# Cryptovirology

**Tecniche di offuscamento degli attacchi informatici.**
**Dove l'Antivirus non arriva...**

All rights reserved

ISACA
Trust in, and value from, information systems

# Agenda

- Intro: Who we are
- Obiettivi
- Definizioni
- La Criptovirologia
- Storia della Criptovirologia
- I moderni malware
- Il «malware reuse»
- Un po' d'azione: esempio pratico

All rights reserved

ISACA
Trust in, and value from, information systems

# Intro: who we are

- Stefano «Ahriman»: Chief Research Officer della divisione che si occupa della malware analysis e di R&D per un Centro di Ricerca italiano.
- È stato nel passato uno dei fondatori di un noto portale dell'underground nonché membro di un famoso gruppo di hacker internazionale.

- Viotto: Cryptoanalyst. È un coder e, nel passato, un malware writer… oggi si è redento ☺ e porta la sua esperienza nella nostra struttura di ricerca.

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Obiettivi

- Il nostro intervento ha l'obiettivo di mostrare i nuovi trend nello sviluppo dei malware
- In particolare vedremo le modalità di «riutilizzo» di malware una volta che essi perdono lo stato di «FUD» (ovvero di Fully UnDetectable) attraverso i Packer e i Crypter
- Faremo poi un excursus tecnico su queste tematiche
- Mostreremo poi un esempio pratico con un crypter da noi sviluppato che ha le stesse modalità in uso ai crypter maliziosi

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Un po’ di definizioni

- Malware
- Packer
- Crypter
- Algoritmi di Cifratura e Chiavi
- RAT
- Stealer
- FUD
- Ratio

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Definizione: Malware

- Malware: software malevolo, solitamente installato su di un computer all'insaputa dell'utente. Il malware si suddivide in numerosi tipi:
  - virus
  - trojan horse
  - backdoor
  - spyware
  - worm
  - ...

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Definizione: Packer

- Un **packer** è uno strumento che permette di rendere difficile l'analisi di un file eseguibile o, semplicemente, di ridurne la sua dimensione.
- I packer vengono sovente usati nelle versioni limitate di prodotti commerciali per impedire, o perlomeno scoraggiare, la creazione di crack.
- Essi usano delle tecniche anti-debug e anti-disassembly sempre più avanzate che, se non sono interpretate nella maniera giusta dal debugger/disassembler, fanno perdere molto tempo al cracker (o al reverser in generale).

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Definizione: Crypter

- **Crypter**: un particolare tipo di malware adibito a rendere un altro malware invisibile ai software di sicurezza (comunemente antivirus).
- Le case di antivirus si occupano di bloccare la distribuzione di un nuovo malware nel minor tempo possibile.
- Gli sviluppatori di crypter si occupano di rimanere un passo avanti agli antivirus creando in breve tempo nuove varianti invisibili agli AV.

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Definizione: Algoritmo di cifratura e Chiave

- **Algoritmo di cifratura**: una funzione che trasforma, attraverso una chiave di cifratura, un input di dati in chiaro in un output di dati criptati non analizzabili.

- **Chiave di cifratura**: una sequenza di byte che specifica come trasformare i dati input nella loro forma cifrata. Se non si è a conoscenza dell'algoritmo di cifratura e della chiave utilizzati, non è possibile riportare i dati nella loro forma originaria.

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Definizione: RAT

- **RAT**: abbreviazione di Remote Administration Tool (o Remote Access Trojan): un malware con cui un hacker è in grado di assumere il controllo completo della macchina su cui è installato. Solitamente i RAT sono composti da 2 parti distinte:
  - **Backdoor**: applicazione installata sul computer vittima che permette, in maniera invisibile all'utente legittimo, l'accesso remoto da parte dell'hacker.
  - **Applicazione di controllo**: programma fornito di interfaccia utente che permette all'hacker di controllare da remoto le macchine infette.

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Definizione: Stealer

- Uno **Stealer** è un particolare tipo di malware, simile ad un keylogger, che ruba informazioni di login dal computer infetto e le invia all'hacker.
- La differenza rispetto ad un keylogger è che quest'ultimo solitamente registra tutti gli input ricevuti dalla tastiera, mentre uno stealer anzichè registrare i tasti premuti cerca nel sistema le informazioni di login salvate.

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Definizione: FUD

Abbreviazione di ***Fully UnDetected*** (completamente non rilevato).

Dicesi di un malware non rilevato da alcun antivirus.

Solitamente i nuovi malware al momento del loro rilascio sono FUD o rilevati solo da alcuni antivirus.

Non appena una compagnia di antivirus riesce a recuperare un file sospetto che non conosce, e analizzandolo ne identifica un comportamento anomalo o malizioso essa lo classifica con una "signature" (firma specifica) al database del proprio antivirus, che verrà poi distribuita agli utenti nel successivo aggiornamento.

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Definizione: Ratio o Detection Rate

Percentuale di rilevamento di un malware in un insieme di antivirus.

