

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

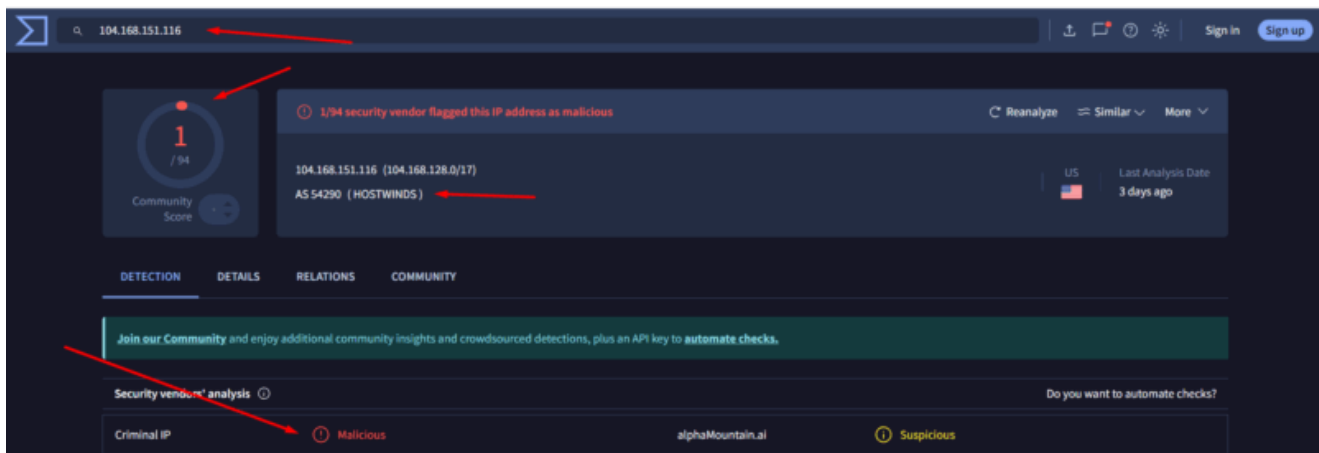
Building Shodan Search Rules for APT38 Infrastructure

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"

The screenshot shows the Shodan search engine interface. The search bar at the top contains the JARM hash: `ssl.jarm:3fd21b20d00000021c43d21b21b43d76e1f79b8645e08ae7fa8f07eb5e4202`. The search results are displayed in a table with columns for IP address, domain, and details. Red boxes highlight the following IP addresses: 104.168.151.116, 192.226.156.20, and 192.119.116.231. The details for each IP include the domain, the JARM hash, and the status code (404 Not Found). The sidebar on the left shows filters for countries (United States, Netherlands) and a map of the world.

