Bluenoroff (APT38) Live Infrastructure Hunting

darkatlas.io/blog/bluenoroff-apt38-live-infrastructure-hunting

June 23, 2025

North Korean threat actor designations often exhibit significant overlap, making attribution complex. As a result, some security researchers collectively refer to all North Korean state-sponsored cyber operations under the umbrella of the **Lazarus Group**, rather than tracking individual clusters or subgroups such as **Andariel**, **APT38 (Bluenoroff)**, and **APT43 (Kimsuky)**. Among these, **Bluenoroff**—also known as **APT38**—is a financially motivated subgroup linked to North Korea's **Reconnaissance General Bureau (RGB)**. Since its emergence around 2014, APT38 has conducted widespread cyber attacks targeting banks, financial institutions, casinos, cryptocurrency exchanges, SWIFT endpoints, and ATMs across at least **38 countries**. Noteworthy incidents include the **2016 Bangladesh Bank heist**, in which the group successfully exfiltrated **$81 million**, and major compromises at **Bancomext** and **Banco de Chile** in 2018, some of which involved **destructive payloads** aimed at covering traces and disrupting incident response efforts.

Differentiating Lazarus Group & Bluenoroff (APT38)

Overview of Lazarus Group

- **State Sponsorship:** Backed by the North Korean government, specifically linked to the *Reconnaissance General Bureau (RGB)*.
- **Active Since:** At least 2009.
- **Core Activities:**
  - Cyber espionage
  - Intellectual property and data theft
  - Disruptive and destructive cyberattacks
- **Global Target Profile:** Political entities, critical infrastructure, corporations, and strategic sectors worldwide.

- **Key Operations:**
  - **Sony Pictures Attack (2014):** A high-profile wiper attack part of *Operation Blockbuster* by Novetta.
  - Associated with several operations such as:
    - *Operation Flame*
    - *Operation 1Mission*
    - *Operation Troy*
    - *DarkSeoul*
    - *Ten Days of Rain*

Attribution & Subgroup Complexity

- **Attribution Challenge:** North Korean APTs often overlap in tools, infrastructure, and personnel.
- **Unified Labeling by Some Researchers:** Some analysts group all North Korean cyber activities under “Lazarus Group,” though distinctions exist.
- **Notable Subgroups:**
  - *Andariel* – military-focused ops
  - *APT38 (Bluenoroff)* – financially motivated
  - *APT43 (Kimsuky)* – espionage and information gathering

Overview of Bluenoroff / APT38

- **Affiliation:** Subgroup of Lazarus, also reporting to the *Reconnaissance General Bureau*.
- **Established:** Around 2014.
- **Primary Focus:** Financial cybercrime on a global scale.
- **Attack Targets:**
  - Banks and financial institutions
  - Cryptocurrency platforms
  - Casinos and ATMs
  - SWIFT system endpoints
- **High-Profile Incidents:**
  - **Bangladesh Bank Heist (2016):** $81 million successfully exfiltrated.
  - **Bancomext (Mexico) & Banco de Chile (2018):** Included both theft and destructive techniques.

Initial Pivot

Pivot Source:
The hunt begins with the IP address **104[.]168[.]151[.]116**, which has been **attributed to APT38 (Bluenoroff)**—a financially motivated subgroup of the North Korean Lazarus Group.

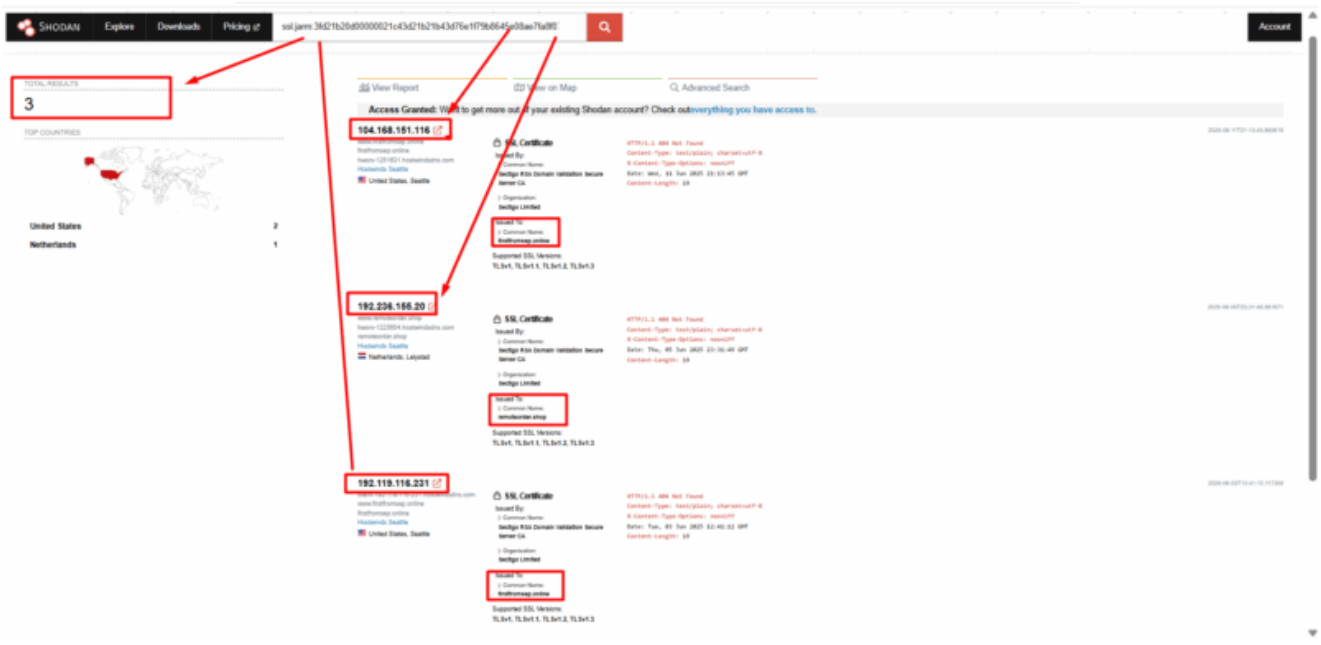
Pivoting Strategy: APT38 IP – 104[.]168[.]151[.]116

