costoso per praticare attività di natura cybercriminale. L'essenza dei programmi di partenariato risiede nel fatto che, in pratica, gli organizzatori degli stessi forniscono ai “partner” l’insieme degli strumenti necessari per commettere il crimine. Il compito dei “partner” è quello di generare il maggior numero possibile di installazioni di software nocivo sui dispositivi degli utenti. In cambio, il proprietario (o i proprietari) del programma di affiliazione condivide (condividono) con i partner i profitti illeciti realizzati a seguito delle infezioni informatiche prodotte. A seconda del tipo di schema fraudolento adottato, può trattarsi di:

* somme di denaro sottratte dagli account degli utenti dei servizi di Internet banking;
* importi pagati dagli utenti in qualità di riscatto, nel caso in cui i criminali ricorrano all’utilizzo di programmi malware in grado di codificare i file custoditi sul computer-vittima;
* denaro proveniente dagli account “prepagati” di cui dispongono gli utenti dei dispositivi mobili, ricavato grazie all’invio segreto di messaggi SMS verso costosi numeri mobile a pagamento, ottenuto attraverso un apposito programma nocivo.

Di per se stessi, la creazione e il mantenimento di un programma di partenariato preposto al furto di denaro, rappresentano ugualmente una forma di cybercrimine, compiuto, in genere, da un gruppo di utenti malintenzionati. Simili progetti criminosi, tuttavia, vengono più di frequente realizzati da gruppi di notevoli dimensioni, ben organizzati, dei quali riferiremo in dettaglio un po’ più avanti.



**Annuncio relativo all'apertura della fase di beta testing di un programma di partenariato preposto alla diffusione di temibili malware crittografici, riconducibili alla categoria dei trojan “estorsori”. A giudicare dalle caratteristiche descritte, l’attività del gruppo si orienta verso società con sede negli Stati Uniti e in Gran Bretagna. Tali elementi si deducono dal testo dell’annuncio, in cui si afferma che il malware distribuito attraverso il programma di affiliazione è in grado di cifrare file con 80 diverse estensioni, molte delle quali riguardano file relativi ad applicazioni utilizzate nell’ambito delle attività di business. Tra i requisiti richiesti al candidato tester, spicca la necessità di dover dimostrare la presenza di traffico o download provenienti dagli USA e dalla Gran Bretagna.**

Secondo le osservazioni effettuate dagli esperti di Kaspersky Lab, in questi ultimi tempi i programmi di affiliazione trovano sempre minore diffusione tra i cybercriminali russofoni. Per lungo tempo, il principale motore della popolarità di tali iniziative criminose è risultato essere lo specifico schema fraudolento volto a realizzare l’infezione dei dispositivi mobili degli utenti mediante l’utilizzo di appositi programmi malware, in grado di procedere al successivo invio di costosi messaggi SMS verso numeri premium. Nella primavera del 2014, tuttavia, le autorità russe hanno introdotto nuovi requisiti riguardo all’allestimento di simili servizi; essi prevedono, tra l’altro, la necessità di dover ulteriormente confermare l’abbonamento in precedenza sottoscritto con un determinato servizio mobile a pagamento. Tali cambiamenti sono divenuti uno dei fattori chiave del quasi totale azzeramento delle attività illecite condotte dai programmi di partenariato nella sfera dei dispositivi mobili. Questa particolare forma di collaborazione tra criminali informatici continua tuttavia ad essere utilizzata da gruppi specializzati nella distribuzione dei famigerati malware “cifratori” ed “estorsori”.

#### Gruppi minori

Questa forma di coinvolgimento nel business cybercriminale si differenzia in primo luogo da quella che prevede la partecipazione ad una specifica partnership, per il fatto che il criminale, o i criminali, in genere, organizza (organizzano) in maniera autonoma lo schema fraudolento. Ad ogni caso, la maggior parte dei componenti necessari per la conduzione dell'attacco informatico (programmi malware e relative varianti e/o modifiche - ottenute tramite apposita ”ricodifica” del software nocivo originario - traffico, server, etc.), viene acquistata sul mercato nero della cybercriminalità. Spesso, coloro che prendono parte a simili gruppi, non sono affatto degli esperti nel settore delle tecnologie informatiche e di rete; tali malintenzionati, tuttavia, riescono ad acquisire le indispensabili conoscenze riguardo a componenti e metodi necessari per poter organizzare gli attacchi rivolti all’ambito finanziario, grazie a fonti web pubblicamente accessibili, rappresentate, in genere, da forum specifici. Le effettive potenzialità nocive che simili raggruppamenti riescono ad esprimere vengono di frequente limitate da una serie di fattori. In particolar modo, l’utilizzo di malware largamente diffusi ha, come conseguenza, la rapida individuazione degli stessi da parte dei programmi adibiti alla protezione IT; tale circostanza obbliga i cybercriminali ad investire maggiori risorse per la distribuzione dei software maligni e per la “ricodifica” degli stessi, con il preciso intento di bypassare il possibile rilevamento del malware da parte delle soluzioni di sicurezza informatica. Tutto questo, ovviamente, riduce in maniera considerevole le disponibilità finanziarie dei malfattori che operano nell’ambito di gruppi criminali di piccole dimensioni.

Gli errori commessi da tali malintenzionati, inoltre, conducono spesso all’identificazione e al conseguente arresto di questi ultimi. Tuttavia, il costo relativamente contenuto che comporta l’ingresso nel business del cybercrimine attraverso questo approccio di tipo decisamente “amatoriale” (a partire da 200 dollari), e la possibilità di potersi appropriare di somme sensibilmente superiori, continuano ad attirare costantemente nuovi “imprenditori” del settore.

Un chiaro esempio di una formazione criminale del genere, a carattere puramente “dilettantesco”, è rappresentato dal gruppo condannato nell’anno 2012, da un tribunale della Federazione Russa, per aver compiuto il furto di oltre 13 milioni di rubli (circa 422.000 dollari USA al cambio dell’epoca), a danno degli utenti del servizio di banking online allestito da un istituto bancario russo. Dopo una complessa indagine, gli esperti di Kaspersky Lab hanno potuto raccogliere le informazioni e gli elementi che hanno consentito alle forze dell’ordine di poter identificare i malfattori che si celavano dietro i furti commessi.

