

phantomsrl.it

# REPORT: DIFESA DELLA RETE

**Prepared by**

Pignatello Giuseppe  
Luca Iannone  
Alessio D'Ottavio  
in arte:  
**PHANTOM SRL**  
San Severo, Foggia  
Vasto, Chieti  
Siracusa, Siracusa



**PHANTOM s.r.l.**  
IMPOSSIBLE IS  
OUR TARGET

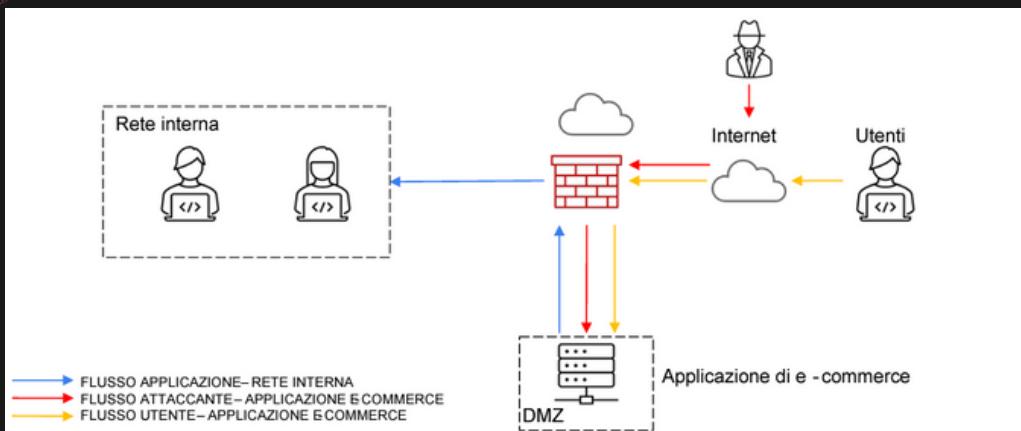
*impossible is our target*

# Content Highlights

- Traccia
- Come difendersi da XSS e SQLi
- Disegno Aggiornato
- Segnalazioni AnyRun
- Ringraziamenti



# Traccia



Con riferimento alla figura in alto, rispondere ai seguenti quesiti.

1. **Azioni preventive :** quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni
2. **Impatti sul business :** l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti . Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica
3. **Response:** l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta .
4. **Soluzione completa :** unire i disegni dell'azione preventiva e della response(unire soluzione 1 e 3)
5. **Modifica più aggressiva dell'infrastruttura integrando eventuali altri sistemi di sicurezza**



# DIFENDERSI DA XSS E SQLi

Per difendere un'applicazione web da attacchi di tipo SQL Injection (SQLi) e Cross-Site Scripting (XSS), è necessario adottare una serie di azioni preventive. Ecco alcune delle principali:

Sanitizzazione dell'Input Utente:

**Assicurarsi che tutti i dati in ingresso (parametri di URL, input dei form, cookie, header HTTP) siano validati e conformi ai requisiti previsti.** Ad esempio, utilizzare regole di validazione per consentire solo caratteri accettabili e rifiutare input non autorizzati.

**Utilizzo di prepared statements o parametrized queries:** Evitare la concatenazione diretta di stringhe per creare query SQL. Invece, utilizzare prepared statements o parametrized queries, che separano i dati dalle istruzioni SQL, riducendo così il rischio di SQL Injection.

**Escapamento dei caratteri speciali:** Se l'utilizzo di prepared statements non è possibile, assicurarsi di effettuare l'escape dei caratteri speciali come apici singoli ('), doppi apici ("), backslashes (), etc., prima di incorporare i dati nelle query SQL.

**Implementazione del principio del "Least Privilege":** Assegnare ai database e agli account di accesso alle applicazioni solo i privilegi strettamente necessari per eseguire le operazioni richieste. Evitare di utilizzare account con privilegi di amministratore per l'accesso alle applicazioni.

**Impostazione di header HTTP per la sicurezza:** Utilizzare header HTTP come Content Security Policy (CSP), X-XSS-Protection e X-Content-Type-Options per fornire ulteriori livelli di protezione contro attacchi XSS.