Vi sono vari siti web che offrono servizi di scan di un file utilizzando numerosi motori antivirus differenti.

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Come funzionano gli Antivirus?

- Ogni file eseguibile, in ambiente Microsoft non è altro che una sequenza di comandi.
- Ogni programma ha sequenze di linee di codice caratteristiche, che lo contraddistinguono e ne identificano le funzioni in modo puntuale.
- Anche i virus hanno sequenze di codice che li identificano in quanto descrivono il loro funzionamento.
- L'antivirus ha nel proprio database queste sequenze, per poterle riconoscere quando scansiona un file.

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Come funzionano gli Antivirus?

- Gli Antivirus operano secondo questo meccanismo:
  - Ogni volta che un file è aperto nel sistema l'Antivirus tende a scansionarlo per verificarne la "bontà".
  - Essi computano e registrano la signature di ogni file e la mantengono nel proprio database.
  - Quando un file viene aperto essi comparano la signature del file con quella presente nel loro database. Se il controllo è coerente il file viene eseguito. In caso di mancata coerenza il file viene considerato corrotto o sospetto e viene bloccato nell'esecuzione con relativa segnalazione all'Utente.
- Alcuni antivirus adottano anche altre tecniche euristiche, ma la sostanza non cambia.

Content is a Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# La Criptovirologia

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# La Crittografia e la Crittanalisi

- **La Crittologia si suddivide in due campi:**
  - La **Crittografia**, dedicata alla creazione di procedure, in grado di garantire la riservatezza, l'autenticazione e l'integrità.
  - Si basa sull'utilizzo di chiavi e/o funzioni matematiche specifiche.
  - La **Criptoanalisi**, dedicata allo studio delle procedure in grado di escludere la riservatezza, l'autenticazione e l'integrità.
  - Si basa solitamente su teorie matematiche complesse.

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# La criptovirologia

- **Criptovirologia (Cryptovirology in inglese)**
- È un campo che studia i metodi di utilizzo della crittografia nella progettazione e nella protezione di malware.
- Il campo è nato a cavallo tra la fine degli anni novanta e i primi anni del nuovo millennio.
- Il primo attacco che ha usato la crittografia è stato registrato nel 1996. Si trattava in quel caso di un tentativo di estorsione[1]. Il Coder aveva progettato un worm in grado di crittare i file delle proprie vittime, impedendo loro di accedere ai propri dati, e chiedeva del denaro in cambio della chiave che avrebbe permesso ai malcapitati di tornare in possesso di versioni "in chiaro" dei propri file.

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

[1] **Young, A., Moti Yung : Cryptovirology: extortion-based security threats and countermeasures**

# La criptovirologia

- La crittografia viene utilizzata dai produttori di software di ogni tipo per garantire la riservatezza della propria base dati e del proprio eseguibile.
- Oggi viene utilizzata anche dai coderz per garantire la riservatezza del codice malevolo e per evitare la rilevazione e la successiva analisi dello stesso.
- Da questo ambito nasce la crittovirologia, il cui intento è quello di studiare meccanismi di sviluppo e di analisi usati dai coderz per impedire la visione del loro codice malevolo.
- Oggi si aggiunge a questo fronte quello dello studio degli specifici metodi di crittografia usati dai coderz per il «malware reuse», il riutilizzo dei malware già identificabili dagli antivirus.

