Notorious Malware, Spam Host “Prospero” Moves to Kaspersky Lab

krebsonsecurity.com/2025/02/notorious-malware-spam-host-prospero-moves-to-kaspersky-lab/

One of the most notorious providers of abuse-friendly “bulletproof” web hosting for cybercriminals has started routing its operations through networks run by the Russian antivirus and security firm **Kaspersky Lab**, KrebsOnSecurity has learned.

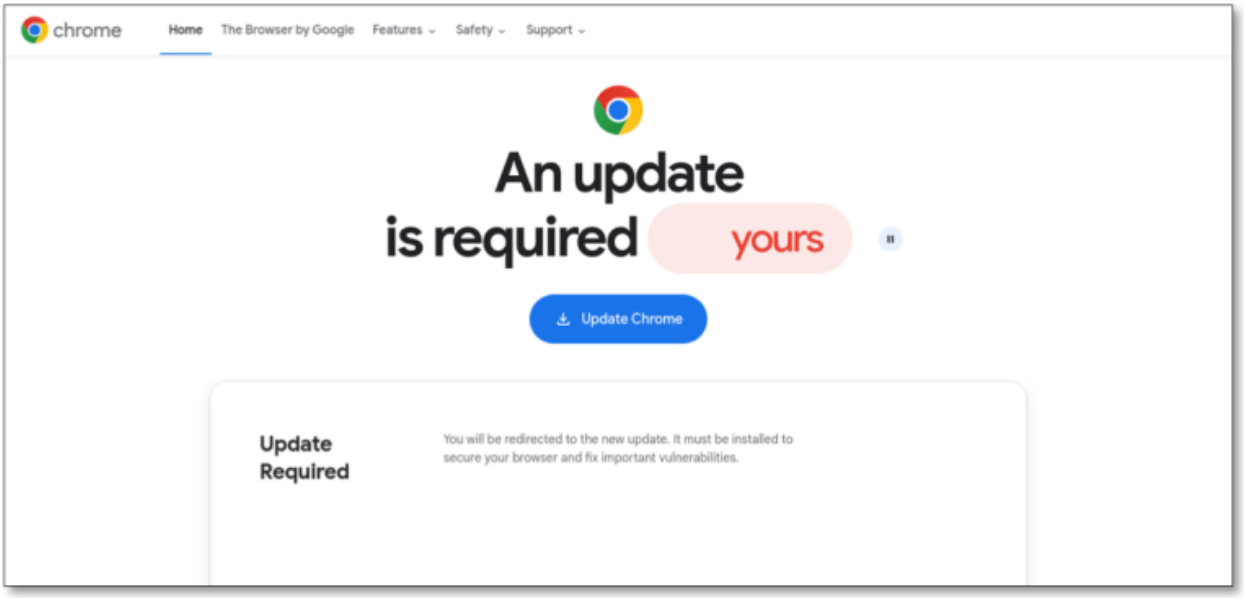
Security experts say the Russia-based service provider **Prospero OOO** (the triple O is the Russian version of “LLC”) has long been a persistent source of malicious software, botnet controllers, and a torrent of phishing websites. Last year, the French security firm **Intrinsec** detailed Prospero’s connections to bulletproof services advertised on Russian cybercrime forums under the names **Securehost** and **BEARHOST**.

The bulletproof hosting provider BEARHOST. This screenshot has been machine-translated from Russian. Image: Ke-la.com.

Bulletproof hosts are so named when they earn or cultivate a reputation for ignoring legal demands and abuse complaints. And BEARHOST has been cultivating its reputation since at least 2019.

“If you need a server for a botnet, for malware, brute, scan, phishing, fakes and any other tasks, please contact us,” BEARHOST’s ad on one forum advises. “We completely ignore all abuses without exception, including SPAMHAUS and other organizations.”

Intrinsec found Prospero has courted some of Russia’s nastiest cybercrime groups, hosting control servers for multiple ransomware gangs over the past two years. Intrinsec said its analysis showed Prospero frequently hosts malware operations such as SocGholish and GootLoader, which are spread primarily via fake browser updates on hacked websites and often lay the groundwork for more serious cyber intrusions — including ransomware.



