proofpoint. | Threat Research

21 JUNE 2023

THREAT SUMMARY

Cybercrime Targeting Italy

EXECUTIVE SUMMARY

- Actors across the threat landscape, including those targeting Italian users, are adopting new delivery methods and moving away from macro-enabled documents.
- Four threat actors specifically target Italy in campaigns.
- Ursnif banking malware is the most frequently observed malware targeting Italian organizations.
- Proofpoint has observed actors spoof Italian government organizations related to financial, postal, and health services.
- Identified threats can enable data theft, reconnaissance, financial loss, and delivery of follow-on malware, including ransomware.

OVERALL THREAT LANDSCAPE TRENDS

Proofpoint has observed multiple major changes impacting the global threat landscape. This includes the shift away from macro-enabled documents, the increased use and availability of credential phishing kits that bypass multi-factor authentication (MFA), and efforts to build trust with targets by initiating benign conversations before sending content with a payload.

From mid-2022 into 2023, the threat landscape experienced one of the largest shifts in threat behaviors across threat actor designations due to Microsoft beginning to block macro-enabled attachments by default in its Office products. This change forced threat actors to adopt new mechanisms of malware delivery, including regularly modifying tactics, techniques, and procedures (TTPs) in campaigns as an attempt to evade detections, and using infrequently observed filetypes.

MFA is becoming a standard security practice and phish kits have evolved to steal these tokens and bypass MFA. Threat actors are using phish kits that leverage transparent reverse proxy, which enables them to conduct “attacker-in-the-middle” during a browser session and steal credentials and session cookies in real-time. Based on Proofpoint visibility, such kits are becoming more widely available.

Proofpoint has also observed an increase in telephone-oriented attack delivery (TOAD) threats, which use social engineering to prompt a recipient to phone a fake customer service representative, which leads to the installation of malware. Proofpoint currently observes hundreds of thousands of these threats per day.

APT actors commonly use benign messages and multi-persona impersonation to entice targets to interact with threat actors before deploying malware or credential capture attempts, but Proofpoint researchers have observed this behavior used by BEC and ecrime actors as well.

ITALY THREAT OVERVIEW

Proofpoint currently tracks four threat actors and multiple unattributed threat clusters that have specifically targeted Italian organizations to distribute malware since 2022. These include TA550, TA551, TA544, and TA554. Since January 2022, Proofpoint has identified nearly 150 cybercriminal campaigns that target users in Italy, many of which can be attributed to known threat actors. This report covers activity observed between January 2022 to May 2023. For the purpose of this report, a campaign is defined as a timebound set of related threat activity analyzed by Proofpoint researchers. Even in cases where no attribution is made, threats from a given campaign result from attacks perpetrated by the same threat actor. Threats may be related by a variety of factors including distribution or hosting infrastructure, overlap in message forensics such as header components, a common payload, or other facets. Threats analyzed in this report are based on tags associated with campaign data, which are manually applied by threat researchers at the time of identification.

Some actors, such as TA542, also known as Emotet, and the Qbot affiliate TA577 include Italian users and Italian language lures among its target set in high-volume campaigns that target entities globally.