Il suddetto tribunale ha condannato i due membri del gruppo cybercriminale a 4,5 anni di libertà vigilata ciascuno. La sentenza emessa dal tribunale non ha tuttavia fermato i criminali in questione, i quali, di fatto, hanno continuato a commettere atti criminosi; in pratica, nei due anni e mezzo successivi, i due malfattori hanno realizzato un considerevole numero di furti, riuscendo a sottrarre, complessivamente, una somma paragonabile a quella sopra indicata. Nel mese di maggio 2015, ad ogni caso, i due criminali sono stati nuovamente arrestati.

#### Gruppi cybercriminali organizzati di grandi dimensioni

I grandi gruppi criminali si differenziano dagli altri, in primo luogo, per le vaste proporzioni delle attività da essi condotte, così come per l’approccio molto più “professionale” e “serio” nei confronti dell’organizzazione del cybercrimine e della definizione dei principi sui quali poggia il funzionamento dell’intero gruppo. Il numero delle persone che compongono tali raggruppamenti può raggiungere alcune decine di unità (non considerando coloro che agiscono nell’ambito dei cosiddetti “drop project”, utilizzati per l’incasso delle somme di denaro illecitamente carpite e per il “lavaggio” delle stesse); inoltre, gli obiettivi degli attacchi informatici sferrati da tali gruppi non si limitano di certo ai clienti privati dell’Internet banking. In effetti, oltre agli utenti privati, simili gang cybercriminali attaccano in particolar modo le società di piccole e medie dimensioni; i gruppi criminali più numerosi e sofisticati, poi, come ad esempio l’APT Carbanak, prendono ugualmente di mira sia le banche che i sistemi di pagamento.

Lo schema che caratterizza l’attività dei grandi gruppi criminali si differenzia sensibilmente dal modus operandi adottato dai raggruppamenti che presentano dimensioni decisamente più contenute. Considerando la struttura e i principi organizzativi su cui si basano i gruppi cybercriminali di dimensioni più estese, è possibile paragonare alcuni di essi ad un’impresa di media grandezza che si occupa dello sviluppo di software.

In particolar modo, i grandi gruppi si contraddistinguono per il fatto di annoverare una sorta di organico, composto da gruppi ben distinti di collaboratori che eseguono i compiti via via assegnati dall’organizzatore della gang, sulla base di un compenso fisso, regolarmente retribuito. Tuttavia, anche nel caso di un gruppo “professionale”, una parte delle mansioni viene di solito affidata a “fornitori” esterni. Ad esempio, le operazioni di “ricodifica” dei programmi malware possono essere effettuate sia dai virus writer che fanno parte dello “staff” interno, sia da quelli appositamente “assunti”, oppure possono essere affidate all’esterno, ad appositi servizi forniti da terze parti attraverso l’utilizzo di un processo automatizzato, che prevede l’impiego di speciali software. Lo stesso discorso vale per numerosi altri componenti dell’infrastruttura IT necessaria per compiere i crimini informatici.

Un esempio di raggruppamento cybercriminale organizzato di considerevoli dimensioni è rappresentato dal noto gruppo denominato Carberp, i cui membri sono stati arrestati sul territorio della Federazione Russa e dell’Ukraina rispettivamente nel 2012 e nel 2013; segnaliamo inoltre, il famigerato gruppo APT Carbanak, le cui attività illecite sono state scoperte da Kaspersky Lab all'inizio del 2015.

Il danno derivante dall’attività dei programmi di partenariato e dei raggruppamenti minori si conta, in genere, in termini di alcune decine o centinaia di migliaia di dollari; le azioni criminose compiute dai grandi gruppi cybercriminali, invece, risultano sensibilmente più pericolose e distruttive. Le perdite finanziarie provocate dal gruppo Carberp sono stimate in alcune centinaia di milioni di dollari, mentre il gruppo Carbanak, secondo le valutazioni di Kaspersky Lab, è riuscito ad impadronirsi di una somma quantificabile, all’incirca, in un miliardo di dollari. Sulla base di questi elementi e di simili cifre, si può ben comprendere come lo studio dei meccanismi su cui poggia il funzionamento di tali cybergang, così come l’analisi delle tattiche e delle strategie da esse adottate, risultino di fondamentale importanza, visto che possono contribuire ad investigare in maniera ancor più efficace sulle temibili attività condotte da tali criminali informatici, e, in definitiva, possono consentire di neutralizzare tali minacce.

## La suddivisione dei ruoli all’interno di un gruppo criminale di notevoli dimensioni

Il cybercrimine finanziario su vasta scala è costituito da atti criminosi a seguito dei quali le organizzazioni sottoposte ad attacco subiscono perdite per milioni di dollari. Questo è il risultato dell’attività di un’ampia cerchia di persone specializzate nel compiere crimini nell’ambito della sicurezza IT e nella sfera finanziaria. In genere, ogni attacco cybercriminale è preceduto da molti mesi di fase preparatoria, nel corso della quale – oltre all’allestimento di una complessa infrastruttura, oltre alla selezione e allo sviluppo di software nocivo – viene realizzato uno studio dettagliato dell’organizzazione presa di mira, allo scopo di chiarire i dettagli del funzionamento interno di tale società, ed individuare i punti deboli della stessa a livello di sicurezza. Ad ognuno dei membri del gruppo criminale vengono assegnate determinate responsabilità.

La suddivisione dei ruoli qui sotto descritta è caratteristica dei gruppi criminali specializzati nel furto di risorse finanziarie. La distribuzione dei ruoli all’interno dei raggruppamenti preposti ad azioni criminose di altro genere può risultare diversa.

### Virus writer\Programmatore

Il virus writer, o programmatore, è responsabile della creazione di software dannoso, ovvero di quei programmi dannosi che consentono agli attacker di penetrare all’interno delle reti informatiche delle organizzazioni sottoposte ad attacco, generare il download di ulteriori programmi nocivi in grado di carpire le informazioni sensibili occorrenti e, in ultima analisi, realizzare il furto di denaro.

La rilevanza del ruolo occupato da tale membro del gruppo, così come la tipologia dei rapporti che egli intrattiene con gli organizzatori della gang cybercriminale, possono variare da un raggruppamento all'altro. Ad esempio, se il gruppo di malfattori si avvale di programmi malware già pronti all’uso, prelevati presso fonti facilmente accessibili, oppure acquistati presso altri autori di virus, le funzioni del virus writer possono essere limitate alla sola messa a punto e modifica di tali software nocivi - per far sì che gli stessi risultino compatibili con le necessità operative e il funzionamento della nuova infrastruttura creata per realizzare un determinato crimine informatico - oppure all’adattamento del suddetto malware per la realizzazione di attacchi informatici nei confronti di istituzioni specifiche. I gruppi più sofisticati e sviluppati, tuttavia, tendono ad utilizzare esclusivamente le proprie “creature”, a livello di malware, allo scopo di rendere i programmi nocivi meno “visibili” alla maggior parte delle soluzioni di sicurezza IT; tale scelta, inoltre, offre maggiori opportunità per l’eventuale creazione delle varianti del malware di volta in volta impiegato. In questo caso, il ruolo del virus writer diviene molto più rilevante, visto che tale figura risponde direttamente dell’architettura e dell’insieme delle funzionalità di cui è provvisto il malware da egli progettato e sviluppato.

