REPORT SULLE MINACCE

Il crimine informatico prende di mira l'Italia

EXECUTIVE SUMMARY

- Gli attori presenti nel panorama delle minacce, compresi quelli che prendono di mira gli utenti italiani, stanno adottando nuovi metodi di distribuzione, allontanandosi dai documenti contenenti macro.
- Quattro attori colpiscono specificamente l'Italia nelle loro campagne.
- Il malware bancario Ursnif è il più frequentemente osservato tra quelli che mirano alle aziende italiane.
- Proofpoint ha osservato attori che hanno simulato organizzazioni governative italiane legate a servizi finanziari, postali e sanitari.
- Le minacce identificate possono consentire il furto di dati, la ricognizione, la perdita finanziaria e l'invio di malware successivi, compresi i

TENDENZE GENERALI DEL PANORAMA DELLE MINACCE

Proofpoint ha osservato numerosi cambiamenti significativi che influenzano il panorama globale delle minacce. Tra questi, l'abbandono di documenti con macro malevole, l'aumento di uso e disponibilità di kit di phishing con credenziali in grado di aggirare l'autenticazione a più fattori (MFA) e la tendenza a intrattenere conversazioni con le vittime selezionate prima di inviare messaggi con payload pericolosi.

Tra la metà 2022 e il 2023, il panorama delle minacce ha registrato uno dei maggiori cambiamenti nei comportamenti dei cybercriminali, a seguito del blocco, da parte di Microsoft, degli allegati contenenti macro tramite impostazione predefinita nei suoi prodotti Office. Questo aggiornamento ha costretto gli attori delle minacce ad adottare nuovi meccanismi per distribuire malware, modificando regolarmente tattiche, tecniche e procedure nelle proprie campagne, per cercare di eludere i rilevamenti di anomalie, utilizzando anche tipologie di file raramente osservati in passato.

Con l'MFA che sta diventando una pratica di sicurezza standard, i kit di phishing si sono evoluti per rubare i token e aggirarla. Gli attori delle minacce utilizzano procedure che sfruttano un reverse proxy trasparente, consentendo loro di effettuare un "attacker-in-the-middle" durante una sessione browser e rubare credenziali e cookie in tempo reale. In base alla propria visibilità Proofpoint ha osservato una diffusione sempre più elevata di questi kit.

È stato evidenziato anche un aumento delle minacce TOAD (telephone-oriented attack delivery), che utilizzano il social engineering per spingere il destinatario a telefonare a un falso rappresentante del servizio clienti, che condurrà successivamente la vittima all'installazione di malware. Attualmente sono centinaia di migliaia le minacce di questo tipo che Proofpoint osserva ogni giorno.

Gli APT utilizzano messaggi apparentemente innocui e tecniche di impersonificazione di più persone per invogliare le vittime designate a interagire con loro prima di distribuire malware o rubare credenziali. I ricercatori di Proofpoint hanno osservato questo comportamento anche da parte di attori specializzati in BEC ed eCrime.

PANORAMICA DELLE MINACCE IN ITALIA

Proofpoint attualmente ha rilevato quattro attori e molteplici cluster di minacce non attribuiti che dal 2022 hanno preso di mira nello specifico aziende italiane per distribuire malware; questi includonoTA550, TA551, TA544 e TA554. Da gennaio 2022 sono state identificate quasi 150 campagne che hanno come obiettivo gli utenti italiani, molte delle quali possono essere attribuite ad attori noti.

Questo report analizza le attività osservate tra gennaio 2022 e maggio 2023. Una campagna è definita come un insieme temporale di attività pericolose correlate analizzate dai ricercatori di Proofpoint. Anche nei casi in cui non vi sia attribuzione, le minacce di una determinata campagna derivano da attacchi perpetrati dallo stesso attore e possono essere correlate da una serie di fattori, tra cui l'infrastruttura di distribuzione o di hosting, la sovrapposizione di dati forensi nei messaggi, come i componenti dell'intestazione, un payload comune o altri aspetti. Le minacce analizzate in questo report si basano su tag associati ai dati delle campagne, applicati manualmente dai ricercatori al momento dell'identificazione.