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

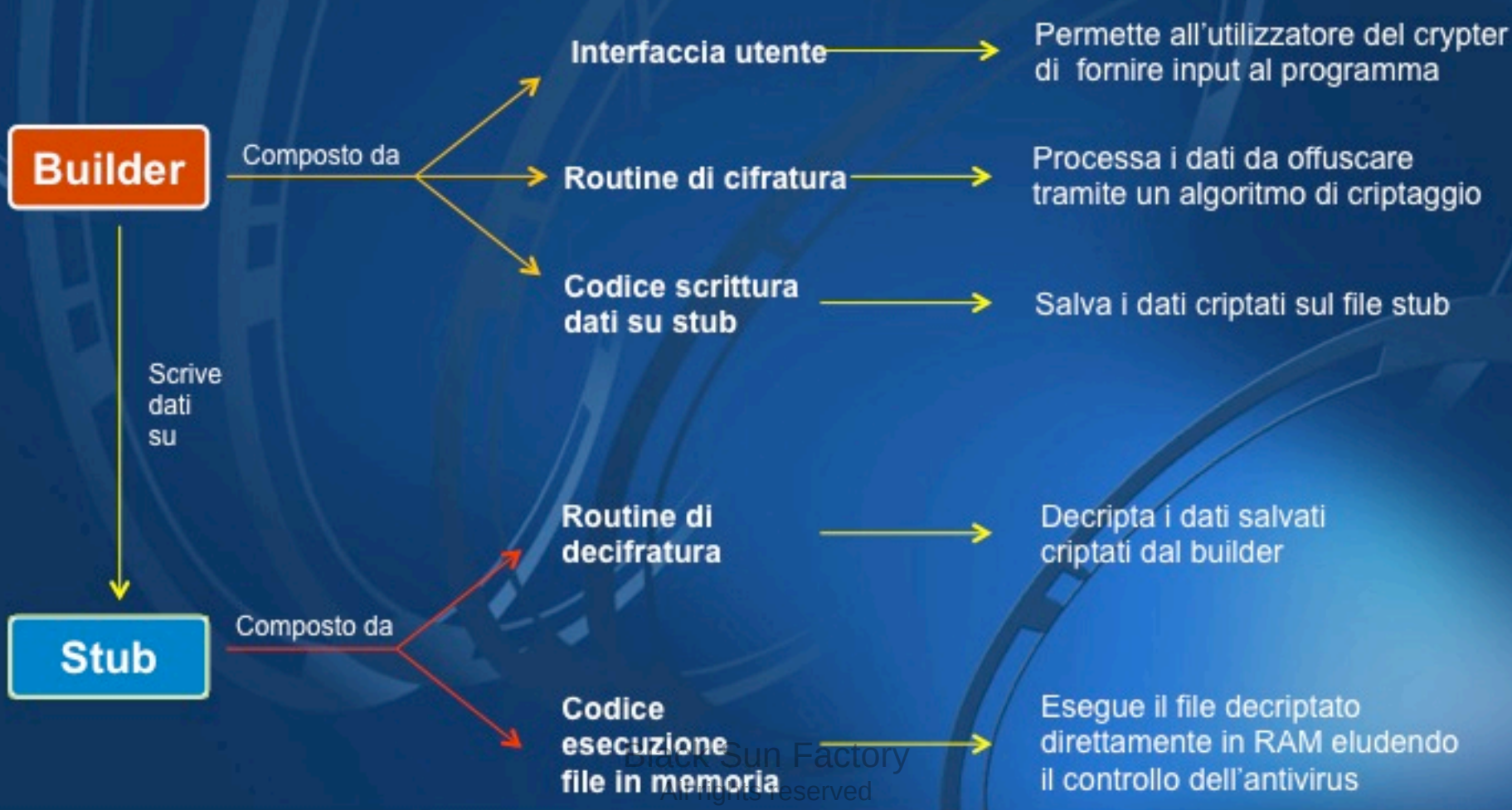
# Un Crypter

- Un antivirus può riconoscere un malware sulla base del codice da cui è composto.
- Se all'interno di un file sono presenti sequenze di codice e di comandi già censiti, allora quel file è, oppure contiene, un virus e l'antivirus lo segnala.
- Un **crypter** ha lo scopo di nascondere quelle parti di codice che un antivirus riconoscerebbe come infette, mascherandole con una porzione di codice pulito e apparentemente innocuo: al momento della scansione con l'antivirus, sarà proprio la parte sostituita a essere esaminata, mentre la parte infetta resterà al sicuro, nascosta dietro di essa. L'antivirus non la vedrà, perché le parti di codice che riconosce come virus gli sono state nascoste, ricoperte da un codice che, invece, non può identificare.

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# I componenti di un Crypter