Allo stesso modo, l’autore di malware può assumere il ruolo di responsabile delle operazioni di “ricodifica” dei programmi maligni via via dispiegati dalla gang cybercriminale. Questo è valido, tuttavia, solo nei casi in cui l’organizzatore intende mantenere all’interno del proprio gruppo il maggior numero possibile di task e attività, e quando, per effettuare la “ricodifica” del programma nocivo, viene utilizzato software originale. Nella maggior parte dei casi, in effetti, tale specifica mansione viene affidata “in appalto” a fornitori esterni, i cosiddetti “servizi di codifica”.

### Tester

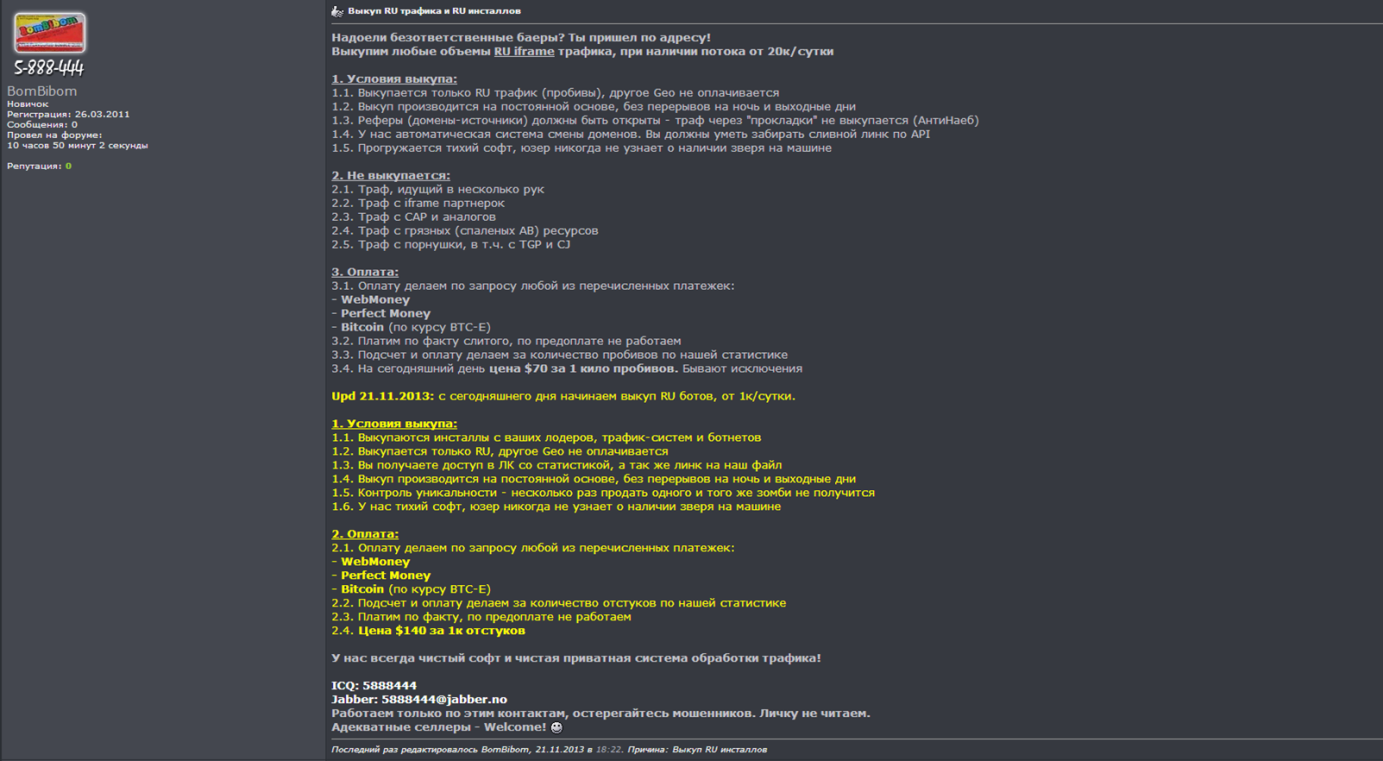
La funzione svolta dai tester che operano all’interno del gruppo cybercriminale non si discosta molto dalla tipologia di attività condotta dai tester che fanno parte dell’organico delle aziende IT legittime. Così come avviene nelle normali società del settore informatico, anche ai tester “criminali” vengono assegnati, da parte dei propri “manager”, specifici compiti di natura tecnica, in relazione alle attività di testing dei programmi malware, da condurre in una serie di ambienti diversi (differenti versioni del sistema operativo, set diversi di applicazioni installate, etc.); i tester sono quindi adibiti allo svolgimento di tali mansioni. Se lo schema fraudolento adottato dalla gang cybercriminale prevede poi l’utilizzo di false interfacce inerenti ai servizi di Internet banking e ai sistemi di pagamento online, sarà ugualmente compito del tester verificare il corretto funzionamento di tali interfacce fasulle.

### Webmaster e programmatori web

In genere, web designer e programmatori web sono collaboratori che operano da remoto; essi hanno il compito di realizzare le pagine ed i siti web di phishing, creare le interfacce falsificate delle applicazioni ed effettuare le operazioni di web injection. Si tratta, in pratica, degli elementi tecnici utilizzati dal gruppo criminale per carpire i dati sensibili necessari per accedere ai sistemi di pagamento e ai servizi di banking online.

### Distributori

I cosiddetti “distributori” hanno il compito di assicurare il download dei programmi malware sul maggior numero possibile di dispositivi. Il risultato auspicato viene raggiunto mediante l’utilizzo di vari strumenti. In genere, l’organizzatore definisce le caratteristiche degli utenti-vittima, i cui computer dovranno essere sottoposti ad infezione informatica, ed acquista presso i cosiddetti “trafogon” (servizi volti ad attirare gli utenti con determinate caratteristiche verso un particolare sito web) la necessaria tipologia di traffico.