Alcuni attori, come TA542, noto anche come Emotet, e TA577, affiliato di Qbot, includono utenti italiani e messaggi esca in lingua italiana nelle loro campagne globali a elevato volume.

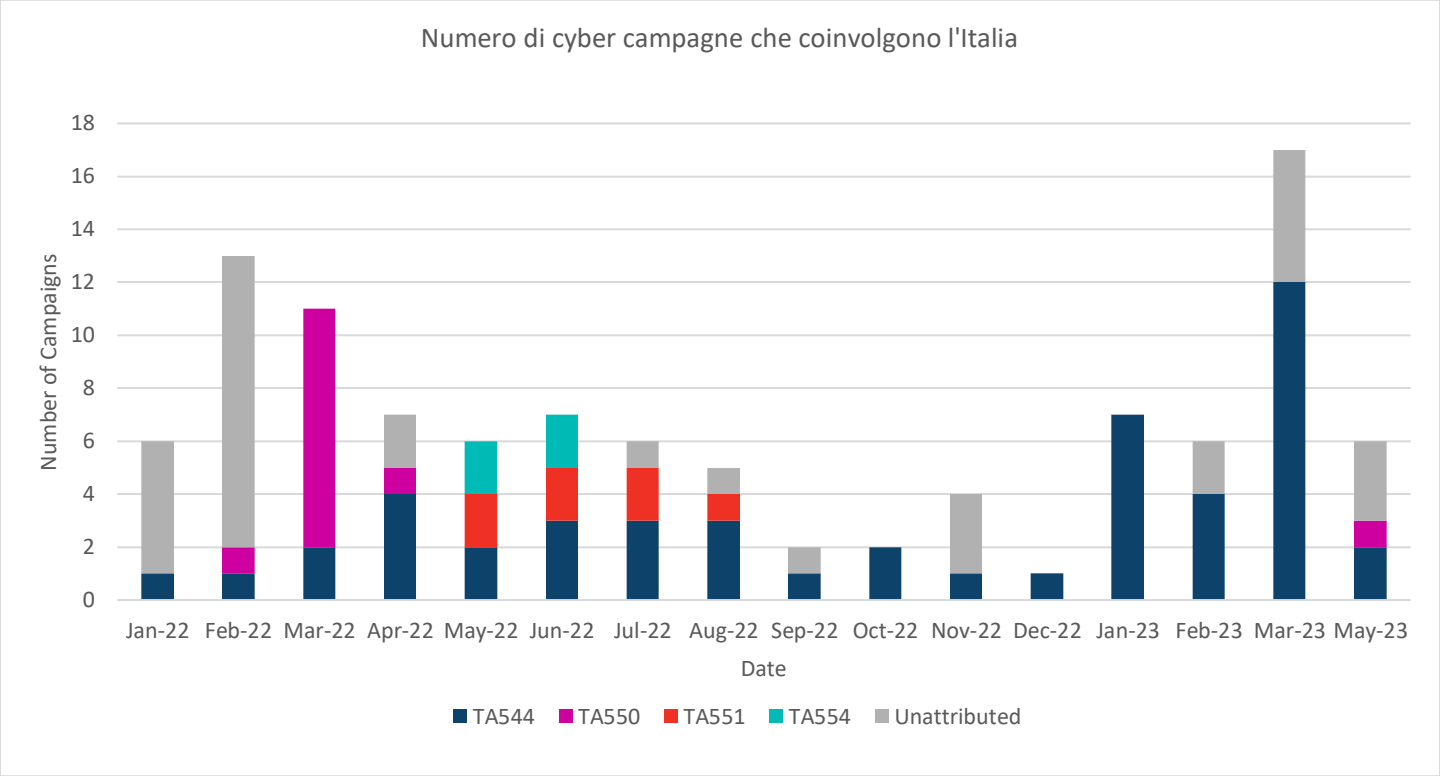

Figura 1. Numero di campagne rivolte anche a utenti italiani.

Proofpoint osserva regolarmente anche minacce a sfondo finanziario che colpiscono gli utenti italiani, che non sono attribuibili ad attori tracciati che utilizzano malware di tipo commodity.

