DDoS

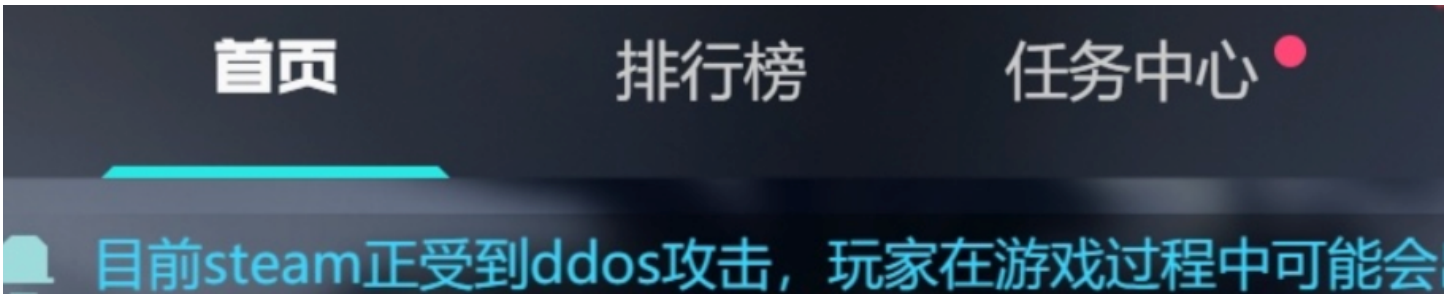
More details on the DDoS attack on the 《Black Myth: Wukong》 distribution platform

Wang Hao, Alex.Turing, daji, Acey9

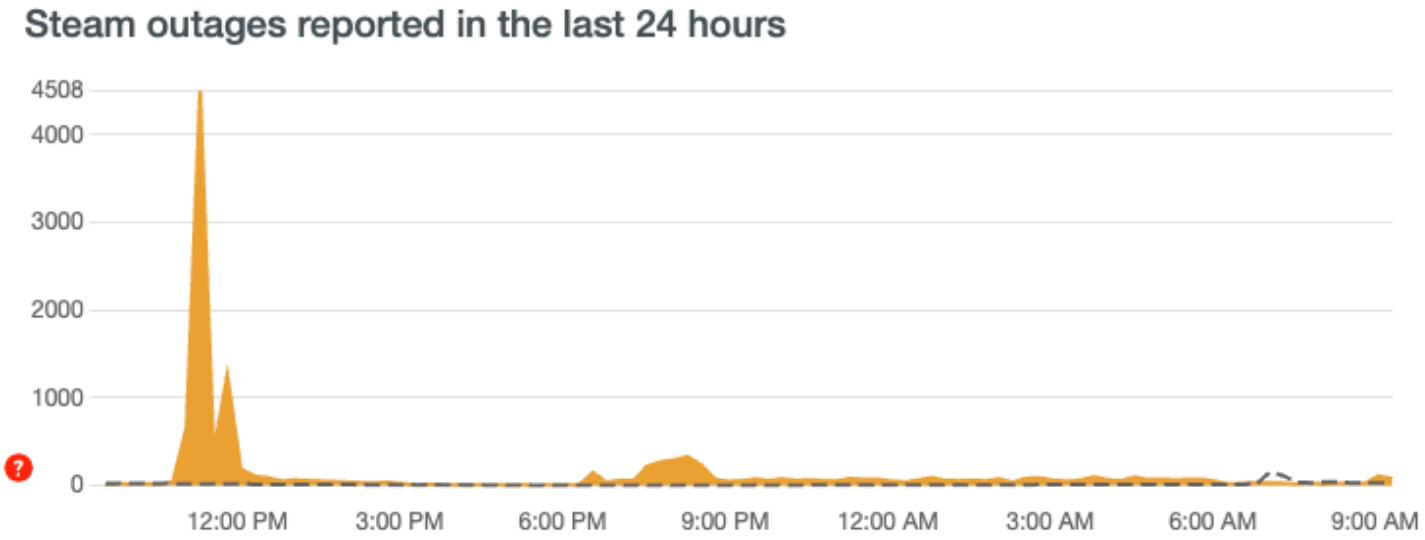
2024年8月29日 • 11 min read

Incident Review

On the evening of August 24th, Steam platform suddenly went down, with players around the world reporting that they were unable to log in. Many players speculate that the crash is caused by too many people online in Black Myth: Wukong. However, according to the announcement of Perfect World Esports Platform, the real cause was a large-scale DDoS attack.



Perfect World Announcement



Downdetector Steam Outages Report

XLab’s Insight

XLAB's CTIA(Cyber Threat Insight Analysis) system conducted an in-depth observation of the DDoS attack. We noticed that the attack involved nearly 60 botnet control nodes, which is much more than regular botnets. These nodes coordinated and commanded a large number of infected bots to launch attacks in waves.