*Annuncio relativo all’acquisto di traffico. I cybercriminali sono disposti a pagare solo le installazioni di software dannoso effettivamente riuscite, al prezzo di $140 ogni 1.000 call back (comunicazioni effettuate dal programma dannoso al server di comando, una volta completata con successo la procedura di installazione)*

L’organizzatore può inoltre commissionare, presso gli appositi servizi esistenti, la conduzione di una campagna di spam nocivo, preposta a recapitare nelle e-mail box delle vittime messaggi di posta elettronica contenenti in allegato un file maligno, oppure messaggi provvisti di un apposito link destinato a convogliare il destinatario dell’e-mail verso il sito web nocivo. In alternativa, gli organizzatori possono scegliere per conto proprio un determinato sito Internet, frequentato da un pubblico adatto agli scopi che si prefiggono, ordinarne la violazione e il successivo collocamento al suo interno di insidiosi kit di exploit. Tutti questi strumenti, naturalmente, possono essere utilizzati in combinazione tra di loro.

### Hacker

Spesso, nel corso di un attacco informatico rivolto ad una determinata società od organizzazione, il corredo di strumenti nocivi (exploit pack e malware di altro genere) di cui dispone il gruppo cybercriminale può rivelarsi non sufficiente per realizzare l’infezione di tutti i computer di fatto necessari per la riuscita dell’attacco, e per insediarsi stabilmente all’interno di questi ultimi. A volte, in effetti, può sorgere la “necessità” di dover effettuare un’operazione di hacking mirato nei confronti di un determinato computer, o di un certo sito web. In tal caso, gli organizzatori ricorrono ai servizi degli hacker; si tratta, in genere, di persone in possesso di una solida preparazione nel campo della sicurezza IT, in grado di svolgere compiti speciali. In numerosi casi esaminati dagli esperti di Kaspersky Lab, gli hacker sono risultati coinvolti in maniera episodica nelle attività della gang criminale; le loro prestazioni, in genere, vengono pagate a cottimo. Tuttavia, quando la necessità di praticare l’hacking diviene costante (ad esempio nel caso di attacchi mirati nei confronti di istituzioni finanziarie), l’hacker si trasforma in un membro permanente della band, divenendone spesso uno degli elementi chiave, assieme agli stessi organizzatori del cybercrimine e ai cosiddetti “prelevatori”, ovvero coloro che si occupano del trasferimento del denaro illecitamente sottratto dagli account bancari compromessi.

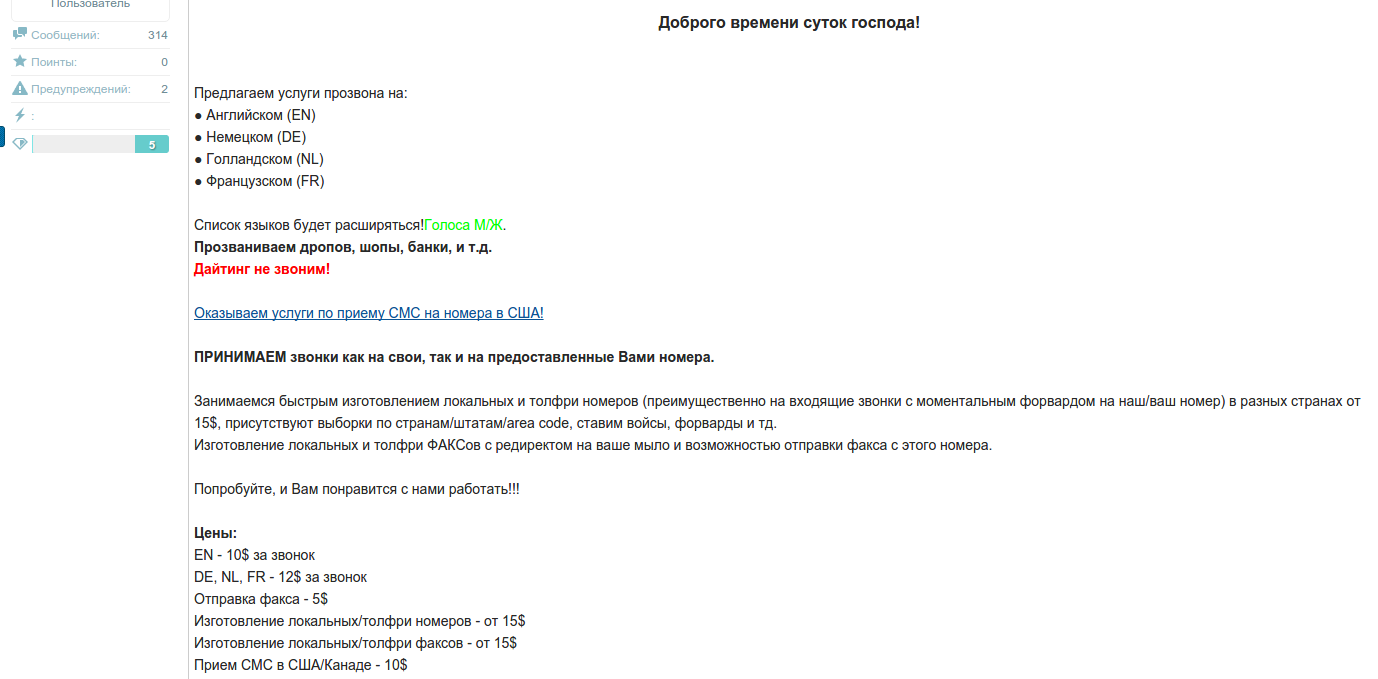
### Amministratori di sistema

Il compito principale svolto dagli amministratori di sistema facenti parte del raggruppamento cybercriminale non si differenzia molto dalle funzioni normalmente svolte dagli abituali amministratori dei sistemi informatici. Fondamentalmente, tale compito riguarda lo sviluppo e l’implementazione delle necessarie infrastrutture IT, così come il mantenimento dell’efficienza operativa delle stesse. Gli amministratori di sistema che operano nel contesto della cybercriminalità si occupano dell’impostazione e della configurazione dei server di comando, acquistano i server ubicati presso hosting di tipo abuse-proof, garantiscono la disponibilità degli strumenti adibiti alla realizzazione di connessioni anonime con i server (VPN) e prendono, infine, decisioni riguardo ad ulteriori compiti di natura tecnica, compresa l’interazione con gli amministratori di sistema che operano da remoto, appositamente ingaggiati per eseguire task di minore entità.