Pivot via HTTP Headers

```
Protocol: HTTP/1.1

 Status Code: `404 Not Found`

Headers:
     `Content-Type`: `text/plain; charset=utf-8`

    `X-Content-Type-Options`: `nosniff`

     `Content-Length`: `19`


JARM  29d29d00029d29d00041d41d000000301510f56407964db9434a9bb0d4ee4a
```

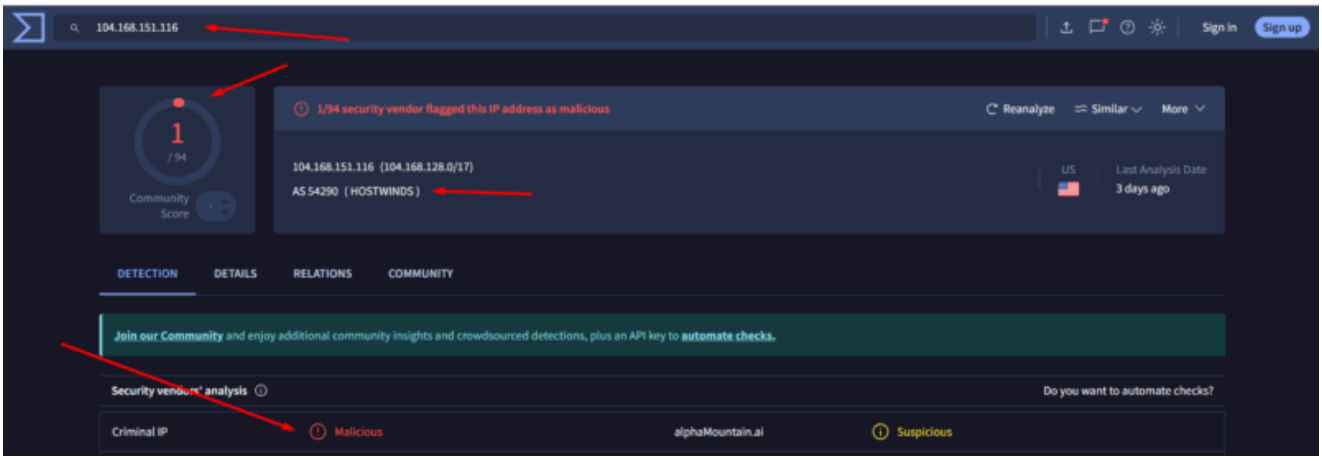
Building Shodan Search Rules for APT38 Infrastructure

```
ssl.jarm:3fd21b20d00000021c43d21b21b43d76e1f79b8645e08ae7fa8f07eb5e4202 HTTP/1.1 404
Not Found Content-Type: text/plain; charset=utf-8 X-Content-Type-Options: nosniff
Content-Length: 19 org:"Hostwinds Seattle"
```

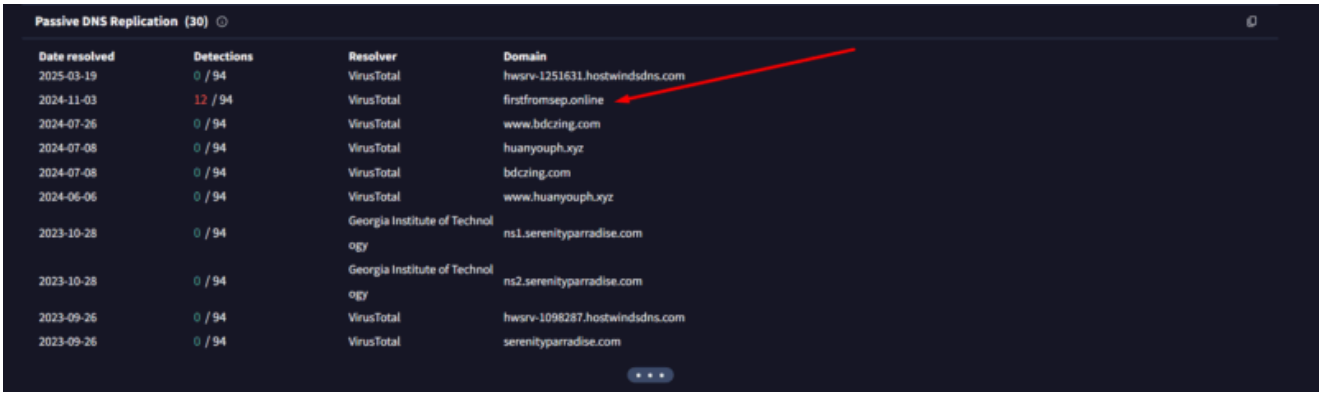


Validating Results

104[.]168[.]151[.]116 > 1/94 detection



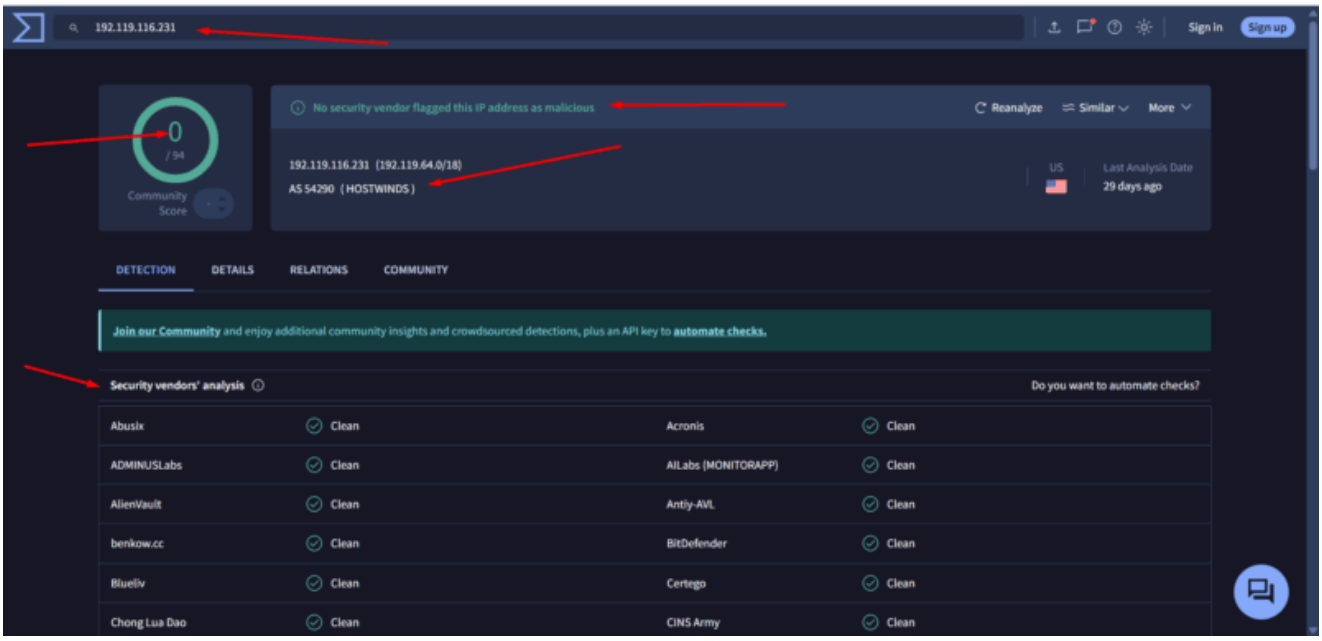
Malicious Use of IP Address: 104[.]168[.]151[.]116