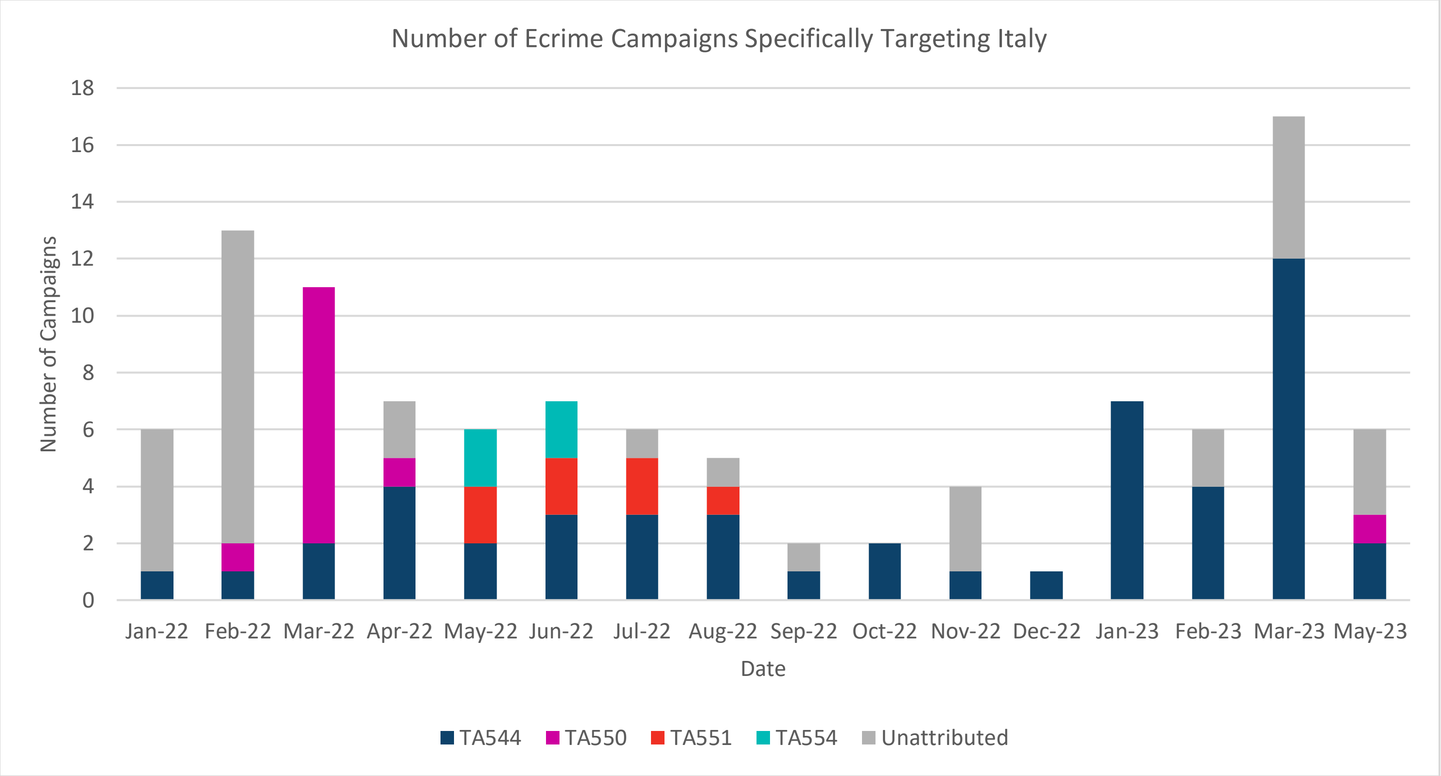


Figure: Number of campaigns with targeting including Italian users.

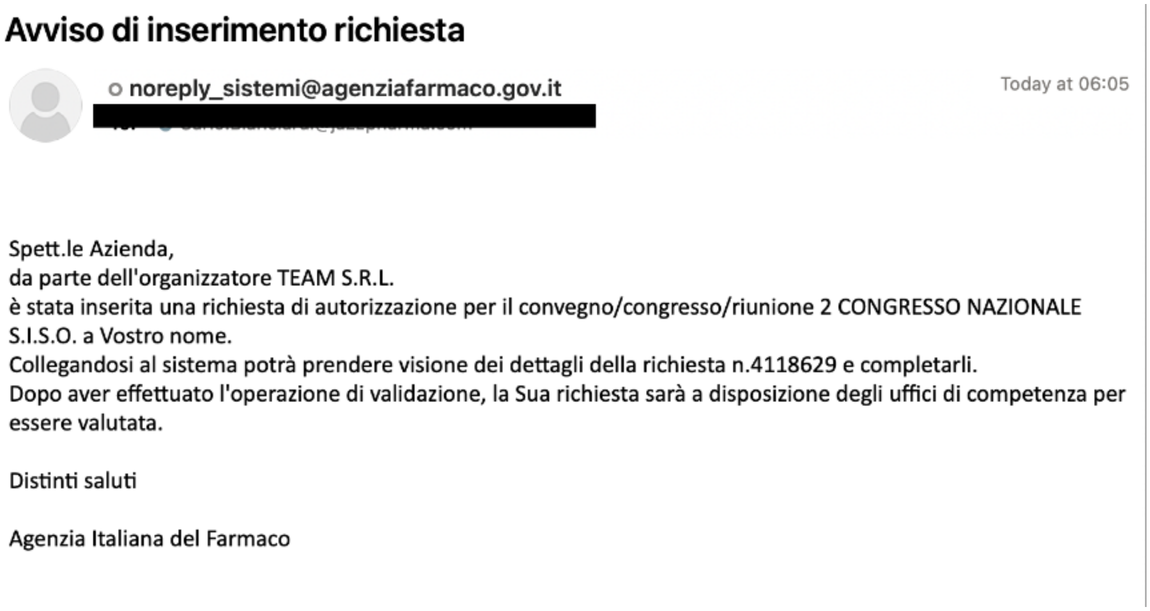
Proofpoint also regularly observes financially motivated threats impacting Italian users that are not attributable to tracked threat actors that use commodity malware.

