Rekoobe Backdoor Discovered in Open Directory, Possibly Targeting TradingView Users

hunt.io/blog/rekoobe-backdoor-discovered-in-open-directory-possibly-targeting-tradingview-users

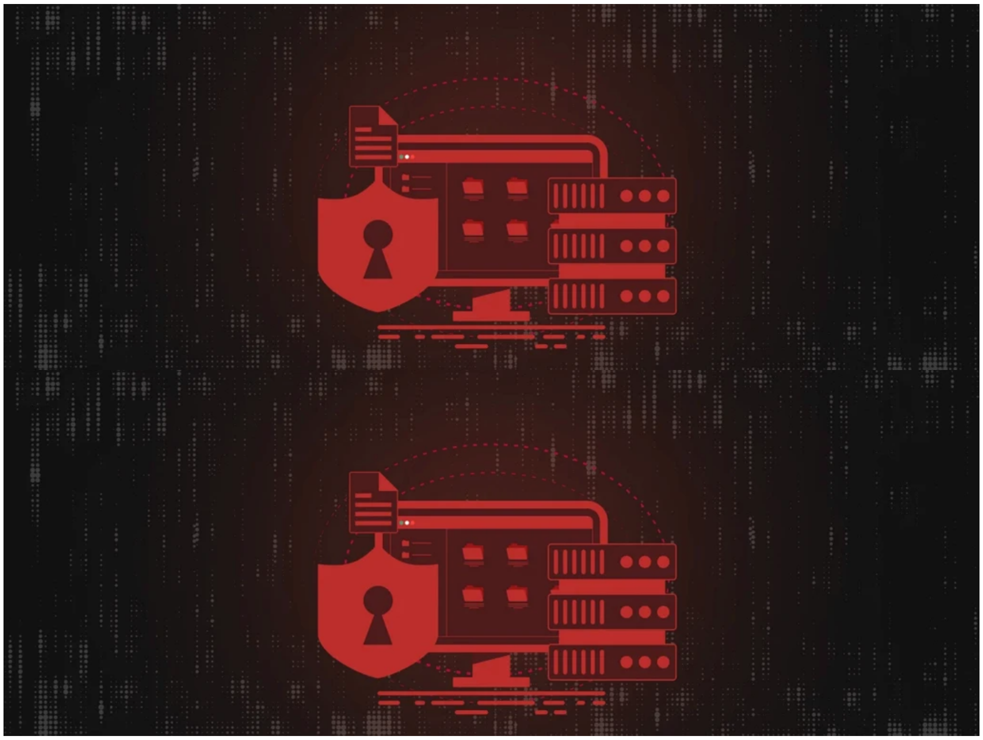


TABLE OF CONTENTS

Introduction

Rekoobe is a versatile backdoor previously deployed by **APT31**, also known as Zirconium, amongst other adversaries involved in cyber espionage and data theft. With code partially based on the publicly available Tiny SHell, the malware has evolved to use enhanced encryption techniques and unique command-and-control configurations to hinder analysis and evade detection.