Validating Results

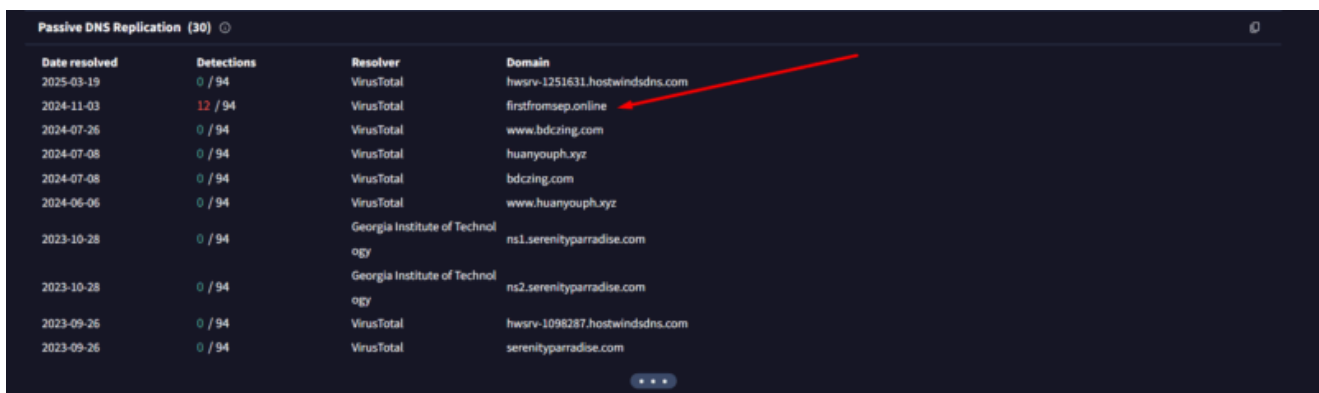
104[.]168[.]151[.]116 > 1/94 detection



The screenshot shows the VirusTotal interface for the IP address 104.168.151.116. The search bar at the top contains the IP address. On the left, a circular gauge shows a 'Community Score' of 1/94. The main header indicates that '1/94 security vendor flagged this IP address as malicious'. Below this, the IP is listed as '104.168.151.116 (104.168.128.0/17)' and 'AS 54290 (HOSTWINDS)'. The 'DETECTION' tab is active, showing a table of security vendor analyses. The table has columns for 'Security vendors' analysis, 'Criminal IP', and 'Do you want to automate checks?'. The first row shows 'Malicious' from 'alphaMountain.ai' with a 'Suspicious' status.

Security vendors' analysis	Criminal IP	Do you want to automate checks?
Malicious	alphaMountain.ai	Suspicious

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



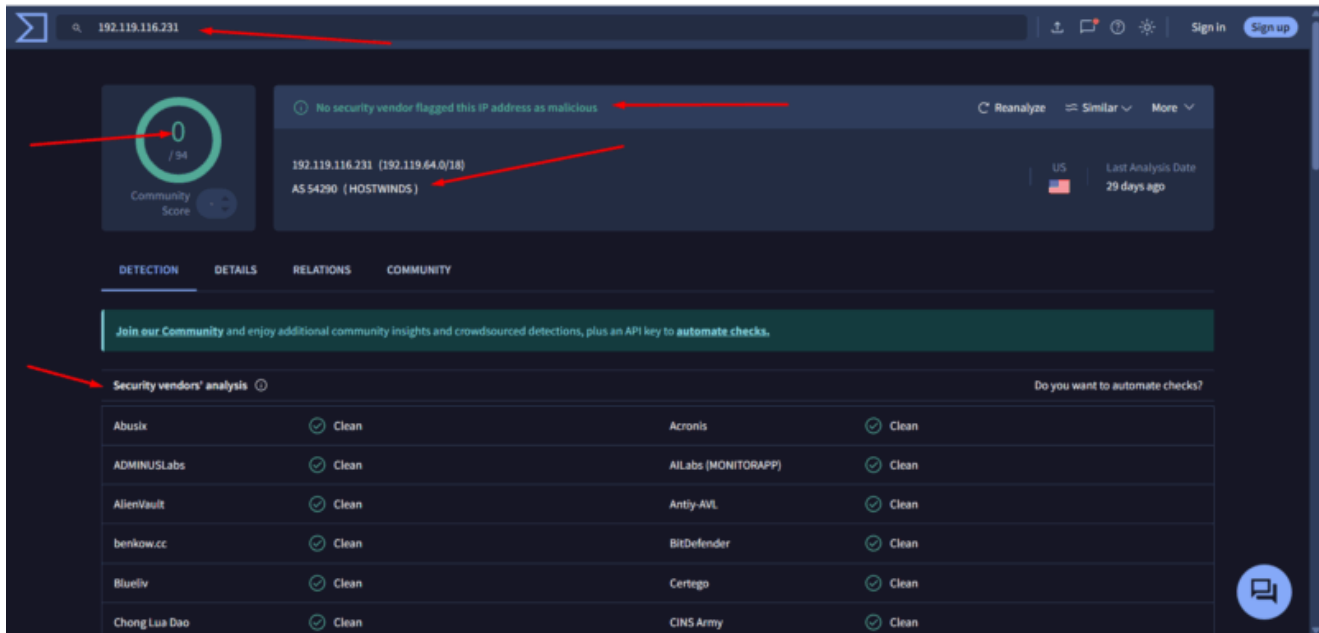
The screenshot shows a table titled 'Passive DNS Replication (30)'. The table has four columns: 'Date resolved', 'Detections', 'Resolver', and 'Domain'. The 'Detections' column shows a score of 12/94. The 'Domain' column lists various domains resolved by the IP. A red arrow points to the domain 'firstfromsep.online'.

