Wordfence®

Ukraine Universities Hacked As Russian Invasion Started

Note: This article has been updated to reflect that the hosting provider "Njalla", which routed the malicious traffic involved in this attack, is based in Sweden, not in Finland, although IP geolocation data indicates that the specific server that the traffic transited may be based in Finland. We have also updated the post title to reflect this change.

The Wordfence team has identified a massive attack on Ukrainian universities that coincided with the invasion of Ukraine by Russia, and resulted in at least 30 compromised Ukrainian university websites. We have identified the threat actor behind the attack, who is part of a group called the Monday group, which the members refer to as "theMx0nday". The group has stated publicly that they support Russia in this conflict.

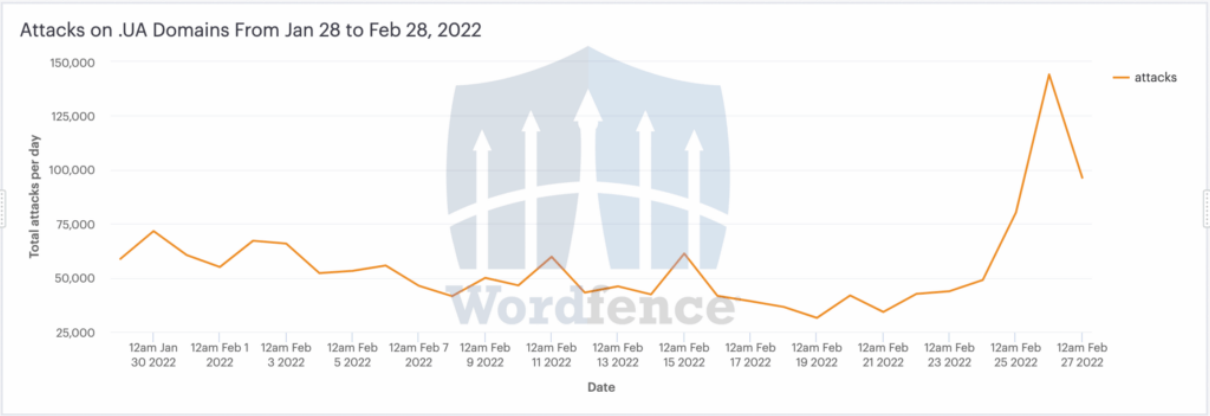
The threat actor is based in Brazil. The majority of attacks transited an internet service provider called Njalla who claim they are *"Considered the worlds most notorious 'Privacy as a Service' provider for domains, VPSs and VPNs"*. Njalla is a Swedish-based hosting provider and is run by Peter Sunde, who is the co-founder of Pirate Bay. The specific Njalla server that the traffic was routed through appears to be based in Finland, based on IP geolocation data, although Njalla claims their servers are based "In secret locations in Sweden".

Wordfence protects over 8,000 websites in Ukraine. In addition to the more than 300 universities we protect in Ukraine, we also protect private, government, military, and police websites. This gives us insight into attacks targeting Ukraine. In this post, we explain how we arrived at the conclusions above, and we provide supporting data, explanations, and visuals.

We are also taking the step of activating our real-time threat intelligence on all sites on the Ukrainian .UA top-level domain (TLD) until further notice. This is normally only available to our paid customers. The vast majority of sites using Wordfence use the free open source version. These sites will benefit from this change by receiving a commercial-grade IP blocklist, real-time firewall rules, and real-time malware detection. Ukrainian site operators do not need to take any action to receive this live threat feed. We deployed the change minutes ago and over 8,000 sites with a .UA extension will update over the next 24 hours with the newest threat intelligence. You can find more details about this change at the end of this article.

Overall Attack Patterns As The Kinetic Russian Invasion Started on 24 February

The Russian invasion of Ukraine started on February 24th. The chart below shows the overall number of exploit attempts on websites that we protect, with the .UA Ukrainian TLD before and after the invasion. This data set includes 8,320 .UA websites. We will use the term "attack" in this blog post to indicate a sophisticated exploit attempt. This does not include simple brute force attacks (login guessing attempts) or distributed denial of service traffic. It only includes attempts to exploit a vulnerability on a target WordPress website, which are the sites that Wordfence protects.



The peak above is just over 144,000 attacks on February 25th, one day after the kinetic attack started. The peak is roughly three times the number of daily attacks from earlier in the month across the Ukrainian websites that we protect.