A fake browser update page pushing mobile malware. Image: Intrinsec.

BEARHOST prides itself on the ability to evade blocking by Spamhaus, an organization that many Internet service providers around the world rely on to help identify and block sources of malware and spam. Earlier this week, Spamhaus said it noticed that Prospero was suddenly connecting to the Internet by routing through networks operated by Kaspersky Lab in Moscow.

Update, March 1, 9:43 a.m. ET: In a written statement, Kaspersky said it is aware of the public claim about the company allegedly providing services to a “bulletproof” web hosting provider. Here is their full statement:

> "Kaspersky denies these claims as the company does not work and has never worked with the service provider in question. The routing through networks operated by Kaspersky doesn't by default mean provision of the company's services, as Kaspersky's automatic system (AS) path might appear as a technical prefix in the network of telecom providers the company works with and provides its DDoS services."
>
> "Kaspersky pays great attention to conducting business ethically and ensuring that its solutions are used for their original purpose of providing cybersecurity protection. The company is currently investigating the situation to inform the company whose network could have served as a transit for a "bulletproof" web hosting provider so that the former takes the necessary measures."

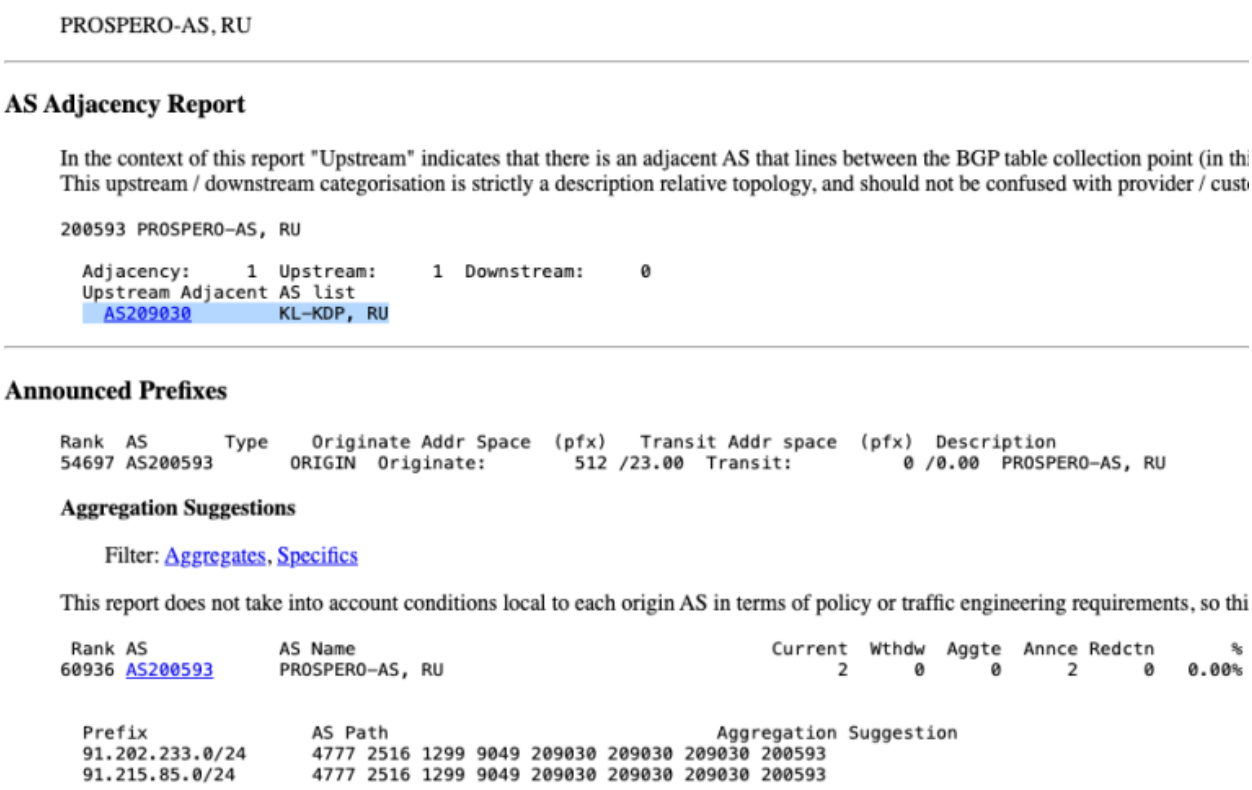
Kaspersky began selling antivirus and security software in the United States in 2005, and the company's malware researchers have earned accolades from the security community for many important discoveries over the years. But in September 2017, the Department of Homeland Security (DHS) barred U.S. federal agencies from using Kaspersky software, mandating its removal within 90 days.