Date resolved	Detections	Resolver	Domain
2025-03-19	0 / 94	VirusTotal	hwsrv-1251631.hostwindsdns.com
2024-11-03	12 / 94	VirusTotal	firstfromsep.online
2024-07-26	0 / 94	VirusTotal	www.bdczng.com
2024-07-08	0 / 94	VirusTotal	huanyouph.xyz
2024-07-08	0 / 94	VirusTotal	bdczng.com
2024-06-06	0 / 94	VirusTotal	www.huanyouph.xyz
2023-10-28	0 / 94	Georgia Institute of Technol ogy	ns1.serenityparadise.com
2023-10-28	0 / 94	Georgia Institute of Technol ogy	ns2.serenityparadise.com
2023-09-26	0 / 94	VirusTotal	hwsrv-1098287.hostwindsdns.com
2023-09-26	0 / 94	VirusTotal	serenityparadise.com

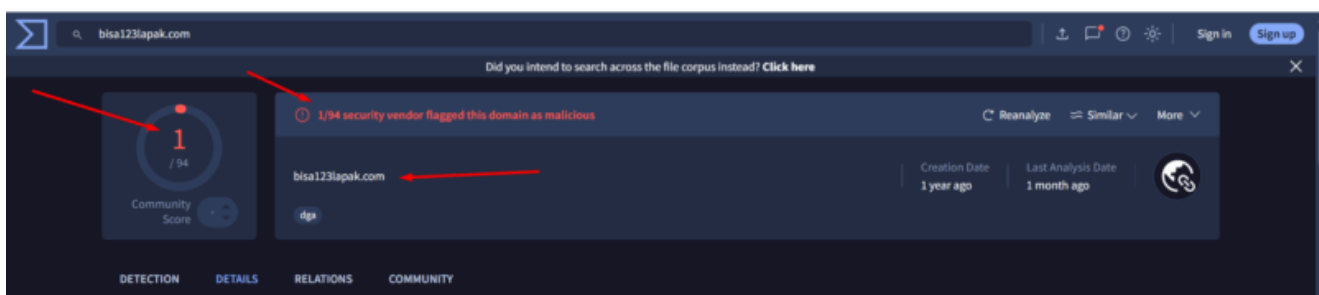
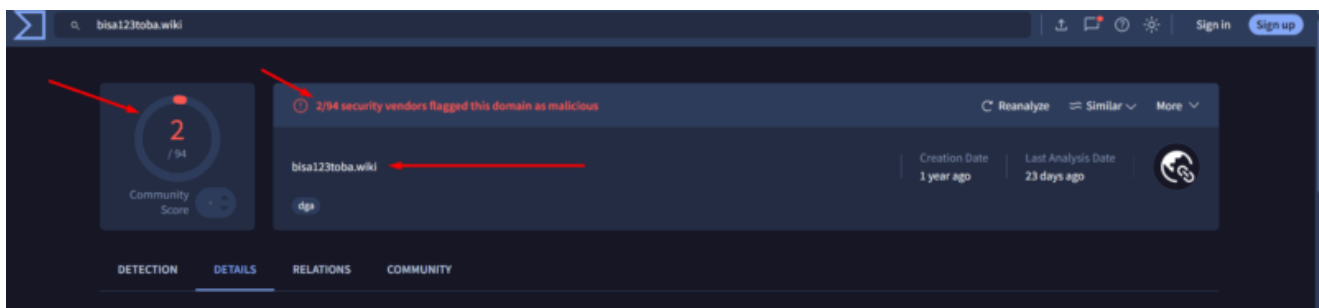
Domain Resolution Pattern

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

Search: 140.82.20.246

Community Score: 10 / 94

10/94 security vendors flagged this IP address as malicious

140.82.20.246 (140.82.0.0/18)
AS 20473 (AS-VULTR)

US | Last Analysis Date: 21 days ago

DETECTION DETAILS RELATIONS COMMUNITY 7

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Vendor	Detection	Vendor	Detection
alphaMountain.ai	Malicious	AlphaSOC	Malware
BitDefender	Malware	CyRadar	Malicious
ESET	Malware	Forcepoint ThreatSeeker	Malicious
G-Data	Malware	Lionic	Malicious
SOCRadar	Malware	Sophos	Malware
ArcSight Threat Intelligence	Suspicious	Abusix	Clean

Do you want to automate checks?