Examining The Spike In Attacks Targeting Ukraine

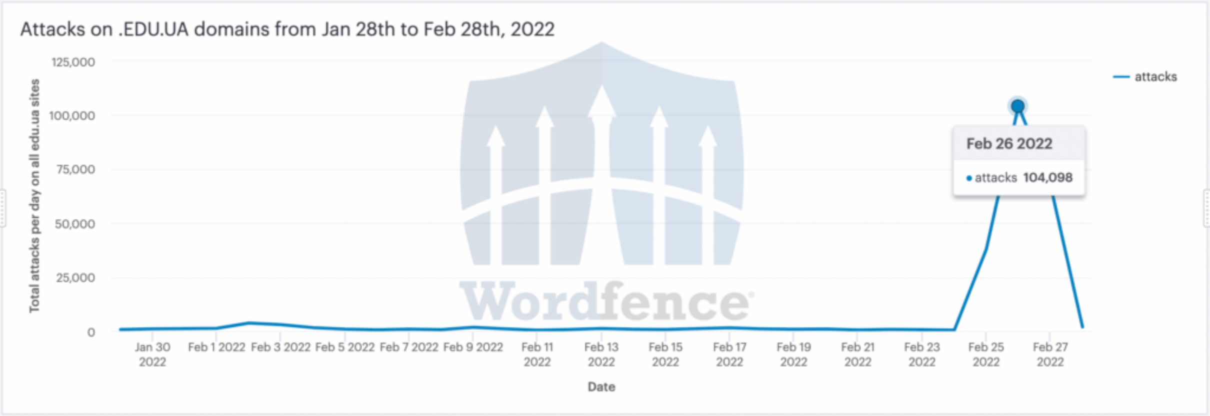
Wordfence protects a broad range of websites in Ukraine, including commercial, local and national government, military, police, academic and private websites. This allows us to sample attack data across a broad range of sectors. We compiled a list of websites that had received at least double the number of attacks from the day before the invasion started, until Monday, February 28th, which is a window of about 5.5 days, compared to the entire 27 days before the attack started. That's about a 10X increase in the average daily number of attacks.

Out of the 8,320 UA websites that we protect, we found a list of 383 websites where attacks had increased dramatically following the invasion. Out of those 383 websites, 229 were sites ending in "EDU.UA". In other words, academic websites and universities in Ukraine.

An attacker was making a concerted effort to attack universities in Ukraine, and they started immediately after the Russian invasion started.

How Big Was The Attack Targeting Ukrainian Universities?

We protect a total of 376 .EDU.UA websites in Ukraine. The chart below shows attack activity across all those sites until Feb 28th. This only shows sophisticated exploit attempts.

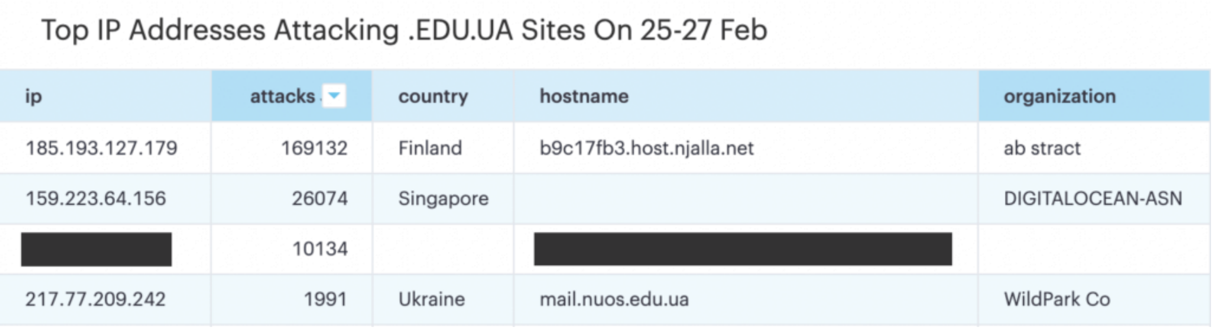


Most of the month showed a few hundred attacks per day across all .EDU.UA sites that we protect. Starting February 25th, we saw a spike that peaked at over 104,000 attacks in a single day targeting these academic websites.

To put this in perspective we saw:

- **479** attacks on Feb 24th
- **37,974** attacks on Feb 25th
- **104,098** attacks on Feb 26th
- **67,552** attacks on Feb 27th

Which IP Addresses Launched This Attack?



Top IP Addresses Attacking .EDU.UA Sites On 25-27 Feb

ip	attacks	country	hostname	organization
185.193.127.179	169132	Finland	b9c17fb3.host.njalla.net	ab stract
159.223.64.156	26074	Singapore		DIGITALOCEAN-ASN
[redacted]	10134		[redacted]	
217.77.209.242	1991	Ukraine	mail.nuos.edu.ua	WildPark Co

The top attacking IP addresses targeting EDU.UA sites during our two-day window as the invasion of Ukraine started are:

- **185.193.127.179 with 169,132 attacks**
- 159.223.64.156 with 26,074 attacks
- x.x.x.x with 10,134 attacks [Redacted for a technical reason]
- 217.77.209.242 with 1991 attacks