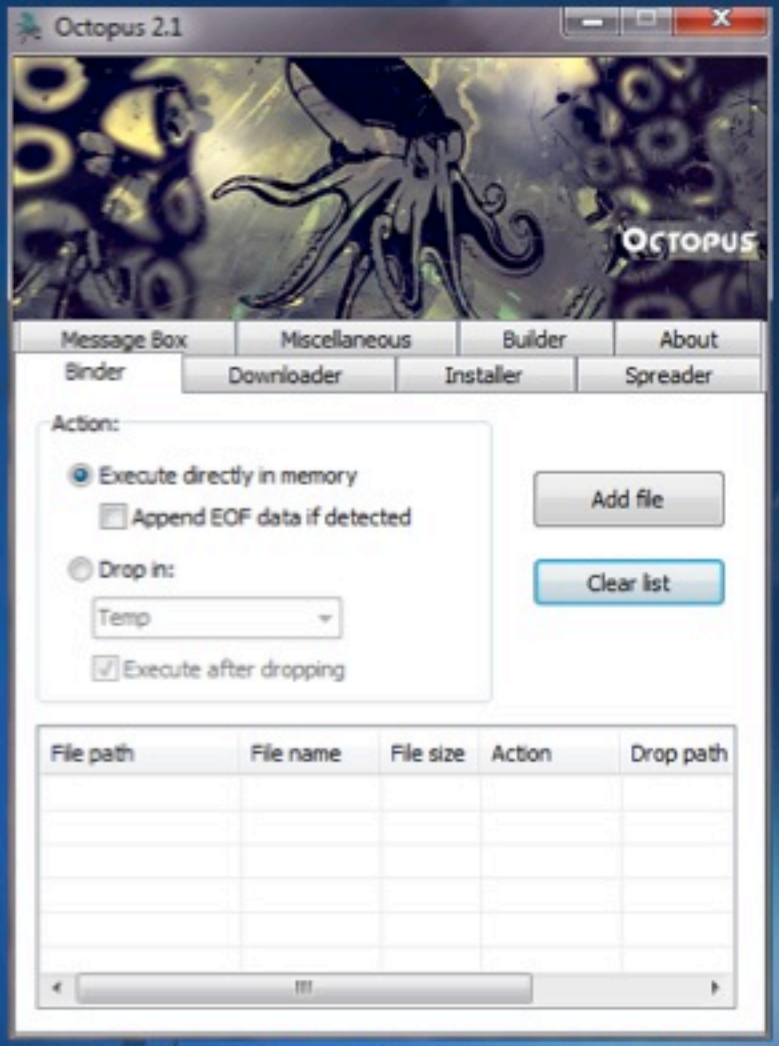



Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Builder

Il builder è la parte del software, normalmente fornita di interfaccia grafica, che permette all'utente malevolo di costruire il payload finale. Nel builder ad esempio è possibile selezionare quale/i file criptare, selezionare il file stub da utilizzare, attivare funzioni aggiuntive ed infine salvare il file output, che consiste nel file stub + i dati salvati su di esso.




*Come si presenta all'apertura l'interfaccia del builder del crypter «Octopus» versione 2.1*

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Routine di Crittografia

- Come si può intuire dal nome stesso, in un **crypter è fondamentale una funzione che cripta il codice dei files da nascondere agli antivirus**.
- Il codice del file malevolo, normalmente rilevato da antivirus, viene processato da un algoritmo di criptaggio adeguato (spesso l'RC4, lo stesso utilizzato negli algoritmi WEP e WPA dedicati alla protezione delle reti wireless) e trasformato in un codice cifrato inutilizzabile e non analizzabile se non viene prima decriptato utilizzando la giusta chiave.
- Gli antivirus in tal modo non possono rilevare il file malevolo, che comunque non può essere eseguito prima della decriptaggio.

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Codice di salvataggio dati

- Dopo aver criptato il file, il builder deve salvarlo (insieme ad altre eventuali configurazioni) all'interno del file stub, che si occuperà al momento della sua esecuzione di decriptare il codice malevolo ed eseguirlo in memoria.
- I metodi utilizzati per scrivere dati su di un file eseguibile sono vari, ad esempio possono essere salvati all'interno di una risorsa o aggiunti alla fine del file .