DETTAGLI SUGLI ATTORI DELLE MINACCE

TA550

Proofpoint ha identificato per la prima volta TA550 come attore nel febbraio 2022. Questo cybercriminale prende di mira quasi esclusivamente organizzazioni italiane ed è stato osservato distribuire i malware Ursnif e IcedID. Da aprile 2022, Proofpoint ha esaminato attività sporadiche da parte di TA550 con l'obiettivo di acquisire account, rubare dati e causare perdite finanziarie.

TA550 fa spesso leva su temi governativi italiani, come informazioni fiscali o altro. Ad esempio, nel dicembre 2022 Proofpoint ha osservato un'esca che, tramite spoofing dell'Agenzia del Farmaco, invitava gli utenti a partecipare a un congresso di oftalmologia.

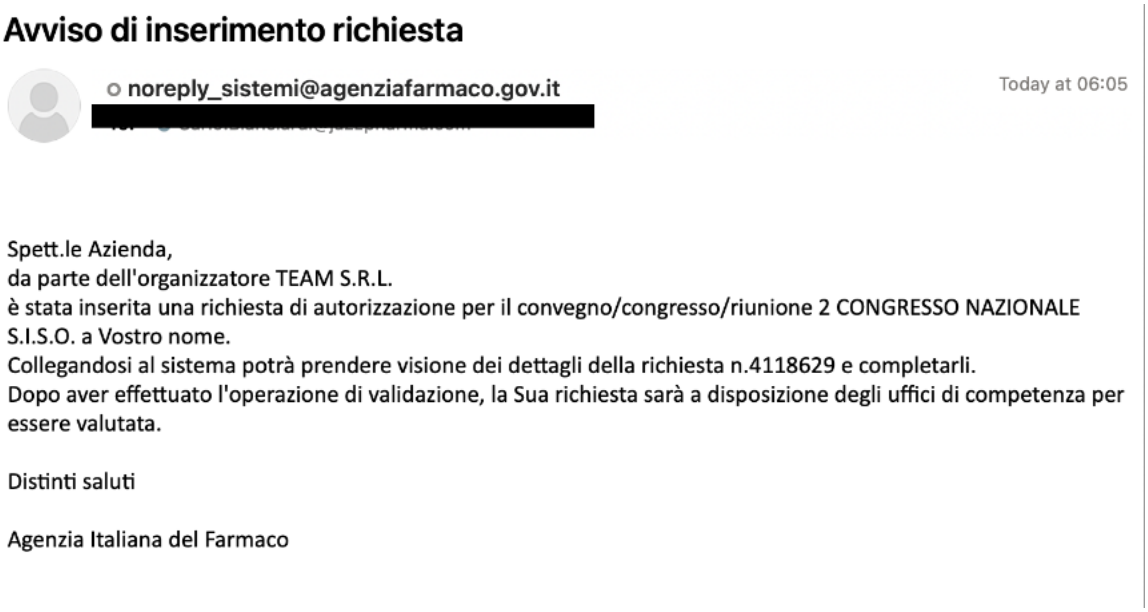

Figura 2. Email esca che riproduce l'Agenzia del Farmaco

I messaggi contenevano allegati dannosi come documenti Microsoft Excel o Word, o HTA zippati, ma anche URL che conducevano a contenuti pericolosi.

TA551

Proofpoint segue TA551 dal 2016. Questo attore distribuisce malware, tipicamente IcedID, ma anche altri payload, tra cui Ursnif, SVCReady e Bumblebee. TA551 può agire come initial access broker (IAB), con infezioni che conducono al ransomware. Generalmente, attua campagne con centinaia o migliaia di messaggi e il suo obiettivo comprende varie aree geografiche. Proofpoint ha osservato che TA551 si rivolge a organizzazioni italiane con specifici messaggi in lingua italiana.

Questo attore è solito allegare file dannosi in risposta a conversazioni legittime, tecnica nota come thread hijacking, ottenendo probabilmente l'accesso ai messaggi rubati che poi sfrutta per le sue campagne email. Utilizza quindi i thread di posta elettronica, rispondendo a uno dei partecipanti con un messaggio come "Si prega di visualizzare l'allegato e confermare" o simile, includendo un URL dannoso. Nel seguente esempio del 31 marzo 2023, TA551 ha utilizzato il thread hijacking per inviare documenti OneNote pericolosi che contenevano uno script incorporato per installare malware.