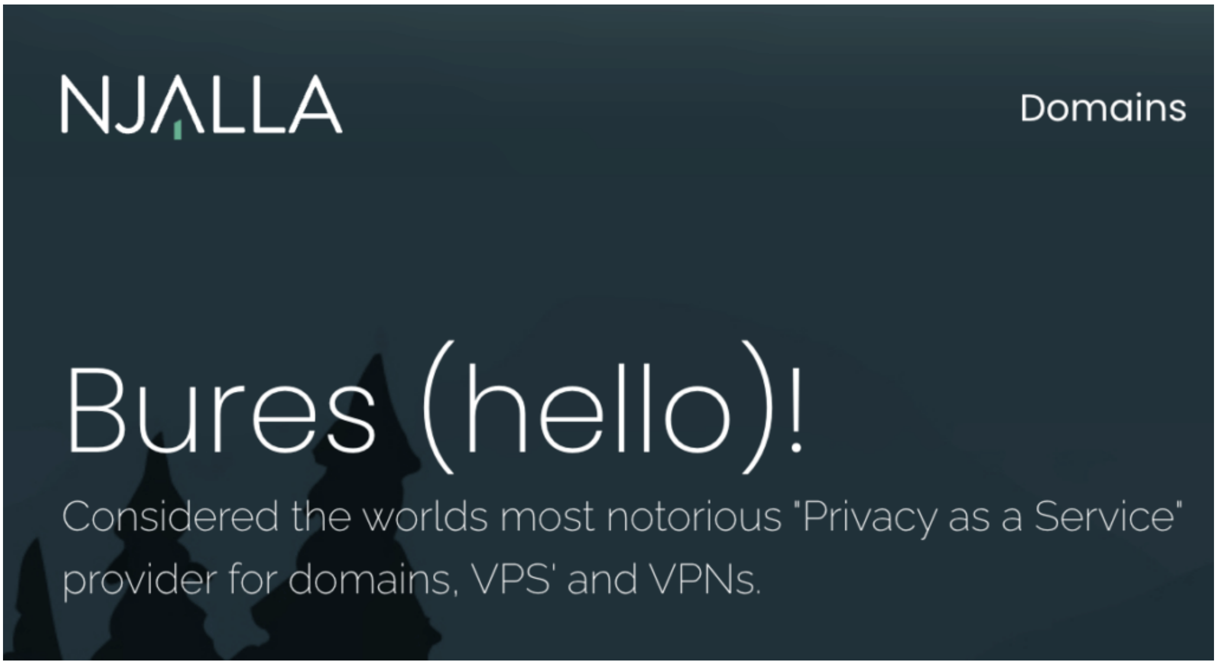
Note: The last server in the list is a .EDU.UA server, and appears to be a compromised machine targeting other EDU.UA sites.

We logged over 7,000 IP addresses during this period, but every single one, other than the four above, logged less than 100 attacks each. The four IP addresses above were by far the biggest offenders. And 185.193.127.179 logged over 6 times the number of attacks versus the second-highest offender.

Who Is Behind 185.193.127.179?

Njalla is the hosting provider for 185.193.127.179 and is run by Peter Sunde, who is the co-founder of Pirate Bay. Njalla say openly on their home page that they are

> **"Considered the worlds most notorious "Privacy as a Service" provider for domains, VPS' and VPNs."**



Bures (hello)!

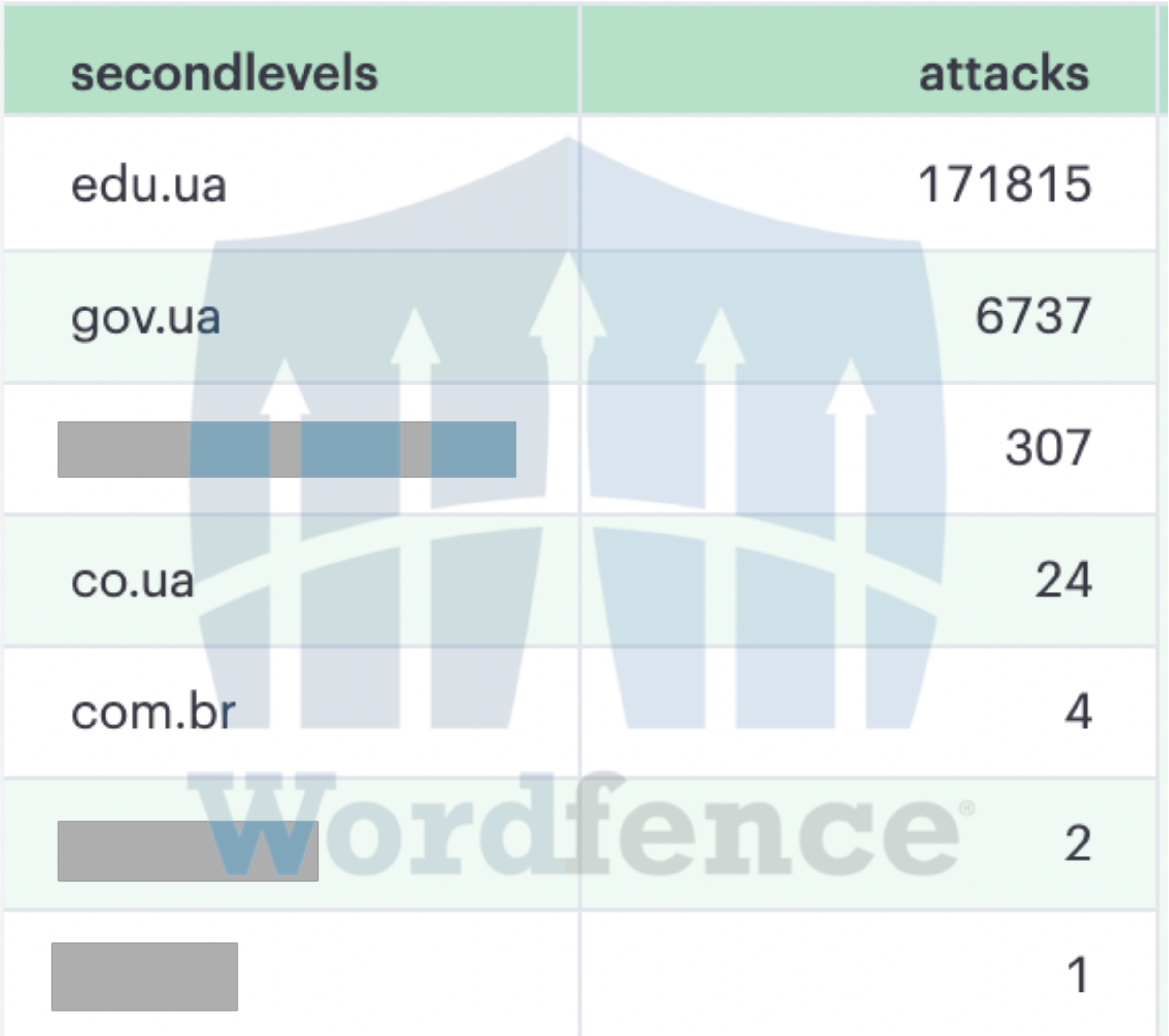
Considered the worlds most notorious "Privacy as a Service" provider for domains, VPS' and VPNs.

