Upgraded JasperLoader Infecting Machines with New Targets & Functional Improvements: What You Need to Know

Archived: 2026-04-05 16:35:17 UTC

A few months ago, JasperLoader (a new malware loader) emerged, infecting systems with various malware payloads, such as the Gootkit Banking Trojan. After a short, initial campaign, the threat actors behind the malware halted their activity and JasperLoader went off the radar for a while. However, since late May, a new and upgraded version of JasperLoader has been spotted infecting machines across Europe.

JasperLoader is distributed via malicious email campaigns, while today's main campaign relies on a certified email services in Italy called Posta Elettronica Certificata (PEC). Using a trusted email service helps the threat actors convince victims that their emails are legitimate, tricking them in to opening the malicious email.

The emails in this campaign do not have a malicious VBS or DOCM file attached like the previous campaign, but rather mention that the original message is attached as an EML file. This additional email (shown below) contains a malicious link posing as the "Tribunale di Napoli" – The court of Naples, Italy.

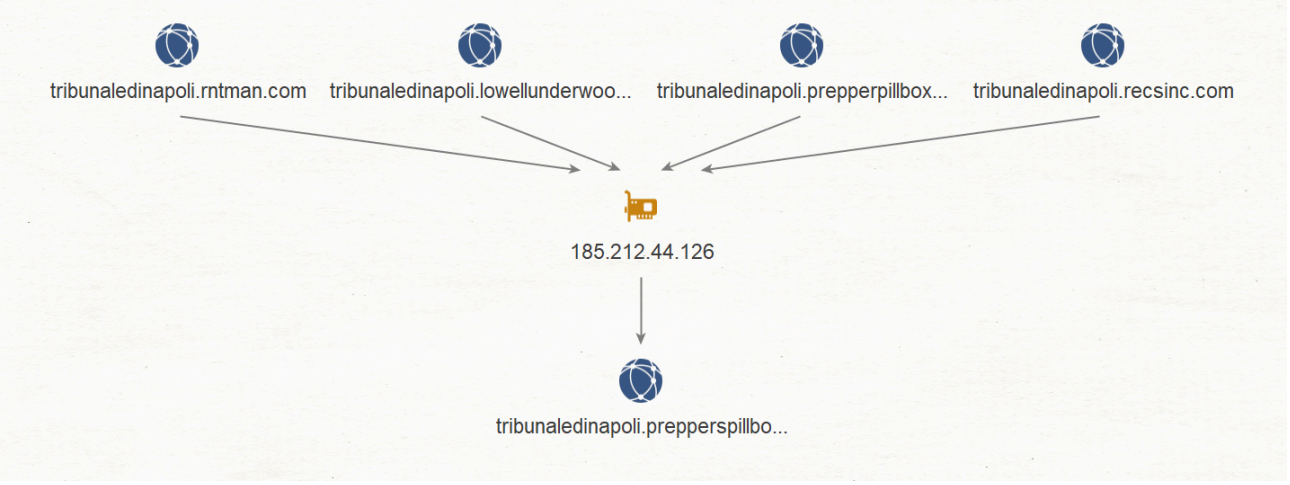
Photo Cred: Talos Blog

If the victim's IP is located in Italy, a ZIP file containing a malicious VBS file is downloaded. Execution of the VBS file starts the infection and JasperLoader installation process.

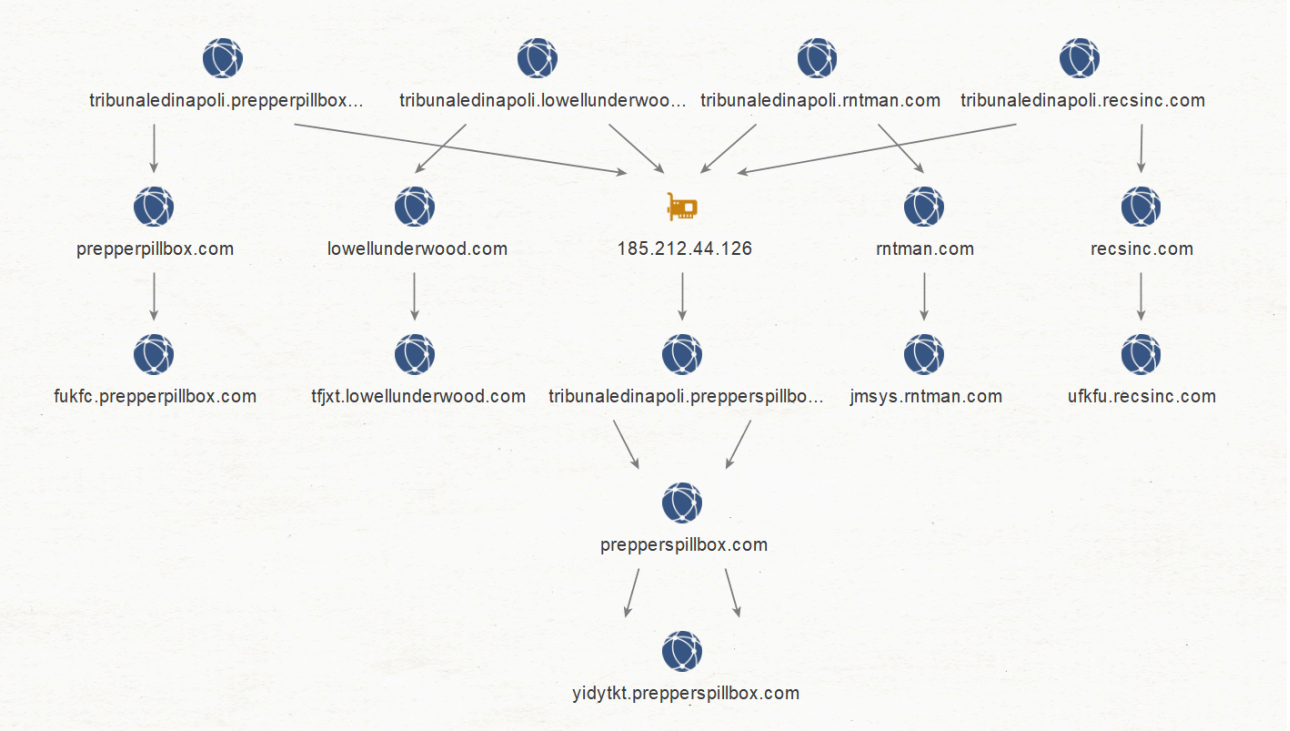
The "Tribune di Napoli" domains used for this infection vector are:

- lowellunderwood.com
- prepperpillbox.com
- recsinc.com
- rntman.com

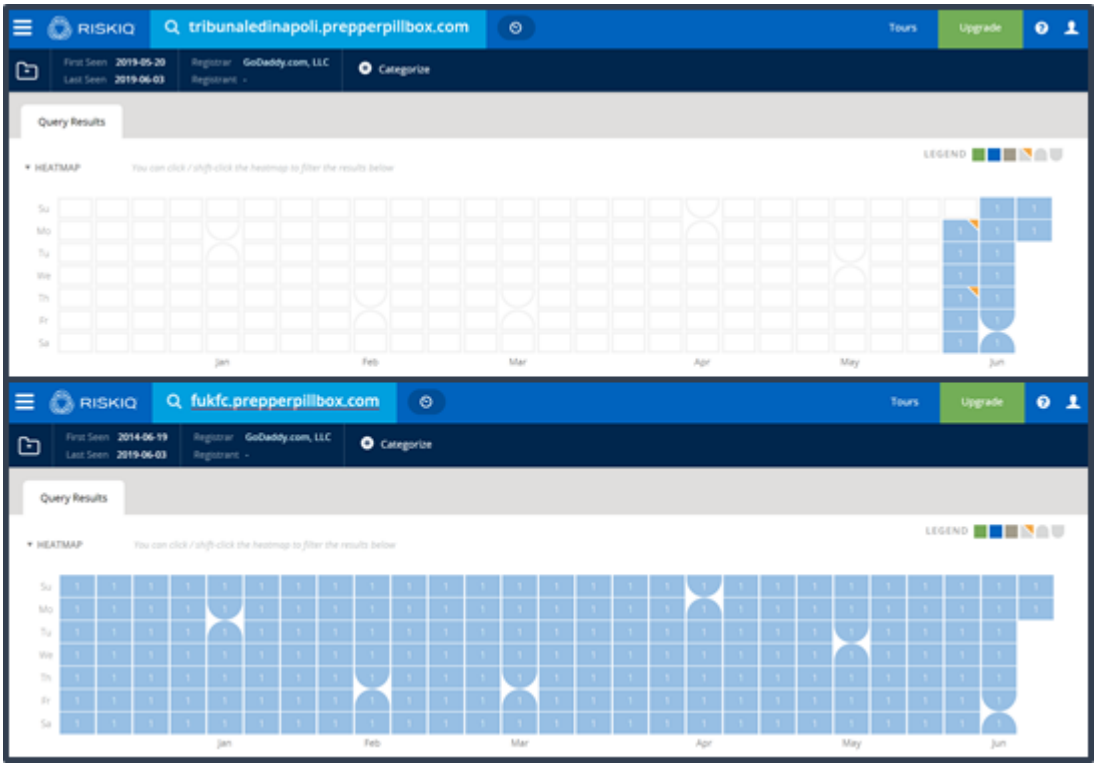
Right at first glance, we can tell that these are not official domains but rather an impersonation attempt. Our security and research team decided to analyze these domains further, and noticed that all four domains are hosted on the same IP, which also hosts the domain tribunaledinapoli[.]prepperspillbox[.]com. This domain has not previously been mentioned in relation to JasperLoader, but is extremely similar to the already-known tribunaledinapoli[.]prepperpillbox[.]com domain.



Another interesting finding is that each of these imposter domains have only one sibling, a gibberish-looking subdomain sharing the same parent domain.



As opposed to the “Tribunale Di Napoli” domains, which have only been active for a few weeks, their siblings have been active for years.



Although these domains have not previously been reported as malicious, it seems quite possible that they are related to the threat actor behind JasperLoader, given the infrastructure symmetry they share with the current campaign.

The new JasperLoader version boasts a variety of upgrades, such as additional layers of obfuscation, VM/Sandbox evasion, a new persistence mechanism, a failback C2 mechanism, and more. It is clear that the threat actors are working quickly at developing the malware's capabilities, making it robust and flexible. We will continue analyzing JasperLoader and updating our coverage of its malicious infrastructure.

If you're interested in learning more about how ThreatSTOP protects you against JasperLoader and other malware loaders, check us out below. Try us out for 14 days free or request a quick demo to see what we're about.

Get a Demo

If you're already a ThreatSTOP user, you're protected against JasperLoader in our TS Originated - Core Threats - IPs and TS Originated - Core Threats - Domains targets.

Source: https://blog.threatstop.com/upgraded-jasperloader-infecting-machines