The targets of the attack included Steam server IPs in 13 regions around the world, including China, the United States, Sngapore, Sweden, Germany, Austria, Spain, the United Kingdom, Japan, South Korea, Australia, Chile and the Netherlands. It is worth noting that in addition to Steam's own servers, the Steam servers of Perfect World in China were also listed as targets of attack. In total, 107 server IPs were attacked.

The attack was mainly divided into four waves. The attackers seemed to intentionally choose to launch attacks during the peak online hours of gamers in various time zones to achieve the greatest destructive effect.

Given the timing of the attack, the geographical distribution, and the simultaneous targeting of both domestic and international Steam servers, it is clear that the attackers' aim is to disrupt the Chinese market significantly while causing comprehensive interference with the normal operations of the Steam platform on a global scale. This organized attack demonstrates the attackers' meticulous planning in strategy and precise targeting of their objectives.

Attack Period Analysis

The attack was mainly divided into four waves, following the time zone. They were Saturday noon in the Eastern Hemisphere, Saturday evening in the Eastern Hemisphere, Saturday evening in the Western Hemisphere, and Sunday evening in Europe, which are all peak times for online gamers. The specific attack time

periods and regions are as follows: (Chart description: the horizontal axis is the attack time, the vertical axis is the attacked area, and the color blocks represent the number of servers attacked in the area)

Detailed attack timeline

- Around 11:00 BST on 24 August, the first wave of attacks affected Steam servers in 7 regions and lasted for nearly 1 hour (Saturday noon in the Eastern Hemisphere).
- Around 21:00 BST on 24 August, the second wave of attacks, affecting 13 regional Steam servers, with intermittent attacks lasting nearly 5 hours (Saturday evening in the Eastern Hemisphere)
- Around 09:00 BST on 25 August, a third wave of attacks, affecting 13 regional Steam servers, attacked for nearly 15 minutes (Saturday night in the Western Hemisphere)
- Around 04:00 BST on 26 August, the fourth wave of attacks, affecting Steam servers in 13 regions, the attacks lasted nearly 2 minutes (Sunday night in Europe)

Detailed time and area of the four waves of attacks

Steam's Attacked Services

Judging from the following keywords of Steam servers, the servers attacked are mainly: content servers, ingest, broadcastcs, and related services.

```
 27 ext2
 27 ext1
 18 cm2
 18 cm1
 11 ext3
  9 ext4
  5 cm5
  5 cm4
  5 cm3
  4 cm6
```

```
    3 ext5
    1 ingest
    1 ext6
    1 cm05
    1 broadcastcs
```

Potential motives

In this attack, we observed a total of 280,000 attack instructions against the Steam platform. According to our long-term observation, as a well-known gaming platform, Steam attacks occur daily, but they are often small-scale attacks on scattered servers, with the number of attack instructions ranging from a few to dozens of times. In this incident, the number of attack instructions increased by more than 20,000 times, and the peak was 250,000. This increase is very rare (see the figure below, the attack instruction trend chart, the huge spike). Steam's servers in various regions around the world were attacked in turn, including the Steam servers represented by Perfect World in China, which were also attacked. Before the launch of Black Myth: Wukong, we rarely saw major attacks targeting the Perfect World servers. And the attack lasted for up to several hours, and the attack was specifically targeted at the peak time when players in various regions were online. This is extremely rare.

The attack trend of Steam platform in the past year

The following is a screenshot of our CTIA System. It shows the ranking of attacked companies in the past month. Steam (Value Company) and Perfect World ranked first and second, far ahead of well-known companies such as Verizon.

The timing of the Steam attack incident coincided with the first weekend after the launch of Black Myth: Wukong on the Steam platform, and prior to the release of Black Myth: Wukong, we had not witnessed many DDoS attacks on Perfect World Steam servers, which primarily serve domestic gamers. Combining these two points, it is difficult not to suspect that this attack was specifically targeted at the Chinese 3A game masterpiece "Black Myth: Wukong".

Main botnets involved

As a worldwide gaming platform, Steam is highly unlikely to be overwhelmed by a smaller-scale botnet. Rather, it is more plausible that numerous botnets were organized and coordinated to launch a concerted attack. It's important to note that no organization in the world possesses an omniscient perspective. This article, from the perspective of XLab, merely analyzes this particular attack incident.

Multiple botnets were involved in this attack, with the main force being the self-proclaimed AISURU botnet. It claimed to have more than 30,000 bots in its Telegram channel, with an attack capability of around 1.3 to 2 terabits per second.

Below is a graph of the botnet's dstat：

In addition the channel also mentioned GSL's Blog, which claimed that it was the largest attack ever reported to the public, and we also found attacks launched from the same time node in the attack logs of this botnet：

Some readers may not have an idea of these numbers, so let's look at the answers from the hottest AI today.