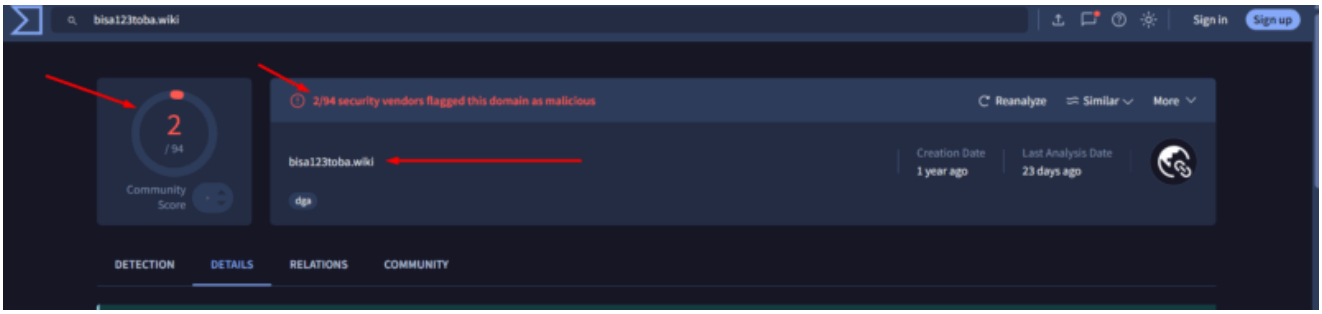
Domain Resolution Pattern

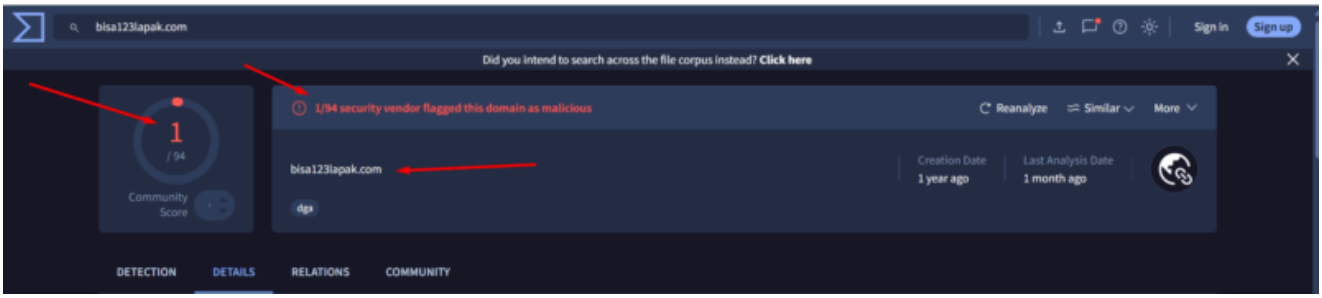
The newly identified phishing domains are **structurally and thematically similar** to those previously resolved by the initial IP address **104[.]168[.]151[.]116**.

192[.]119[.]116[.]231 > 1/94 detection



The observed phishing domains show **strong structural and thematic resemblance** to domains previously resolved

