

● Jammer - deception ad alta interazione

L'avversario in trappola. L'intelligence sotto controllo.

Jammer riproduce in modo credibile, sotto forma di digital twin, i servizi IT, OT e AI dell'organizzazione. Chiunque interagisca con questi servizi è ostile per definizione: viene trattenuto nella trappola, ogni suo comando è registrato e ne risulta una threat intelligence con valore di evidenza, senza falsi allarmi.

FALSI POSITIVI

≈0

Ogni contatto con una trappola è malevolo o sospetto per definizione

TEMPO OPERATIVO RISPARMIATO

60-65%

Nel disaster recovery e nel rilevamento di accessi non autorizzati e movimenti laterali

TATTICHE MITRE ATT&CK

10-12/14

Fino a 10-12 tattiche su 14, contro le 4-5 del rilevamento tradizionale

COPERTURA DELLE TRAPPOLE

IT/OT/AI

Un ampio portafoglio di servizi emulati, in costante crescita: dai database ai PLC, fino all'hosting di modelli LLM

Dati: Infinitaware, gennaio 2026. I risultati dipendono dal posizionamento delle trappole e dall'integrazione.

◆ IL PRINCIPIO

Un segnale che non si può ignorare, perché nessuna attività legittima lo genera.

Le firme e i modelli comportamentali procedono per ipotesi. Una trappola no: nessun utente, servizio o processo legittimo ha motivo di interagire con essa.

Jammer fa di questa certezza un vantaggio operativo: individua per tempo intrusioni e movimenti laterali, impegna l'avversario su bersagli fittizi e ne acquisisce per intero payload, shell, canali C2 e tecniche. Il tutto affiancando gli strumenti già in uso, senza sostituirli.

◆ COME FUNZIONA

Attrarre. Contenere. Osservare. Reagire.

Un meccanismo in tre fasi, progettato per inserirsi in modo non invasivo a valle degli strumenti di sicurezza esistenti, senza il lock-in tipico delle grandi suite.



01

Servizi reali o simulati

Le trappole ad alta interazione funzionano come digital twin di servizi reali oppure come simulazioni fedeli, abbastanza credibili da trarre in inganno operatori umani e strumenti APT, non soltanto scanner automatici.



02

L'attaccante resta nella trappola

Ogni trappola è un ambiente isolato e configurabile, in cui l'attività ostile viene dirottata e contenuta senza mai raggiungere i sistemi di produzione.



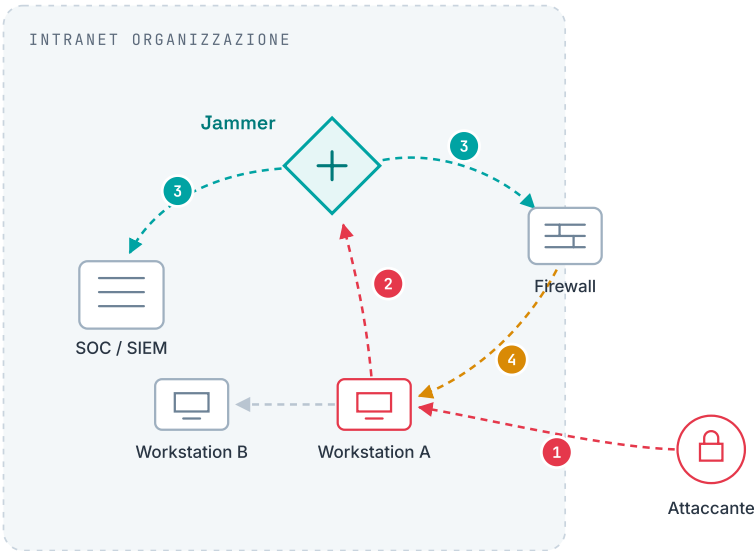
03

Sonde invisibili registrano ogni azione

Sonde non rilevabili dall'attaccante registrano l'intera sessione: comandi, script, file e connessioni di rete. È la base per l'analisi forense e per la produzione di threat intelligence.

SCENARIO D'ATTACCO

Da una singola workstation infetta a un avversario bloccato.



- 1 Compromissione iniziale**
Un payload malevolo infetta una workstation. Gli strumenti perimetrali spesso non lo rilevano, soprattutto quando la tecnica utilizzata è nuova.
- 2 Movimento laterale verso una trappola**
L'intruso esplora la rete e raggiunge una trappola di Jammer che si presenta come un servizio di valore. Questo solo contatto costituisce un indicatore di compromissione inequivocabile.
- 3 Notifica e inoltro della sessione**
Jammer invia una notifica al firewall e inoltra l'intera sessione malevola (comandi, payload, IOC) al SOC o al SIEM per l'analisi.
- 4 Contenimento**
Le connessioni da e verso la workstation infetta vengono bloccate. L'avversario è isolato e l'organizzazione dispone di una registrazione completa di quanto ha fatto e di come lo ha fatto.