**Aggiornamento e patching regolari:** Mantenere tutti i componenti del sistema (server web, database, framework, librerie) aggiornati e applicare regolarmente le patch di sicurezza per mitigare le vulnerabilità note.

**Monitoraggio e registrazione delle attività sospette:** Implementare sistemi di monitoraggio delle attività degli utenti e dei tentativi di attacco tramite SIEM, nonché registrazioni dettagliate degli accessi e delle operazioni eseguite per consentire l'analisi forense in caso di incidente.

**Formazione e consapevolezza:** Fornire formazione agli sviluppatori, agli amministratori di sistema e agli utenti finali sull'importanza della sicurezza informatica e sulle pratiche consigliate per prevenire gli attacchi.

**Test di sicurezza:** Condurre test regolari di sicurezza, come test di penetrazione e scansioni di vulnerabilità, per identificare e correggere eventuali falle di sicurezza nell'applicazione web.



Per calcolare l'impatto finanziario dell'attacco DDoS sull'applicazione Web, possiamo seguire questa procedura:

Identificare il fatturato perso durante i 10 minuti di non raggiungibilità:  
Fatturato perso = Fatturato medio per minuto\* Durata dell'attacco in minuti

Quindi il fatturato perso durante l'attacco DDoS sarà uguale a 15.000 €.

Valutare le azioni preventive per mitigare l'impatto dell'attacco DDoS:

**Utilizzare un servizio di mitigazione DDoS:** Esistono servizi dedicati che possono aiutare a mitigare gli attacchi DDoS, filtrando il traffico dannoso prima che raggiunga il server.

**Utilizza un sistema di rilevamento degli intrusi (IDS) o di prevenzione degli intrusi (IPS):** Questi sistemi possono aiutare a rilevare e mitigare gli attacchi DDoS in tempo reale.

**Monitoraggio costante:** Monitora costantemente il traffico in ingresso per individuare eventuali anomalie che potrebbero indicare un attacco in corso.

Inoltre ricordiamo che è importante proteggere non solo il server, ma anche i dispositivi e le reti che lo circondano. Inoltre, è sempre consigliabile contattare le autorità competenti se si sospetta di essere vittime di un attacco DDoS.



Per gestire una situazione in cui un'applicazione Web è stata infettata da un malware e la priorità è prevenire la propagazione del malware sulla rete senza rimuovere l'accesso dell'attaccante alla macchina infettata, è possibile adottare le seguenti azioni preventive:

**Isolamento della macchina infetta:** Isolare fisicamente o virtualmente la macchina infetta dalla rete principale per impedire la propagazione del malware ad altri dispositivi sulla rete. Questo può essere fatto tramite segmentazione di rete o utilizzando strumenti di isolamento come le VLAN.

**Analisi approfondita del malware:** Condurre un'analisi dettagliata del malware per comprendere il suo funzionamento, le sue capacità e il suo comportamento. Questo può aiutare a identificare eventuali backdoor o meccanismi di propagazione e a sviluppare contromisure appropriate.

**Implementazione di controlli di sicurezza avanzati:** Reforzare i controlli di sicurezza sulla macchina infetta e sulla rete circostante per prevenire ulteriori compromissioni e limitare l'accesso dell'attaccante. Questo potrebbe includere l'implementazione di firewall avanzati, sistemi di rilevamento delle intrusioni (IDS) e sistemi di prevenzione delle intrusioni (IPS).