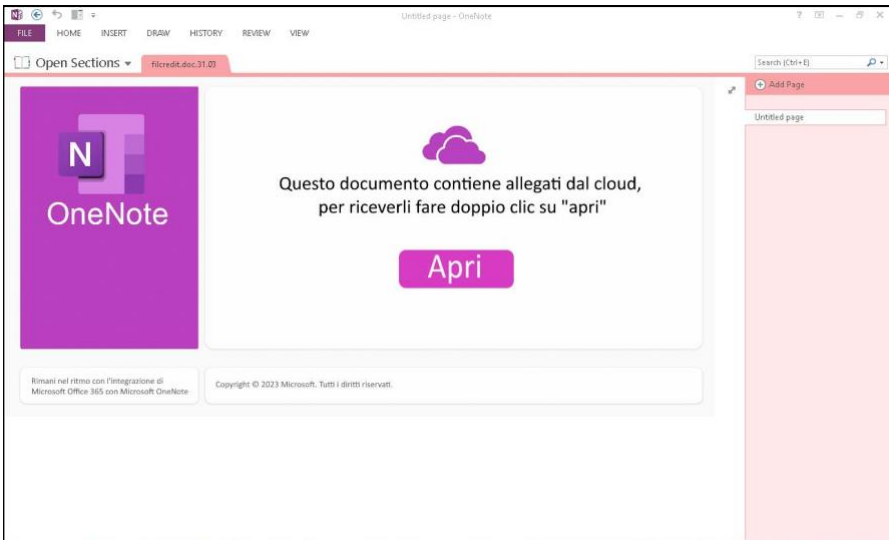

Figura 3. Esempio di TA551

Gli attacchi di TA551 possono portare al furto di dati, a perdite finanziarie e, eventualmente, a successive infezioni, ad esempio, ransomware.

TA544

TA544 è un attore criminale che distribuisce soprattutto malware bancari e la maggior parte delle sue campagne colpisce aziende italiane. Diffonde quasi esclusivamente il trojan bancario Ursnif, anche se i ricercatori l'hanno osservato utilizzare anche IcedID e SVCReady. Da gennaio 2022, Proofpoint ha identificato sue campagne per un totale di quasi 1 milione di messaggi e circa 50 iniziative con impatto sull'Italia.

In una recente attività, i messaggi sembravano provenire da un'azienda logistica italiana e contenevano un PDF con un URL che conduceva a un file JavaScript compresso che installava Ursnif.