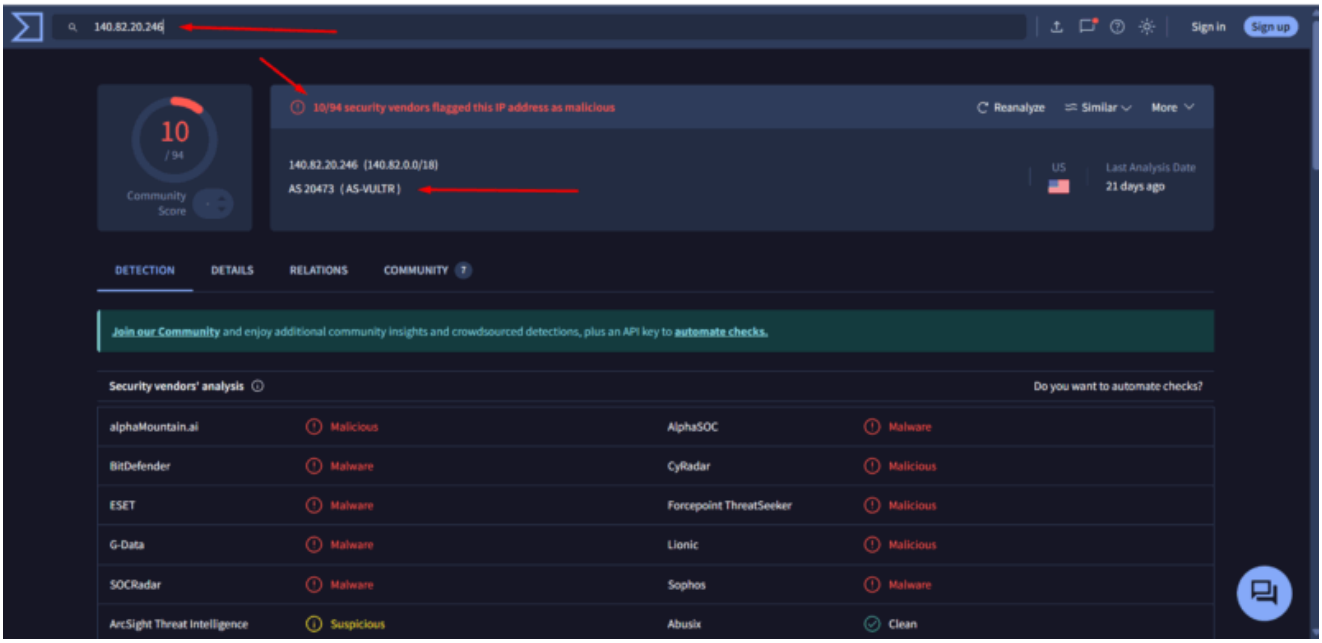




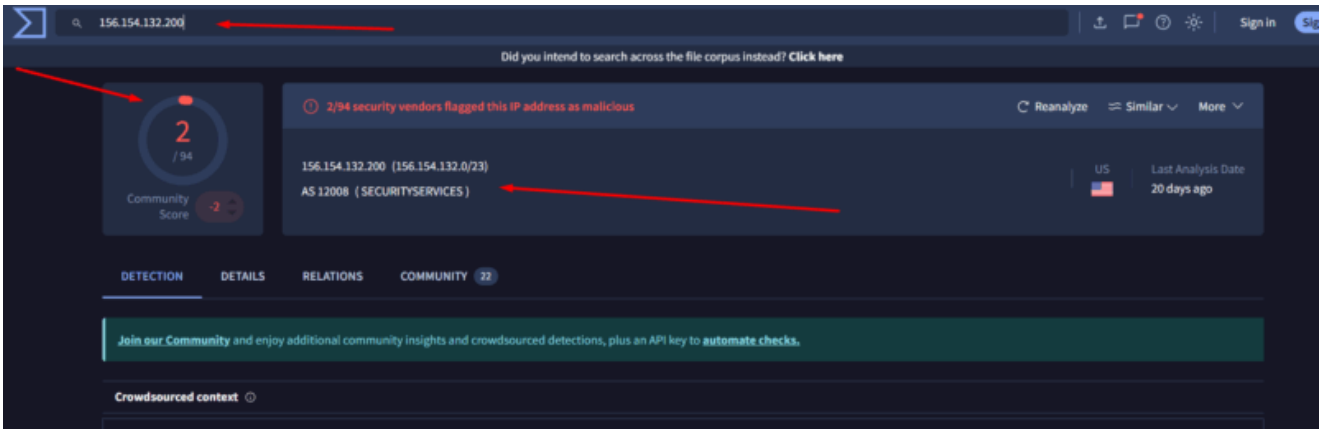
By pivoting on each domain we got another 4 IPs

```
140.82.20.246
156.154.132.200
198.57.247.218
192.64.119.169
```