> *A botnet with 30,000 bots and an attack capability between 1.3 Tbps (terabits per second) and 2 Tbps represents a very powerful network attack capability. To understand this concept, the following aspects can be analysed：*
>
> 1. ***Scale of attack***：*Attack traffic of 1.3 Tbps to 2 Tbps is already huge enough to cause a serious Distributed Denial of Service attack (DDoS), which can cripple a target server, network or application. Typically, traditional enterprise network bandwidth is well below this level, so such an attack can have a devastating impact on the target.*
> 2. ***Number of bots***：*30,000 bots means that 30,000 controlled devices are involved in the attack. Each bot may contribute a certain amount of*

bandwidth to launch the attack, aggregating to a total attack traffic of 1.3 Tbps to 2 Tbps。

3. ***Practical effect***：*A DDoS attack of this magnitude can easily overwhelm most Internet services unless the attacked party has very strong protections and sufficient bandwidth redundancy. This type of attack is commonly seen in high-profile hacking campaigns targeting large corporations, government agencies, or critical infrastructure.*

AISURU Botnet Technical Details

Just as Rome wasn't built in a day, the AISURU botnet has its own development history. In fact, we captured samples of this botnet back in October 2023, but it disappeared after a brief period of operation. It wasn't until early May of this year that it re-emerged in our sights under the name `NAKOTNE`, and then entered a period of rapid development. It successively exploited more than a dozen 0-day vulnerabilities to build its botnet, ultimately evolving into today's AISURA.

The AISURA's tactics and technical aspects are closely related to the Fodcha botnet we discovered and named in 2022. Fodcha has become notorious in the cybersecurity community for its involvement in influential attacks on health codes and Navicat, among other incidents, earning it the nickname "DDoS Maniac" from us. Ultimately, under our series of exposures and strikes, it was forced to shut down.

In our view, AISURA seems to be a "follower" or "disciple" of Fodcha, effectively inheriting Fodcha's legacy in both technology and tactics, yet it has also developed a distinctive style, with a threat level no less significant than that of Fodcha.

From the tactical aspects, it is similar to Fodcha in that it enjoys provoking security companies and hopes to be publicly named and exposed by well-known security firms to gain attention and boost traffic. By using this unconventional advertising approach, it seeks to gain an advantage in the fiercely competitive

cybercrime industry, seemingly well aware of the saying, "Even fine wine fears a deep alley."

In the early samples of AISURA, it expressed its "respect" for the security community in this way: `N3tL4b360G4y` , `paloaltoisgaytoo` . "paloalto" refers to Palo Alto Networks, a very famous security company in the United States with a market value of over 100 billion; what about `N3tL4b360` ? In fact, it is a Hexspeak that is quite popular in the security community, which refers to the name of our former team. After we disclosed this batch of samples, it quickly and tactfully replaced `N3tL4b360G4y` with `xlab gay` in the new samples. Undoubtedly, this has once again brought us exposure. AISURU also pays great attention to our blog. In the latest sample, another message was added: "today at xlab, botnet operators learn how to dance macarena," which reminds us of the previously disclosed Rimasuta botnet, which once left a message in the sample `this week on netlab 360 botnet operator learns chacha slide.` Today learning chacha slide, tomorrow practicing macarena, both of which are dancing, could it be that the operators of botnets are mostly dance enthusiasts? In this regard, we would like to say to the botnet community, "practice well, and develop a more exciting 'botnet dance' to amaze us!"

In the samples, the C2 domain name `foxnointel.ru` is mentioned, which has a humorous connotation. It plays on the ID of an active security researcher on platform X, **Fox_threatintel**, who regularly shares threat intelligence. AISURA's use of the C2 domain `foxnointel` suggests `fox no intel` , as if mocking the researcher having no intelligence.

From the technical aspects, AISURA has retained some of Fodcha's style in its `code structure` , such as using a similar switch-case approach for handling various network stages; in terms of `infrastructure investment` , it has continued Fodcha's "sense of crisis," mapping the C2 domain to more than 20 IPs, distributed across multiple countries including the United States, the United Kingdom, South Korea, Japan, and Russia, while also being spread across platforms like Azure, Linode, Vdsina, and Google, greatly increasing the difficulty

of remediation. The geographical distribution of AISURA's main control is as follows:

```
      8 United States
      3 United Kingdom
      3 South Korea
      3 Russia
      2 Singapore
      2 Japan
      2 India
      1 The Netherlands
      1 Switzerland
      1 Poland
      1 Brazil
```

Of course, **the botnet that likes to stand out is certainly not willing to be labeled as an imitator**. AISURA has implemented its own unique innovations in aspects of `encryption`, `network communication` and others.

String Encrypt

Earlier versions used CHACHA20 to encrypt the strings in the samples, and in later versions XXTEA encryption was used.