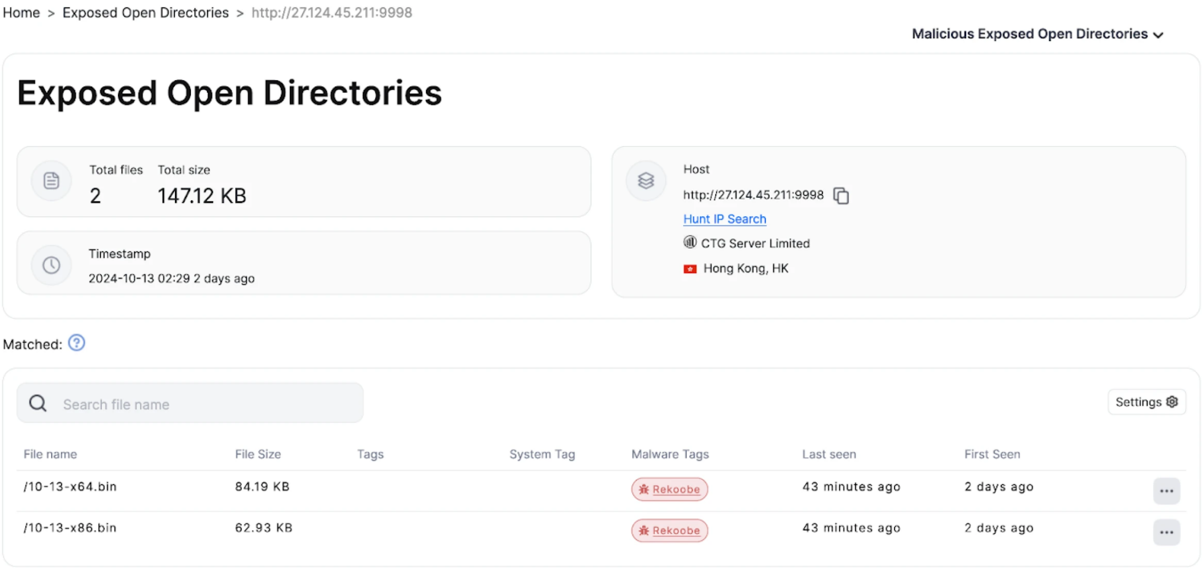
While researching open directories, we uncovered two Rekoobe samples, prompting a deeper investigation into the hosting IP. Upon further analysis, we discovered a handful of domains resembling TradingView, a widely used platform for worldwide charting, trading, and sharing financial insights traders use.

These suspicious domains suggest a potential interest in targeting the site's community. By pivoting on shared SSH keys, we identified additional infrastructure potentially linked to this campaign and another open directory.

Discovery of the Open Directory & Malware

We found an open directory at **27.124.45[.]146:9998** running Python version 3.12.4, SimpleHTTP 0.6, which exposed two binaries: 10-13-x64.bin and 10-13x86.bin. Both files were identified as Rekoobe by Hatching Triage, and their SHA-256 hashes are as follows:

- **10-13-x64.bin**: a1c0b48199e8a47fe50c4097d86e5f43a1a1c9a9c1f7f3606ffa0d45bb4a2eb3 (renamed na.elf in Triage)
- **10-13-x86.bin**: 28382231cbfe3bf7827c1a874b3d7f18717020ced516b747a2a1bb7598eabe0b



Home > Exposed Open Directories > http://27.124.45.211:9998

Malicious Exposed Open Directories

Exposed Open Directories

Total files 2 | Total size 147.12 KB

Timestamp 2024-10-13 02:29 2 days ago

Host http://27.124.45.211:9998
Hunt IP Search
CTG Server Limited
Hong Kong, HK

Matched:

Search file name | Settings

File name	File Size	Tags	System Tag	Malware Tags	Last seen	First Seen
/10-13-x64.bin	84.19 KB			Rekoobe	43 minutes ago	2 days ago
/10-13-x86.bin	62.93 KB			Rekoobe	43 minutes ago	2 days ago