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

Search: 156.154.132.200

Did you intend to search across the file corpus instead? [Click here](#)

Community Score: 2 / 94

2/94 security vendors flagged this IP address as malicious

156.154.132.200 (156.154.132.0/23)
AS 12008 (SECURITYSERVICES)

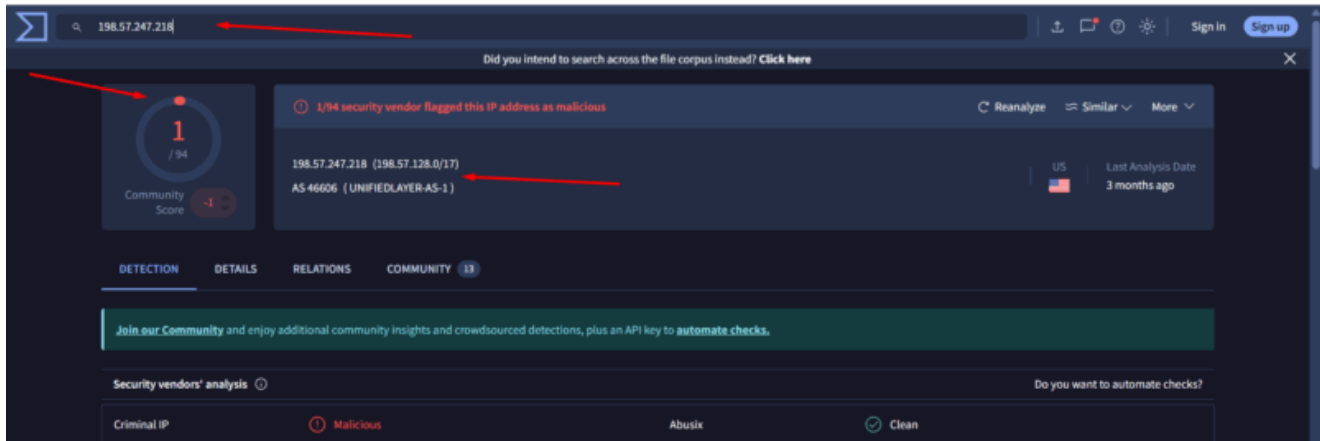
US | Last Analysis Date: 20 days ago

DETECTION DETAILS RELATIONS COMMUNITY 22

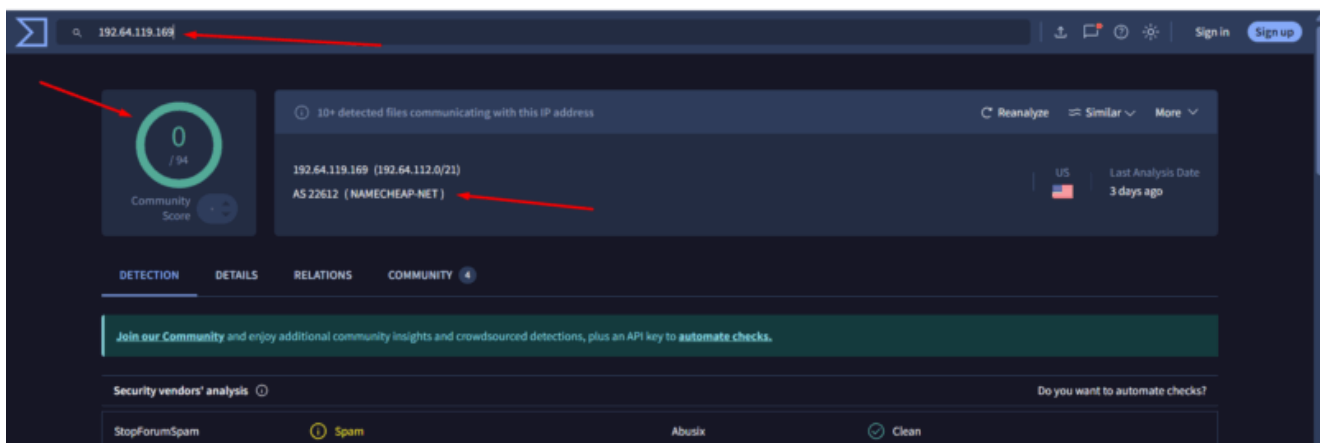
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Crowdsourced context

