

LA CARTA D'IDENTITÀ DEI CYBERCRIMINALI

Autore di Trojan – programmi che carpiscono informazioni all'insaputa degli utenti	
Età	26
Reddito	I Trojan possono valere fino a 3.000 dollari sul mercato clandestino e, a seconda della località di residenza, possono essere addirittura un lavoro a tempo pieno.
Ruolo attuale	Programmatore: <ul style="list-style-type: none"> - Sviluppa esclusivamente virus - Crea codice pericoloso professionalmente sulla base delle esigenze e delle specifiche dei committenti. - Vende inoltre soluzioni "all-in-one" che includono manuali, tool di configurazione, pagine server, supporto e aggiornamenti - Fornisce ai clienti Trojan aggiornati
Competenze principali	<ul style="list-style-type: none"> - Programmatore altamente competente - Molto aggiornato in materia di software e tecnologie antivirus - Buone competenze linguistiche
Formazione	<ul style="list-style-type: none"> - Esperienza di programmazione - Corso di informatica di livello universitario - Autodidatta frequentando forum - Ha iniziato a utilizzare malware gratuito prelevato dai forum
Personalità	<ul style="list-style-type: none"> - Paziente - Trascorre moltissimo tempo nello sviluppo di un Trojan in quanto la qualità deve necessariamente rispondere a standard molto elevati a causa dello scenario competitivo - Geek - Seduto al computer tutto il giorno - Introverso – Non ama pubblicizzare il suo lavoro
	-

Esperto di exploit – Sistemi per carpire dati nel settore dell'home banking	
Età	23
Reddito	<ul style="list-style-type: none"> - 10.000 dollari per un exploit mai sfruttato prima (exploit 0-day) - 6.000 - 10.000 dollari per exploit venduti a software house legittime - Non è una professione a tempo pieno in quanto gli exploit possono richiedere anche mesi per essere sviluppati
Ruolo attuale	Sviluppatore <ul style="list-style-type: none"> - Sviluppa kit semplici da usare - Trova exploit '0-day' e crea codice che può infettare gli utenti con payload pericolosi restando nascosto e infettando i visitatori che si connettono a un determinato sito Web. - Fa parte di un team tecnico, riesce a combinare exploit multipli in un kit "tutto in uno".

Competenze principali	<ul style="list-style-type: none"> - Livello di sviluppo più basso - Molto tecnico - Adatto al lavoro in squadra - Necessità di sapere ciò che è disponibile sul mercato - Attenzione al dettaglio - Come ad esempio modificare gli exploit per comprendere le loro modalità di funzionamento. - Pieno di risorse - Non ci sono molti strumenti né consigli nei forum per aiutare a trovare exploit
Formazione	<ul style="list-style-type: none"> - Autodidatta frequentando forum – Ha iniziato a utilizzare codice altrui, modificandolo e adattandolo successivamente
Personalità	<ul style="list-style-type: none"> - Paziente – Non molti fanno questo lavoro vista la mole di lavoro che comporta - Geek - Seduto al computer tutto il giorno
	-

Venditore di traffico su Internet per il phishing (es. bot header) –	
Età	32
Reddito	<ul style="list-style-type: none"> - Stabile: coinvolto solo per denaro (1 euro per ogni 1.000 click)
Ruolo attuale	<p>Reindirizzatore di siti</p> <ul style="list-style-type: none"> - Dirotta i click degli utenti verso siti pericolosi utilizzando un iFrame nascosto sul suo sito Web o violando siti Web utilizzando account FTP rubati. - In contatto con i "bot header" o bot header personalmente (Bot header = controllo di una grande quantità di computer che sono stati infettati da un Trojan)
Competenze principali	<ul style="list-style-type: none"> - Organizzato - Raccoglie il traffico e lo dirotta verso un sito diverso - Proattivo - Approccio imprenditoriale - Ottime capacità di relazione interpersonale
Formazione	<ul style="list-style-type: none"> - Corso di business/marketing - Corso di informatica
Personalità	<ul style="list-style-type: none"> - Mentalità business - Sicuro di sé/ arrogante
	-

Società di rogue hosting – Il vertice della piramide del cybercrime

Età	45
Reddito	Considerevole
Ruolo attuale	<ul style="list-style-type: none">- Fornisce un valido servizio di hosting e un'infrastruttura di rete affidabile, anonima, non tracciabile e protetta da L.E.- Si tratta di aziende vere e proprie abbastanza pulite per essere registrate (come attività legittime) ma altrettanto in buoni rapporti con i criminali del malware da riuscire a entrare nel giro.
Competenze principali	<ul style="list-style-type: none">- Servizio a prova di bomba- Conosce a perfezione il settore e i relativi trucchi del mestiere- Sa anticipare potenziali episodi di disastro.
Formazione	Nessuna formazione - formazione sul campo
Personalità	<ul style="list-style-type: none">- Mentalità "non si fanno prigionieri"- Freddo, riservato- Interessato solo a fare soldi- Ben addentro all'economia sommersa

Ideatore di frodi

Età	Tutte (18 – 45)
Reddito	<ul style="list-style-type: none">- Dipende dal livello di rischio intrapreso- Deciso a fare carriera: più rischi = più soldi = più successo
Ruolo attuale	<p>Criminale</p> <ul style="list-style-type: none">- Raccolgo tutti i dati rubati e li rivende sul mercato sommerso (in base alla qualità delle informazioni)- Talvolta utilizzo personalmente tali dati per sottrarre denaro
Competenze principali	<ul style="list-style-type: none">- Ben informato dei temi del momento- Ben addentro all'ambiente, con accesso a tutte le conversazioni tra i "VIP" del sottobosco criminale.- So come fare colpi per guadagnare velocemente
Formazione	<ul style="list-style-type: none">- Corso informatica- Formazione criminale- Formazione sul campo- Ho probabilmente avuto un buon mentore
Personalità	<ul style="list-style-type: none">- Bugiardo- Immorale- Senza rimorsi- Ambizioso - farei qualsiasi cosa per il successo- Traditore
Modalità per bloccarlo	<ul style="list-style-type: none">- Tecnologia: Protezione browser- Il creatore di frodi può comprare informazioni dall'economia sommersa, in questo caso esce dal lato informatico della faccenda e dunque non siamo in grado di fornire protezione. Tuttavia alcuni di questi

	<p>personaggi utilizzeranno Trojan per raccogliere dati, incontrando gli stessi problemi dell'autore di Trojan; altri raccolgono informazioni utilizzando tecniche di phishing come per esempio il dirottamento degli utenti verso pagine fasulle. In questo caso i nostri prodotti per la protezione del browser avvisano gli utenti nel momento in cui passano a navigare su un sito illegittimo.</p>
--	---