Security Brief: TA544 Targets Italian Organizations with Ursnif Malware

proofpoint.com/us/blog/security-briefs/ta544-targets-italian-organizations-ursnif-malware

September 28, 2021

Blog
Threat Insight
Security Brief: TA544 Targets Italian Organizations with Ursnif Malware

September 29, 2021 Selena Larson and Proofpoint Staff

Proofpoint threat researchers identified an increase in targeted threats impacting Italian organizations in 2021. This spike in observed threats is largely driven by a group called TA544 leveraging the Ursnif banking trojan. Proofpoint has observed nearly 20 notable campaigns distributing hundreds of thousands of messages targeting organizations in Italy so far this year, which equals 80% of the total number of similar campaigns in the entirety of 2020. As many as 2,000 organizations were targeted in each of the Italian-language campaigns.

TA544 is a cybercriminal threat actor that distributes banking malware and other payloads in various geographic regions including Italy and Japan. Proofpoint has tracked this actor since 2017. Typically, this group varies its payloads which appear to be targeted by region – for example, in 2021, all TA544 Ursnif campaigns have specifically targeted Italian organizations while Dridex payloads associated with this threat actor do not have specific geographic targeting.

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. Although this malware is used by multiple cybercriminal threat actors, TA544's activity targeting Italy differentiates it from other actors. Between January and August 2021, the number of observed Ursnif campaigns impacting Italian organizations surpassed the total number of observed Ursnif campaigns targeting this region in all of 2020.

Campaign Details

In recently observed campaigns, TA544 purports to be Italian courier or energy organizations soliciting payments from the targeted individual.