Peter Sund says on his blog that he is “worried of the centralisation of power to the EU”. According to his Wikipedia entry, Mr Sunde was arrested in 2014 on charges related to The Pirate Bay case and served two-thirds of his 8-month sentence.

Njalla is a service provider for VPNs, which makes it possible that the attack may have come from one of their customers, a hacked server belonging to one of their customers, or from a VPN exit node. We suspect their VPN was used as an exit node to mask a threat actor, which we describe below.

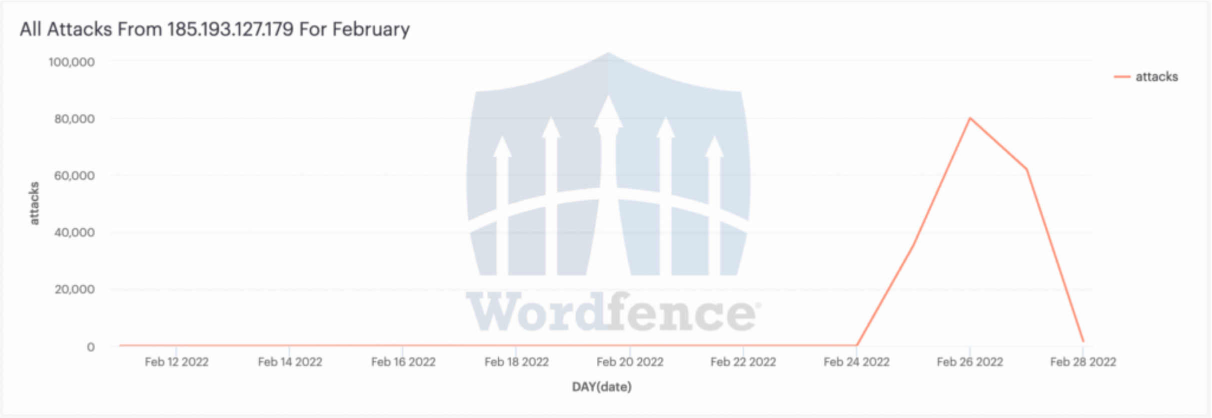
The vast majority of attacks from 185.193.127.179 were targeted at educational institutions in Ukraine, with over **171,000 attacks targeting EDU.UA sites**. They went after a few government sites and three individual websites (redacted).

They launched 24 attacks against companies in Ukraine and four attacks against companies in Brazil. The Brazil connection will become clear below.



secondlevels	attacks
edu.ua	171815
gov.ua	6737
[redacted]	307
co.ua	24
com.br	4
[redacted]	2
[redacted]	1

This IP was not attacking before the invasion of Ukraine by Russia. Then ramped up for three days during the invasion, specifically targeting universities in Ukraine. Then dropped back down to zero.

