SCHEDA CORSO MALWARE ANALYST E REVERSE ENGINEER

Dati del corso

Voce	Dettaglio
Titolo	Malware Analyst e Reverse Engineer
Erogato da	Fata Informatica S.r.l. – CybersecurityUP
Modalità	E-learning
Struttura	4 moduli indipendenti, acquistabili singolarmente, in 2 path consigliati o come Path completo
Durata video	19 ore 45 min complessive (11 h 55 min Dynamic Malware Analyst · 7 h 50 min Reverse Engineer)
Lingua	Italiano
Accesso	h24, per 12 mesi
Piattaforma pratica	HackMeUP: 1 anno di accesso incluso nel percorso completo
Docenti	Docenti universitari e professionisti del settore
Attestati	Attestato di partecipazione al termine di ogni modulo; unico attestato al termine del Path completo
Certificazioni	CDMA e CPRE, solo con il Path completo
Prezzo	Pagamento unico o rateale: vedi sezione «Prezzi e modalità di pagamento»

Presentazione e finalità

Il percorso accompagna il discente dalla comprensione del comportamento del malware fino alle competenze avanzate di reverse engineering, partendo dalle basi fino all'analisi del codice a basso livello.

I corsi sono guidati da docenti universitari e professionisti del settore, per garantire un apprendimento pratico e di alto livello. Il percorso è articolato in 4 moduli formativi indipendenti, acquistabili singolarmente, in path consigliati (Dynamic Malware Analyst, Reverse Engineer) o come Path completo, che li comprende tutti e include benefit esclusivi.

Solo completando il Path completo è possibile accedere agli esami finali per le certificazioni CDMA (Certified Dynamic Malware Analyst) e CPRE (Certified Professional Reverse Engineer). Il Path completo include 1 anno di accesso a HackMeUP, l'ambiente di laboratorio dove analizzare malware su scenari reali per consolidare le competenze operative acquisite.

A chi è rivolto e requisiti per iscriversi

Il percorso è rivolto a chi desidera specializzarsi nell'analisi del malware e nel reverse engineering, con particolare riferimento a ruoli tecnici in ambito cybersecurity, SOC, CERT, incident response e analisi delle minacce. È indicato per aspiranti Malware Analyst, analisti SOC che vogliono approfondire i comportamenti malevoli, penetration tester e security specialist che intendono ampliare le competenze tecniche, o figure già operative che vogliono strutturare e certificare le proprie competenze.

Moduli	Competenze richieste
Malware Analysis Foundation, Professional Malware Analyst (Dynamic Malware Analyst)	Non sono richieste competenze tecniche avanzate. È consigliata una buona conoscenza dei sistemi Windows; competenze base di programmazione possono facilitare l'apprendimento ma non sono necessarie.
Reverse Engineering Foundation	È consigliata la conoscenza dei principi di programmazione almeno in un linguaggio di alto livello, preferibilmente C. Il modulo include un'introduzione al linguaggio C e una sull'Assembly.
Professional Reverse Engineer	È consigliata la conoscenza degli argomenti del corso Dynamic Malware Analyst o di competenze equivalenti, e dei principi di programmazione in un linguaggio di alto livello, preferibilmente C, in particolare in ambito Windows.

I prerequisiti specifici di ciascun modulo sono indicati nel programma dettagliato. Fata Informatica non fornisce consulenza sulle esigenze formative del Cliente: la scelta dei moduli è responsabilità dell'acquirente.

Obiettivi formativi

Al termine del Path completo il discente sarà in grado di:

- Riconoscere le principali famiglie e caratteristiche del malware.
- Analizzare comportamenti sospetti in ambienti controllati.
- Comprendere le tecniche di persistenza, injection e hooking.
- Osservare e documentare le modifiche generate da un malware su processi, file system, registri e rete.
- Leggere e interpretare codice a basso livello.
- Applicare metodologie di reverse engineering per comprendere il funzionamento di un software.
- Documentare le evidenze raccolte durante l'analisi.

Gli obiettivi specifici di ogni modulo sono riportati nel programma dettagliato.

Struttura del percorso: moduli e path

Il percorso è articolato in 4 moduli formativi indipendenti, acquistabili singolarmente, in path consigliati o come Path completo.

