

Project 3

Artifacts Manual

From : Sainsburys Department<azmireengineeringworks@gmail.com>

Recipient : ixxxx@xxxxxxxxx.com

Reply-to :

Date and Time: 10 July 2023 at 19:09 (Delivered after 163 seconds)

Subject Line : Confirmation-I1055*RIk5I

Sending IP: 209.85.220.41

rDNS Host: None

Suspected Link URL : vedomosti-ru-ru.blogspot.com

Attachment: None

Email Description

The email content is presented in the form of a Sainsbury leaflet promoting a lottery campaign offering a chance to win a free Ninja air fryer. Towards the end, the sender includes that if I no longer wish to receive emails, I can click on a hidden link labeled "here." The text in some areas of the email appears blurry and difficult to read.

URL Analysis

WHOIS : Scanning "vedomosti-ru-ru.blogspot.com" has shown an IP address 142.251.33.105 is hosting **28 other websites on the same server**. The server is located in Dallas, Texas, United States, and is owned by Google. The domain status is listed as "**Registered And No Website**". The domain has been hosted by 4 different registrars and has had hosting changes on 2 unique name servers over a period of 19 years. Based on this information, there is no indication of any suspicious activity.

URLSCAN.IO: —> [http://vedomosti-ru-ru.blogspot\[.\]com](http://vedomosti-ru-ru.blogspot[.]com)

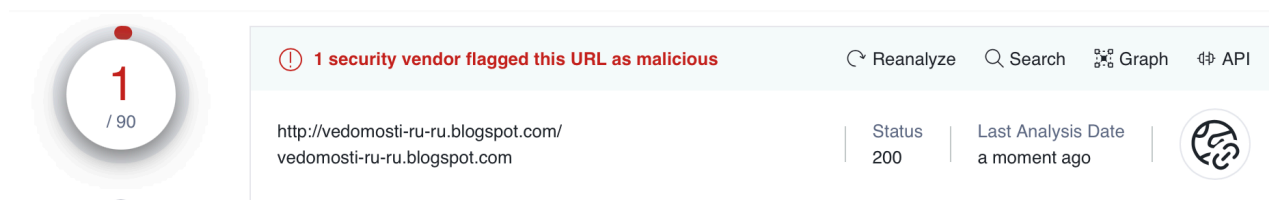
The website in question has contacted 4 different IPs located in 2 countries and interacted with 4 domains, carrying out a total of 7 HTTP transactions. The main IP address, 185.66.88.174, is located in Ukraine and belongs to the YURTEH-AS network. The IP has been scanned 2 times on urlscan.io, with no specific classification provided on Google Safe Browsing. Based on the information provided, there is no indication of suspicious activity associated with the website or the IP address.

URL2PNG : —> [http://vedomosti-ru-ru.blogspot\[.\]com](http://vedomosti-ru-ru.blogspot[.]com)

The domain status is listed as **Registered And No Website**

VirusTotal :

VirusTotal has provided notable findings indicating that 1 security vendors have classified this URL as phishing.