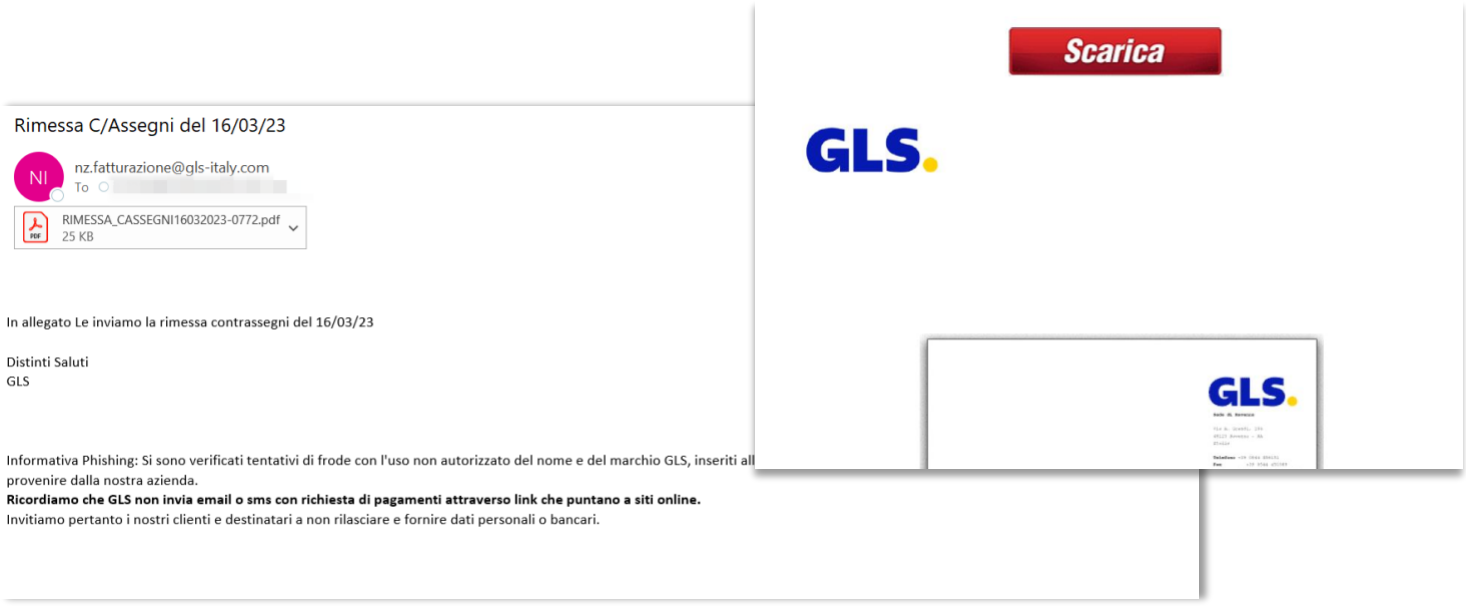

Figura 4. TA544, email di richiamo che si riferiscono alla spedizione e che contengono un PDF

Gli attacchi di TA544 potrebbero portare al furto di dati, a perdite finanziarie e potenzialmente a infezioni successive come il ransomware. Sulla base di segnalazioni open source correlate ai dati interni di Proofpoint, le campagne TA544 hanno condotto a ransomware come Nokoyawa.

TA554

Proofpoint monitora TA554 dal 2017, anche se questo attore non era più stato rilevato da settembre 2019 a novembre 2021. TA554 ha condotto quattro campagne nel 2022 e nel 2023 non è ancora stato rintracciato. Tutte le iniziative hanno avuto come obiettivo aziende italiane, distribuendo sLoad, un downloader che fornisce payload successivi come trojan bancari.

TA554 utilizza diversi temi e tipi di esche, tra cui allegati e URL. In diverse campagne, ha effettuato lo spoofing o abusato del servizio PEC italiano (Posta Elettronica Certificata) per distribuire allegati dannosi che hanno condotto a sLoad.

TA542

TA542, noto anche come Emotet, è tra le minacce con il più alto volume di traffico nei dati a disposizione di Proofpoint. A differenza degli altri attori identificati, TA542 non prende di mira specificamente le organizzazioni italiane, ma include esche in lingua italiana nelle sue campagne di grandi dimensioni che mirano a più aree geografiche. Ha colpito migliaia di clienti con decine di migliaia di messaggi e, in alcuni casi, il loro volume supera il milione per campagna.

Delle nove campagne Emotet osservate a marzo 2023, sette includevano tra gli obiettivi aziende italiane. Emotet è una delle minacce cybercriminali più prolifiche che colpisce le organizzazioni a livello globale e i suoi attacchi possono provocare perdite finanziarie e, potenzialmente, ransomware.

DETTAGLI SULLE MINACCE INFORMATICHE

Sulla base dei dati delle campagne rivolte specificamente agli utenti italiani, il malware più spesso rilevato è Ursnif. Si tratta di un trojan che può essere utilizzato per rubare dati dai siti web, con l'aiuto di iniezioni web, proxy e connessioni VNC; sottrarre informazioni come password memorizzate e scaricare aggiornamenti, moduli o altri malware. Nell'ultimo anno, quasi l'80% delle campagne Ursnif mirate all'Italia sono state associate a TA544 o TA550.

Al secondo e terzo posto tra i malware più osservati vi sono SVCReady e IcedID, con campagne quasi interamente associate rispettivamente a TA551 e TA554. Entrambe le famiglie sono loader che possono essere utilizzati per colpire una vittima compromessa con ulteriori payload malware.

