BlueHornet – One APT to Terrorize Them All

By Research Team

Published: 2022-04-14 · Archived: 2026-04-05 14:35:42 UTC

- Table of contents
- Introduction
- Debut
- No Threat Group is Safe
- Poking the Bear
- Hunting China and Russia
- Alibaba Cloud
- WeChat
- MyBank
- Amazon China
- Who is BlueHornet?
- Odd Announcement or Hard Truth
- Curtain Call
- Summary

The author

The Cyberint Research Team work round the clock to unearth the latest threats to SMBs and enterprises. They are on top of the latest TTPs and monitor rising threat groups, malwares and trends.

Table of contents

- Introduction
- Debut
- No Threat Group is Safe
- Poking the Bear
- Hunting China and Russia
- Alibaba Cloud
- WeChat
- MyBank
- Amazon China
- Who is BlueHornet?
- Odd Announcement or Hard Truth
- Curtain Call
- Summary

Related Articles

Introduction

One thing that we've learned from the Russia-Ukraine conflict is that the cybersecurity and the cyber-warfare world is going to change, if it hasn't already.

While Anonymous, the TI Army of Ukraine, and more hacktivist groups are actively participating in the conflict, a relatively new group brings something new to the table.

At first, BlueHornet, aka AgainstTheWest, aka APT49, seemed like a daring hacktivist group targeting major organizations and APTs originating in Russia, China, Iran and North Korea, but recent revelations by the group suggest that we are dealing with something much greater.
Either if the group was hacktivists or nation-sponsored, we are convinced that they are one of the more interesting groups currently in play.

With five different threat groups compromised and leaked by the BlueHornet crusade, including APT28 (aka Fancy Bear), APT 38 (aka The Lazarus Group) and APT40 (aka Kryptonite Panda) after only a few months of operation, this group's capabilities position them as one of the best yet.
Although the identity of the group's puppeteer is unknown, the nation sponsoring BlueHornet, clearly has interests against China, Russia, Iran and North Korea.

Debut

Like other groups that emerged and went public on Twitter when the Russia-Ukraine conflict started, at glance, BlueHornet, seemed to be "yet another group" that joined the fight against Russia, but quickly they hit waves with several campaigns against threat groups supporting Russia while using more sophisticated and targeted attacks against their victims.

No Threat Group is Safe

As mentioned, BlueHornet, which was claimed by the group in the beginning, started out as a data leaks group named "AgainstTheWest" in around October 2021, found a handful of potential targets when about 30 groups sided with Russia at the beginning of the conflict. The Cyberint Research Team documented the cyberwarfare map at the beginning of this huge event and ATW was one of them.

COOMIGPROJECT

The talented hunters' first prey was the French group CoomingProject. In the first days of the conflict, many groups took sides, and CoomingProject was no different. The group announced they were siding with Russia and would target anyone challenging them (Figure 1).

Figure 1: CoomingProject announcement of siding with Russia

It didn't take much time, and a day after the announcement, BlueHornet published that it had leaked the CoomingProject's sensitive data to the relevant authorities in France (Figure 2).

Figure 2: BlueHornet, aka AgainstTheWest, announcing leaking CoominProject data to the authorities

Poking the Bear

While most threat groups and hacktivists try not to get in the way or have any sort of conflict with APT groups, BlueHornet put APT groups on top of their "to-do list".
After a series of breaches published on the Telegram channel of various organizations that we will elaborate on later, on April 3, BlueHornet published highly sensitive information including not just email accounts and social media profiles but also, family members, bank accounts, current location, and additional details about every aspect of the lives of five different members associated with different APTs.

APT 3 – GOTHIC PANDA

APT3, aka Gothic Panda, is a nation-state sponsored group, originating in China, and have been active since at least 2010.
The group mainly targets North America and Eastern Asia, while focusing on strategic sectors such as high tech, telecommunications, defense, aerospace, and more.
The first APT member that BlueHornet leaked was an individual who lives in Shanghai, as they published highly sensitive information such as the street and room number where this individual lives, along with his phone number (Figure 3).
According to the group, this individual, or at least some of the information published about him, was known to the FBI.

Figure 3: Leaked information about the APT3 member

APT 40 – Kryptonite Panda

APT 40, AKA Kryptonite Panda, is another espionage group that is related to China. It has been active for more than a decade with operations documented since 2009 targeting governmental organizations, universities, and other tech-related sectors such as robotics across North America, Europe, and the Middle East.