### Call service

L’ingegneria sociale svolge un ruolo di primaria importanza, nel garantire il successo dell’insieme delle attività svolte nell’ambito dell’impresa cybercriminale. Questo risulta valido, in particolar modo, quando si tratta di portare attacchi nei confronti di determinate organizzazioni, assalti informatici attraverso i quali viene realizzato il furto di ingenti somme di denaro. Nella maggior parte dei casi, anche se i malintenzionati riescono ad ottenere il pieno controllo del computer-vittima, tramite il quale è possibile eseguire la transazione fraudolenta, per completare con successo l’operazione criminosa in corso occorre far sì che la stessa venga sottoposta ad una procedura di conferma, che ne possa in qualche modo attestare la “legittimità”. È proprio questo il compito abitualmente svolto dai cosiddetti “call service”. Al momento opportuno, coloro che effettuano tali servizi assumono il ruolo del dipendente dell’organizzazione sottoposta ad attacco, oppure del funzionario della banca alla quale si appoggia l’azienda presa di mira, e, in tal modo, provvedono a confermare la “legittimità” del pagamento.

Gli “operatori” adibiti alla funzione di call service possono prendere parte ad un determinato crimine informatico in qualità di membri effettivi del team che compone una divisione vera e propria dell’impresa cybercriminale, oppure possono agire in veste di organizzazione esterna, coinvolta in maniera non continuativa nell’esecuzione di un particolare compito, remunerato a cottimo. I forum che costituiscono un abituale luogo di ritrovo e di comunicazione per gli utenti della Rete coinvolti in attività cybercriminali, abbondano di annunci pubblicitari relativi alla prestazione di simili servizi.



*Annuncio pubblicitario in cui vengono offerti servizi di chiamata telefonica in varie lingue: inglese, tedesco, olandese e francese. Il gruppo dichiara di essere specializzato in telefonate a negozi Internet, banche, e anche nelle chiamate ai cosiddetti “drop”, ovvero i “money mules” (muli del denaro). Il gruppo in questione propone ugualmente un veloce allestimento di numeri telefonici gratuiti a carattere locale, da utilizzare nell’ambito di schemi fraudolenti, per simulare i servizi di assistenza clienti; tra gli ulteriori servizi offerti, spicca la ricezione di messaggi SMS e l’invio di fax. Per effettuare una singola chiamata, i malfattori richiedono dai 10 ai 12 dollari. L’importo richiesto per la ricezione degli SMS è di $10, mentre la creazione dei numeri toll-free, atti a simulare i servizi di supporto per la clientela, viene offerta a partire da $15.*

Secondo le osservazioni effettuate da Kaspersky Lab, i grandi gruppi cybercriminali ricorrono raramente all’utilizzo di servizi “call service” forniti da terze parti, preferendo, di fatto, organizzarne di propri.

### Prelevatori

I cosiddetti “prelevatori” sono quei membri del gruppo cybercriminale che entrano in gioco quando sono stati già eseguiti tutti i compiti tecnici relativi all’organizzazione dell’attacco (scelta degli obiettivi ed infezione degli stessi, insediamento nell’infrastruttura informatica presa di mira), e tutto è quindi pronto per realizzare il furto. I “prelevatori”, in pratica, sono le persone che provvedono al trasferimento del denaro illegalmente sottratto dai conti bancari violati. La loro partecipazione allo schema criminale, tuttavia, non si limita esclusivamente alla pressione di alcuni tasti; essi, in effetti, svolgono un ruolo decisivo all’interno dell’impresa specializzata nel crimine informatico.

I prelevatori (o “trasferitori”, che dir si voglia), in genere, hanno una conoscenza approfondita della struttura, del regolamento e delle modalità operative interne dell’organizzazione sottoposta ad attacco (persino al punto da sapere l’orario esatto in cui va a pranzo il dipendente che lavora sul computer dal quale verrà poi effettuata la transazione fraudolenta); essi, inoltre, conoscono nel dettaglio il funzionamento dei sistemi anti-frode automatizzati, e sanno perfettamente come agire per bypassare tali sistemi di sicurezza. In altre parole, i prelevatori, oltre all’evidente ruolo criminoso di “rapinatori” diretti del denaro, svolgono ugualmente determinati compiti da “esperti”, che possono essere difficilmente (o in nessun caso) automatizzati. Probabilmente, proprio a causa di questo status speciale, i prelevatori sono tra i pochi membri della gang la cui partecipazione alle operazioni criminali viene pagata non con uno “stipendio” fisso, bensì riconoscendo una percentuale sulla somma rubata.

Spesso, poi, i prelevatori assumono le funzioni di operatore della botnet in precedenza allestita, ovvero il membro del raggruppamento cybercriminale preposto all’analisi e alla classificazione delle informazioni ottenute attraverso i computer infetti (presenza di accessi ai sistemi di banking online; presenza di denaro sui conti bancari per i quali risulta disponibile l’accesso; organizzazione presso la quale si trova il computer infetto, etc.).

Oltre alla categoria dei prelevatori, lavorano con condizioni simili soltanto coloro che dirigono i cosiddetti “drop project”.

### Capo del “drop project”

Colui che è alla testa del cosiddetto “drop-project” è, in pratica, un rappresentante di un gruppo criminale ben distinto, che interagisce strettamente con il raggruppamento specializzato nel compiere il furto del denaro. La funzione del drop project consiste nel ricevere i soldi illecitamente sottratti, procedere al loro incasso e trasferire di nuovo al gruppo cybercriminale la quota percentuale dovuta, precedentemente stabilita. Per realizzare tutto questo, il drop project provvede ad allestire una propria infrastruttura, la quale si compone di persone giuridiche e persone fisiche, provviste dei propri conti bancari, sui quali vengono convogliate le somme rubate, e attraverso i quali, poi, gli importi sottratti vanno a finire direttamente nelle tasche dei malfattori. Il manager del progetto criminoso definito con l’appellativo di “drop project“, interagisce con l’organizzatore del gruppo criminale, e fornisce a quest’ultimo i numeri dei conti bancari verso i quali il “prelevatore” indirizza il denaro illecitamente sottratto. I drop project, al pari dei prelevatori, operano sulla base di commissioni; secondo le informazioni raccolte da Kaspersky Lab nel corso delle indagini svolte, le percentuali richieste possono raggiungere persino la metà dell’importo complessivamente rubato.

### I “drop project”

I “drop project” rappresentano un elemento indispensabile nell’ambito di qualsiasi attività cybercriminale collegata alla sfera finanziaria. Tali specifici gruppi risultano composti da uno o più organizzatori, così come dai cosiddetti “drops”, o “money mules” (muli del denaro), il cui numero può raggiungere diverse decine di unità.