THREAT ACTOR DETAILS

TA550

Proofpoint first designated TA550 as a tracked actor in February 2022. This actor almost exclusively targets Italian organizations and has been observed distributing Ursnif and IcedID malware. Since April 2022, Proofpoint has observed sporadic threat activity from TA550. Activity associated with TA550 can lead to account takeovers, data theft, and financial loss.

TA550 often leverages Italian government themes, such as tax information or other issues. For example, Proofpoint observed a lure in December 2022 spoofing Agenzia del Farmaco inviting users to participate in an ophthalmology congress.



Avviso di inserimento richiesta

noreply_sistemi@agenziafarmaco.gov.it

Today at 06:05

[redacted]

Spett.le Azienda,
da parte dell'organizzatore TEAM S.R.L.
è stata inserita una richiesta di autorizzazione per il convegno/congresso/riunione 2 CONGRESSO NAZIONALE S.I.S.O. a Vostro nome.
Collegandosi al sistema potrà prendere visione dei dettagli della richiesta n.4118629 e completarli.
Dopo aver effettuato l'operazione di validazione, la Sua richiesta sarà a disposizione degli uffici di competenza per essere valutata.

Distinti saluti

Agenzia Italiana del Farmaco

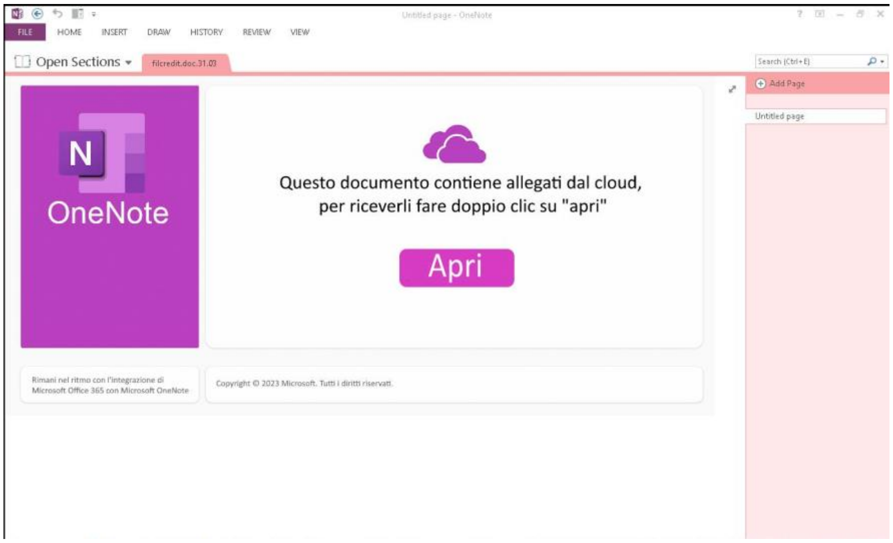
Figure: Italian-language lure spoofing Agenzia del Farmaco, the Italian medicines agency.