**File output (stub + dati criptati)**

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

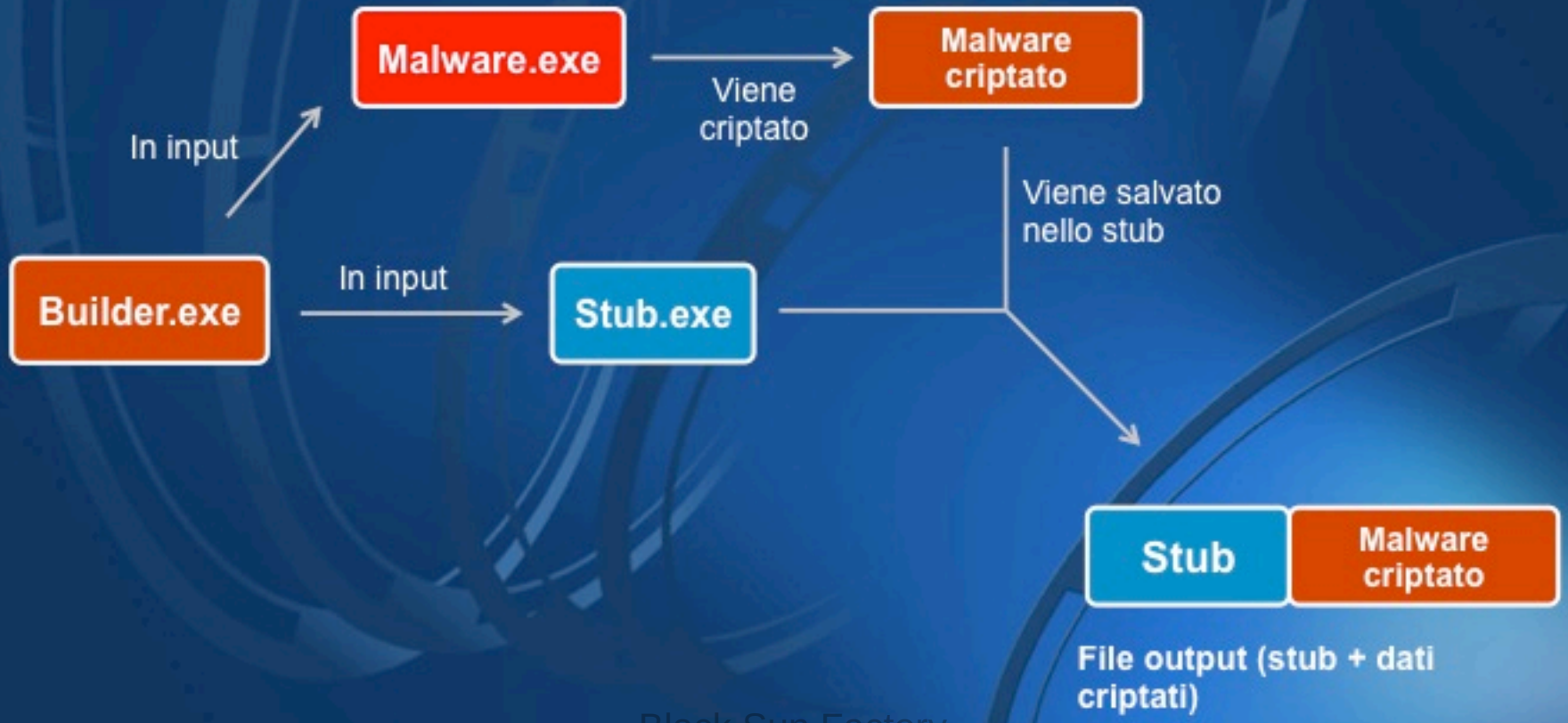
# Lo Stub

- Lo stub (letteralmente: «moncone») è il file malevolo vero e proprio.
- In esso  vengono scritte le impostazioni ed i dati criptati dal builder.
- Il suo nome deriva dal fatto che questo file per essere funzionante necessita dei dati scritti dal builder, che devono essere decriptati e processati.
- Questo file,  una volta eseguito, legge le impostazioni fornite dal builder, decripta il file e lo esegue, il tutto direttamente in memoria bypassando i controlli dell'antivirus.

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Struttura delle operazioni effettuate dal builder




Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Routine di decifratura

- Una funzione analoga a quella di cifratura presente nel builder.
- Riporta i dati offuscati nella loro forma originaria ed eseguibile, salvandoli in una variabile. Salvata da qualche parte all'interno dello stub deve essere presente la chiave di cifratura (una sequenza di byte) che permette di decifrare correttamente i dati criptati.

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

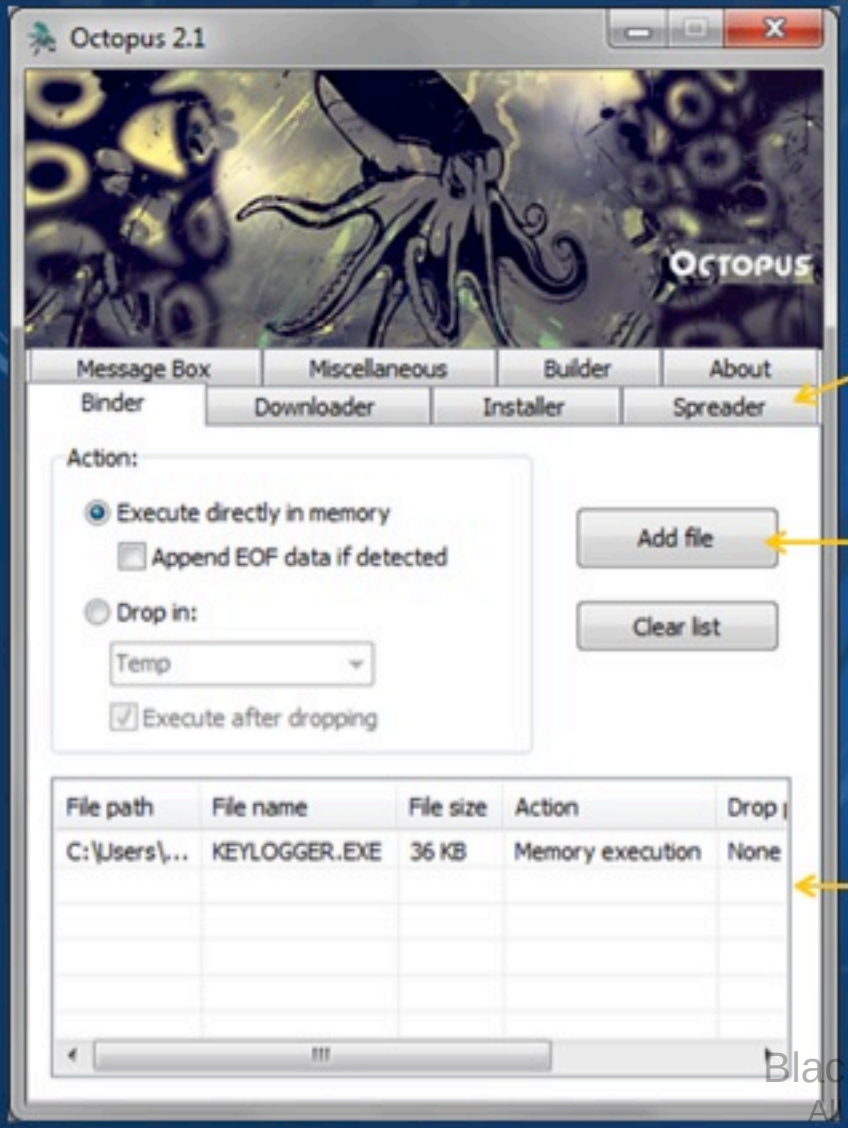
# Funzione di esecuzione file in memoria

- Codice che esegue il file malevolo decriptato. Il file , non essendo mai presente nella sua forma decriptata sul disco rigido, non viene bloccato da antivirus. La funzione di esecuzione in  memoria, infatti, esegue il file salvato in una variabile direttamente nella RAM.