Cod.	Modulo	Path	Durata video
MAL-FND	Malware Analysis Foundation	Dynamic Malware Analyst	04:30:00
MAL-PRO	Professional Malware Analyst	Dynamic Malware Analyst	07:25:00
MAL-REF	Reverse Engineering Foundation	Reverse Engineer	03:00:00
MAL-PRE	Professional Reverse Engineer	Reverse Engineer	04:50:00
	Totale		**19:45:00**

Path

Path	Codice	Moduli inclusi	Durata video
Dynamic Malware Analyst	MAL-DMA	Malware Analysis Foundation, Professional Malware Analyst	11:55:00
Reverse Engineer	MAL-REENG	Reverse Engineering Foundation, Professional Reverse Engineer	07:50:00
Path completo	MAL-PKG-FULL	Tutti i 4 moduli + HackMeUP (1 anno)	19:45:00

Dynamic Malware Analyst forma una figura capace di analizzare il malware in modalità statica e dinamica: fondamenti di cybersecurity, sistema Windows e formato PE, poi analisi statica e dinamica, persistenza, injection e hooking. **Reverse Engineer** riunisce i moduli dedicati al funzionamento interno del software: linguaggio C, Assembly e lettura del codice a basso livello, poi reversing di programmi Windows, offuscamento, anti-debugging e manual unpacking. Il **Path completo** è l'unica opzione che dà accesso agli esami finali delle certificazioni CDMA e CPRE.

Modalità di erogazione e metodologia didattica

E-learning

Il corso è fruibile 24 ore su 24 dalla piattaforma di formazione di Fata Informatica, con credenziali personali (username e password). Ogni modulo comprende:

- video lezioni registrate;
- test ed esercizi di valutazione;
- laboratori didattici (vedi tabella dei moduli);
- materiale scaricabile;
- e-mail di supporto per interagire con i docenti;
- Uppy, l'AI Tutor addestrato sui materiali ufficiali del corso, disponibile 24/7;
- attestato di partecipazione al termine del modulo.

Il Path completo include inoltre 1 anno di accesso a HackMeUP, l'esame e la certificazione finale.

Uppy – il tutor AI

Uppy è incluso nel percorso formativo e risponde in modo istantaneo sui temi complessi, assiste durante le esercitazioni di laboratorio e aiuta nel ripasso mirato prima degli esami, 24 ore su 24.

HackMeUP – la piattaforma dove il malware si analizza sul campo

Nella Malware Analysis non basta conoscere le tecniche: occorre saper osservare il comportamento di un campione, riconoscere le sue tecniche e interpretare ciò che accade all'interno di un sistema compromesso. HackMeUP è la piattaforma pratica inclusa nel Path completo (1 anno di accesso; acquistabile anche singolarmente):

- analisi su scenari reali: campioni di malware, macchine compromesse, processi, registri e traffico di rete per ricostruire comportamenti e tecniche di attacco;
- approccio operativo strutturato: analisi statica e dinamica, osservazione del comportamento malevolo e documentazione delle evidenze raccolte;
- casi pratici, dall'analisi comportamentale al reversing di programmi Windows;
- strumenti e tecniche professionali realmente utilizzati nell'analisi del malware e nel reverse engineering;

- laboratori aggiornati per riflettere nuove tecniche di offuscamento, persistenza e packing e nuovi campioni da analizzare.

Verifiche, attestati e certificazioni

Ogni modulo prevede test di valutazione dell'apprendimento, composti da domande a risposta multipla e/o prove pratiche. Il superamento dei test è requisito necessario per completare il percorso.

Titolo	Chi lo ottiene	Come
Attestato di partecipazione	Chi acquista singoli moduli o path consigliati (Dynamic Malware Analyst, Reverse Engineer)	Al termine di ciascun modulo, dopo aver completato i materiali e superato i test; rilasciato su richiesta
Attestato di partecipazione unico	Chi acquista il Path completo	Al termine del Path completo
CDMA – Certified Dynamic Malware Analyst	Chi acquista il Path completo	Esame finale, le cui modalità sono illustrate durante le lezioni
CPRE – Certified Professional Reverse Engineer	Chi acquista il Path completo	Esame finale, come sopra

L'accesso agli esami finali e alle certificazioni CDMA e CPRE è riservato a chi acquista il Path completo, che rilascia un unico attestato di partecipazione e dà accesso ai due esami finali. Il mancato superamento dell'esame non consente di conseguire la certificazione.