Once again, BlueHornet leaked detailed information about an individual who lives in Shenzhen, China, including the fake name he uses, links to all of his social media accounts, and showing an alarming direct link between APT 40 and the Alibaba Cloud infrastructure – backed up by screenshots and documents (Figure 4).

Figure 4: APT 40 member's leaked information

APT 28 – Fancy Bear

APT 28, aka Fancy Bear, is a well-known cyberespionage group, which was linked several times in the past to GRU, the Russian military intelligence agency.

It is one of the most famous groups of the bunch, with operations all over the world, mainly targeting North America, NATO, and Ukraine. The group was documented as being responsible for operations since 2014, but some speculations claim that they have been operational for over a decade now.

Fancy Bear is likely one of the leaks that BlueHornet is very proud of.

Like the rest of the information about other APTs, BlueHornet has leaked the information of Dmitriy Sergeyevich Badin, one of the FBI's most wanted criminals (Figure 5).

Figure 5: Dmitriy's wanted ad

Linked to several intelligence units of the Russian government, Dmitriy is a well-known hacker. To date, not much information has been revealed about him, if any.

Like the others, BlueHornet published mostly private details about Dmitriy along with information about his relatives, such as his wife (Figure 6).

Figure 6: Dmitriy Sergeyevich Badin's leaked information

APT 38 – Lazarus Group

APT 38, aka the Lazarus Group, is another well-known espionage group that has been operating since at least 2009.

Given the nature of the group, Lazarus compromised a wide range of victims worldwide. Some intrusions resulted in the exfiltration of data while others were disruptive.

APT 38 campaigns also contained DDoS botnets, keyloggers, remote access tools (RATs), and wiper malware.

The group was linked to North Korea.

In this case, the person BlueHornet chose to focus on was Park Jin Hyok. This individual also on the FBI's most-wanted list (Figure 7).

Figure 7: Park Jin Hyok's wanted ad

Along with many personal details, BlueHornet also tried to focus on the allegations against him and to find evidence of his links to moles in the US congress and oblivious companies working with North Korea (Figure 8).

Figure 8: Park Jin Hyok investigations conducted by BlueHornet

When it comes to Park, BlueHornet had much more to work with or much more interest in publishing everything they knew about this particular individual, presumably because of his relationships with the US and NATO scandals.

Marking New Targets

It seems that BlueHornet is not familiar with the term "rest" and were constantly on the lookout for new victims and threat groups they could leak.

A relatively new ransomware group named Stormous announced that they are about to target French entities in the coming weeks. As expected, it didn't take too much time for BlueHornet to reply to their announcement with "Stormouse, you're next" (Figure 9).

Figure 9: BlueHornet's announcement that is was going after Stormous

Drawing The Heat

As expected, BlueHornet is drawing a lot of heat mostly from Russian and Chinese threat groups.

In addition to publicly sharing information about their exploits on their Twitter account, BlueHornet also shares information about the compromise attempts (Figure 10).

Figure 10: BlueHornet announcement about Russian actors trying to breach their Twitter account

Hunting China and Russia

BlueHornet is by any means not a copycat of the Lapsus$ group, but one thing they have adopted is Lapsus$'s "Next Victim" polls.

As their followers' numbers increase by the hour, they prefer an interactive approach with their crowd and let them decide who the next victims or industry will be (Figures 11, 12).

Figure 11: BlueHornet's Poll on what industry should they go after

Figure 12: BlueHornet's poll on who will be the next individual they will leak

While it seemed that BlueHornet is the ultimate vigilante against the APTs of Russia, China, North Korea and Iran, they are also responsible for major data breaches and leaks of big organizations in these countries too.

BlueHornet's leak channel is their Telegram channel (Figure 13) and a known breach forum named BreachForums. Their Telegram channel already has more than 1000 subscribers and was created on March 22nd.

Figure 13: BlueHorne's Telegram channel

Alibaba Cloud

One of the most dominant organizations in China is Alibaba. With allegations of having APT infrastructures deployed in their cloud services, Alibaba seemed like an obvious target.

On March 30, BlueHornet published 30GB of sensitive information on the known leak site `Breached.Co` and announced it on their Telegram channel (Figure 14).