Emails historically contain malicious attachments such as Microsoft Excel or Word documents, or zipped HTA attachments, but Proofpoint has also observed TA550 distributing URLs linking to malicious content.

TA551

Proofpoint has tracked TA551 since 2016. This actor distributes malware, typically IcedID, but with other payloads including Ursnif, SVCReady, and Bumblebee. TA551 can act as an initial access broker (IAB), with infections leading to ransomware. Typically, this actor distributes campaigns with hundreds to thousands of messages, and its targeting includes various geographies. Proofpoint has observed TA551 specifically target Italian organizations with Italian language lures, but it is not exclusively targeting this region.

Proofpoint researchers typically observe TA551 injecting malicious attachments as replies to legitimate conversations, known as thread hijacking. The actor likely gains access to stolen messages which it then uses for its email campaigns. The attacker then uses the email threads and replies to one of the participants with a text such as "Please see attached and confirm" or similar text and includes a malicious attachment or URL. In the following example from 31 March 2023, TA551 used thread hijacking to send malicious OneNote documents that contained an embedded malicious script to install malware.



Questo documento contiene allegati dal cloud, per riceverli fare doppio clic su "apri"

Rimani nel ritmo con l'integrazione di Microsoft Office 365 con Microsoft OneNote

Copyright © 2023 Microsoft. Tutti i diritti riservati.

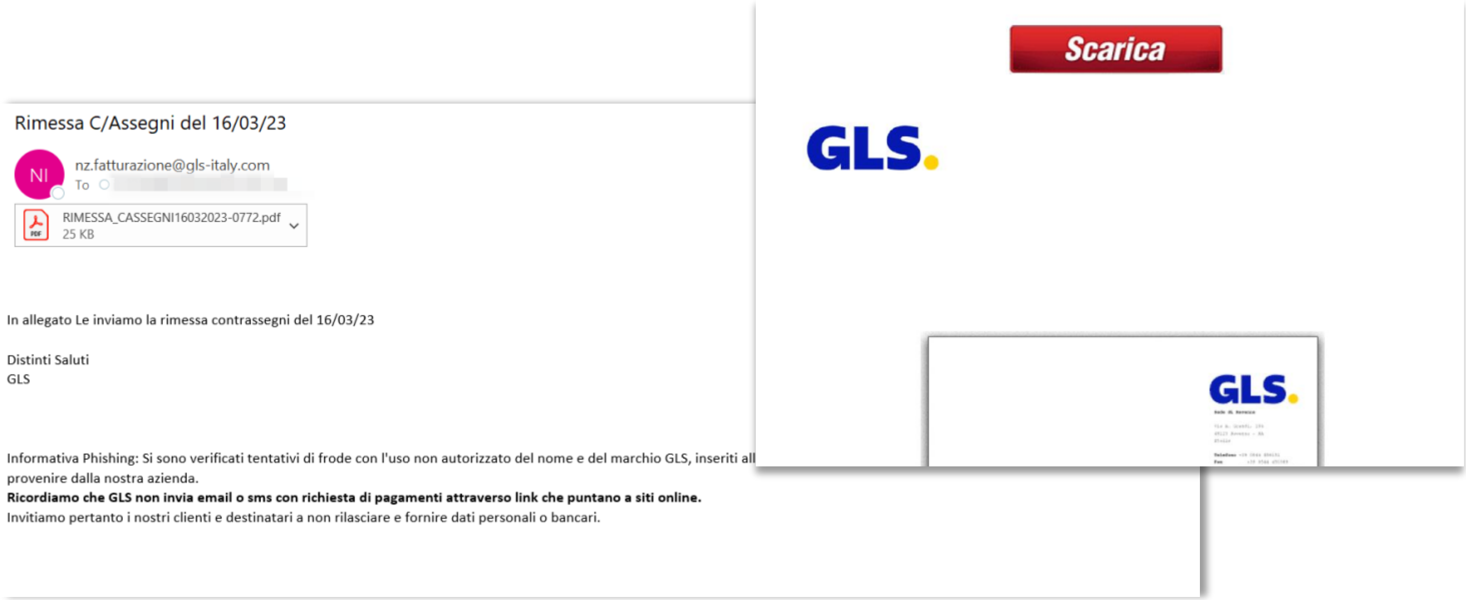
Figure: TA551 example.