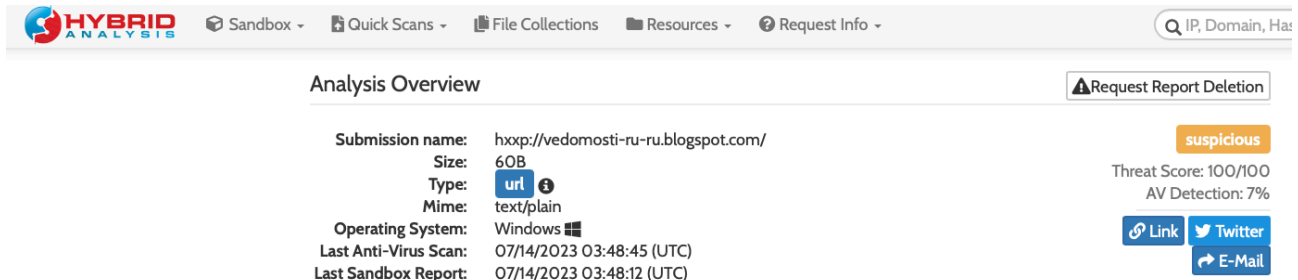


The image shows the VirusTotal analysis interface for the URL <http://vedomosti-ru-ru.blogspot.com/>. On the left, a circular progress indicator shows '1 / 90' with a red dot above the number 1. The main panel has a light blue header with a warning icon and the text '1 security vendor flagged this URL as malicious'. To the right of this header are links for 'Reanalyze', 'Search', 'Graph', and 'API'. Below the header, the URL is listed twice. To the right of the URL, there are two columns: 'Status' with the value '200' and 'Last Analysis Date' with the value 'a moment ago'. On the far right is a circular icon with a network diagram.

Status	Last Analysis Date
200	a moment ago

HYBRID ANALYSIS

HYBRID ANALYSIS has classified “**Suspicious**” with Threat Score of 100/100 and AV Detection of 7%.



The screenshot shows the Hybrid Analysis web interface. At the top, there's a navigation bar with the Hybrid Analysis logo and several menu items: Sandbox, Quick Scans, File Collections, Resources, and Request Info. A search bar is on the right. Below the navigation bar, the 'Analysis Overview' section is displayed. It contains a table of submission details: Submission name (hxxp://vedomosti-ru-ru.blogspot.com/), Size (60B), Type (url), Mime (text/plain), Operating System (Windows), Last Anti-Virus Scan (07/14/2023 03:48:45 (UTC)), and Last Sandbox Report (07/14/2023 03:48:12 (UTC)). To the right of the table, there's a status box labeled 'suspicious' with a threat score of 100/100 and AV detection of 7%. Below this, there are buttons for Link, Twitter, and E-Mail, and a 'Request Report Deletion' button.

Submission name:	hxxp://vedomosti-ru-ru.blogspot.com/
Size:	60B
Type:	url
Mime:	text/plain
Operating System:	Windows
Last Anti-Virus Scan:	07/14/2023 03:48:45 (UTC)
Last Sandbox Report:	07/14/2023 03:48:12 (UTC)

suspicious
Threat Score: 100/100
AV Detection: 7%

[Link](#) [Twitter](#) [E-Mail](#) [Request Report Deletion](#)

Defensive Measures

[1] The sender intentionally misrepresented “Sainsbury Department” but the sending IP revealed it was actually a Gmail address. [2] Therefore, blocking the sending server would have a negative impact on the business as legitimate emails would be blocked.

[ActionTaken] - Blocking the sender email “azmireengineeringworks@gmail.com” only would stop more malicious emails being delivered to me by Idriss JAMA on the 14 July 2023.

[3] The URL used within the credential harvester is a malicious domain “[http://vedomosti-ru-ru.blogspot\[.\]com](http://vedomosti-ru-ru.blogspot[.]com)” hidden within the leaflet to look more effective when glancing at the link. [8] After investigating the domain, it was created purely for malicious purposes, and there is no business justification for me to visit it, and we can block the entire domain to prevent users (Family) from visiting.

[ActionTaken] - The malicious URL “[http://vedomosti-ru-ru.blogspot\[.\]com](http://vedomosti-ru-ru.blogspot[.]com)” is blocked to prevent future attempts. It was blocked by Idriss JAMA on the 14 July 2023.

The investigating analyst

- The sending email is not a legitimate and has successfully impersonated “Sainsbury”.
- The defensive measure was to block the sender email address rather than the entire the Gmail server and doing so would have a negative impact on the business as legitimate emails would be blocked.
-
- The URL was purely operating in a malicious intent and there is no legitimate reason for me and family to visit the domain.
- Therefore, it was also blocked to prevent future attempts. It was blocked by Idriss Jama on Friday the 14 July 2023.