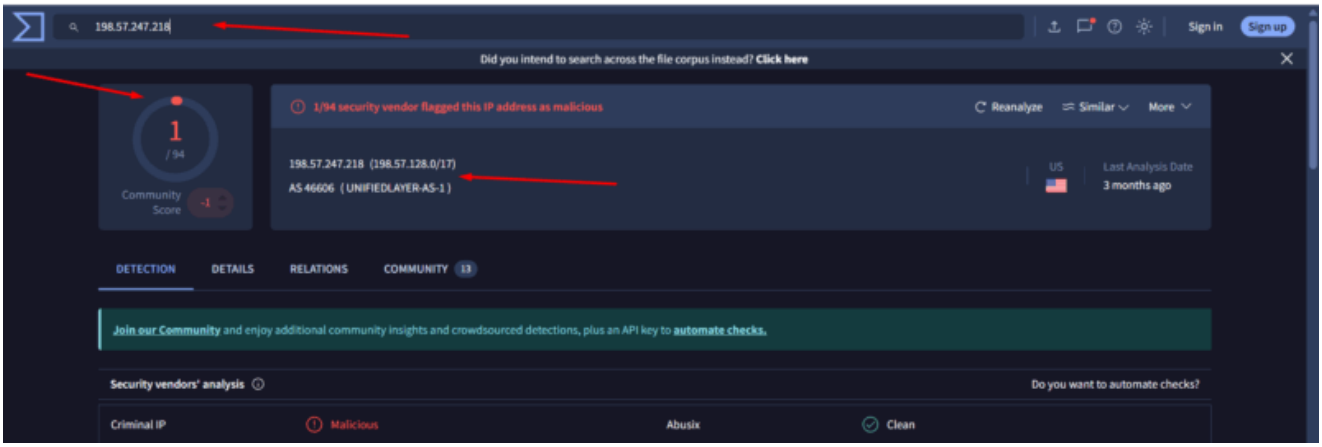
140[.]82[.]20[.]246 > 10/94 detection



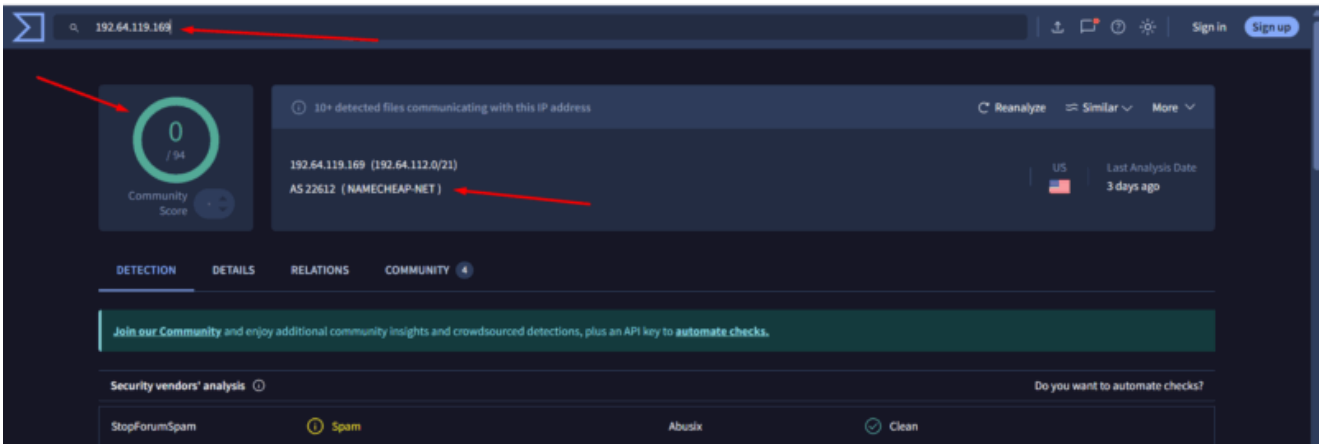
156[.]154[.]132[.]200 > 2/94 detection



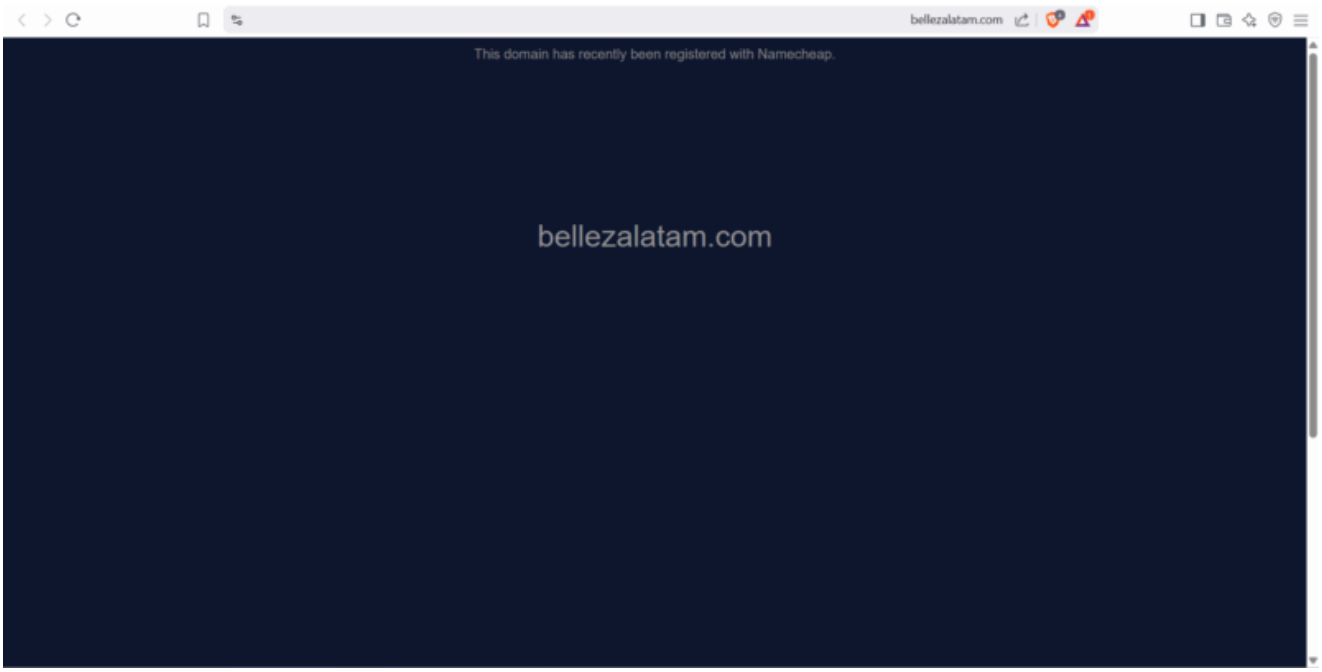
198[.]57[.]247[.]218 > 1/94 detection

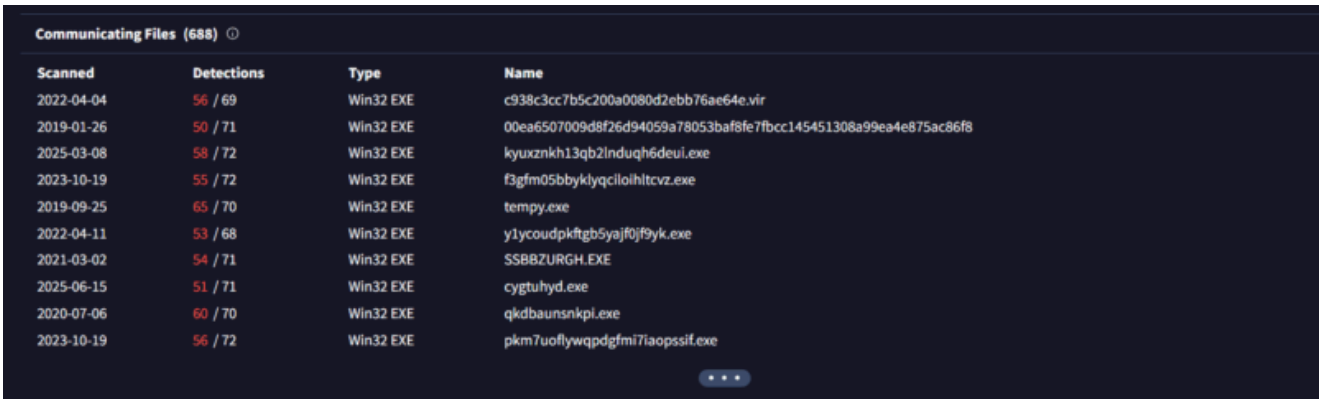


192[.]64[.]119[.]169 > 0/94 detection



this IP resolves **bellezalatam[.]com**

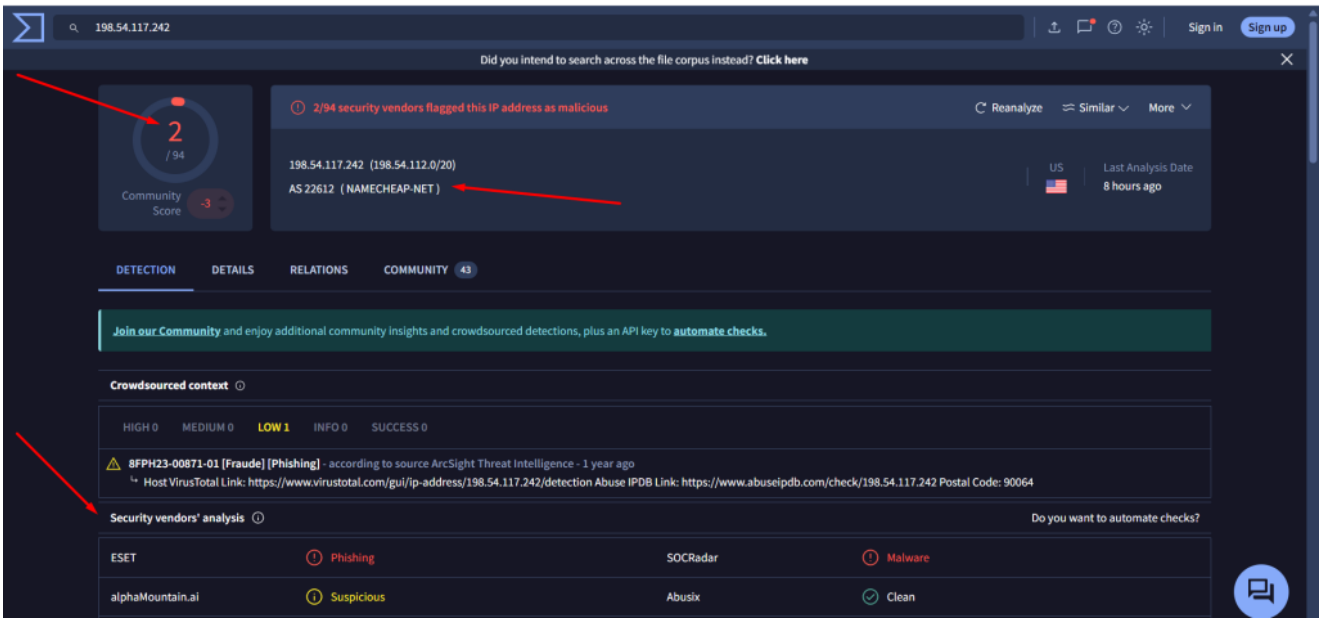




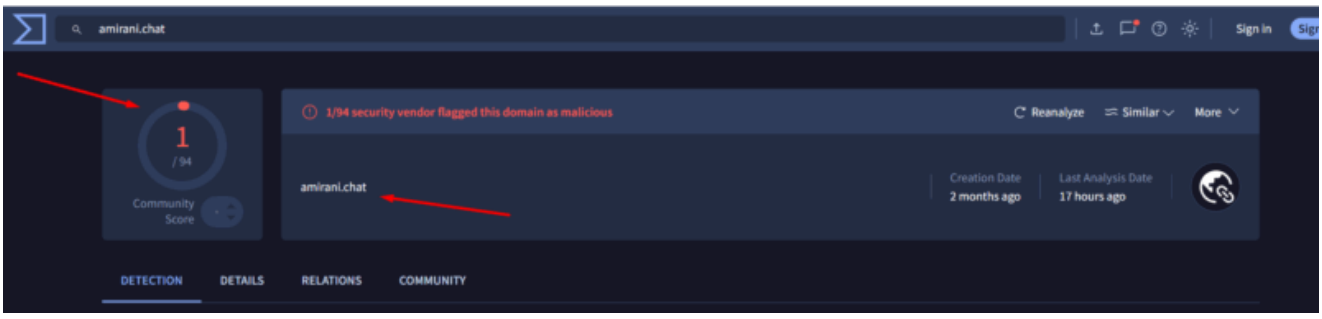
Communicating Files (688)

Scanned	Detections	Type	Name
2022-04-04	56 / 69	Win32 EXE	c938c3cc7b5c200a0080d2ebb76ae64e.vir
2019-01-26	50 / 71	Win32 EXE	00ea6507009d8f26d94059a78053baf8fe7fbcc145451308a99ea4e875ac86f8
2025-03-08	58 / 72	Win32 EXE	kyuxznkh13qb2lnduqh6deui.exe
2023-10-19	55 / 72	Win32 EXE	f3gfm05bbyklyqciloihltcvz.exe
2019-09-25	65 / 70	Win32 EXE	tempy.exe
2022-04-11	53 / 68	Win32 EXE	y1ycoudpkftgb5yajf0jf9yk.exe
2021-03-02	54 / 71	Win32 EXE	SSBBZURGH.EXE
2025-06-15	51 / 71	Win32 EXE	cygtuhyd.exe
2020-07-06	60 / 70	Win32 EXE	qkdbaunsnkpi.exe
2023-10-19	56 / 72	Win32 EXE	pkm7uoflywqpdgfmi7iaopssif.exe