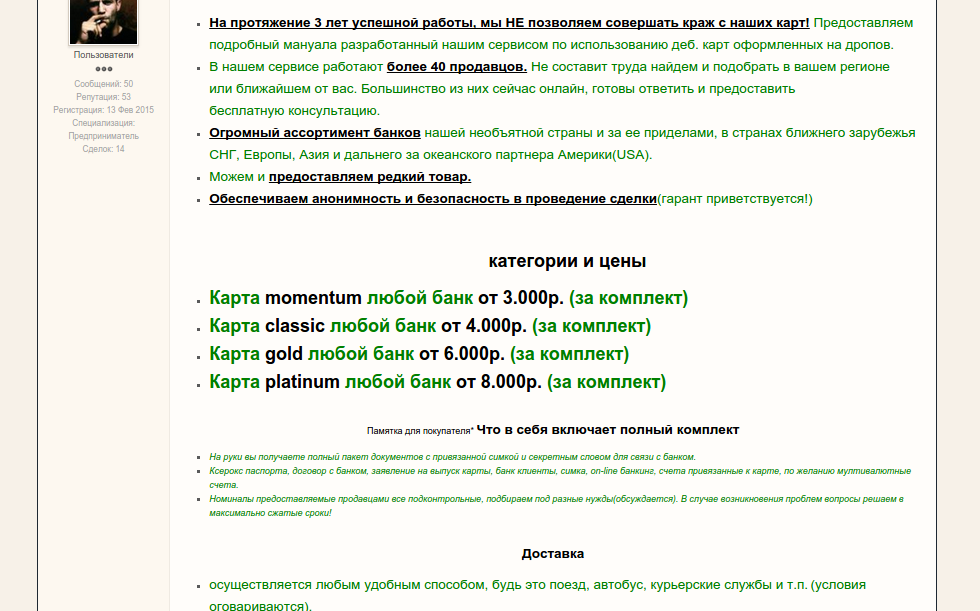
I “money mules”, in sostanza, sono i titolari degli strumenti finanziari; essi, su ordine impartito dal cosiddetto “dropovod” (una figura criminale intermedia, che si colloca tra il capo del “drop service” e il “drop” stesso), provvedono all’incasso del denaro rubato giunto sul conto bancario da essi posseduto; in alternativa, l’importo sottratto può essere trasferito dai “money mules” su un altro account, indicato dal “dropovod “.

I “muli del denaro” si suddividono in due distinte tipologie: da una parte, coloro che non sono consapevoli di partecipare ad un piano criminoso; dall’altra, quelli che, invece, ne sono pienamente coscienti. La prima categoria è composta da quelle persone che, perlomeno nelle fasi iniziali della collaborazione intrapresa con il “dropovod”, non si rendono conto di essere coinvolti in un’iniziativa legata al cybercrimine finanziario. In genere, il compito relativo al ricevimento e al trasferimento delle somme di denaro illecite viene presentato, a tale genere di “money mules”, facendo ricorso ad un pretesto apparentemente plausibile. Il “dropovod”, ad esempio, può creare un soggetto giuridico, ed assumere, per un incarico esecutivo a livello dirigenziale (magari in qualità di direttore generale o finanziario), proprio la persona adibita a svolgere la mansione di “drop” in maniera inconsapevole: il “money mule” firmerà così i documenti societari che, in realtà, serviranno poi da copertura legale per realizzare il prelievo e il trasferimento del denaro rubato.

I “drop” consapevoli, da parte loro, conoscono invece perfettamente lo scopo per cui eseguono i compiti assegnati dai “dropovod”.

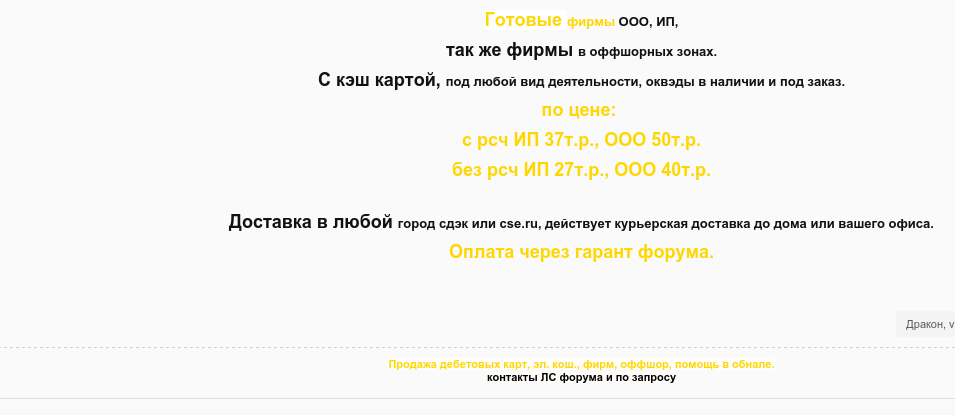
Esistono numerosi metodi, nell’ambito dei “drop project”, per effettuare il trasferimento delle somme di denaro illegalmente sottratte. A seconda dell’importo rubato, possono essere utilizzati sia i titolari di carte di pagamento private - pronti a trasformare in contanti ed incassare, per un compenso limitato, i fondi pervenuti sui loro account, per poi trasferire gli stessi a colui che rappresenta, di fatto, il “dropovod” - sia persone giuridiche appositamente costituite, i cui esponenti organizzano i cosiddetti “progetti stipendio” (un considerevole numero di carte di pagamento per i dipendenti della società, allo scopo di trasferire gli importi relativi ai salari percepiti) nell’ambito dell’istituto bancario al quale si appoggia la suddetta persona giuridica.

Un altro metodo standard, utilizzato per l’esecuzione di schemi fraudolenti nell’ambito dei “drop project”, è rappresentato dall’apertura in massa di account, in vari istituti bancari, da parte dei “money mules” consapevoli delle attività illecite svolte.