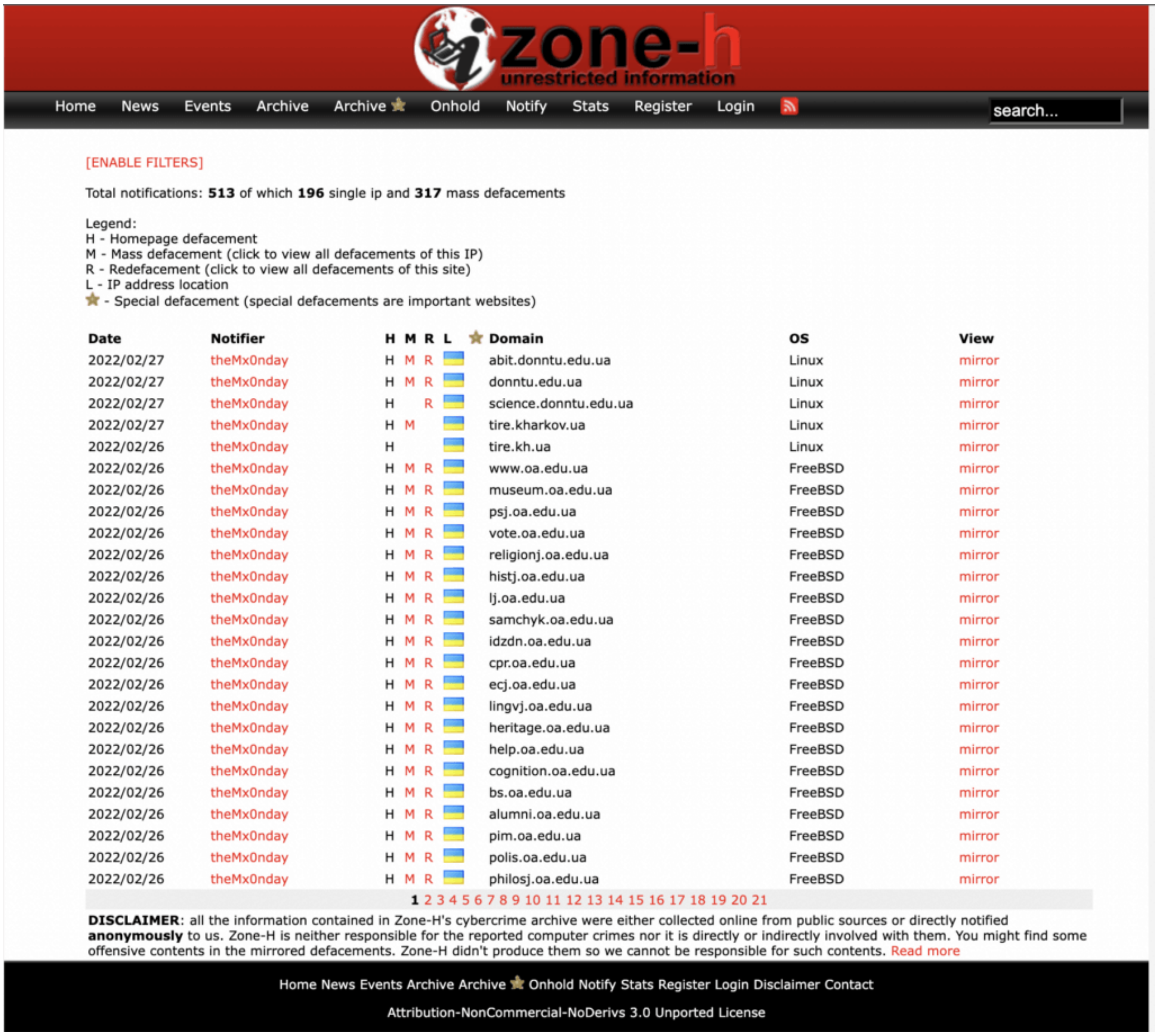


All Attacks From 185.193.127.179 For February

The Attacks Are Compromising Universities

In our analysis of malware payloads attempting to target EDU websites, we saw information that provided us with the name of the group targeting these sites.

The group goes by **"theMx0nday"** and in this post, we will refer to them as the "Monday" group. The website Zone-H.org provides an archive of defaced websites. Once we had the threat actors handle, we could search ZoneH for sites that were related and had been hacked. We found this:



[ENABLE FILTERS]

Total notifications: **513** of which **196** single ip and **317** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★	Domain	OS	View
2022/02/27	theMx0nday	H	M	R	🇺🇦		abit.donntu.edu.ua	Linux	mirror
2022/02/27	theMx0nday	H	M	R	🇺🇦		donntu.edu.ua	Linux	mirror
2022/02/27	theMx0nday	H		R	🇺🇦		science.donntu.edu.ua	Linux	mirror
2022/02/27	theMx0nday	H	M		🇺🇦		tire.kharkov.ua	Linux	mirror
2022/02/26	theMx0nday	H			🇺🇦		tire.kh.ua	Linux	mirror
2022/02/26	theMx0nday	H	M	R	🇺🇦		www.oa.edu.ua	FreeBSD	mirror
2022/02/26	theMx0nday	H	M	R	🇺🇦		museum.oa.edu.ua	FreeBSD	mirror
2022/02/26	theMx0nday	H	M	R	🇺🇦		psj.oa.edu.ua	FreeBSD	mirror
2022/02/26	theMx0nday	H	M	R	🇺🇦		vote.oa.edu.ua	FreeBSD	mirror
2022/02/26	theMx0nday	H	M	R	🇺🇦		religionj.oa.edu.ua	FreeBSD	mirror
2022/02/26	theMx0nday	H	M	R	🇺🇦		histj.oa.edu.ua	FreeBSD	mirror
2022/02/26	theMx0nday	H	M	R	🇺🇦		lj.oa.edu.ua	FreeBSD	mirror
2022/02/26	theMx0nday	H	M	R	🇺🇦		samchyk.oa.edu.ua	FreeBSD	mirror
2022/02/26	theMx0nday	H	M	R	🇺🇦		idzdn.oa.edu.ua	FreeBSD	mirror
2022/02/26	theMx0nday	H	M	R	🇺🇦		cpr.oa.edu.ua	FreeBSD	mirror
2022/02/26	theMx0nday	H	M	R	🇺🇦		ecj.oa.edu.ua	FreeBSD	mirror
2022/02/26	theMx0nday	H	M	R	🇺🇦		lingvj.oa.edu.ua	FreeBSD	mirror
2022/02/26	theMx0nday	H	M	R	🇺🇦		heritage.oa.edu.ua	FreeBSD	mirror
2022/02/26	theMx0nday	H	M	R	🇺🇦		help.oa.edu.ua	FreeBSD	mirror
2022/02/26	theMx0nday	H	M	R	🇺🇦		cognition.oa.edu.ua	FreeBSD	mirror
2022/02/26	theMx0nday	H	M	R	🇺🇦		bs.oa.edu.ua	FreeBSD	mirror
2022/02/26	theMx0nday	H	M	R	🇺🇦		alumni.oa.edu.ua	FreeBSD	mirror
2022/02/26	theMx0nday	H	M	R	🇺🇦		pim.oa.edu.ua	FreeBSD	mirror
2022/02/26	theMx0nday	H	M	R	🇺🇦		polis.oa.edu.ua	FreeBSD	mirror
2022/02/26	theMx0nday	H	M	R	🇺🇦		philosj.oa.edu.ua	FreeBSD	mirror