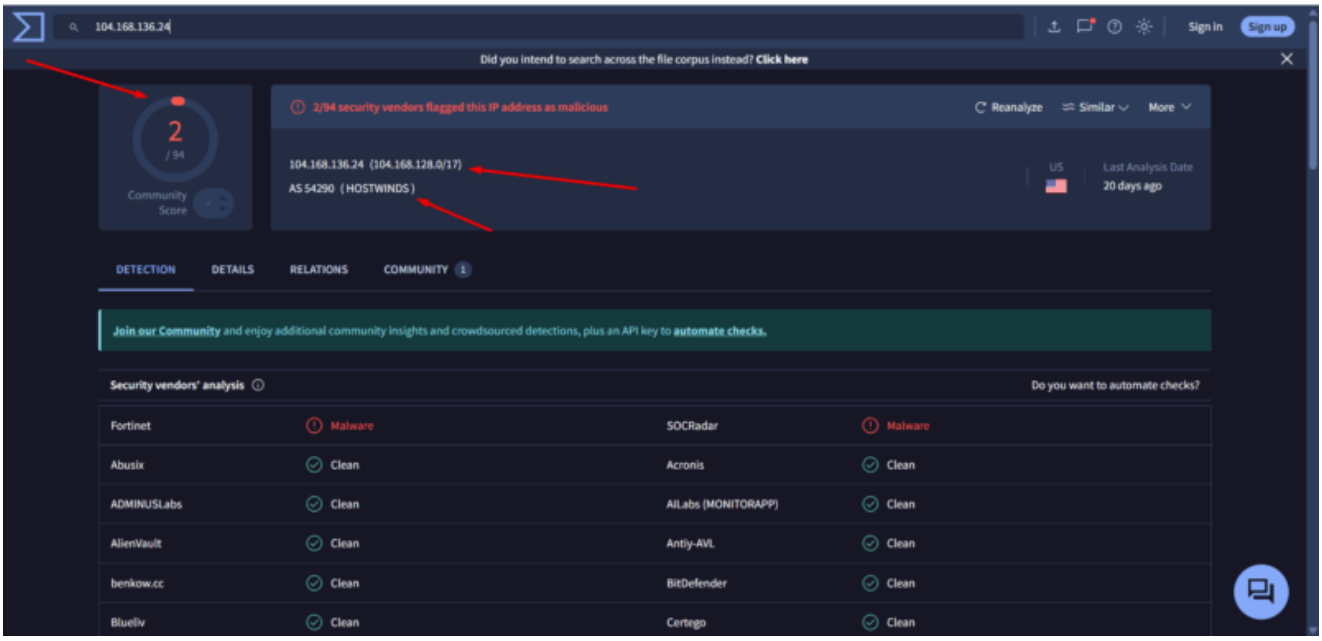
198[.]54[.]117[.]242 > 2/94 detection



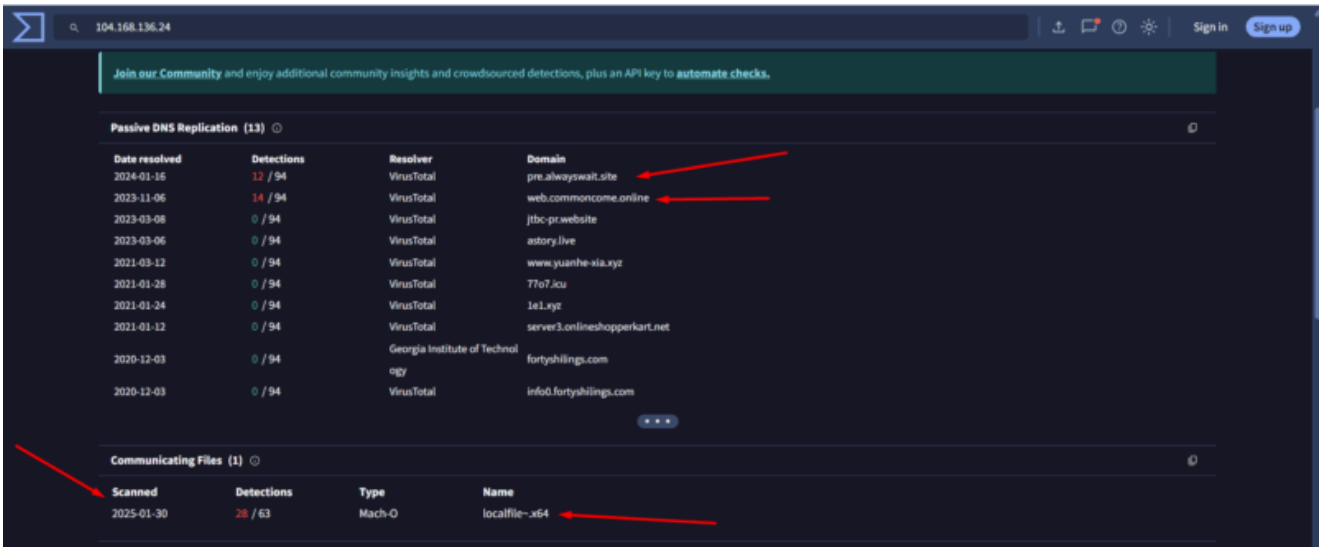
This IP resolves to **amirani.chat**

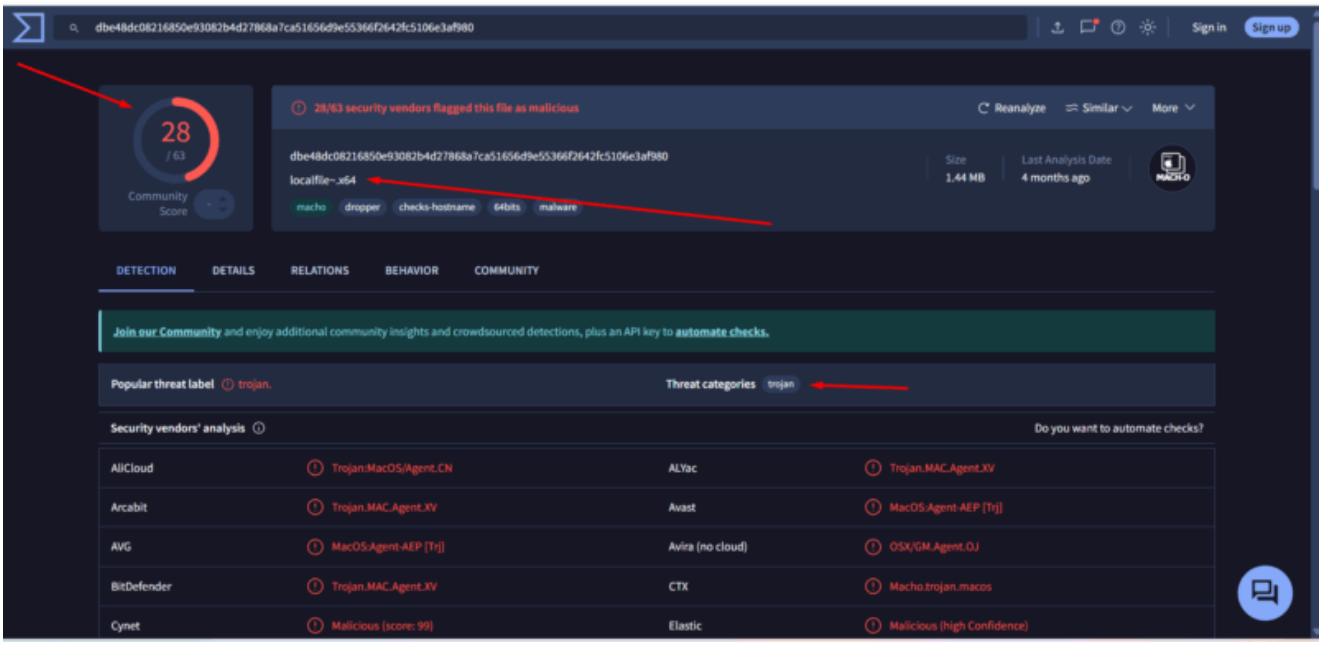


The malware has been identified communicating with a known **Command and Control (C2) server** at IP address **104[.]168[.]136[.]24**.