Grazie al supporto di Uppy e alla pratica su scenari realistici con HackMeUP, il percorso non si limita alla teoria, ma accompagna il discente nello sviluppo di competenze operative, concrete e spendibili nel mondo della cybersecurity.

Programma dettagliato

Ogni modulo include: e-learning, video lezioni registrate, accesso h24, test ed esercizi di valutazione, laboratori didattici, materiale scaricabile, attestato di partecipazione, e-mail di supporto per interagire con i docenti e Uppy, l'AI Tutor disponibile 24/7. Di seguito, per ciascun modulo, sono indicati i numeri specifici.

MAL-FND – Malware Analysis Foundation

Introduzione. Introduce i fondamenti per la professione di Malware Analyst, dalla conoscenza dei rudimenti della cybersecurity alla conoscenza e classificazione dei malware. Si introduce il sistema Windows, le sue componenti, dalle componenti software ai processi, dall'infrastruttura di rete al registro. Infine si scende nel dettaglio della struttura di un file eseguibile, quale prevalente oggetto di indagine per capire i segreti di una eventuale contaminazione da malware.

Obiettivi

- Riconoscere le principali famiglie e caratteristiche del malware.
- Comprendere l'architettura dei sistemi Windows: processi, thread, registri e primitive.
- Padroneggiare la struttura del formato PE (header e sezioni).

A chi è rivolto. A chi desidera specializzarsi nell'analisi del malware, con particolare riferimento a ruoli tecnici in ambito cybersecurity, SOC, CERT, incident response e analisi delle minacce.

Competenze richieste. Non sono richieste competenze tecniche avanzate. È consigliata una buona conoscenza dei sistemi Windows; competenze base di programmazione possono facilitare l'apprendimento ma non sono necessarie.

Programma del corso

1. **Introduzione alla Cybersecurity.** Introduzione · La kill chain · Analisi di un attacco.

2. **Il Malware.** Introduzione al malware · Il formato PE · Le DLL · Kernel vs User Mode · Le API · Le caratteristiche del malware · Le firme · Obfuscation and Mutation · Malware polimorfico e metamorfico · Mutation engines · Persistenza · DLL Hijacking · Trojanized System Binaries · Tipologie di malware (virus, backdoor, adware, spyware, keylogger, trojan, RAT, cryptojacking) · Rootkit · Ransomware & Co · Il mercato del malware.
3. **Il sistema Windows.** Il sistema Windows · Processi · Virtual Address Space · Thread · Fasi di caricamento di un processo · Context switch · WOW64 · Principali processi Windows · Registry · Interrupts · Primitive Windows · Manipolazione processi, file e registri · Socket · Caricamento DLL.
4. **Il formato PE.** RVA, VA e ImageBase · Header · DOS Header · NT Header · Optional Header · Section Header · Sezioni (.text, .rdata, .data, .edata, .rsrc).

MAL-PRO – Professional Malware Analyst

Introduzione. Insegna ad analizzare il malware in modalità statica e dinamica, comprendendone comportamenti, tecniche e impatti sui sistemi Windows. Dalle tipologie di codice malevolo al formato PE, dall'architettura dei processi Windows alle tecniche di persistenza, injection e hooking: è il livello che forma una figura capace di eseguire analisi malware senza la necessità iniziale di deassemblatori o debugger.

Obiettivi

- Eseguire l'analisi statica e dinamica del malware con gli strumenti dedicati.
- Riconoscere le tecniche di persistenza, injection e hooking in ambiente Windows.
- Osservare e documentare le modifiche generate da un malware su processi, file system, registri e rete.

A chi è rivolto. A chi desidera specializzarsi nell'analisi del malware, con particolare riferimento a ruoli tecnici in ambito cybersecurity, SOC, CERT, incident response e analisi delle minacce.