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Esempio di crypter avanzato: Octopus




Varie funzioni addizionali

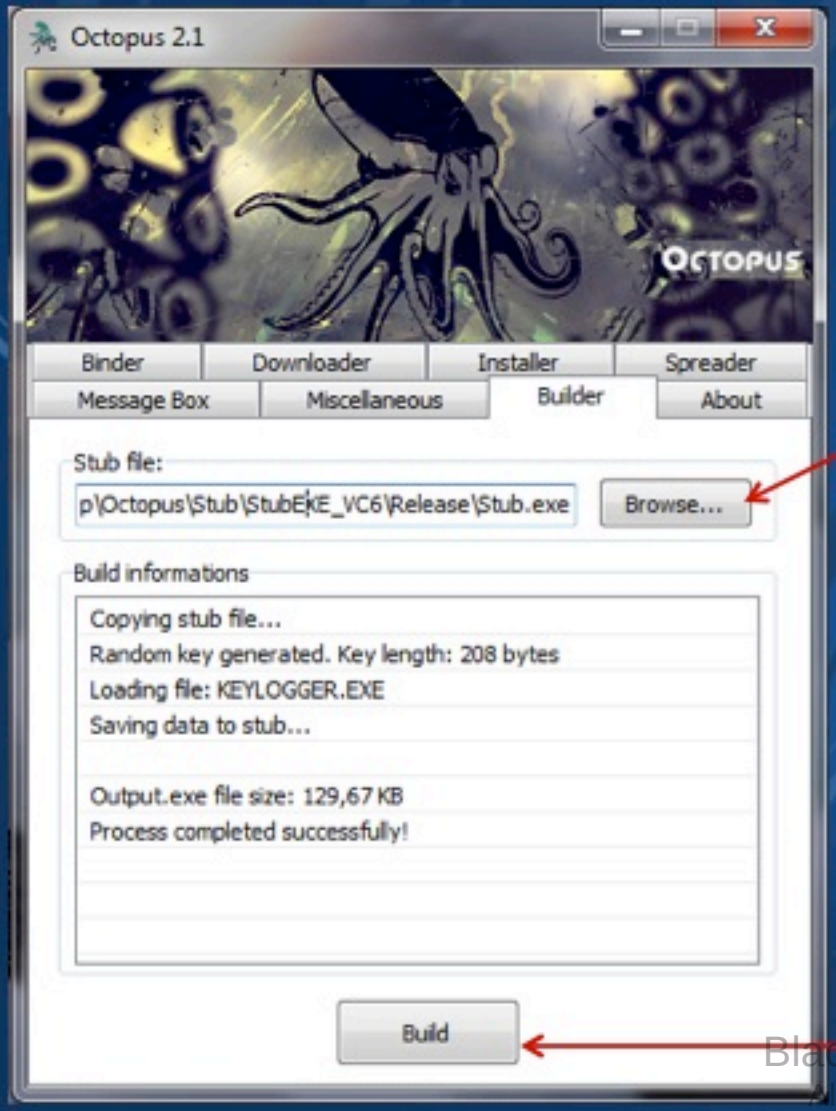
Bottone per aggiungere file da criptare

Lista di file che verranno salvati nello stub

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Esempio di crypter avanzato: Octopus