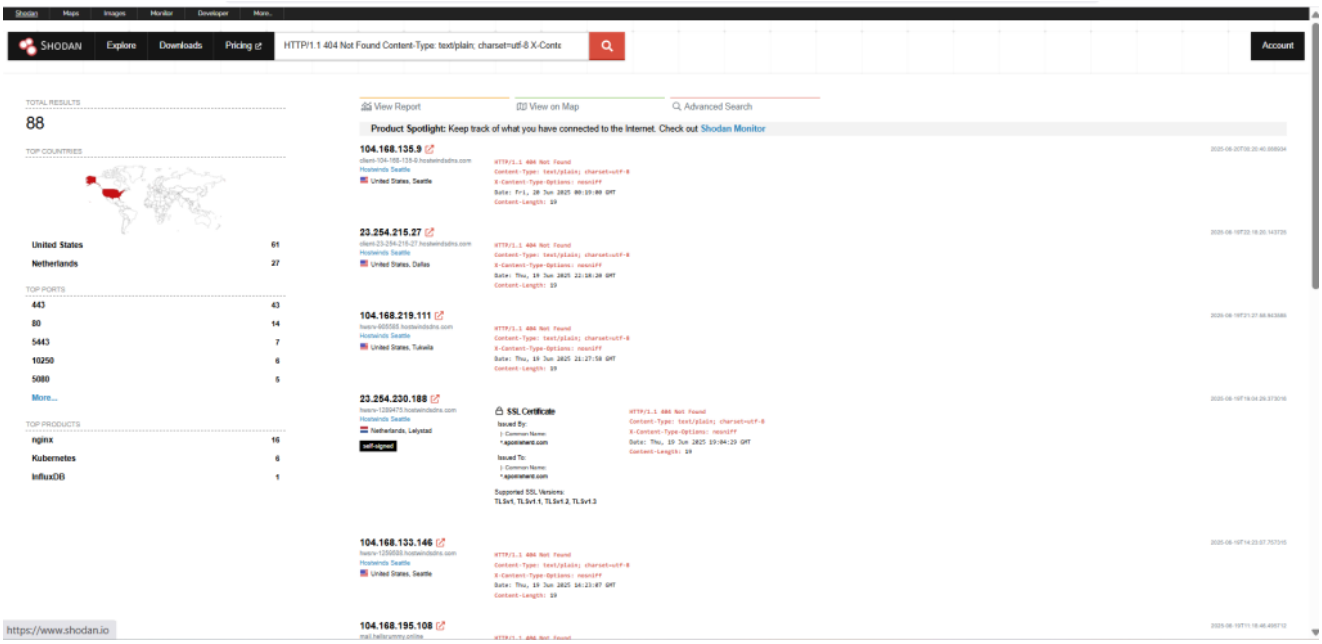
The malware sample **:** `localfile~.x64` **(SHA-256:** `dbe48dc08216850e93082b4d27868a7ca51656d9e55366f2642fc5106e3af980`) has been identified as part of the **Cosmic Rust** malware family, which is attributed to **APT38 (Bluenoroff)**—a financially motivated subgroup of North Korea's Lazarus Group. Cosmic Rust specifically targets **macOS platforms**.

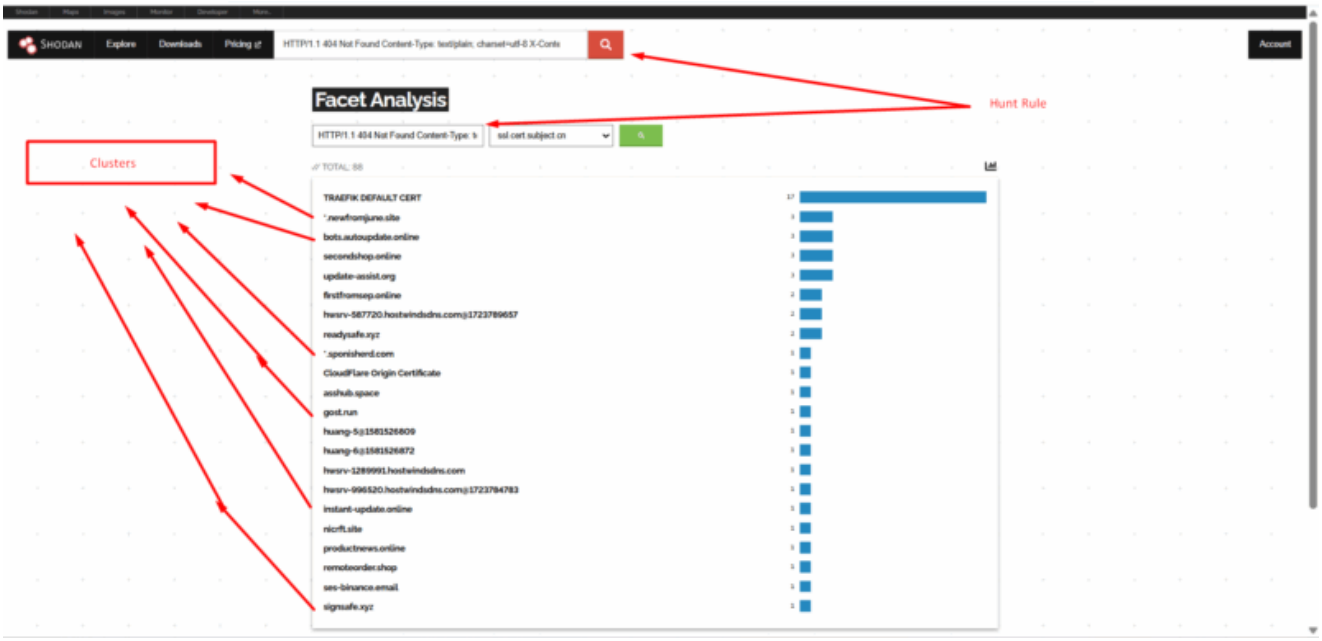




I'm preparing an additional **Shodan hunting rule** to gather more information and expand the scope of the investigation.

```
HTTP/1.1 404 Not Found Content-Type: text/plain; charset=utf-8 X-Content-Type-Options:
nosniff Content-Length: 19 org:"Hostwinds Seattle"
```





IOCS

```
140.82.20.246
156.154.132.200
198.57.247.218
192.64.119.169
198.54.117.242
104.168.136.24
firstfromsep.online
socialsuport.com
gost.run
nicrft.site
instant-update.online
huang-5@1581526809
huang-6@1581526872
hwsrv-587720.hostwindsdns.com@1723789657
```