Competenze richieste. Non sono richieste competenze tecniche avanzate. È consigliata una buona conoscenza dei sistemi Windows; competenze base di programmazione possono facilitare l'apprendimento ma non sono necessarie.

Programma del corso

1. **Analisi statica e dinamica.** Analisi statica · Antivirus scanner · Hashing · Stringhe · Malware compresso · DLL e funzioni · Analisi dinamica · Sandbox · Esecuzione del malware · Monitoraggio dei processi e dei registri · Simulazione di una rete · Packet sniffing.
2. **Malware Behaviour.** Tecniche di persistenza (chiavi di registro, file system, processi, servizi) · Tecniche di injection (DLL/Code Injection, Image File Execution Option, DLL Search Order Hijacking, Process Injection, Process Hollowing, APC Injection, Extra Windows Memory Injection) · Tecniche di hooking (API Hooking, IAT Hooking).

MAL-REF – Reverse Engineering Foundation

Introduzione. Si apprende il linguaggio assembly, in particolare con il confronto con un linguaggio di alto livello (linguaggio C), comprendendo l'uso delle istruzioni assembly per costruire i maggiori costrutti di programmazione che traggono la loro origine da un linguaggio ad alto livello e non solo, fornendo la capacità di seguire un flusso di programma durante la sua evoluzione e comprendere cosa accade veramente all'interno dello stesso.

Obiettivi

- Comprendere le basi del linguaggio C.
- Leggere e interpretare codice Assembly e riconoscere strutture, cicli e funzioni a basso livello.
- Utilizzare debugger e strumenti di analisi (IDA, OllyDBG).

A chi è rivolto. A chi vuole approfondire il reverse engineering per comprendere il comportamento interno del software, in particolare professionisti di cybersecurity, penetration tester e analisti che vogliono ampliare le competenze tecniche.

Competenze richieste. È consigliata la conoscenza dei principi di programmazione almeno in qualche linguaggio di programmazione di alto livello, preferibilmente C.

Programma del corso

1. **Il linguaggio C.** Hello World · Costanti e variabili · Tipi di dati primitivi · Conversioni di tipo · Operatori aritmetici, relazionali e logici · Controllo del flusso (IF, Switch, For, While) · Funzioni · Passaggio di parametri · Stack · Ricorsione · Tipi di dati derivati · Puntatori e array · Allocazione dinamica della memoria.
2. **Il linguaggio Assembly.** Il codice Assembly · Le istruzioni · Funzioni e stack · Architettura x64.
3. **Riconoscere strutture e cicli in Assembly.** Cicli e istruzioni · Array e struct · Debugger · Hot patching.

MAL-PRE – Professional Reverse Engineer

Introduzione. Approfondisce il funzionamento interno del software ed in particolare quello in ambito Windows, comprendendo l'uso della API del sistema anche vedendole dal punto di osservazione di un debugger. Infine si analizzeranno le tecniche di offuscamento, di antidebugging e di packering adottate dai malware per sfuggire al controllo degli analisti.

Obiettivi

- Analizzare programmi in esecuzione su sistema Windows nelle più comuni e utilizzate operazioni tipiche dei malware.
- Riconoscere tecniche di offuscamento, anti-debugging e packing.
- Eseguire attività di manual unpacking.

A chi è rivolto. A chi vuole approfondire il reverse engineering per comprendere il comportamento interno del software, in particolare professionisti di cybersecurity, penetration tester e analisti che vogliono ampliare le competenze tecniche.

Competenze richieste. È consigliata la conoscenza degli argomenti trattati nel corso Dynamic Malware Analyst o il possesso di competenze equivalenti, in particolare è consigliata la conoscenza dei principi di programmazione almeno in qualche linguaggio di programmazione di alto livello, preferibilmente C, ed in special modo in ambito Windows.

Programma del corso

1. **Reversing Windows.** Analizzare programmi Windows e le operazioni su registri, file, processi, socket e servizi.
2. **Tecniche di offuscamento.** Algoritmi di offuscamento standard e personalizzati · Algoritmi di crittazione · Tecniche anti-debugger.
3. **Manual Unpacking.** I packer · Trovare l'Original Entry Point · Tail Jump · ESP trick · SEH handling.