Integrazione e potenziamento

Jammer rafforza le capacità di rilevamento e risposta senza sostituire alcuno strumento: affianca quelli esistenti e si integra a valle delle soluzioni già in uso, assicurando una reale interoperabilità.

Protezione dalle minacce sconosciute

Una barriera avanzata, in grado di rilevare e contrastare qualsiasi violazione. Poiché si basa sul comportamento e non sulle firme, riduce il vantaggio delle nuove minacce e delle vulnerabilità non ancora note.

Reazione mirata

Un'analisi forense dettagliata su origine, dinamica e impatto di ogni incidente consente di individuare con precisione la vulnerabilità sfruttata, contenere rapidamente i danni e rafforzare le difese contro i tentativi successivi.

DIFESA • PUBBLICA AMMINISTRAZIONE • INFRASTRUTTURE CRITICHE

DIFESA E GOVERNO	Allerta precoce e inequivocabile nelle reti segmentate	Le trappole, collocate nei segmenti più sensibili, replicano sistemi reali: qualsiasi contatto è un indicatore di compromissione ad alta affidabilità. I movimenti laterali emergono subito e le tecniche degli attori APT vengono registrate per intero, anziché ricostruite a posteriori.
INFRASTRUTTURE CRITICHE	Deception per OT/ICS	Le trappole Modbus, Siemens S7, Omron e MQTT rilevano le attività di ricognizione contro i sistemi di controllo industriale prima che raggiungano i PLC reali.
CERT • CSIRT • CTI	Intelligence condivisibile	TTP, payload e indicatori C2 completi, esportati in formato STIX 2.1. ORB Spotter ricostruisce l'infrastruttura di rilancio utilizzata nelle campagne.
INFRASTRUTTURE AI	Esche per i sistemi basati su LLM	Esche basate su Ollama intercettano i tentativi di attacco alle piattaforme che ospitano i modelli, compresi quelli volti a estrarre credenziali dai sistemi LLM.
OPERATORI REGOLAMENTATI	Evidenze a supporto della NIS2	Registrazioni delle sessioni con valore forense, a supporto degli obblighi di rilevamento, analisi e notifica degli incidenti.

◆ COPERTURA DELLE TRAPPOLE

Un ampio portafoglio di servizi emulati per ambienti IT, OT e AI.

Le trappole riproducono i sistemi che gli attaccanti prendono di mira per primi: dagli archivi di dati all'accesso remoto, fino ai controllori industriali e alle piattaforme che ospitano modelli di intelligenza artificiale.

01 Database e storage

I dati sono il primo obiettivo degli attaccanti: database relazionali e NoSQL, motori di ricerca e di analisi.

MariaDB PostgreSQL MongoDB
Redis Elasticsearch

02 Accesso remoto e gestione

Shell, console e desktop remoto, primo punto di appoggio nella maggior parte delle intrusioni.

SSH Telnet RDP Finger

03 Industriale e IoT (OT/ICS)

Protocolli industriali e PLC tipici delle infrastrutture critiche, oltre ai sistemi di messaggistica IoT.

Modbus Omron Siemens S7
MQTT

04 Applicazioni web e hosting AI

Web server, proxy e dashboard, oltre a esche che simulano l'hosting di modelli LLM, esposte ai più recenti vettori di attacco contro l'intelligenza artificiale.

Apache httpd NGINX Kibana
Ollama

05 Servizi di rete essenziali

Routing, risoluzione dei nomi, monitoraggio, gestione dei segreti e orchestrazione.

BGP DNS SNMP Vault
Nomad

06 Trasferimento file e comunicazione

Condivisione di file, posta elettronica e streaming video, compresi gli endpoint RTSP tipici delle telecamere IP.

