PROSPERO & Proton66: Uncovering the links between bulletproof networks

By David Sardinha

Published: 2024-11-20 · Archived: 2026-04-05 15:05:23 UTC

Key findings

This report presents:

- The Russian autonomous system ***PROSPERO*** **(AS200593)** could be linked with a high level of confidence to ***Proton66*** **(AS198953)**, another Russian AS, that we believe to be connected to the **bulletproof services** named '**SecureHost**' and '**BEARHOST**'. We notably observed that both network's configurations are almost identical in terms of peering agreements and their respective share of loads throughout time.
- Amongst the activities shared by the two networks, we noticed that both **GootLoader** and **SpyNote** malwares recently changed their infrastructure of **command-and-control servers** and **phishing pages** from to *Proton66*. Additionally, the domains hosting the phishing pages deploying SpyNote were hosted on either one of the two AS and had already been used in previous campaigns delivering **revoked AnyDesk** and **LiveChat versions** for both **Windows** and **Mac**.
- Regarding the other malicious activities found on *PROSPERO*'s IPs, we found that throughout September, multiple **SMS spam campaigns** targeting citizens from various countries were leading to phishing domains hosted on *PROSPERO* and *Proton66*. While most phishing templates were **usurping bank login pages** to steal credit card details, we also noticed that some of them were used to deploy **android spywares** such as **Coper** (a.k.a. **Octo**).
- **SocGholish**, another **initial access broker (IAB)** that we found to be hosting a major part of its infrastructure on *Proton66*, continues to leverage this autonomous system to host **fingerprinting scripts** contained on the websites it infects. Along SocGholish, we found out that **FakeBat**, another loader that infects systems through compromised websites, was using the **same IPs** to host both screening and redirection scripts.

Introduction

In the continuity of our constant monitoring of bulletproof networks, we discovered **an autonomous system named *PROSPERO OOO* (AS200593)** based in **Russia**. We believe that it could be linked to ***Proton66 OOO* (AS198953)**, another Russian and anonymous autonomous system that we previously found to be connected to a bigger infrastructure composed of multiple AS and offshore companies all operated by a common Russian national. This individual notably promotes its bulletproof hosting businesses named '**UNDERGROUND**' and '**BEARHOST**' on various Russian-speaking underground marketplaces stating that the service is "*100% bulletproof […] we completely ignore all abuses and complaints, including Spamhaus*". He notably used to work

with another bulletproof provider named '**SecureHost**', advertised on the same underground platforms that we believe with a high level of confidence to be the present operator of both *PROSPERO OOO* and *Proton66 OOO*.

Bulletproof hosting

A bulletproof hosting service is a type of web hosting service known for offering **high levels of privacy**, security, and **leniency** regarding the content and activities allowed on their servers. These services typically provide robust protection against **takedown requests**, **legal actions**, and **law enforcement investigations**, often by locating their servers in jurisdictions with **minimal regulations** or weak enforcement of international laws. Bulletproof hosting is often associated with **hosting illicit content** or activities, such as **malware distribution**, **spam operations**, or **copyright-infringing materials**, due to its permissive stance and commitment to client confidentiality. However, it's important to note that not all uses of such services are illegal, as some users may seek such hosting for **legitimate privacy concerns**.

The connection between *PROSPERO* and *Proton66* could be made through similarities in the way both networks are operated, notably in their respective peering agreements shared with other Russian networks. Additionally, we noticed that botnets operated by **GootLoader**, an initial access broker, and **SpyNote**, an android RAT, had moved their infrastructure from *PROSPERO* to *Proton66*, or would sometimes host their command-and-control servers on both AS. Along those finds, this report aims to provide an overview of all the malicious activities that are hosted on *PROSPERO OOO*.

Legal format of Russian companies

As a reminder, the Russian format "**OOO**" stands for "**Obschestvo s Ogranichennoy Otvetstvennostyu**" which corresponds to the Anglo-Saxon format "**LLC**" or "**limited liability company**".

Intrinsec's CTI services

Organisations are facing a rise in the sophistication of threat actors and intrusion sets. To address these evolving threats, it is now necessary to take a proactive approach in the detection and analysis of any element deemed malicious. Such a hands-on approach allows companies to anticipate, or at least react as quickly as possible to the compromises they face.

For this report, shared with our clients in July 2023, Intrinsec relied on its Cyber Threat Intelligence service, which provides its customers with high value-added, contextualized and actionable intelligence to understand and contain cyber threats. Our CTI team consolidates data & information gathered from our security monitoring services (SOC, MDR …), our incident response team (CERT-Intrinsec) and custom cyber intelligence generated by our analysts using custom heuristics, honeypots, hunting, reverse-engineering & pivots.

Intrinsec also offers various services around Cyber Threat Intelligence:

- Risk anticipation: which can be leveraged to continuously adapt the detection & response capabilities of our clients' existing tools (EDR, XDR, SIEM, …) through:
    - **an operational feed of IOCs based on our exclusive activities.**
    - **threat intel notes & reports, TIP-compliant.**
- Digital risk monitoring:

- **data leak detection & remediation**
- **external asset security monitoring (EASM)**
- **brand protection**

For more information, go to our CTI's website

Follow us on Linkedin and X]