TA551 infections can lead to data theft, financial loss, and possibly follow-on infections such as ransomware.

TA544

TA544 is a cybercriminal threat actor that distributes mostly banking malware. Nearly all its targeted campaigns impact Italian organizations. TA544 almost exclusively distributes the Ursnif banking trojan, though researchers have also observed this actor distribute IcedID and SVCReady. Since January 2022, Proofpoint has observed TA544 conduct campaigns with nearly 1 million messages total, and with nearly 50 campaigns impacting Italy.

In one recent campaign, messages purported to be from an Italian shipping organization and contained a PDF with a URL leading to a compressed JavaScript file that installed Ursnif.



Rimessa C/Assegni del 16/03/23

nz.fatturazione@gls-italy.com
To [redacted]

RIMESSA_CASSEGNI16032023-0772.pdf
25 KB

In allegato Le inviamo la rimessa contrassegni del 16/03/23

Distinti Saluti
GLS

Informativa Phishing: Si sono verificati tentativi di frode con l'uso non autorizzato del nome e del marchio GLS, inseriti all
provenire dalla nostra azienda.
Ricordiamo che GLS non invia email o sms con richiesta di pagamenti attraverso link che puntano a siti online.
Invitiamo pertanto i nostri clienti e destinatari a non rilasciare e fornire dati personali o bancari.

Figure: TA544 email lure purporting to relate to shipping, containing a PDF.

Infections from TA544 could lead to data theft, financial losses, and potentially lead to follow-on infections such as ransomware. Based on open source reporting correlated with internal Proofpoint threat data, TA544 campaigns have led to ransomware such as Nokoyawa.

TA554

Proofpoint has tracked TA554 since 2017, however TA554 was absent from Proofpoint data between September 2019 and November 2021. TA554 conducted four campaigns in 2022, and has not been observed so far in 2023. All of the campaigns targeted Italian organizations. This actor typically distributes sLoad, a downloader that delivers follow-on payloads such as banking trojans.

TA554 uses multiple themes and lure types, including distributing attachments and URLs. In multiple campaigns, TA554 either spoofed or abused the Italian PEC service (Certified Email in Italian Posta Elettronica Certificata) to deliver malicious attachments that ultimately led to sLoad.

TA542

TA542, also known as Emotet, is among the most high-volume threats in Proofpoint data. Unlike the other identified actors, TA542 does not specifically target Italian organizations in campaigns, but does include Italian-language lures in targeting in large campaigns that target multiple geographic regions. TA542 has targeted thousands of customers with tens of thousands of messages. In some cases, the message volume reaches over one million per campaign.

Of the nine Emotet campaigns observed in March 2023, seven included Italian organizations in their target set. Emotet is one of the most prolific cybercriminal threats targeting organizations globally. Infections can lead to financial losses, and potentially ransomware.

MALWARE DETAILS

Based on campaign data for threats specifically targeting Italian users, the most observed malware is Ursnif. Ursnif is a trojan that can be used to steal data from websites, with the help of web injections, proxies and VNC connections; steal data such as stored passwords; and download updates, modules, or other malware. In the last year, nearly 80% of Italian-targeted Ursnif campaigns were associated with either TA544 or TA550.

SVCReady and IcedID malware are the second and third most observed malware, with campaigns almost entirely associated with TA551 and TA554, respectively. Both these malware families are loaders that can be used to infect a compromised victim with additional malware payloads.