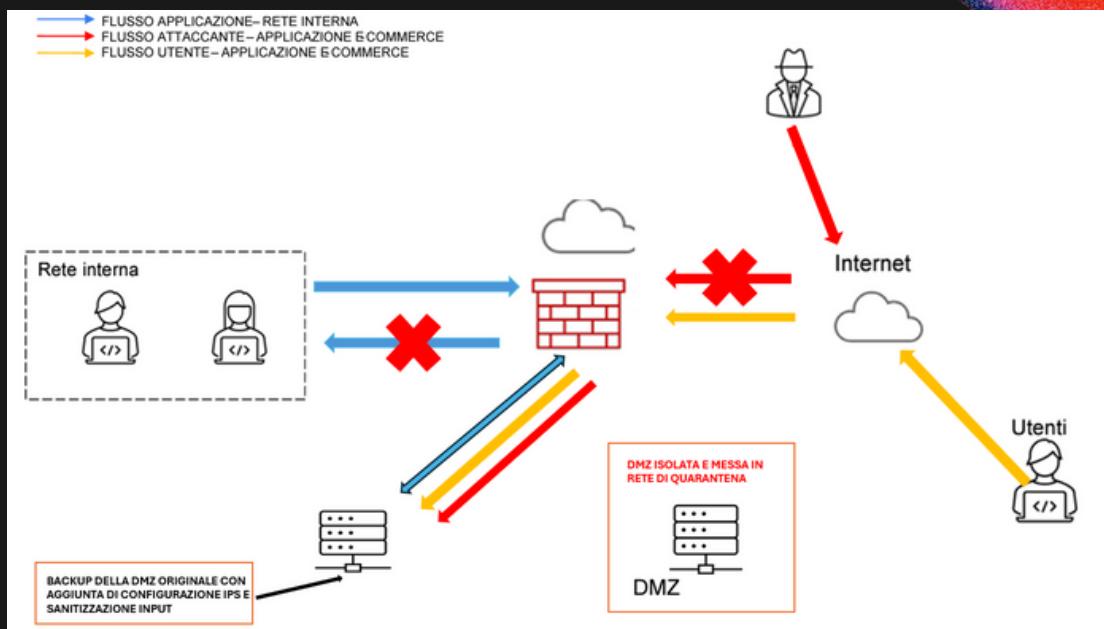
**Monitoraggio costante:** Monitorare costantemente l'attività sulla macchina infetta e sulla rete per rilevare eventuali tentativi di propagazione del malware o attività sospette da parte dell'attaccante. Utilizzare strumenti di monitoraggio dei log, di analisi del traffico e di rilevamento delle anomalie per individuare tempestivamente comportamenti anomali.

**Risposta rapida agli incidenti:** Avere procedure e piani di risposta agli incidenti ben definiti per affrontare tempestivamente eventuali violazioni o tentativi di propagazione del malware. Assicurarsi che il personale responsabile della sicurezza sia addestrato e pronto a rispondere in modo efficace agli eventi di sicurezza.

**Backup e ripristino dei dati:** Mantenere regolari backup dei dati critici e dei sistemi per consentire un ripristino rapido in caso di necessità. Assicurarsi che i backup siano memorizzati in modo sicuro e che siano testati regolarmente per garantire la loro integrità e disponibilità.

**Patching e aggiornamenti regolari:** Mantenere tutti i software e i sistemi operativi aggiornati con le ultime patch di sicurezza per mitigare le vulnerabilità note e ridurre il rischio di compromissione da parte di malware noti.

# GRAPHICAL EXAMPLE OF THE NETWORK CONFIGURATION IMPLEMENTING THE DISASTER RECOVERY MANUAL



**COME POSSIAMO VEDERE DOPO AVER ESEGUITO LE PROCEDURE PREVISTE DAL DISASTER RECOVERY ABBIAMO IMPOSTATO I SEGUENTI PARAMETRI :**

- - REIMPOSTAZIONE DEI PARAMETRI DI CONFIGURAZIONE DEL FIREWALL
- - BLOCCO DELL'IP DELL'ATTACCANTE
- - CREAZIONE DI UNA NUOVA DMZ CON DATI DI BACKUP
- - ISOLAMENTO E MESSA IN RETE DI QUARANTENA VECCHIA DMZ

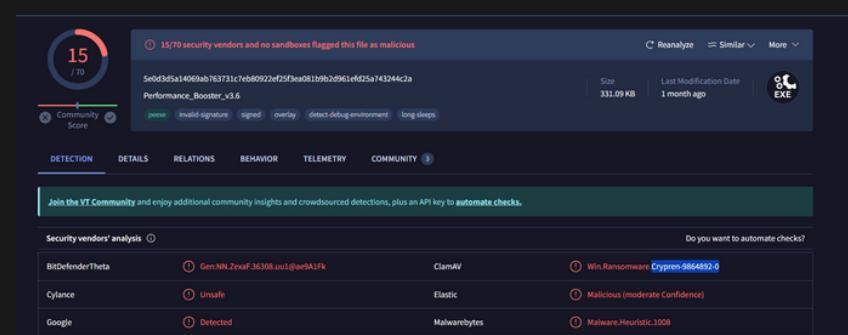
# PRIMA ANALISI:

L'attività prevedeva l'esecuzione di un file denominato "PERFORMANCE BOOSTER\_v3.6.exe" dalla cartella temporanea dell'utente, seguita dalla creazione di un file batch e dalla modifica delle impostazioni dei criteri di esecuzione di PowerShell. L'albero del processo mostra una catena di eventi che parte dall'esecuzione iniziale del file fino alla modifica delle chiavi di registro relative a PowerShell e alle impostazioni Internet. Inoltre, durante l'attività sono stati creati diversi file nella cartella temporanea.

Gli eventi più interessanti in questa attività includono l'esecuzione di un file batch dalla cartella temporanea, che è una tecnica comune utilizzata dal malware per mantenere la persistenza. La modifica del criterio di esecuzione di PowerShell su "Illimitato" indica un tentativo di aggirare le restrizioni di sicurezza ed eseguire script potenzialmente dannosi.

Inoltre, la creazione di file nella cartella temporanea e la modifica di chiavi di registro relative alle impostazioni Internet suggeriscono potenziali attività dannose volte a mantenere il controllo sul sistema ed esfiltrare dati.

In conclusione, l'attività prevedeva l'esecuzione di un file sospetto dalla cartella temporanea, con conseguente creazione di file aggiuntivi, modifica delle impostazioni di PowerShell e modifiche del registro relative alle impostazioni Internet. Queste azioni indicano un potenziale tentativo di stabilire la persistenza, aggirare le misure di sicurezza e potenzialmente esfiltrare dati dal sistema compromesso. Gli analisti di malware dovrebbero prestare molta attenzione a questi indicatori quando indagano sulle potenziali minacce.



| Security vendor  | Analysis                       | Do you want to automate checks?  |
|------------------|--------------------------------|----------------------------------|
| BitDefenderTheta | Gen.NN.Zexif.36308.us1@av9A1Fk | Win.Ransomware.Crypren-9864892-0 |
| Cylance          | Unsafe                         | Elastic                          |
| Google           | Detected                       | Malwarebytes                     |
|                  |                                | Malware.Heuristic.1008           |

## TROJAN.MULTI.CRYPTEN

|  |
|--|
| Home > Threats > Trojan > Trojan.Multi.Crypten   |
| Detect Date 08/13/2015   |
| Class Trojan   |
| Platform Multi   |
| Description This family includes attempts to rename files remotely—behavior characteristic of many ransomware Trojans. |

Dopo un'attenta analisi sia dei comportamenti che da uno studio di derivazione del malware sia sulla tipologia che sulla versione possiamo accettare che si tratta di un trojan denominato "CRYPREN" con all'interno un ransomware dormiente.

# COME DIFENDERSI

1. Disconnetti il computer dalla rete: Questo aiuterà a impedire al trojan di comunicare con i suoi server di comando e controllo e di ricevere istruzioni dannose.
2. Avvia il computer in modalità provvisoria: Riavvia il computer e, durante il processo di avvio, premi ripetutamente il tasto F8 (o un altro tasto appropriato a seconda del sistema operativo) per accedere alle opzioni di avvio avanzate. Seleziona "Modalità provvisoria" per avviare il sistema con un insieme limitato di driver e servizi, che può rendere più facile individuare e rimuovere il trojan.
3. Utilizza un software antivirus o anti-malware: Esegui una scansione completa del sistema con un programma antivirus o anti-malware affidabile. Assicurati che il software sia aggiornato con le definizioni più recenti prima di eseguire la scansione. Segui le istruzioni del software per eliminare qualsiasi minaccia trovata.
4. Rimuovi manualmente i file sospetti: Dopo la scansione, esamina i risultati per individuare eventuali file sospetti o maliziosi e rimuovili manualmente. Assicurati di non eliminare file di sistema importanti.
5. Rimuovi le voci di registro dannose: Usa l'Editor del Registro di sistema (regedit.exe su Windows) per cercare e rimuovere voci di registro correlate al trojan. Fai attenzione a non eliminare voci di registro critiche per il sistema.
6. Esegui una scansione con strumenti specializzati: Alcuni trojan possono essere particolarmente ostinati e richiedere strumenti specializzati per la rimozione. Cerca online per trovare strumenti consigliati per il tipo specifico di trojan che hai.
7. Ripristina il sistema da un punto di ripristino: Se il tuo sistema operativo supporta i punti di ripristino, prova a ripristinare il sistema a un punto precedente all'infezione. Questo può eliminare le modifiche apportate dal trojan.
8. Aggiorna il sistema e i programmi: Assicurati di avere il sistema operativo e tutti i programmi aggiornati con le patch di sicurezza più recenti. Molte volte i trojan sfruttano vulnerabilità note che sono state risolte con patch.
9. Cambia le password: Se il trojan potrebbe aver rubato le tue credenziali, cambia immediatamente tutte le tue password, specialmente per account importanti come email e banche.
10. Proteggi il tuo sistema per il futuro: Installa e mantieni aggiornato un buon software antivirus/anti-malware. Pratica abitudini online sicure e sii cauto nell'aprire allegati e link da fonti sconosciute o non attendibili.