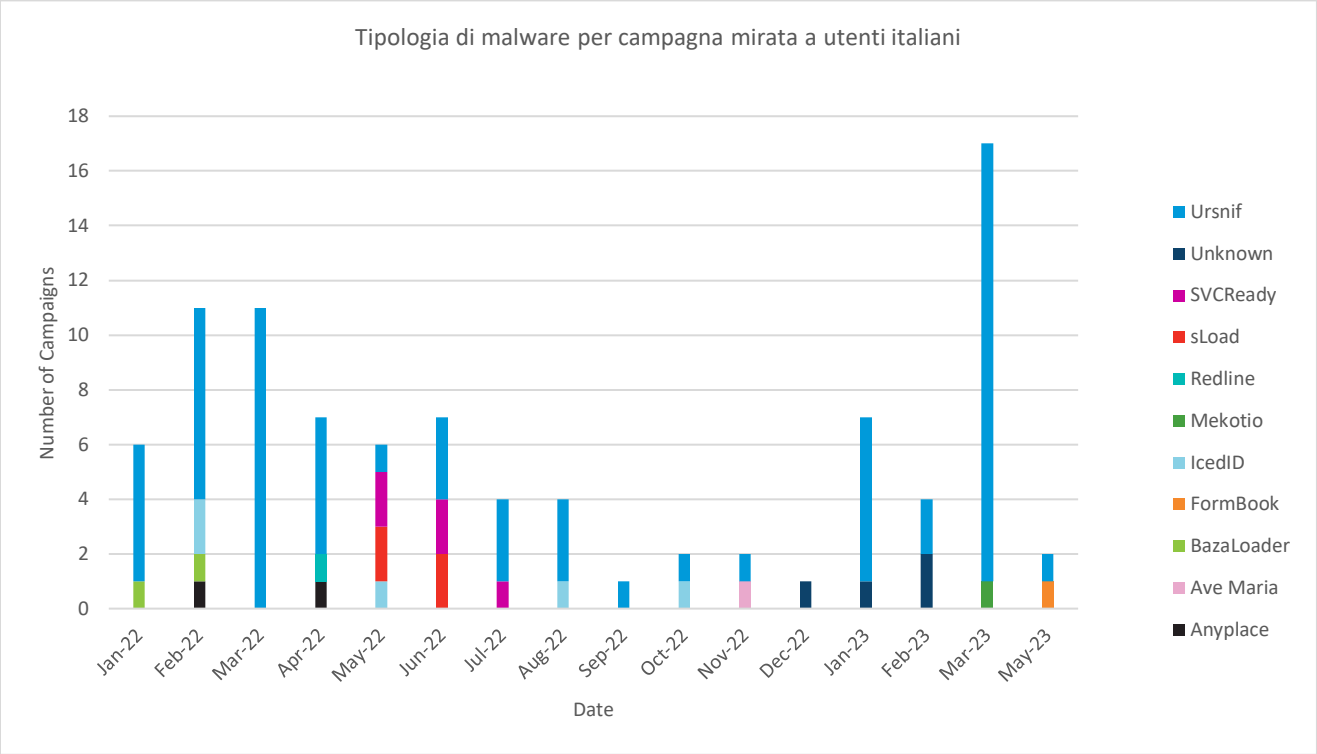

Figura 5. Campagne malware rivolte nello specifico a utenti italiani

Proofpoint osserva spesso campagne di malware commodity che colpiscono utenti italiani: si tratta in questo caso di malware disponibili per l'acquisto o reperibili in repository open source, non per forza utilizzati da attori specifici. Circa il 24% delle campagne identificate che ha preso di mira aziende italiane non è stato attribuito a un cybercriminale noto e di queste, il 35% ha distribuito malware commodity, tra cui Formbook, AgentTesla e RedLine.

Questa tipologia di malware spesso utilizza elementi di social engineering diversi per coinvolgere gli utenti rispetto ai metodi utilizzati dagli attori tracciati. Ad esempio, a maggio 2023, Proofpoint ha osservato un'esca in lingua italiana che utilizzava temi generici di ordini/fatturazione con l'obiettivo di colpire utenti in Italia e in Europa.