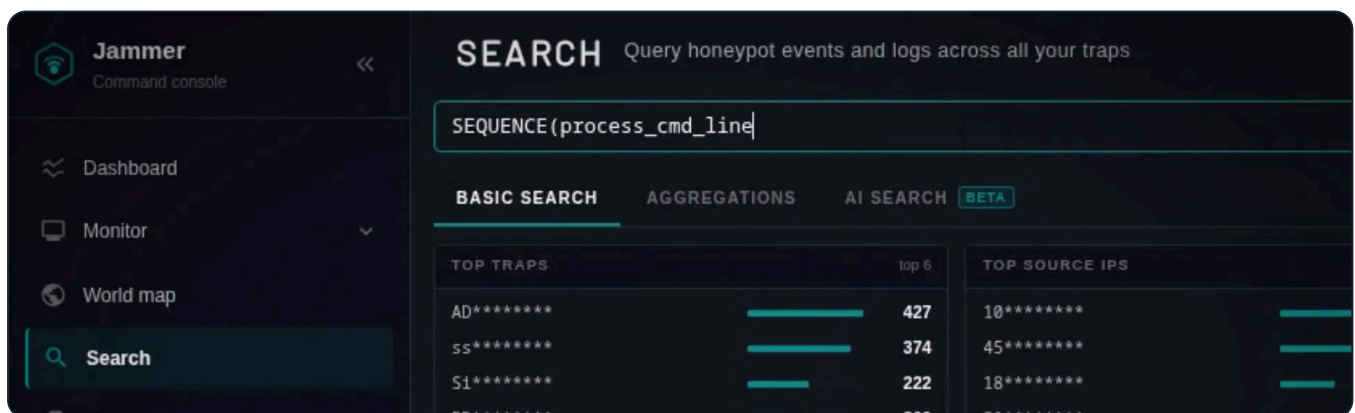
FTP SMB/CIFS SMTP RTSP

Trappole su misura. Il portafoglio è in costante crescita e può essere esteso con trappole che riproducono servizi e applicazioni specifici dell'organizzazione cliente.

◆ LA PIATTAFORMA

Dalle sessioni registrate all'intelligence operativa.

Una console web per l'analisi in tempo reale e a posteriori, affiancata da API e strumenti di automazione.



Console web di Jammer, vista ricerca. I dati identificativi sono oscurati.

Tutti i dati in un unico punto

Un'unica dashboard aggrega trappole, sorgenti, organizzazioni e minacce di tutti i sensori.

Monitoraggio in tempo reale

Una mappa mondiale di trappole e sessioni attive, aggiornata mentre l'attacco è in corso.

Ricerca avanzata delle sessioni

Un linguaggio di query su ogni sessione registrata, dalla console e tramite REST API.

Routine post-attacco

Un motore visuale concatena filtri e azioni e li esegue a intervalli programmati per l'assegnazione di tag, la reportistica e l'arricchimento dei dati.

◆ PERCHÉ LA DECEPTION

Rilevamento tradizionale e Jammer a confronto.

CRITERIO	RILEVAMENTO TRADIZIONALE	JAMMER
Falsi positivi	Frequenti: eventi benigni possono sembrare malevoli	Quasi nulli: ogni accesso al digital twin è di per sé un'anomalia
Onere di manutenzione	Alto: richiede aggiornamenti costanti delle firme	Basso: nessuna firma da aggiornare, ogni interazione è sospetta
Rilevamento dei movimenti laterali	Medio: richiede una complessa correlazione tra eventi	Alto, con trappole posizionate nei segmenti chiave
Visibilità sul comportamento dell'attaccante	Limitata a eventi registrati o segnalati	Completa: ogni script, comando e azione viene monitorato
Capacità di attrarre l'attaccante	Nessuna	Alta: le trappole stimolano l'interazione
Copertura delle tattiche MITRE ATT&CK	4-5 su 14 (es. initial access, execution)	Fino a 10-12 su 14
Intercettazione delle minacce APT	Complessa, spesso a compromissione avvenuta	Alta: un'esca credibile per gli operatori APT
Valore delle informazioni raccolte	Limitato	Alto: payload, shell, C2, tecniche

Dati: Infinitaware, gennaio 2026. I risultati dipendono dal posizionamento delle trappole e dall'integrazione.

◆ INTEGRAZIONI

Nessuna sostituzione degli strumenti in uso e nessun vincolo verso un unico fornitore: Jammer fornisce rilevamenti e intelligence all'infrastruttura esistente tramite standard aperti.

STIX 2.1 Condivisione dell'intelligence in formato standard	REST API Interrogazione ed esportazione programmatica dei dati	IDS / IPS Invio dei rilevamenti ai sensori esistenti	Firewall Attivazione del blocco delle sorgenti ostili	SIEM / SOC Inoltro delle sessioni d'attacco complete per l'analisi
---	--	--	---	--

◆ PERCHÉ LE ORGANIZZAZIONI PIÙ ESIGENTI SCELGONO INFINITAWARE

Ingegneria europea e italiana

Progettato e sviluppato in Italia da Infinitaware, parte del Gruppo Sistematica.

Opera all'interno del perimetro

Le trappole sono installate nella rete del cliente e l'intelligence raccolta resta di sua esclusiva proprietà.

Installazione non invasiva

Si installa senza modificare l'infrastruttura esistente e affianca gli strumenti di sicurezza già in uso, preservando gli investimenti effettuati.

Oltre 10 anni di esperienza

Un team che da oltre dieci anni si occupa della sicurezza di governi, istituzioni e imprese.

Soluzioni su misura

Trappole, protocolli e integrazioni adattati alle esigenze specifiche di ciascun contesto operativo.

Competenze offensive

L'esperienza maturata nel red teaming e nel reverse engineering consente di realizzare trappole credibili anche per avversari esperti.

Richiedi un briefing riservato.

Il briefing, calibrato sul contesto operativo, illustra come Jammer può inserirsi nell'infrastruttura esistente. Si parte da un progetto pilota circoscritto a un segmento di rete chiave, per decidere sulla base di risultati concreti.

JAMMER E PARTNERSHIP

jammer@infinitaware.com

INFORMAZIONI GENERALI

info@infinitaware.com

WEB

infinitaware.com