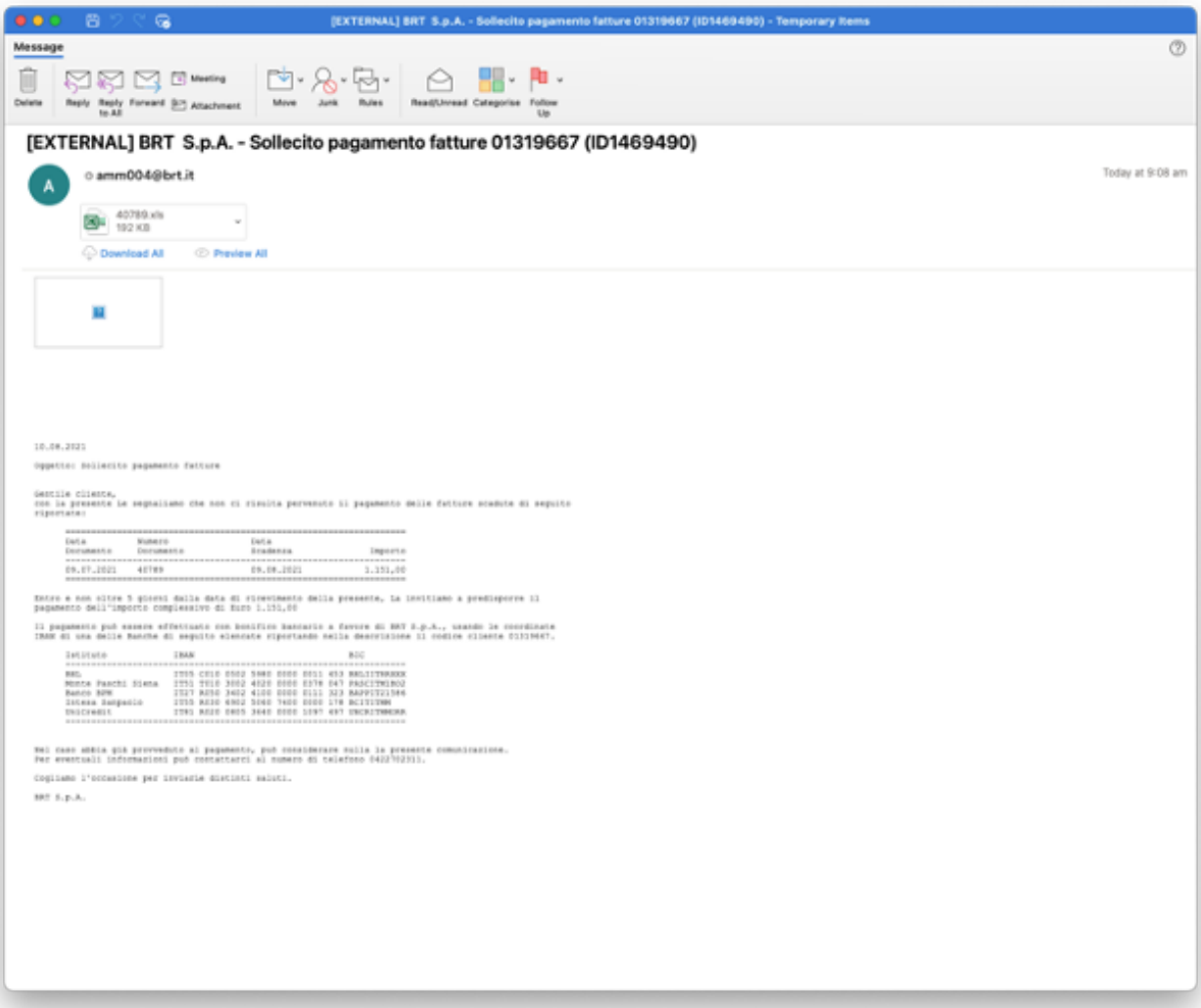

Figure 1: Phishing email masquerading as logistics/courier service BRT.

Attached to the emails are malicious Microsoft Office documents containing macros. If the macros are enabled, the document will download Ursnif malware.