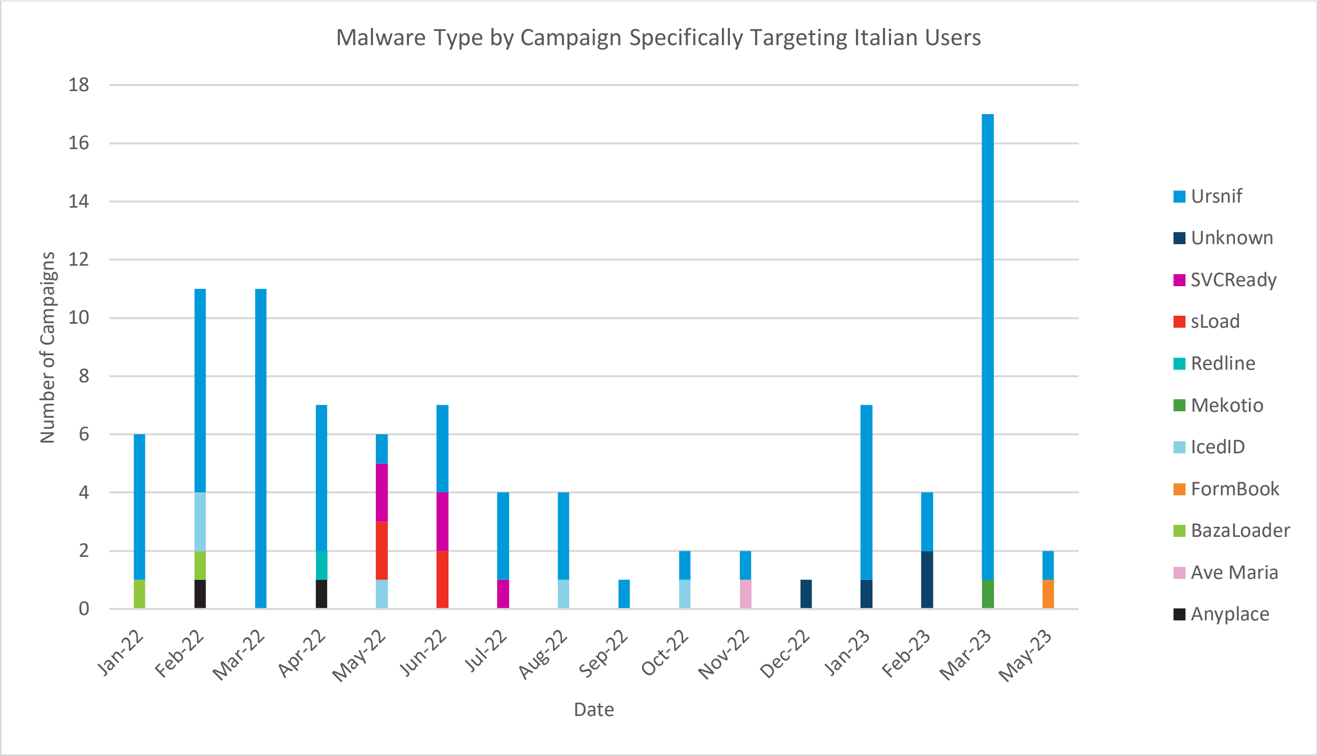
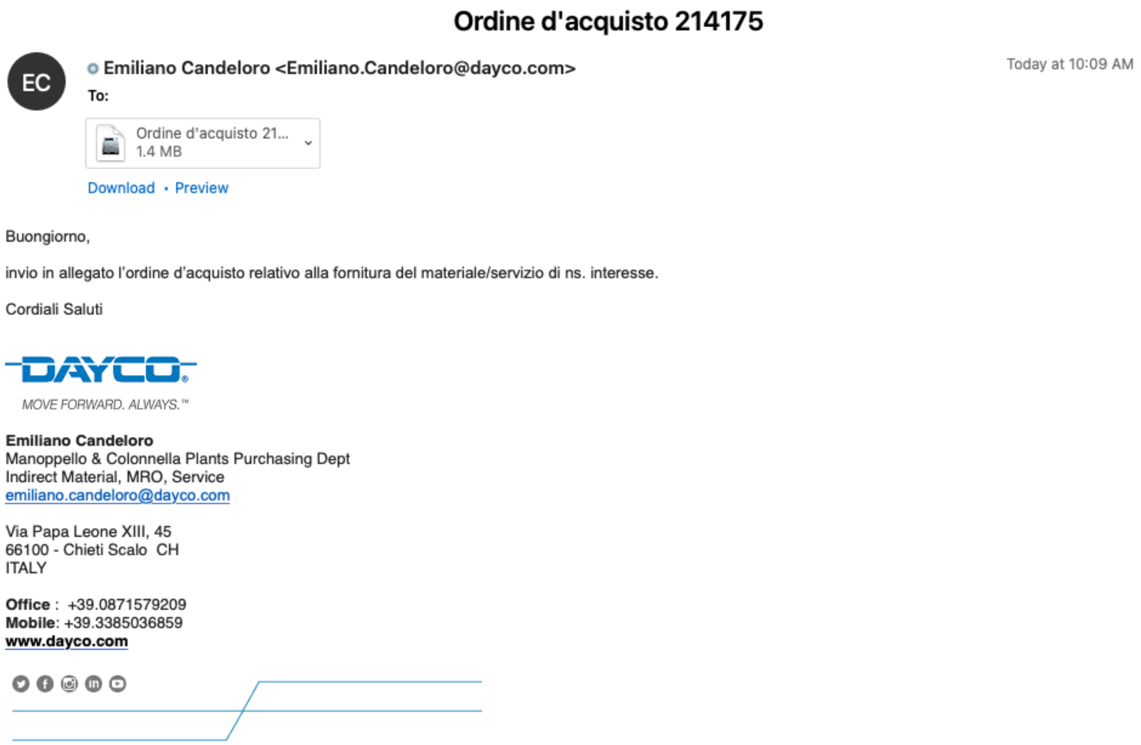