Requisiti hardware e software

Per accedere al corso il Cliente deve disporre dei requisiti seguenti. La verifica è a carico del Cliente (Condizioni di Vendita, art. 4 e art. 11).

Componente	Requisito
Personal computer	Per le sessioni di teoria e pratica sono necessari PC desktop o notebook, mentre per la fruizione dei contenuti teorici è possibile utilizzare dispositivi mobile. In particolare nelle sessioni pratiche è suggerito l'uso di PC con processori 64 bit, almeno quad-core, con supporto Intel VT-x / AMD-V o tecnologia equivalente per compatibilità con ambienti di virtualizzazione locali, con minimo 8 GB di RAM (consigliati almeno 16 GB) e almeno 80 GB di spazio libero su disco per l'installazione e l'esecuzione delle macchine virtuali. Monitor con risoluzione minima consigliata di 1280 × 720 pixel. Scheda audio e cuffie o altoparlanti. Webcam e microfono qualora siano previste attività formative in modalità blended.

Componente	Requisito
Software di virtualizzazione	La postazione dedicata alle sessioni pratiche dovrà consentire l'installazione e l'utilizzo di un software di virtualizzazione compatibile con le macchine virtuali messe a disposizione per le esercitazioni, o comunque suggerite nell'ambito dei laboratori quale strumento per la costruzione di un proprio insieme di strumenti. Le VM saranno distribuite in formato OVA. Per la realizzazione di VM al fine della costruzione di un proprio laboratorio è consigliato seguire l'esempio d'uso di ciascun corso al fine di rendere speculare l'esperienza nelle videolezioni con la pratica. In ambito aziendale/corporate è del tutto evidente che l'utente dovrà disporre dei permessi necessari per installare, configurare ed eseguire software e macchine virtuali sulla propria postazione o avere soddisfatti in modo alternativo i requisiti. Per garantire la piena fruibilità delle attività formative e dei laboratori, è pertanto raccomandato l'utilizzo di un PC personale sul quale l'utente disponga di privilegi amministrativi.
Browser	È necessario utilizzare una versione aggiornata e supportata di uno dei principali browser web, quali: • Google Chrome • Mozilla Firefox • Microsoft Edge • Apple Safari Il browser dovrà consentire l'esecuzione di JavaScript, l'utilizzo dei cookie, il download di file e la riproduzione di contenuti multimediali.
Connettività	Connessione Internet ad alta velocità e stabile, necessaria per lo streaming dei video e per accesso ai laboratori

Componente	Requisito
Requisiti di rete e sicurezza	La postazione e la connessione utilizzate devono consentire l'accesso ai servizi Internet necessari alla fruizione della piattaforma e allo svolgimento delle esercitazioni. Eventuali firewall, proxy, VPN, sistemi di filtraggio, DNS filtering, endpoint security o altre policy di sicurezza applicate da reti aziendali/corporate non devono impedire o limitare: • L'accesso alla piattaforma di erogazione e agli eventuali servizi esterni integrati; • Il download dei materiali didattici e delle immagini delle macchine virtuali • La riproduzione di contenuti audio/video • L'utilizzo di cookie, JavaScript e degli altri servizi web richiesti • Eventuali connessioni necessarie allo svolgimento dei laboratori pratici (VPN via UDP in porta non standard) Qualora venga utilizzata una postazione o una rete aziendale soggetta a restrizioni, l'utente dovrà verificare preventivamente la disponibilità dei permessi di installazione, virtualizzazione e accesso alla rete necessari. Per garantire la piena fruibilità delle attività formative e dei laboratori, è pertanto raccomandato l'utilizzo di un PC personale sul quale l'utente disponga di una connessione Internet non soggetta a restrizioni corporate incompatibili con le attività previste.
Lettura documenti	Software di lettura di file in formato .pdf
Audio e video	Software e dispositivi per la riproduzione di file audio e video (casse o cuffie)
Laboratori	I laboratori potranno essere fruibili attraverso: • Materiale scaricabile da sottoporre a strumenti locali (la cui installazione è a carico dell'utente), quali simulatori, analizzatori, ecc. Questi strumenti potranno essere collocati su proprio PC o in apposita VM sperimentale • Connessione Web diretta a piattaforma di simulazione/esercitazione • Connessione VPN (tramite differenti porte) ad infrastrutture virtuali remote. Gli strumenti di indagine devono essere predisposti dall'utente nel proprio PC o all'interno di VM predisposte all'esercitazione. In alcun caso viene fornito un ambiente di analisi o strumentazione di attacco attraverso le piattaforme. **ATTENZIONE**! In alcuni casi è possibile che il laboratorio trattino materiale pericoloso quale exploit o malware. È fondamentale trattare questi casi in VM isolate e protette in modo da evitare contaminazioni o incidenti alle infrastrutture estranee ai laboratori.