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	kyuxznkh13qb2Induqh6deui.exe
2023-10-19	55 / 72	Win32 EXE	f3gfm05bbyklyqciloilhtcvz.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	SS8BZURGH.EXE
2025-06-15	51 / 71	Win32 EXE	cygtuhyd.exe
2020-07-06	60 / 70	Win32 EXE	qkdbaunsnkpl.exe
2023-10-19	56 / 72	Win32 EXE	pkm7uoflywqpdgfm7iaopssif.exe

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

Did you intend to search across the file corpus instead? [Click here](#)

2 / 94
Community Score

2/94 security vendors flagged this IP address as malicious

198.54.117.242 (198.54.112.0/20)
AS 22612 (NAMECHEAP-NET)

US | Last Analysis Date: 8 hours ago

DETECTION DETAILS RELATIONS COMMUNITY 43

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Crowdsourced context

HIGH 0 MEDIUM 0 LOW 1 INFO 0 SUCCESS 0

⚠️ 8FPH23-00871-01 [Fraude] [Phishing] - according to source ArcSight Threat Intelligence - 1 year ago
Host VirusTotal Link: <https://www.virustotal.com/gui/ip-address/198.54.117.242/detection> Abuse IPDB Link: <https://www.abuseipdb.com/check/198.54.117.242> Postal Code: 90064

Security vendors' analysis

ESET	Phishing	SOCradar	Malware
alphaMountain.ai	Suspicious	Abusix	Clean

Do you want to automate checks?

This IP resolves to **amirani.chat**

amirani.chat

1 / 94
Community Score

1/94 security vendor flagged this domain as malicious

amirani.chat

Creation Date: 2 months ago | Last Analysis Date: 17 hours ago

DETECTION DETAILS RELATIONS COMMUNITY

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

Did you intend to search across the file corpus instead? [Click here](#)

2 / 94
Community Score

2/94 security vendors flagged this IP address as malicious

104.168.136.24 (104.168.128.0/17)
AS 54290 (HOSTWINDS)

US Last Analysis Date
20 days ago

DETECTION DETAILS RELATIONS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Vendor	Result	Vendor	Result
Fortinet	Malware	SOCRadar	Malware
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	Antiy-AVL	Clean
benkow.cc	Clean	BitDefender	Clean
Blueliv	Clean	Certigo	Clean

Do you want to automate checks?

The malware sample : **localfile~.x64** (SHA-256: **db4e48dc08216850e93082b4d27868a7ca51656d9e55366f2642fc5106e3af980**) 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**.

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Passive DNS Replication (13)

Date resolved	Detections	Resolver	Domain
2024-01-16	12 / 94	VirusTotal	pre.alwayswait.site
2023-11-06	14 / 94	VirusTotal	web.commoncome.online
2023-03-08	0 / 94	VirusTotal	jfbic-pr.website
2023-03-06	0 / 94	VirusTotal	astory.live
2021-03-12	0 / 94	VirusTotal	www.yuanhe-xia.xyz
2021-01-28	0 / 94	VirusTotal	77o7.icu
2021-01-24	0 / 94	VirusTotal	1e1.xyz
2021-01-12	0 / 94	VirusTotal	server3.onlineshopperkart.net
2020-12-03	0 / 94	Georgia Institute of Technol	fortyshillings.com
2020-12-03	0 / 94	egy	info6.fortyshillings.com

Communicating Files (1)

Scanned	Detections	Type	Name
2025-01-30	28 / 63	Mach-O	localfile~.x64

dbef48dc08216850e93082b4d27868a7ca51656d9e55366f2642fc5106e3af980

28/53 security vendors flagged this file as malicious

Size: 1.44 MB | Last Analysis Date: 4 months ago

localfile-x64

malicious | dropper | checks-hostname | 64bits | malware

Popular threat label: trojan

Threat categories: trojan

Security vendors' analysis

Vendor	Detection	Confidence	
AllCloud	Trojan.MacOS.Agent.CN	ALYac	Trojan.MAC.Agent.XV
Arcabit	Trojan.MAC.Agent.XV	Avast	MacOS.Agent-AEP [Trj]
AVG	MacOS.Agent-AEP [Trj]	Avira (no cloud)	OSX/GM.Agent.OJ
BitDefender	Trojan.MAC.Agent.XV	CTX	Machos.trojan.macos
Cyren	Malicious (score: 99)	Elastic	Malicious (high Confidence)

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"