Figure 14: BlueHornet publishing Alibaba Cloud leaks on Telegram

WeChat

WeChat is a well-known instant messaging application in China, and is broadly used by its citizens. On March 28, Blue Hornet announced: “WeChat data coming soon”.

No more than 12 hours later, they published the source code of the application on their Telegram (Figure 15), using the anonymous file sharing platform Anonfiles.

Figure 15: WeChat source code leak

MyBank

In their pursuit of compromising and leaking major Chinese organizations, BlueHornet published sensitive information about the first internet-based bank in China, “MyBank”.

On April 9, BlueHornet announced the leak on their Telegram channel, as they do with all of their victims (Figure 16).

Figure 16: MyBank leak on BlueHornet’s Telegram channel

Amazon China

Amazon, possibly the most frightening victim on BlueHornet’s list, was also breached by the group (Figure 17).

In this case, we saw that the group was targeting Amazon, but only in China.

Figure 17: BlueHornet announced a breach of Amazon China

Although we have only mentioned four victims out of the long list of compromised organizations, it seems that BlueHornet is mainly focusing on organizations from the finance, technology and government sectors in China, Russia, North Korea and Iran.

Who is BlueHornet?

So given all their exploits and extremely daring campaigns, the only question left unanswered is who is BlueHornet? Are they the next generation Anonymous? Are they a hero in our story, or just another group taking law and order into their own hands?

Although many hacktivist groups are going as a “movement” containing tens and hundreds of thousands of members, BlueHornet seems to be comprised of very few people and claims they are only five members, which is very surprising given the effect they have.

AgainstTheWest is From The West?

In an interview BlueHornet gave to databreaches.net, the group does not say where they are from exactly, but gives several hints, saying that they “*have some political protection in place*.” and joking about “*being drone striked and poisoned*”. The assumption is that the group originated in North America or another NATO country.

While assessing their social management and communication with their audience, it seems that BlueHornet is a group of adults. They do not play any attention or ego games, and their exploits are straightforward without any need to “show off”, so to speak.

BlueHornet insists that they will never target western countries, governments, persons, or companies at all. Hospitals and schools are also off-limits.

Given an opportunity to get some answers from the group by threat analyst Tom Malka (Figure 18), it appears that the group is currently looking to assert as much pressure as possible on big organizations and governments in order to end the conflict.

Figure 18: BlueHornet talking about their intentions

Skilled Vigilante

BlueHornet is no script-kiddies and certainly no Anonymous. Looking at their exploits and their compromised personas and organizations, we can make a fair assessment of their talent.

When introducing themselves, it seems that the members of the group claim to be ex-intelligence figures holding several certificates and degrees such as CIE, CEH V10, CISSP and Masters in Cyber Security and Computer Science.

In addition, they also claim that the group’s members work in the ethical hacking sector, helping government agencies since the start of the Ukraine invasion, mostly in Germany and the US.

While the tools BlueHornet use are not familiar but purported to be “manual only”, they have claimed to possess several zero-day vulnerabilities in the following systems:

- Django (Latest Version – 02/2022)
- Bitnami
- GitLab
- SonarQube
- Nginx

Nginx Zero-Day

While we do not have any information on the group’s zero-days on Django, Bitnami, GitLab and SonarQube, BlueHornet shed some light on the recently discovered zero-day in Nginx.

A major zero-day event appears to be breaking loose in the coming weeks or even days. BlueHornet with its “sister group”, BrazenEagle, discovered a zero-day vulnerability that allows a Remote Code Execution (RCE) in Nginx version 1.18.

At the moment, not much is clear regarding this vulnerability, but the module related to the `LDAP-auth` daemon within Nginx is affected, and anything that involves LDAP optional logins is vulnerable as well.

Also, it seems that default and common configurations of Nginx are a good setup for exploiting this vulnerability.

The only information regarding mitigating some of the exploitation, ironically came from the BlueHornet group, claiming that the `ldapDaemon.enabled` should be disabled and to change `ldapDaemon.ldapConfig` properties.

In addition to this major teaser in their GitHub account, BlueHornet also published that they are currently working on a supply chain attack with BrazenEagle, probably looking to utilize this vulnerability in the process (Figure 19).

Figure 19: BlueHornet announcement about working with BrazenEagle on a supply chain attack

The group has announced that they have contacted Nginx in order to get paid in case they have a bug bounty group. Once Nginx rejected their request for bug bounty, BlueHornet looked to sell the zero-day to the highest bidder but surprisingly rejected a 200K offer from several underground forums.