HijackLoader è un caricatore di malware che ha guadagnato notorietà negli ultimi mesi grazie alla sua architettura modulare.

Pur non essendo dotato di funzionalità avanzate, riesce a utilizzare una varietà di moduli per l'iniezione e l'esecuzione del codice. Ecco alcuni punti chiave riguardanti il HijackLoader:

**Funzionamento:** Questo malware loader modulare utilizza chiamate di sistema per eludere la sorveglianza delle soluzioni di sicurezza. È in grado di rilevare processi specifici basandosi su una lista di blocchi incorporata e può ritardare l'esecuzione del codice fino a 40 secondi. La sua caratteristica distintiva è l'uso di moduli incorporati per l'iniezione e l'esecuzione del codice, una caratteristica insolita tra gli altri caricatori di malware.

**Tecniche di evasione:** Il HijackLoader utilizza diverse tecniche di evasione, come il caricamento dinamico delle funzioni API di Windows, il test di connettività HTTP a un sito web legittimo e il ritardo dell'esecuzione del codice. Questo gli consente di fornire varie opzioni di caricamento di payload dannosi.

**Modulo AVDATA:** Interessante è l'inclusione del modulo AVDATA su HijackLoader, che contiene una serie di nomi di processo. Quando il modulo rileva un processo, il comportamento di quest'ultimo potrebbe modificarsi.

**Diffusione futura:** Gli sviluppatori di malware potrebbero sempre più affidarsi al HijackLoader per diffondere nuove minacce. Pertanto, i ricercatori continueranno a monitorare attentamente questa minaccia e condivideranno i risultati con la community.

# COME DIFENDERSI

Consigliamo vivamente di scaricare solo da canali ufficiali e verificati. Inoltre, tutti i programmi devono essere attivati e aggiornati utilizzando funzioni/strumenti legittimi forniti da sviluppatori autentici, poiché gli strumenti di attivazione illegale ("cracking") e gli aggiornamenti di terze parti possono contenere malware.

Un'altra raccomandazione è fare attenzione durante la navigazione poiché i contenuti online falsi e dannosi di solito appaiono legittimi e innocui. Consigliamo di prestare attenzione alle e-mail in arrivo e ad altri messaggi. Gli allegati o i collegamenti presenti nella posta sospetta non devono essere aperti poiché possono essere virulenti.

Ecco a voi una lista di antivirus che hanno il blocklist questo malware: 360 Safeguard, 360 Total Security, Avast, AVG, Avira, BitDefender, ByteFence, Comodo Internet Security, Emsisoft, ESET, Internet Security Essentials, Kaspersky, Malwarebytes, McAfee, Microsoft Defender, Norton 360, Symantec Event Manager, Trend Micro Internet Security e Webroot.

phantomsrl.it

---

# GRAZIE

## PHANTOM SRL

**Prepared by**

PHANTOM SRL  
San Severo, Foggia



**PHANTOM s.r.l**  
**IMPOSSIBLE IS  
OUR TARGET**

*impossible is our target*