*Annuncio relativo alla vendita di kit inerenti a varie tipologie di carte di pagamento (carta, documenti attraverso i quali è stata emessa, carta SIM alla quale è collegato il relativo conto bancario); tali kit possono essere di fatto utilizzati per procedere all’incasso del denaro rubato. Il venditore offre carte di pagamento emesse da banche situate in Russia e nei paesi limitrofi, nonché in vari paesi europei, asiatici e negli Stati Uniti. Il kit denominato Momentum viene valutato 3.000 rubli (meno di $50); il set che comprende la carta della categoria Platinum viene invece offerto a 8.000 rubli (circa $120).*

Quando il furto di denaro avviene al di fuori dei confini della Russia, in qualità di “money mule” consapevole compare un cittadino, o un gruppo di cittadini di uno dei paesi dell'Europa Orientale, i quali, in breve tempo, si recano in varie nazioni del continente, e in ognuno di tali paesi aprono dei conti bancari a proprio nome. Successivamente, questi “muli del denaro” comunicano al “dropovod” i dati necessari per accedere a tutti gli account bancari, i quali vengono di conseguenza utilizzati per il trasferimento delle somme illegalmente sottratte.



*Esempio di annuncio relativo alla vendita di società già costituite nella Federazione Russa e in aree geografiche off-shore. Nella circostanza, i criminali offrono i loro servizi ad un prezzo che va dai 560 ai 750 $.*

### Stuffer

Il termine gergale “stuffer” deriva dalla parola inglese “stuff”, sinonimo utilizzato per indicare, nello slang, la “merce” o la “roba”. Una delle modalità di cui si avvalgono i malintenzionati per trasferire e “riciclare” il denaro rubato è rappresentata dall’acquisto di prodotti nei negozi online, mediante l’utilizzo dei mezzi finanziari illecitamente sottratti; gli articoli in questione vengono poi rivenduti, mentre ai rapinatori informatici viene restituita la percentuale prestabilita, calcolata sul valore del’importo rubato. Gli “stuffer” si occupano proprio di questo; si tratta dei membri del gruppo cybercriminale che spendono i soldi depositati sui conti bancari violati, per l’acquisto di merci nei negozi Internet.

Di fatto, lo “stuffer” costituisce una variante della figura del “prelevatore”, anche se, nella circostanza, il trasferimento del denaro rubato, tramite l’acquisto di prodotti e articoli di vario tipo, viene in genere praticato nel caso di furti di entità relativamente limitata. Di solito, gli stuffer operano a stretto contatto con coloro che si accaparrano le somme rubate. Tale collaborazione significa, spesso, l’esecuzione di specifici ordini, emessi dagli “accaparratori”, riguardo all’acquisto di un determinato tipo di merce; talvolta, vengono persino richiesti, da questi ultimi, particolari marche e modelli.

### Organizzatore

Se consideriamo il cybercrimine alla stregua di un progetto, allora l’organizzatore del gruppo di malfattori potrebbe essere indicato come il general manager dello stesso. I principali compiti che egli abitualmente svolge sono i seguenti: finanziamento della fase preparatoria dell’attacco informatico; assegnazione degli incarichi ai relativi esecutori; monitoraggio dell’effettiva realizzazione dei task distribuiti; interazione con gli elementi esterni, quali i “drop project” e i “call service” (nel caso in cui l’organizzatore non disponga di servizi del genere all’interno del proprio gruppo). L'organizzatore definisce gli obiettivi degli attacchi, effettua la selezione degli “esperti” necessari per la loro realizzazione e si occupa della retribuzione dei collaboratori.

## Fasi di realizzazione degli attacchi

Occorre innanzitutto evidenziare come la classificazione sopra descritta non risulti ad ogni caso rigida. In alcuni casi, ad esempio, uno stesso membro del gruppo cybercriminale può svolgere e combinare tra loro vari ruoli. Le funzioni e gli incarichi sopra elencati, tuttavia, indipendentemente dal numero di persone che provvedono al loro compimento, possono essere praticamente individuati, nel corso delle indagini svolte, nell’ambito di qualsiasi crimine di natura informatica collegato al furto del denaro. Descriveremo, qui di seguito, le specifiche modalità che determinano il funzionamento e l’interconnessione “in tempo reale” dei vari ruoli assegnati all’interno della gang cybercriminale.

1. **Esplorazione preliminare.** Nel caso di un assalto mirato nei confronti di una determinata società, l’organizzatore del gruppo ordina inizialmente ai propri collaboratori di raccogliere informazioni riguardo alla società da sottoporre ad attacco; questo consente, di fatto, di poter sviluppare schemi di ingegneria sociale ancor più plausibili, i quali saranno poi dispiegati nella prima fase dell’attacco. Nel caso, invece, di un attacco rivolto ad utenti privati, la fase di prospezione preliminare non viene in pratica realizzata, oppure si limita alla scelta di un “pubblico mirato”, ovvero il target potenziale del crimine (ad esempio gli utenti dei servizi di Internet banking implementati da specifici istituti bancari); a questo si aggiungono la composizione di messaggi e-mail di phishing, e la realizzazione di siti web di phishing di analogo contenuto.

2. **Infezione** La penetrazione nella rete informatica interna viene effettuata mediante l’invio mirato (spear-phishing), o in massa, di e-mail di phishing, contenenti in allegato un documento redatto in maniera apposita, oppure provviste di un link nocivo destinato a condurre l’utente-vittima verso un sito web dannoso. L’apertura del documento allegato al messaggio e-mail, o il fatto di cliccare sul link dannoso presente in quest’ultimo, genera l’infezione del sistema informatico, realizzata attraverso uno specifico programma malware. Spesso, l’infezione informatica si produce in maniera automatica, all’insaputa dell’utente, senza che quest’ultimo compia un’azione specifica in tal senso; in effetti, semplicemente seguendo il link nocivo, viene avviato in modalità automatica il download di un programma maligno (drive by download) sul computer-vittima; il software nocivo viene poi eseguito all’interno del sistema sottoposto ad attacco.

In altri casi, l'infezione viene realizzata attraverso siti web compromessi; si tratta, in genere, di siti particolarmente popolari presso il pubblico della Rete, all’interno dei quali viene collocato un apposito strumento dannoso per il redirecting furtivo degli utenti verso un sito Internet nocivo, che ospita un temibile kit di exploit. Una volta che l’utente sarà giunto su tale sito, il computer-vittima verrà infettato dal malware.

In seguito, i cybercriminali ricorrono all’utilizzo di una serie di strumenti dannosi, i quali consentono al malware di consolidare la propria presenza all’interno del sistema infetto. Vengono ad esempio violati e infettati, tramite apposito software nocivo, i siti interni dell’organizzazione presa di mira, per garantire l’eventuale nuova installazione del malware, nel caso in cui il software di sicurezza presente nei computer sottoposti ad attacco abbia rimosso la precedente versione del malware dispiegato. Spesso, inoltre, i malintenzionati provvedono ad installare, all’interno dell’infrastruttura-vittima, un apposito software che consente di ottenere un facile accesso, dall’esterno, alle reti informatiche interne di cui è provvista l’organizzazione.