Allies

Allies are something any threat group, of any kind, might want and need in order to get their work done. Several times BlueHornet has mentioned in all its communication channels their relations with hacktivist groups such as Intrusion Truth, Anonymous, Belarusian Cyber Partisans, GhostSec, Anonymous Taiwan, and PucksReturn, although it seems that the group that has the closest relationship with BlueHornet is BrazenEagle.

The BrazenEagle and BlueHornet alliance was published in several cases. BlueHornet has shared information with the group regarding a campaign they ran against the Main Directorate of the General Staff of the Armed Forces of the Russian Federation, asking for help.

In addition, the group has worked with BrazenEagle on the Nginx vulnerability zero-day and announced it on their GitHub, while suggesting that more zero-days are coming (Figure 20).

Figure 20: BlueHornet announcement about their cooperation with BrazenEagle in the Nginx vulnerability

Friend or Foe?

In their announcements they tend to make things very clear about their intentions – they are only targeting the countries and sectors mentioned, and, ironically, will never go against the west.

BlueHornet also insists they always share their findings with several stats intelligence agencies.

In the only interview their leader gave [3], when asked about their future, he said: *“Hopefully, we can actually finish ATW after the APT groups have been exposed and get employed by these countries we’re trying to help.”* And they are certainly having fun with the idea, posting another poll asking their subscribers “Should we go whitehat?” (Figure 21). The majority wanted them to stay vigilant

Figure 21: BlueHornet’s poll on whether to retire and go whitehat

Odd Announcement or Hard Truth

Probably the most confusing and interesting announcement from the team since its establishment was the announcement that they are a state-sponsored group (Figure 22).

Figure 22: BlueHornet's announcing they are nation-state sponsored

The game-changer announcement was published on April 14 and raised many questions about the group.

Throughout their whole operation time, BlueHornet did not act or managed themselves as the "Typical" nation-state APT. We haven't seen other APTs giving interviews [3] and talking publicly about their exploits, communicating with their followers and so on.

For example, the polls BlueHornet used are not something APTs usually do, for the simple reason, they are mostly managed and get instructions by the sponsoring state – not their Twitter followers.

Another unusual characteristic of the group is their allies. As mentioned, most of the groups BlueHornet talked about in an aspect of alliances are hacktivist groups which suggested that they are also part of this community. The only group BlueHornet was in good relations with that was not identified as hacktivists was BrazenEagle.

In addition, the hunt for APTs' members was also unusual behavior by the typical nation-state-sponsored groups. They are supposed to serve the country that is sponsoring them so leaking the findings should do the opposite.

All these unusual actions by the group, including talking freely about the vulnerabilities they possess and of course trying to sell one, raise the question, should we believe them?

Cyberint Research Team's observation, in this case, is that BlueHornet did start as a hacktivist, leakage group. The members gave certain ethical hacking services to the governments that are siding with Ukraine in this conflict.

It seems that BlueHornet tried to become sponsored group by whatever country they originated in and what is a better business card than leaking your enemy's top espionage groups?

After getting these countries' attention and announcing their desire to be recruited several times, we are convinced they got recruited and were told to lay low for a while resulting in this announcement.

Curtain Call

As suspected for several days, the show was about to end. In their Telegram channel. BlueHornet have deleted all the leaks and former messages and left only three messages that are related to the Nginx vulnerability, while the last one (Figure 23) was talking about one member that, in the last several days, revealed his intentions which were against the ideology of the group (persuit for money) and is no longer part of it.

Figure 23: BlueHornet's last announcement in their Telegram channel

The most interesting part of the last message was the "Goodbye" BlueHornet left us with, announcing that they are going back to their "ordinary" lives *"for a better future in white hat ethical hacking."*

Summary

There is not a single doubt that BlueHornet is one of the most interesting and exciting groups that have come to the front of the stage in 2022. Although the unfortunate reality of the Russia-Ukraine conflict has pushed these unique individuals to do what they do, this unusual group compromised infrastructures and highly dangerous individuals that are linked, mostly, to either Russia or China.

While their identities and origin is still unknown, their talent and the impact they had will be something to remember them by.

Along with the question rather if they are actual nation-sponsored APT or hacktivist group, many other questions remain while some might be answered in time and some will remain buried.