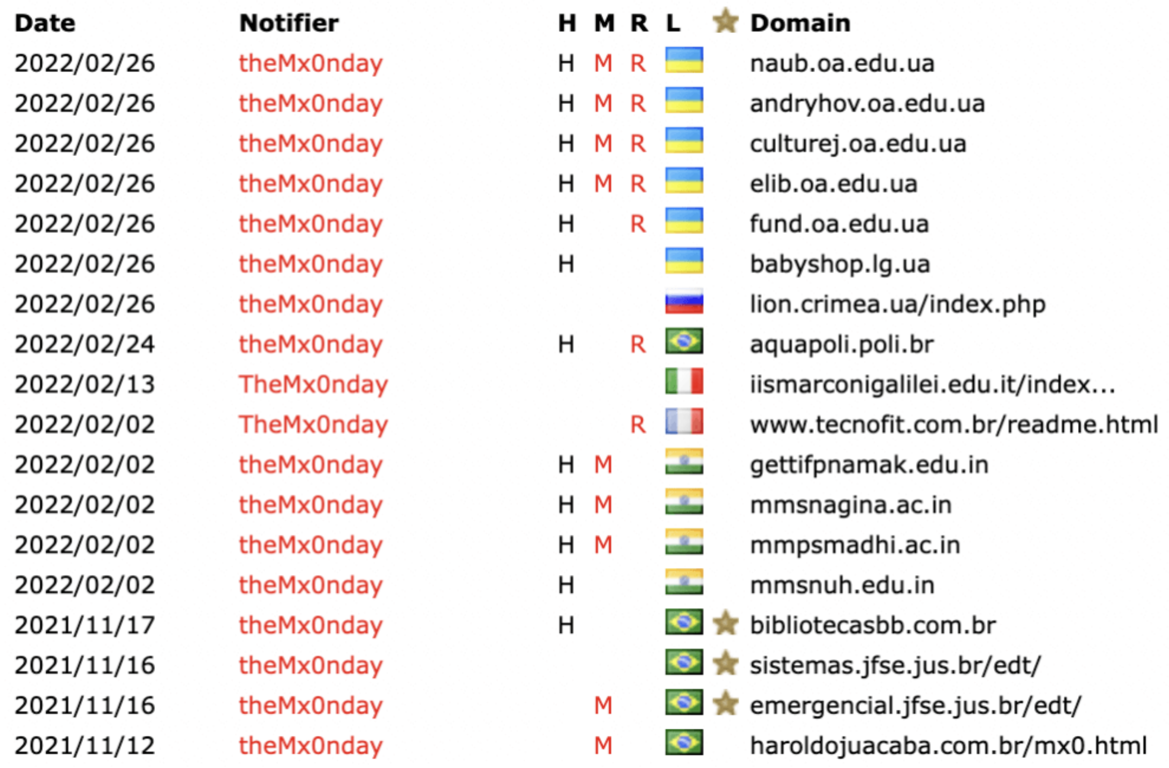
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21

DISCLAIMER: all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified **anonymously** to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents. Read more

Home News Events Archive Archive ★ Onhold Notify Stats Register Login Disclaimer Contact

A huge list of compromised EDU.UA websites attributed to the Monday group, dated the 26th of February, right after we saw a spike in attacks targeting EDU.UA websites.

As you can see below, the defaced EDU.UA sites listed on ZoneH abruptly start on the 26th. As the invasion started, this threat actor made the decision to specifically target Ukrainian universities.