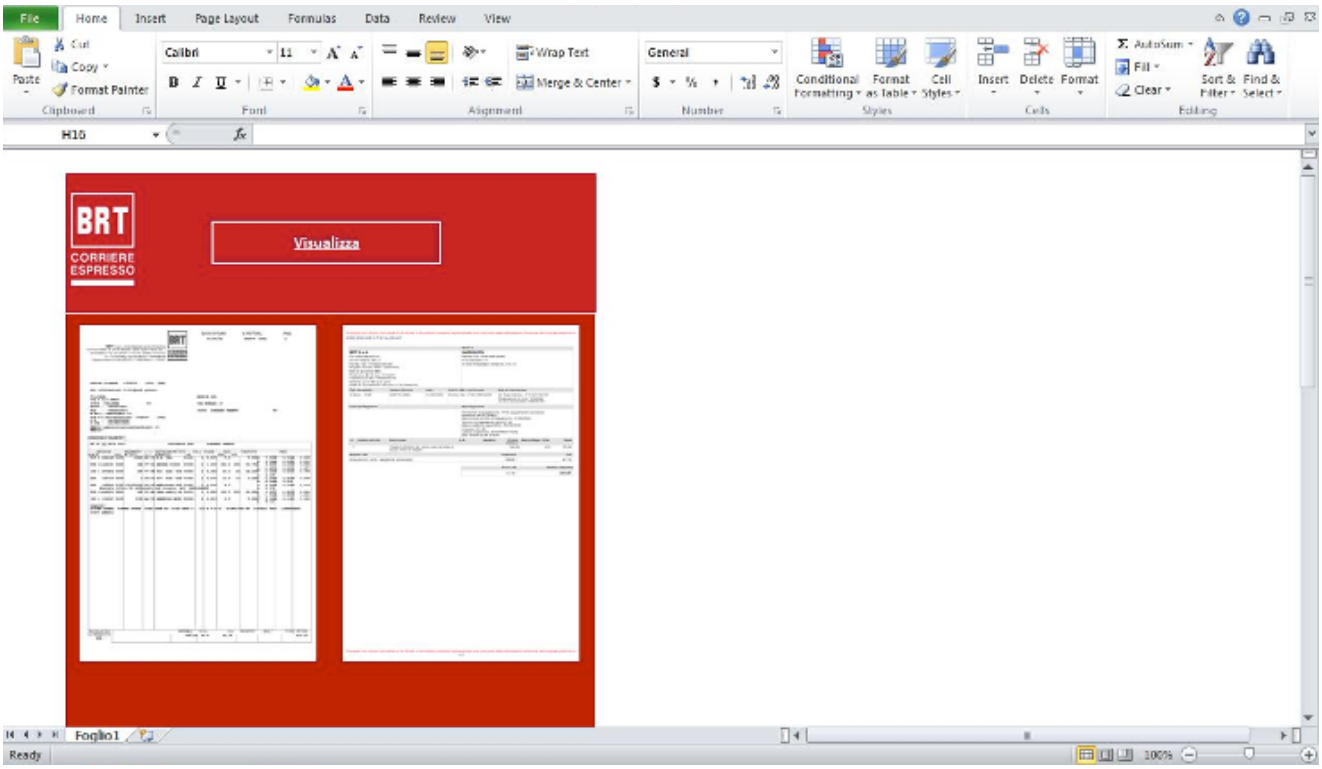

Figure 2: Malicious Excel document distributing Ursnif.

In the observed campaigns, TA544 often uses geofencing techniques to detect whether recipients are in targeted geographic regions before infecting them with the malware. For example, in recent campaigns, the document macro generates and executes an Excel 4 macro written in Italian, and the malware conducts location checks on the server side via IP address. If the user was not in the target area, the malware command and control would redirect to an adult website. So far in 2021, Proofpoint has observed nearly half a million messages associated with this threat targeting Italian organizations.

According to Proofpoint data, Ursnif is currently the most frequently observed malware targeting Italian organizations based on campaign data. Earlier this year, Proofpoint researchers observed multiple Emotet campaigns targeting the region as well – however, following the disruption of the Emotet botnet in January 2021, all Emotet activity has disappeared and this malware is no longer an ongoing threat. Credential phishing is also a frequently observed threat targeting Italian organizations, and threat actors have attempted to steal credentials relating to logistics or banking services, for example.

Web Injects

Recent TA544 Ursnif campaigns included activity that targeted multiple sites with web injects and redirections once the Ursnif payload was installed on the target machine. Web injects refer to malicious code injected to a user's web browser that attempts to steal data from certain targeted websites. The list included dozens of targeted sites. For example, the list of impacted sites includes login portals related to:

- UniCredit Group
- Agenziabpb
- ING
- BNL
- Ebay
- Amazon
- Paypal
- Banca Sella
- CheBanca!
- IBK

The identified web injects are designed to steal credentials from a wide variety of sites and services likely to be used by Italian users. Although Ursnif has previously leveraged web inject capability to infect targeted users. This indicates TA544 is not interested exclusively in obtaining banking credentials, but also usernames and passwords affiliated with websites associated with major retailers.

Conclusion

Today's threats – like TA544's campaigns targeting Italian organizations – target people, not infrastructure. That's why you must take a people-centric approach to cybersecurity. That includes user-level visibility into vulnerability, attacks and privilege and tailored controls that account for individual user risk.

Here's what we recommend as a starting point.

- Train users to spot and report malicious email. Regular training and simulated attacks can stop many attacks and help identify people who are especially vulnerable. The best simulations mimic real-world attack techniques. Look for solutions that tie into real-world attack trends and the latest threat intelligence.
- Threat actors frequently distribute documents that require macros to be enabled to deploy the malicious payload. Ensure macros are disabled for all employees and include macro-laden attack simulations in security training demonstrations.
- At the same time, assume that users will eventually click some threats. Attackers will always find new ways to exploit human nature. Find a solution that spots and blocks inbound email threats targeting employees before they reach the inbox. Invest in a solution can manage the entire spectrum of email threats, not just malware-based threats. Some threats—including business email compromise (BEC) and other forms of email fraud—can be hard to detect with conventional security tools. Your solution should analyze both external and internal email—attackers may use compromised accounts to trick users within the same organization. Web isolation can be a critical safeguard for unknows and risky URLs.

Subscribe to the Proofpoint Blog