NAKOTEN_XXTEA_KEY_HEX: `1234567890ABCDEFFEDCBA9876543210`

In the latest version, the previous KEY is still retained in the sample, but the length has been shortened to 4 and the algorithm is moving towards simplicity by replacing it with BYTES_XOR.

AISURU_BYTES_KEY_HEX: `12345678`

The following is a table of decrypted strings:

```
0x1a42c snow slide
0x1a6d0 a|b|c|d|e|f|g|h|j|k:printerconsulting.ru|foxnointel.ru
0x1a438 reports.printerconsulting.ru
0x1a708 5.35.45.162|5.35.44.21|166.1.160.38|194.147.35.35
0x1a458 /login|/products|/contact|/register|/user
0x1a484 /dev/null
```

```
0x1a490 /dev/tty
0x1a49c /dev/pts/1
0x1a4a8 /dev/console
0x1a4b8 /.ai
0x1a4c0 /proc/
0x1a4c8 /proc/self/exe
0x1a4d8 /proc/net/tcp
0x1a4e8 /cmdline
0x1a4f4 /exe
0x1a4fc /proc/uptime
0x1a50c /maps
0x1a514 /fd/
0x1a51c socket
0x1a524 wget|curl|ftp|ntpdate|echo
0x1a540 telnetd|upnpc-static|udhcpc|/usr/bin/inetd|ntpclient|boa|lighttpd|httpd|goa
0x1a5f4 /dev/watchdog
0x1a604 /dev/misc/watchdog
0x1a618 TSource Engine Query
0x1a630 xlab gay
0x1a63c paloaltoisgaytoo
0x1a650 shell
0x1a658 system
0x1a660 enable
0x1a668 sh
0x1a73c /bin/busybox AISURU
0x1a66c AISURU: applet not found
0x1a688 ncorrect
0x1a694 today at xlab, botnet operators learn how to dance macarena
```

Network Protocol

The October 2023 version utilized `N3tL4b360G4y` as the first payload package and embedded this string in its raw form within the sample. Following exposure, we received a new "response": from the `NAKOTNE` version onwards, `xlab gay` was adopted as the first payload package, and it was encrypted and encoded into the string table.

Extract C2

In the past, domain names or IPs were directly encrypted and encoded in the string table. However, in the samples we found at the beginning of August, a new mechanism was used to extract C2.

In the decrypted string table above, the following suspicious strings exist:

```
[1] a|b|c|d|e|f|g|h|j|k:printerconsulting.ru|foxnointel.ru
[2] 5.35.45.162|5.35.44.21|166.1.160.38|194.147.35.35
[3] /login|/products|/contact|/register|/user
```

After analysis, the new mechanism uses the following steps to obtain C2：

1. Split subdomains and second-level domains in [1] by `:`, then split each item by `|`
2. Randomly select a subdomain and a second-level domain name, splice them together to get a C2 domain
3. If resolve the above C2 domain fails, split [2], [3] with `|` to get IP and URI
4. Constructs a GET request based on IP and URI and sends it
5. Get the C2 IP in the response payload in 4-byte increments

The port used by C2 is hardcoded in the sample, randomly selecting from the following 21 ports:

```
2348,12381,8932,8241,38441,23845,8745,6463,7122,1114,6969,1337,4200,3257,7214,2474,
```

Network Communication

The communication process has remained unchanged across multiple versions, using a switch-case similar to that of `Fodcha` for processing each stage：

1. First payload: `xlab gay`
2. Key Exchange
   - Use XXTEA to decrypt the payload to get CHACHA20_KEY, CHACHA20_Nonce
   - Hardcoded NET_XXTEA_KEY_HEX: `428723212B0106344C7A095322236921`

3. Key Verify
    - Decrypt the data using the exchanged key and verify the key consistency by comparing the decrpyted string `paloaltoisgaytoo`
4. Sned Bot Group Info
    - Send the length of group information first, then send the CHACHA20 encrypted payload

With this, the introduction of the main technical details of the AISURU botnet is concluded. DDoS, an ancient threat to the network, one of the archenemies of the gaming industry, is so simple yet brutally effective.

Summary

Our team has been focusing on the field of large-scale botnet discovery and tracking for more than 10 years, and has participated in the early warning, defense and collaboration of many well-known and undisclosed attacks around the world. However, the organization and intensity of this attack still surprised us. What it the motivie here, is anyone upset that a game from China has reached the top of the rankings?

Contact Us

Readers are always welcomed to reach us on twitter.

Partial IOC

SHA1:

```
b6e5c9e65682ccac071b65743595dae475f7a8b8
458d541bc93937ae6d0139f3f9d42b50fe255636
f0760aeaa0d667a1c100e3d348dbc383451587b1
```

Domain:

```
nakotne.pirate
nvr.libre
a.printerconsulting.ru
```