Figure: Observed malware campaigns specifically targeting Italian users.

Proofpoint frequently observes commodity malware campaigns impacting Italian users. Commodity malware is available for purchase or in open-source repositories for threat actors to obtain and is not used by specific threat actors. Approximately 24% of identified campaigns targeting Italian organizations were not attributed to a known threat actor, and of these, 35% distributed commodity malware including Formbook, AgentTesla, and RedLine malware.

Commodity malware often uses different types of social engineering to engage users than methods used by tracked threat actors. For example, in May 2023, Proofpoint observed an Italian language lure using generic order/invoicing themes to target users in Italy and elsewhere in Europe.



Ordine d'acquisto 214175

Emiliano Candeloro <Emiliano.Candeloro@dayco.com>
To:

Today at 10:09 AM

Buongiorno,

invio in allegato l'ordine d'acquisto relativo alla fornitura del materiale/servizio di ns. interesse.

Cordiali Saluti

DAYCO
MOVE FORWARD. ALWAYS.™

Emiliano Candeloro
Manoppello & Colonnella Plants Purchasing Dept
Indirect Material, MRO, Service
emiliano.candeloro@dayco.com

Via Papa Leone XIII, 45
66100 - Chieti Scalo CH
ITALY

Office : +39.0871579209
Mobile: +39.3385036859
www.dayco.com

Figure: Invoice theme lure delivering AgentTesla.

Proofpoint also observed unattributed IcedID and Ursnif campaigns targeting Italian users. These malware families are modular trojans that are typically operated by more sophisticated criminal threat groups than commodity operators and have been linked to ransomware payload delivery by third-party researchers.

BUSINESS EMAIL COMPROMISE

Proofpoint regularly observes business email compromise (BEC) threats targeting Italian organizations, though many of these emails are in English. These messages will purport to be business-relevant content such as invoices or purchasing inquiries and attempt to defraud organizations.

Losses from BEC threats can range from tens of thousands to millions of dollars.

CONCLUSION

Multiple threat actors target Italian organizations for financial gain. Such actors leverage social engineering techniques including spoofing Italian government entities or purporting to be replies to existing conversations to trick users into trusting and engaging with the content.

Threat actors demonstrate many objectives for exploitation, including stealing data and taking over accounts, obtaining banking details to steal funds, or install follow-on malware including potentially ransomware. Such threats can have major financial impacts, with losses totaling millions of dollars.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.