Bottone per selezionare il file stub su cui salvare i dati

Bottone che avvia il processo di costruzione del file di output

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

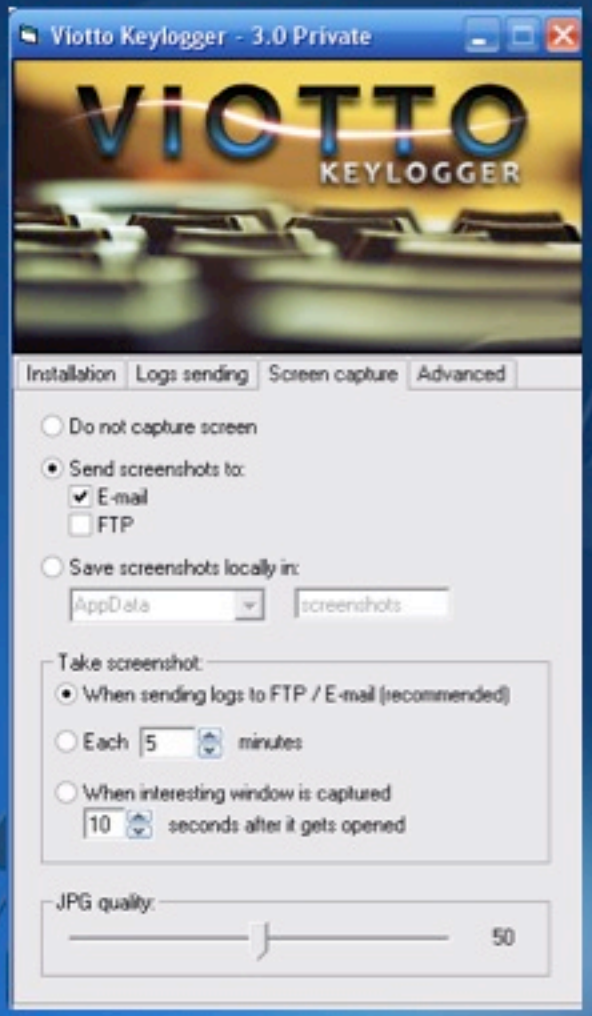
# Esempio Pratico

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Viotto Keylogger

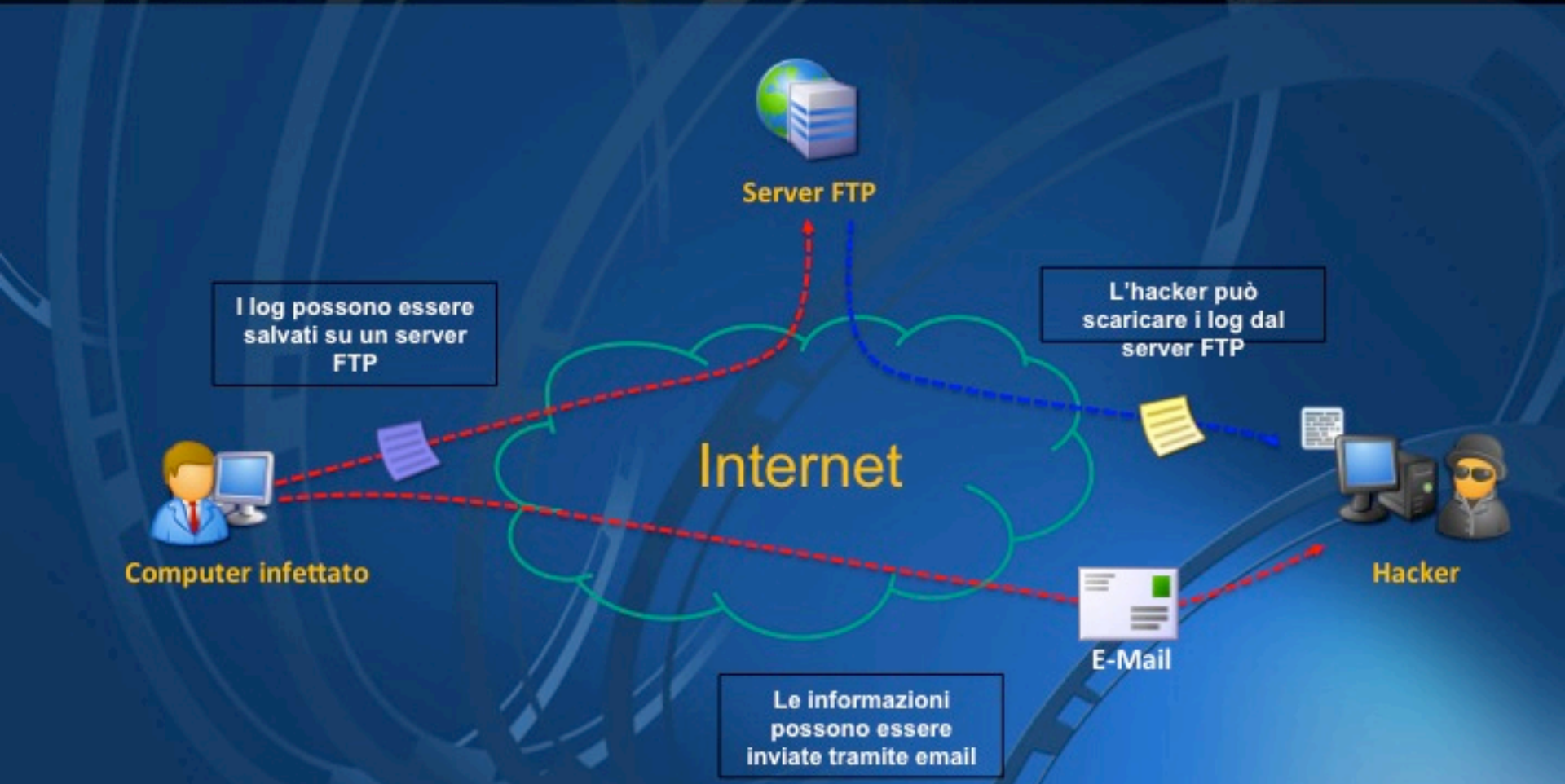
In questo esempio utilizzeremo uno spyware denominato Viotto Keylogger. Questo programma si installa di nascosto sul computer ospite ed è in grado di registrare input sulla tastiera, screenshots, titoli delle finestre aperte, dati copiati o incollati tramite clipboard, intervallo di inattività se l'utente non è al computer, ed altro ancora. Queste informazioni sono poi inviate tramite FTP o email all'hacker, secondo dei parametri specificati nel builder.




Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Schema di invio dati di Viotto Keylogger



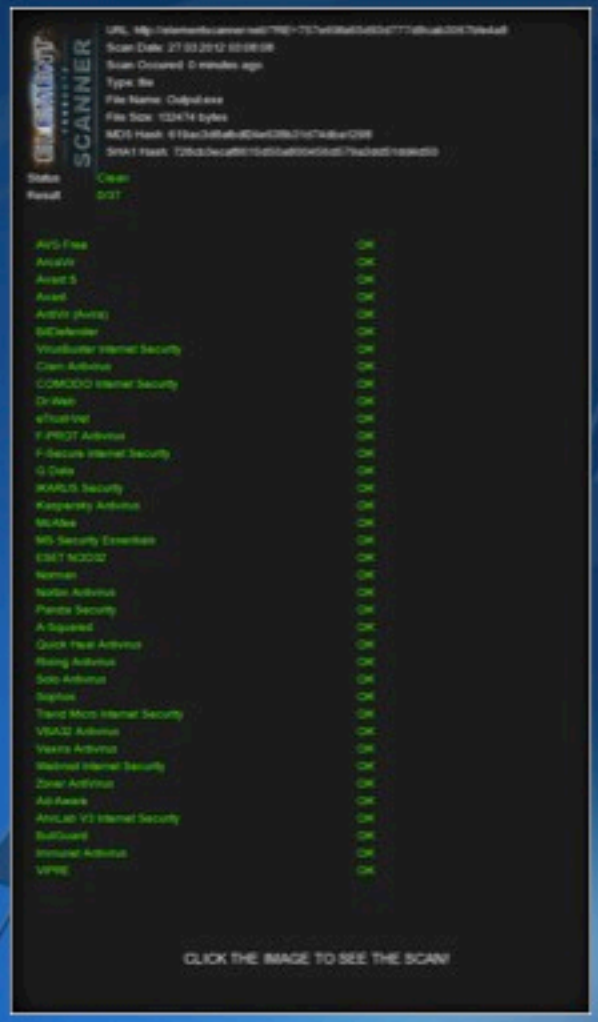

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Viotto Keylogger Ratio: prima e dopo…

Octopus crypter

Il keylogger viene criptato utilizzando il crypter Octopus, che lo rende FUD

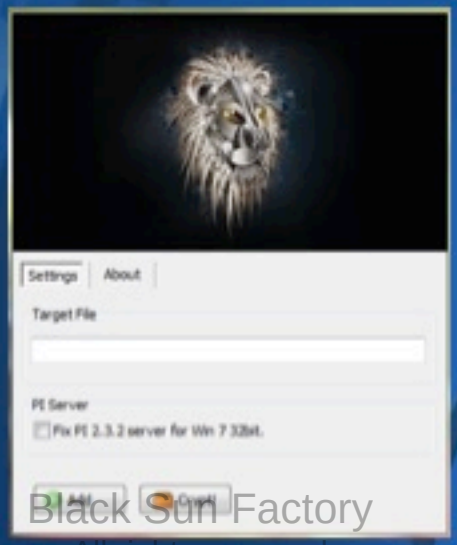


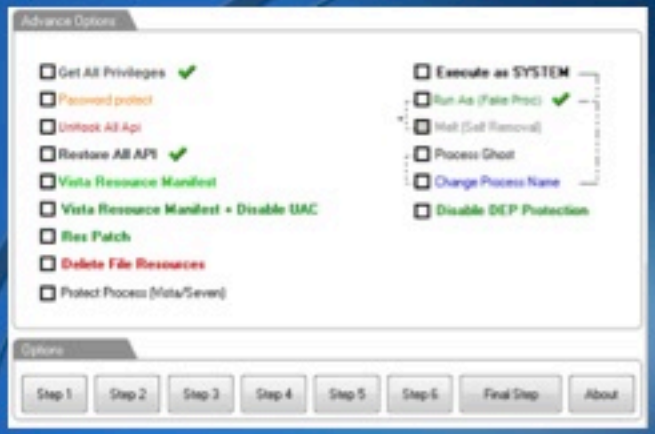

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Altri esempi di Crypter recenti

- La scena dell'underground vede oggi un proliferare di questi strumenti, segno che un bacino sempre maggiore di utenti maliziosi è interessato ai Crypter, d'altra parte è più semplice utilizzare malware ormai «maturi» e stabili attraverso l'ausilio della crittografia che non acquistare e usare malware meno affidabili.




Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Q&A

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems

# Grazie dell'attenzione

Black Sun Factory
All rights reserved

ISACA
Trust in, and value from, information systems