Cybersecurity reporter **Kim Zetter** notes that DHS didn't cite any specific justification for its ban in 2017, but media reports quoting anonymous government officials referenced two incidents. Zetter wrote:

> According to one story, an NSA contractor developing offensive hacking tools for the spy agency had Kaspersky software installed on his home computer where he was developing the tools, and the software detected the source code as malicious code and extracted it from his computer, as antivirus software is designed to do. A second story claimed that Israeli spies caught Russian government hackers using Kaspersky software to search customer systems for files containing U.S. secrets.
>
> Kaspersky denied that anyone used its software to search for secret information on customer machines and said that the tools on the NSA worker's machine were detected in the same way that all antivirus software detects files it deems suspicious and then quarantines or extracts them for analysis. Once Kaspersky discovered that the code its antivirus software detected on the NSA worker's machine were not malicious programs but source code in development by the U.S. government for its hacking operations, CEO Eugene Kaspersky says he ordered workers to delete the code.

Last year, the U.S. Commerce Department banned the sale of Kaspersky software in the U.S. effective July 20, 2024. U.S. officials argued the ban was needed because Russian law requires domestic companies to cooperate in all official investigations, and thus the Russian government could force Kaspersky to secretly gather intelligence on its behalf.

Phishing data gathered last year by the **Interisle Consulting Group** ranked hosting networks by their size and concentration of spambot hosts, and found Prospero had a higher spam score than any other provider by far.



PROSPERO-AS, RU

AS Adjacency Report

In the context of this report "Upstream" indicates that there is an adjacent AS that lines between the BGP table collection point (in thi
This upstream / downstream categorisation is strictly a description relative topology, and should not be confused with provider / custo

```
200593 PROSPERO-AS, RU

  Adjacency:     1  Upstream:     1  Downstream:     0
  Upstream Adjacent AS list
    AS209030        KL-KDP, RU
```

Announced Prefixes

```
Rank  AS       Type    Originate Addr Space  (pfx)   Transit Addr space  (pfx)  Description
54697 AS200593       ORIGIN  Originate:        512 /23.00  Transit:          0 /0.00  PROSPERO-AS, RU
```

Aggregation Suggestions

Filter: Aggregates, Specifics

This report does not take into account conditions local to each origin AS in terms of policy or traffic engineering requirements, so thi

```
 Rank AS            AS Name                                    Current  Wthdw  Aggte  Annce Redctn       %
60936 AS200593      PROSPERO-AS, RU                                  2      0      0      2      0   0.00%

  Prefix              AS Path                              Aggregation Suggestion
  91.202.233.0/24     4777 2516 1299 9049 209030 209030 209030 200593
  91.215.85.0/24      4777 2516 1299 9049 209030 209030 209030 200593
```

AS209030, owned by Kaspersky Lab, is providing connectivity to the bulletproof host Prospero (AS200593). Image: cidr-report.org.

It remains unclear why Kaspersky is providing transit to Prospero. **Doug Madory**, director of Internet analysis at **Kentik**, said routing records show the relationship between Prospero and Kaspersky started at the beginning of December 2024.

Madory said Kaspersky's network appears to be hosting several financial institutions, including Russia's largest — **Alfa-Bank**. Kaspersky sells services to help protect customers from distributed denial-of-service (DDoS) attacks, and Madory said it could be that Prospero is simply purchasing that protection from Kaspersky.

But if that is the case, it doesn't make the situation any better, said **Zach Edwards**, a senior threat researcher at the security firm **Silent Push**.

"In some ways, providing DDoS protection to a well-known bulletproof hosting provider may be even worse than just allowing them to connect to the rest of the Internet over your infrastructure," Edwards said.