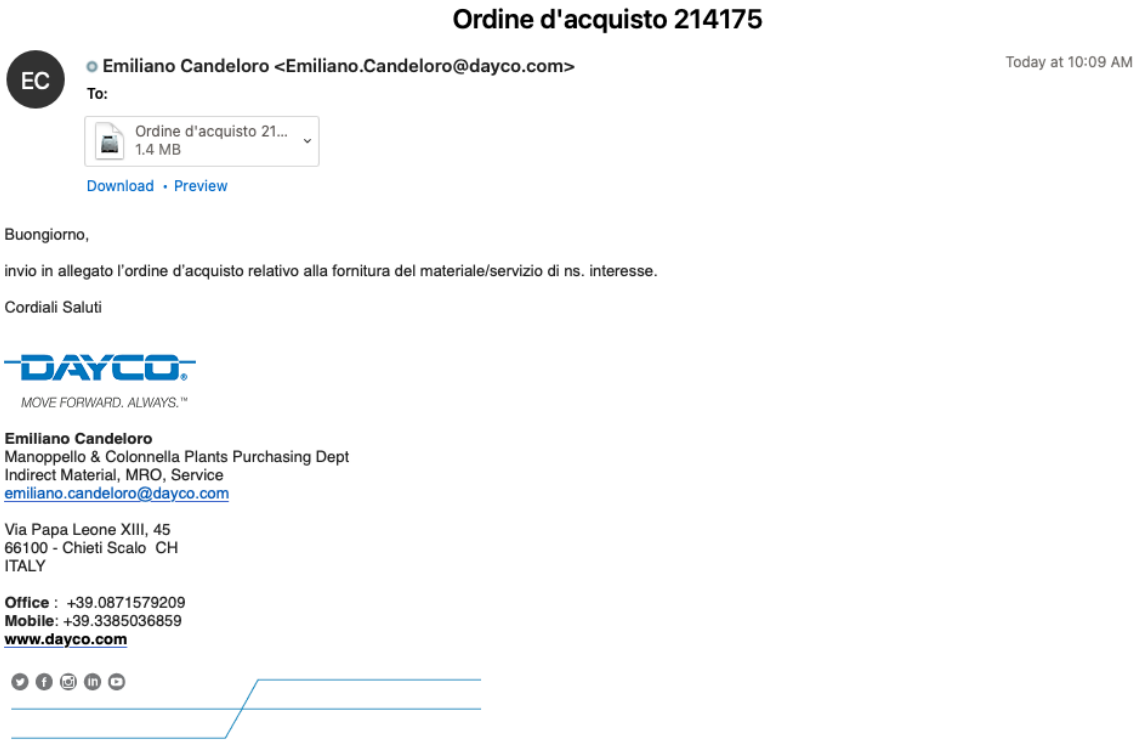

Figura 6. Fattura esca che distribuisce AgentTesla

Proofpoint ha anche osservato campagne non attribuite di IcedID e Ursnif rivolte a utenti italiani. Queste famiglie di malware sono trojan modulari generalmente gestiti da gruppi criminali più sofisticati rispetto agli operatori di base, collegati alla consegna di payload ransomware da ricercatori di terze parti.

COMPROMISSIONE DELLE EMAIL AZIENDALI

Proofpoint rileva regolarmente minacce di business email compromise (BEC) rivolte all'Italia, nonostante molti di questi messaggi siano in inglese. Fingono di essere contenuti rilevanti per le aziende, come fatture o richieste di acquisto, al fine di frodarle.

Le perdite causate dalle minacce BEC possono variare da decine di migliaia a milioni di dollari.

CONCLUSIONE

Sono diversi gli attori delle minacce che prendono di mira le organizzazioni italiane a scopo di lucro, sfruttando tecniche di social engineering, tra cui lo spoofing di enti governativi italiani o fingendo di essere risposte a conversazioni esistenti, per indurre gli utenti a fidarsi e condividere contenuti.

I cybercriminali dimostrano di avere molti obiettivi, tra cui furto di dati, takeover di account, recupero di informazioni bancarie per rubare fondi o installare malware successivi, tra cui potenzialmente il ransomware. Minacce che possono avere un forte impatto finanziario, con perdite di milioni di dollari.

SCOPRI DI PIÙ

Per ulteriori informazioni, visita **proofpoint.com**.

proofpoint.