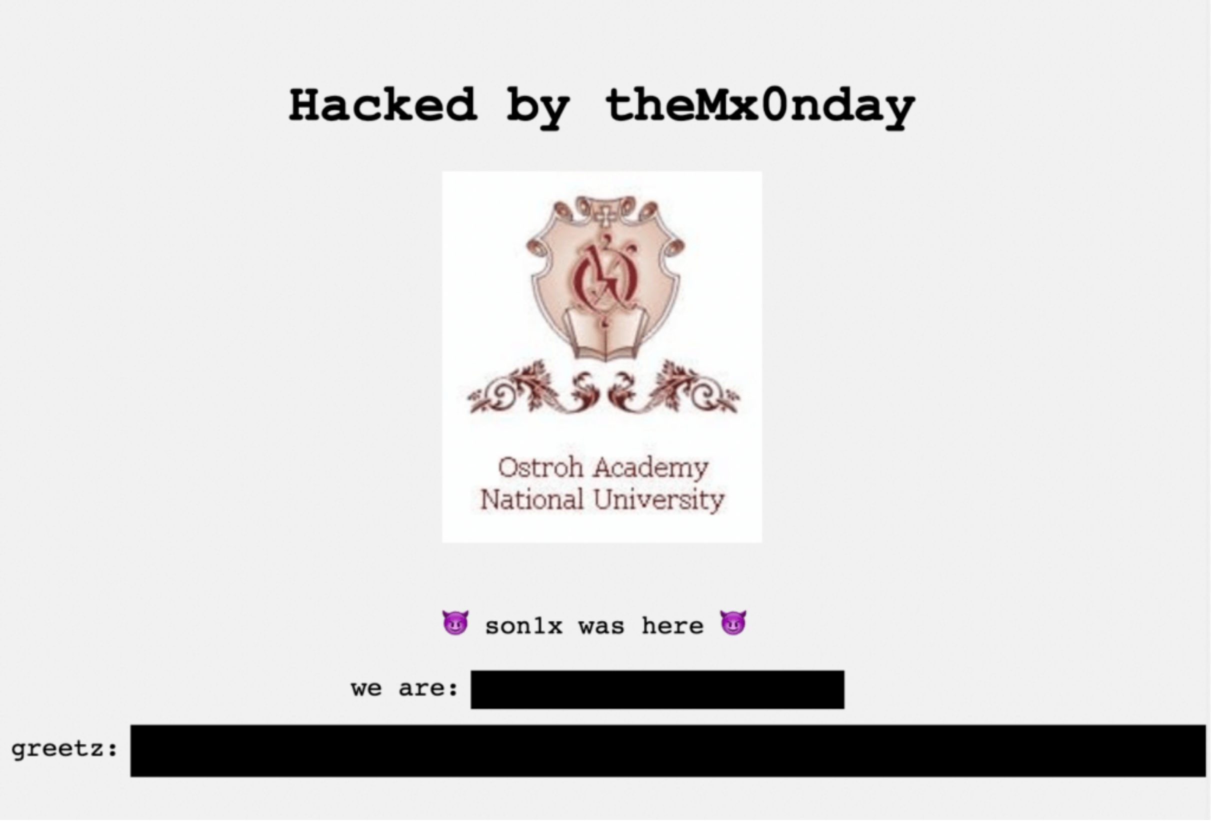


Date	Notifier	H	M	R	L	★	Domain
2022/02/26	theMx0nday	H	M	R	🇺🇦		naub.oa.edu.ua
2022/02/26	theMx0nday	H	M	R	🇺🇦		andryhov.oa.edu.ua
2022/02/26	theMx0nday	H	M	R	🇺🇦		culturej.oa.edu.ua
2022/02/26	theMx0nday	H	M	R	🇺🇦		elib.oa.edu.ua
2022/02/26	theMx0nday	H		R	🇺🇦		fund.oa.edu.ua
2022/02/26	theMx0nday	H			🇺🇦		babyshop.lg.ua
2022/02/26	theMx0nday				🇷🇺		lion.crimea.ua/index.php
2022/02/24	theMx0nday	H		R	🇧🇷		aquapoli.poli.br
2022/02/13	TheMx0nday				🇮🇹		iismarconigalilei.edu.it/index...
2022/02/02	TheMx0nday			R	🇫🇷		www.tecnofit.com.br/readme.html
2022/02/02	theMx0nday	H	M		🇮🇳		gettifpnamak.edu.in
2022/02/02	theMx0nday	H	M		🇮🇳		mmsnagina.ac.in
2022/02/02	theMx0nday	H	M		🇮🇳		mmpsmadhi.ac.in
2022/02/02	theMx0nday	H			🇮🇳		mmsnuh.edu.in
2021/11/17	theMx0nday	H			🇧🇷	★	bibliotecasbb.com.br
2021/11/16	theMx0nday				🇧🇷	★	sistemas.jfse.jus.br/edt/
2021/11/16	theMx0nday		M		🇧🇷	★	emergencial.jfse.jus.br/edt/
2021/11/12	theMx0nday		M		🇧🇷		haroldojuacaba.com.br/mx0.html

Attacker Motivations

You'll notice the Brazilian sites listed on ZoneH in the above screenshot, credited to the Monday group. Recall, we saw a few hits targeting Brazil from the Njalla IP address above.

The archive on ZoneH of the defaced page for National University Ostroh Academy, which is a well known University that dates its heritage back to 1576, looks like this. This image is partially redacted to avoid promoting threat actors.