SHODAN

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

TOTAL RESULTS: 88

TOP COUNTRIES

Country	Count
United States	61
Netherlands	27

TOP PORTS

Port	Count
443	43
80	14
5443	7
10250	6
5080	5

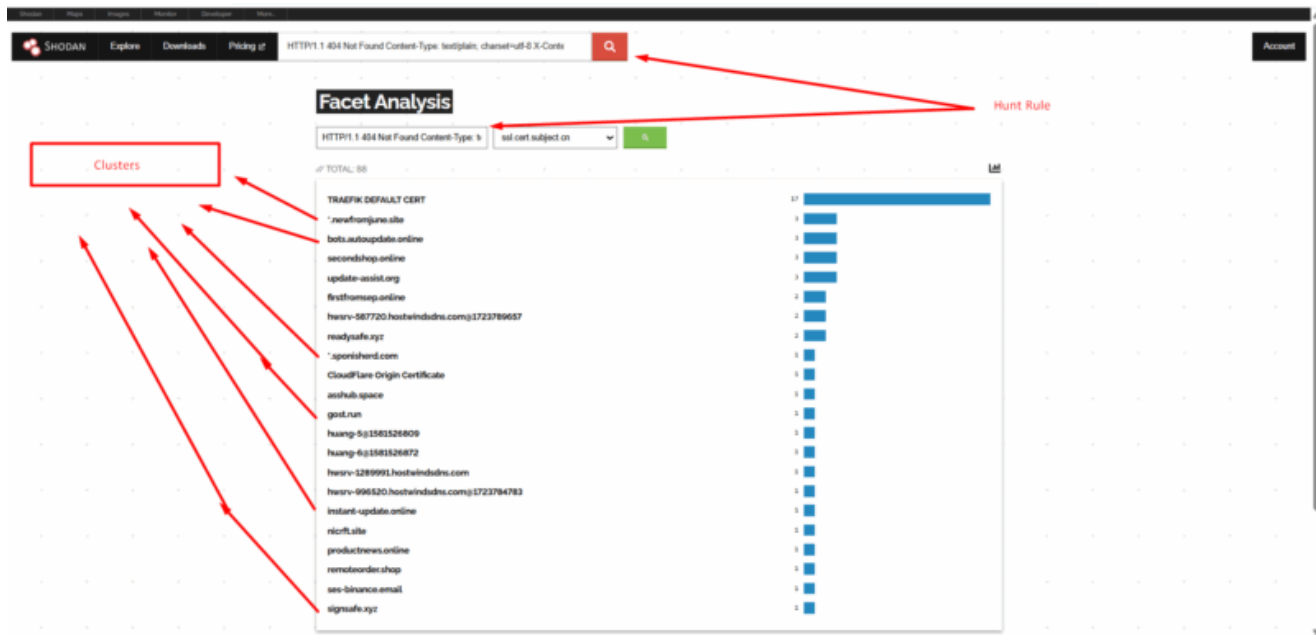
TOP PRODUCTS

Product	Count
nginx	15
Kubernetes	6
InfluxDB	1

Product Spotlight: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

IP Address	Domain	Location	HTTP Status	Content-Type	Content-Length	Organization
104.168.135.9	client-104-168-135-9.hostwinds.com	United States, Seattle	HTTP/1.1 404 Not Found	text/plain; charset=utf-8	19	Hostwinds Seattle
23.254.215.27	client-23-254-215-27.hostwinds.com	United States, Dallas	HTTP/1.1 404 Not Found	text/plain; charset=utf-8	19	Hostwinds Dallas
104.168.219.111	client-104-168-219-111.hostwinds.com	United States, Tulsa	HTTP/1.1 404 Not Found	text/plain; charset=utf-8	19	Hostwinds Tulsa
23.254.230.188	client-23-254-230-188.hostwinds.com	Netherlands, Lelystad	HTTP/1.1 404 Not Found	text/plain; charset=utf-8	19	Hostwinds Lelystad
104.168.133.146	client-104-168-133-146.hostwinds.com	United States, Seattle	HTTP/1.1 404 Not Found	text/plain; charset=utf-8	19	Hostwinds Seattle
104.168.195.108	client-104-168-195-108.hostwinds.com	United States, Seattle	HTTP/1.1 404 Not Found	text/plain; charset=utf-8	19	Hostwinds Seattle

<https://www.shodan.io>



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