



**Monitoraggio, intervento, protezione**

**670%** crescita dei log di esfiltrazioni sui mercati criminali.

**96 milioni** Il numero approssimativo di log di infostealer messi in commercio nel periodo tra luglio 2021 e giugno 2022

#### In questa scheda:

- Sistema di monitoraggio furto di credenziali
- Raccolta dati
- Analisi
- Report
- Esempio di infostealer

## Sistema di monitoraggio furto di credenziali

**Uno dei principali vettori di attacco è il furto di credenziali.**

Ad esempio nel 2022 Microsoft, Nvidia, Uber e Rockstar Games hanno subito violazioni a causa di credenziali di dipendenti compromesse.

Questo ci ha portati a offrire un nuovo servizio che monitora direttamente i sistemi informatici utilizzati per rubare credenziali e raccoglierne i log, in modo da poter individuare se credenziali relative ai domini protetti vengono raccolte.

In questo modo è possibile intervenire tempestivamente per bloccare ulteriori attacchi e mettere in sicurezza le credenziali di autenticazione compromesse.



☎ 06 565 69307

✉ info@gruppoLT.com

🌐 www.gruppolt.com



## Raccolta dati

Il team di analisti raccoglie dati da innumerevoli fonti come:

- ▶ Underground forums
- ▶ Darknet Marketplaces
- ▶ Gruppi Privati
- ▶ Cloud log collectors Privati

Attualmente vengono raccolti giornalmente tra i 10 e i 20 GB di dati relativi a nuove compromissioni.



## Analisi

I dati vengono conservati in ambienti sicuri e analizzati da un team di esperti per eliminare possibili falsi positivi.



## Report

Report di compromissioni vengono quindi inviati al cliente monitorato, in modo che possa prendere consapevolezza della compromissione e possa intervenire tempestivamente.

### Esempio di Infostealer (malware per l'esfiltrazione di credenziali e dati)

Documento infetto distribuito via mail



Decodifica ed esecuzione di codice malevolo sul dispositivo attaccato



Raccolta informazioni dal dispositivo compromesso



I dati vengono compressi ed inviati a sistemi di raccolta



Le informazioni raccolte dai criminali vengono analizzate da sistemi dedicati



Le informazioni raccolte vengono utilizzate per ricattare le vittime o vengono vendute ad altri criminali




## Contatti e recapiti

### ENTRA IN CONTATTO CON LA NOSTRA REALTÀ

Richiedi subito una consulenza

---

 06 565 69307

 [info@gruppoLT.com](mailto:info@gruppoLT.com)

 [www.gruppolt.com](http://www.gruppolt.com)

#### Lazio

- Via della Conciliazione, 10  
00193 Roma

#### Lombardia

- Via Achille Grandi, 8  
25125 Brescia

- Viale Sabotino, 22  
20135 Milano

#### Sicilia

- Piazza Paola Frassinetti, 1  
95040 Mirabella Imbaccari (CT)