Il Cliente si impegna ad adeguare i propri sistemi hardware e software in caso di aggiornamenti o mutamenti della piattaforma. Fata Informatica non risponde dei difetti di fruizione dovuti al mancato possesso dei requisiti minimi di sistema.

Durata dell'iscrizione, accesso e assistenza

Il Cliente deve svolgere personalmente le lezioni e i test. Eventuali ulteriori informazioni aggiornate sono comunicate dalla parte tecnica il primo giorno di lezione.

Voce	Dettaglio
Validità dell'iscrizione – singolo modulo	12 mesi dalla data di iscrizione
Validità dell'iscrizione – path o Path completo	12 mesi dalla data di iscrizione
Scadenza	Terminato il periodo, l'iscrizione viene disattivata automaticamente: lezioni e test vanno completati entro la scadenza
Accesso ai materiali	h24, con username e password personali, non cedibili
Area personale	Elenco dei corsi frequentati e dei materiali correlati
Credenziali	Generate automaticamente e inviate dal tutor didattico dopo l'iscrizione e il pagamento
Assistenza didattica	Sistema di ticket per domande ai docenti e allo staff, attivo per tutta la durata dell'iscrizione; e-mail di supporto supportodidattico@fatainformatica.it; tutor AI Uppy 24/7
Reclami	Per iscritto a Fata Informatica, Via Tiburtina 912, 00156 Roma; esito comunicato entro 20 giorni lavorativi
Accesso HackMeUP	1 anno, incluso nel Path completo dalla data di iscrizione

Prezzi e modalità di pagamento

I prezzi sono espressi in euro, IVA inclusa. Ogni opzione è acquistabile in un'unica soluzione oppure, dove indicato, a rate. Il pagamento avviene online tramite il servizio Stripe. Fata Informatica non gestisce né memorizza i dati degli strumenti di pagamento. Eseguito il pagamento, viene emessa la fattura. Il pagamento a rate è disponibile solo ove espressamente indicato. Completata l'iscrizione e saldato il prezzo, il Cliente riceve le credenziali di accesso. Il pagamento a rate comporta una maggiorazione del 5%.

Recesso e condizioni di vendita

L'acquisto è regolato dalle Condizioni di Vendita dell'e-commerce di Fata Informatica S.r.l (Rev. 03 del 07.10.2026) che il Cliente accetta con modalità point and click prima dell'acquisto. Il Cliente dichiara di aver letto questa Scheda del Corso prima di acquistare.

- **Recesso (consumatori).** 14 giorni dalla data di acquisto, senza motivazione e senza costi (art. 52 Codice del Consumo).
- **Perdita del recesso.** Il diritto non è più esercitabile dopo l'invio delle credenziali che danno accesso immediato alla piattaforma. Chi vuole recedere deve attendere i 14 giorni prima di ricevere le credenziali.
- **Fruizione immediata.** Il Cliente può chiedere, durante l'ordine, di accedere subito al corso, accettando di perdere il diritto di recesso (art. 59, comma 1, lett. o). Riceve conferma del contratto e ricevuta via e-mail.
- **Rimborso.** In caso di recesso valido, entro 60 giorni dall'esercizio, con riaccredito sullo stesso strumento di pagamento.

- **Diritto d'autore.** Videolezioni, slide e materiali sono di proprietà di Fata Informatica: è vietato copiarli, distribuirli o cederli. Le credenziali sono personali e non cedibili.
- Il testo completo delle Condizioni di Vendita prevale su quanto qui sintetizzato.