Hacked by theMx0nday

😈 son1x was here 😈

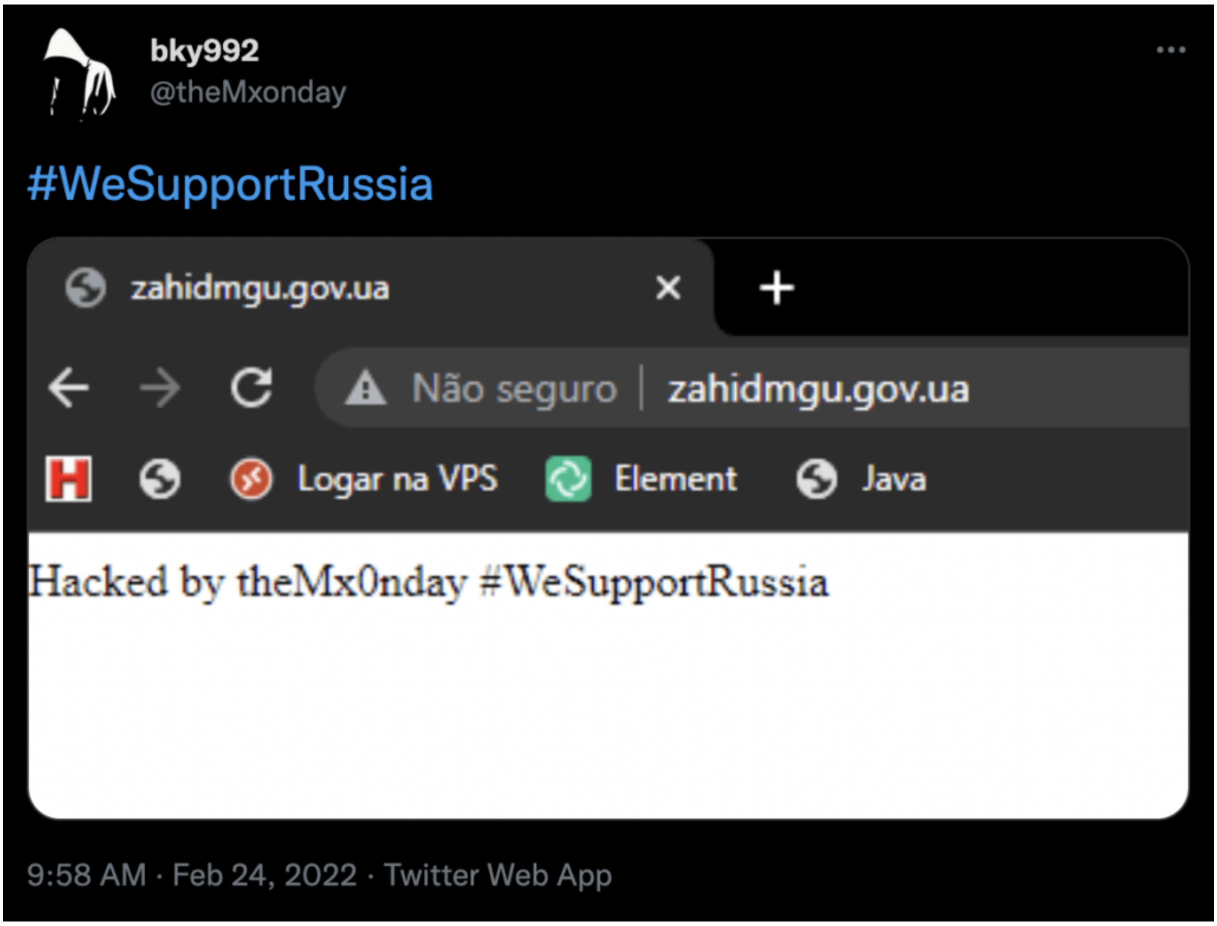
we are: [redacted]

greetz: [redacted]

We have retained the handle son1x in the above image because this threat actor has a history of stealing sensitive data. In October last year, this threat actor defaced the website of the

Indonesian Cyber and Code Agency (BSSN), and in November, the same attacker stole Indonesian police personnel records. This threat actor also goes by “son1x777” on a now-suspended Twitter account.

The group this threat actor belongs to, the Monday group, has a Twitter account that expressed support for Russia, days before the Russian invasion started and before they started hacking Ukrainian universities.


bky992
@theMxonday

#WeSupportRussia

Hacked by theMx0nday #WeSupportRussia

9:58 AM · Feb 24, 2022 · Twitter Web App

The Monday group has historically targeted a large number of Brazilian sites. They embed a Brazilian rap video in the HTML of the sites they deface. Their Twitter account is in Portuguese. From this, we can infer that they are based in Brazil and are Brazilian.

The Full Attack Path

We have determined that the threat actor is based in Brazil. They used a range of IP addresses to launch an attack on Ukrainian universities as the Russian invasion of Ukraine commenced. The majority of attacks were routed via Njalla, based in Sweden. Njalla claims that their servers are “In secret locations in Sweden” although the specific exit node appears to be in Finland, based on IP geolocation data. Njalla is backed by Peter Sunde who is the co-founder of The Pirate Bay and prides himself in masking the identity of his customers. The attacks compromised at least 30 Ukrainian university websites, which are listed in ZoneH, with evidence of the compromises.

Wordfence Is Deploying Real-Time Threat Intelligence to Ukrainian Websites

The National University Ostroh Academy is one of the affected schools that suffered a hacked website.

Effective immediately, we are providing real-time firewall rules, real-time malware signatures, and our IP blocklist to **all websites under the .UA top-level domain protected by Wordfence**.

Normally our real-time threat intelligence is only available to our Premium, Care and Response customers at a minimum cost of $99 per year per website. We are doing this to assist in blocking cyberattacks targeting Ukraine. This update requires no action from users of the Free version of Wordfence on the UA top-level domain. We are activating this live security feed for UA websites automatically until further notice. Within the next few hours, over 8,000 Ukrainian websites running the free version of Wordfence will automatically become far more secure against attacks, like these, that are targeting them.

The malicious IP addresses involved in this attack are included in our blocklist, which will completely block access to WordPress and other PHP applications installed alongside WordPress. The list is updated in real-time as attackers rotate through fresh IP addresses. We also regularly deploy new firewall rules and malware detection to block and detect emerging attacks and malicious activity. Instead of our usual 30-day delay for free customers, Ukrainian websites will start receiving these security updates in real-time, until further notice.

Again, this requires no action from Ukrainian users of the free version of Wordfence, and does not require any payment or personally identifiable information from them. They will simply become more secure over the next few hours.

This is the first time in the history of our company that we are taking this action. We are doing it as a response to the crisis that has unfolded in Ukraine.

#WeSupportUkraine

Mark Maunder – Wordfence Founder & CEO

This post was written by Mark Maunder with significant contributions from the Wordfence Threat Intelligence Team.