3. **Realizzazione dell’attacco**. Sui computer violati vengono caricati programmi nocivi adibiti all’amministrazione e alla gestione furtiva da remoto, attraverso il cui utilizzo i criminali cercano di impossessarsi dei dati sensibili relativi agli account abitualmente utilizzati dagli amministratori dei sistemi. Nella circostanza, viene fatto ampio uso di programmi di fatto legittimi, adibiti all’amministrazione e alla gestione da remoto, le cui funzionalità sono peraltro note a molti utenti.

4. **Furto del denaro.** Nella fase finale viene effettuato l’accesso ai sistemi che permettono di interagire con le risorse finanziarie prese di mira, ed il successivo trasferimento delle somme di denaro, sottratte dagli account dell’organizzazione sottoposta ad attacco, sui conti bancari riconducibili ai “drop project”; in alternativa, [il prelievo del denaro rubato viene realizzato direttamente attraverso gli apparecchi bancomat](https://securelist.ru/blog/issledovaniya/23950/tyupkin-manipulirovanie-bankomatami-s-pomoshhyu-vredonosnogo-po/).

## Conclusioni

L’ampia diffusione, in questi ultimi anni, del cybercrimine finanziario organizzato da criminali russofoni è dovuta a numerose cause. Le principali sono indubbiamente le seguenti:

* quantità insufficiente di personale qualificato nell’ambito delle forze dell’ordine;
* falle a livello legislativo, le quali, nella maggior parte dei casi, consentono ai cybercriminali di poter sfuggire alle loro precise responsabilità, o ricevere pene piuttosto lievi;
* assenza di procedure consolidate di collaborazione, su scala internazionale, tra forze dell’ordine ed esperti di società ed organizzazioni di vari paesi.

A differenza di quanto avviene nel mondo reale, le rapine compiute nel cyberspazio, in genere, passano inizialmente inosservate; spesso, poi, le prove digitali relative al reato commesso possono essere raccolte solo in un intervallo di tempo estremamente limitato, dopo che l’atto criminoso è stato ormai compiuto. Inoltre, per i criminali informatici non è affatto necessario trovarsi fisicamente sul territorio del paese in cui viene realizzato il furto di denaro.

Per il momento, purtroppo, le condizioni attualmente esistenti si dimostrano, per il cybercriminale russofono, quantomai favorevoli: vi è, in effetti, un basso rischio di essere perseguito penalmente, mentre il potenziale guadagno che può essere realizzato si prospetta decisamente elevato; tutto questo lascia ovviamente intravedere, al malintenzionato, il buon esito dell’impresa criminale che egli intende realizzare. Di conseguenza, il numero dei crimini finanziari risulta in costante crescita; peraltro, le perdite economiche da essi provocate si stanno amplificando, mentre sta aumentando in maniera considerevole il giro di affari che ruota attorno al mercato dei servizi cybercriminali.

L’assenza di meccanismi consolidati di collaborazione internazionale gioca inevitabilmente a favore dei criminali informatici: gli esperti di Kaspersky Lab, ad esempio, sanno che i membri di alcuni gruppi dediti al cybercrimine soggiornano e “lavorano” in maniera permanente sul territorio di paesi limitrofi alla Russia. Al contrario, vi sono cittadini dei paesi confinanti, persone chiaramente coinvolte in attività criminose, che si trovano, ed operano di frequente, sul territorio della Federazione Russa.

Kaspersky Lab sta facendo tutto il possibile per neutralizzare le attività nocive condotte dai gruppi cybercriminali, ed invita le altre società, così come le forze dell'ordine di tutti i paesi, ad una fattiva collaborazione.

L’indagine a carattere internazionale avviata dalla nostra società in merito alle attività svolte dal famigerato gruppo Carbanak costituisce il primo esempio di una cooperazione di successo su scala internazionale; tuttavia, per far sì che possano prodursi cambiamenti davvero radicali, riguardo alla situazione del cybercrimine finanziario, dovranno necessariamente intervenire numerosi altri esempi del genere.

## Informazioni aggiuntive riguardo alla Divisione per le Indagini sugli Incidenti Informatici istituita da Kaspersky Lab

Kaspersky Lab è una società conosciuta, in primo luogo, in qualità di sviluppatore di sistemi di protezione nei confronti dei programmi malware. L’attività dell’azienda, tuttavia, è ugualmente focalizzata sulla fornitura di servizi volti ad offrire una protezione efficace e completa per dati e informazioni sensibili; rientrano nel novero di tali iniziative i servizi che prevedono la conduzione di apposite indagini riguardo agli incidenti informatici.

Le prove che testimoniano quanto è avvenuto in relazione agli incidenti informatici che si verificano di volta in volta, presentate principalmente in forma di dati digitali, debbono essere rilevate, raccolte e registrate in modo tale che, nel momento in cui la vittima dichiara di aver subito l’atto criminale, tali elementi non suscitino dubbi, sia durante la conduzione delle indagini, sia durante il successivo svolgimento del processo legale.

I principali compiti a cui è preposta la Divisione per le Indagini sugli Incidenti Informatici allestita da Kaspersky Lab, sono i seguenti:

* pronta reazione nei confronti degli incidenti informatici che riguardano la sicurezza IT ed immediata analisi operativa della situazione;
* raccolta delle prove digitali relative agli incidenti informatici occorsi; definizione delle circostanze ad essi correlate, in conformità alle metodologie elaborate.
* analisi degli elementi raccolti in qualità di prova; ricerca in Internet di informazioni collegate alle circostanze dell'incidente; risoluzione delle problematiche riscontrate;
* preparazione del materiale occorrente alla vittima per rivolgersi alle forze dell’ordine;
* adeguato supporto, da parte di esperti, nella conduzione delle attività investigative ed operative.

Nel processo di pronta reazione nei confronti degli incidenti informatici inerenti alla sicurezza IT, e di supporto delle indispensabili attività investigative ed operative, si presenta la necessità di dover lavorare con massicce quantità di dati, la cui analisi, assieme allo studio dei dati statistici relativi agli oggetti nocivi individuati, contribuisce in maniera determinante a mettere in luce i complessi meccanismi e la costante evoluzione che caratterizzano i vari modelli di comportamento criminale nell’ambito del cyberspazio.

Il dipartimento qui sopra descritto è stato creato nell'anno 2011. Nella divisione operano 6 esperti forensi.