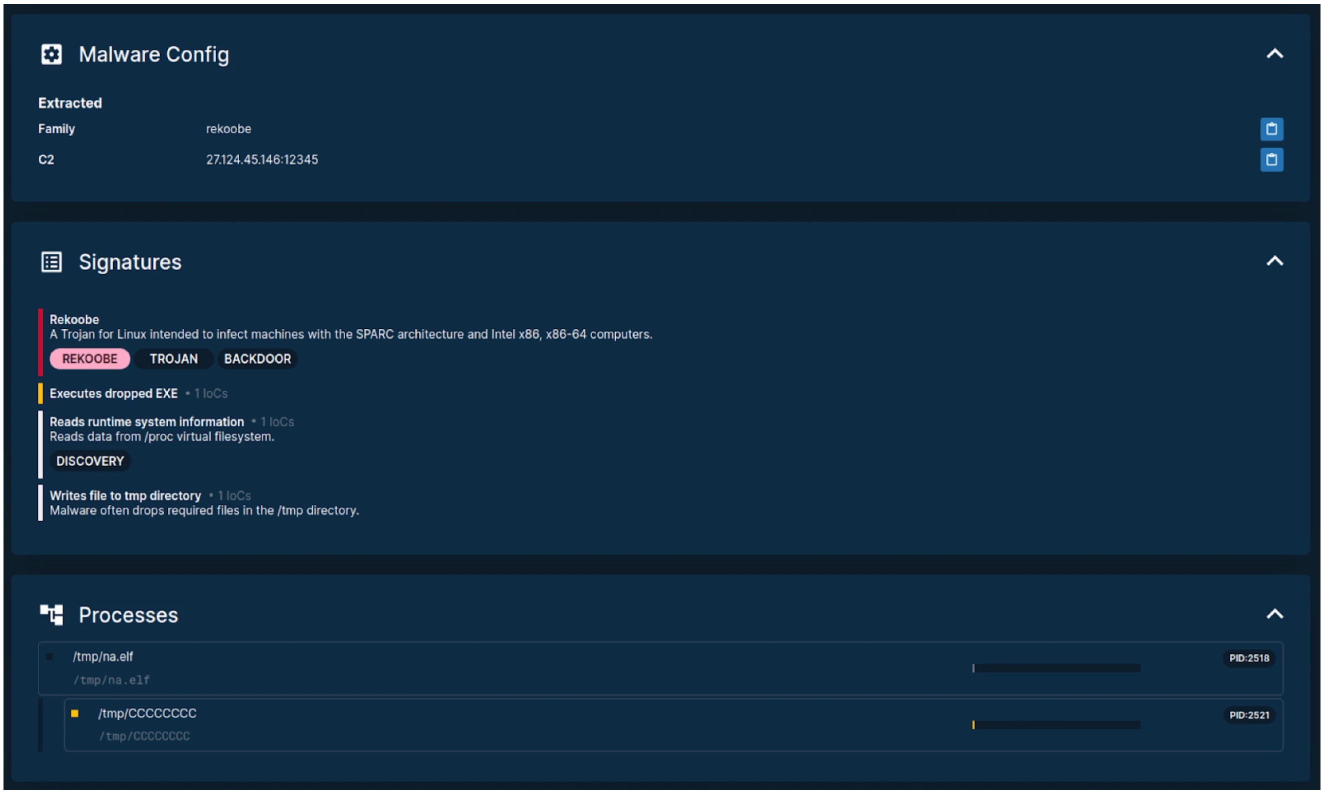
Figure 1: Open directory page for 27.124.45[.]146

During dynamic analysis, both binaries attempted to communicate with the same IP address hosting the open directory, specifically targeting port **12345**. The naming convention of the files, which follows a month-day-architecture format, is consistent with other Rekoobe samples we've seen in open directories.

In our analysis of na.elf, we observed behavior closely resembling that identified by AhnLab as "NoodRAT" and Trend Micro as "Noodle RAT." Specifically, the file changes its process name and copies itself to the **/tmp/CCCCCCCC** directory, where it executes from.

However, it's important to note that this alone does not definitively confirm that the binaries in this case are NoodRAT or Noodle RAT. The similarities in behavior could indicate the work of a copycat, but additional analysis would be required to make a conclusive attribution.

Figure 2 depicts the process tree of na.elf as seen in the Hatching Triage analysis.



Malware Config

Extracted

Family	rekoobe
C2	27.124.45.146:12345

Signatures

Rekoobe
A Trojan for Linux intended to infect machines with the SPARC architecture and Intel x86, x86-64 computers.
REKOOBE TROJAN BACKDOOR

Executes dropped EXE • 1 IoCs

Reads runtime system information • 1 IoCs
Reads data from /proc virtual filesystem.
DISCOVERY

Writes file to tmp directory • 1 IoCs
Malware often drops required files in the /tmp directory.

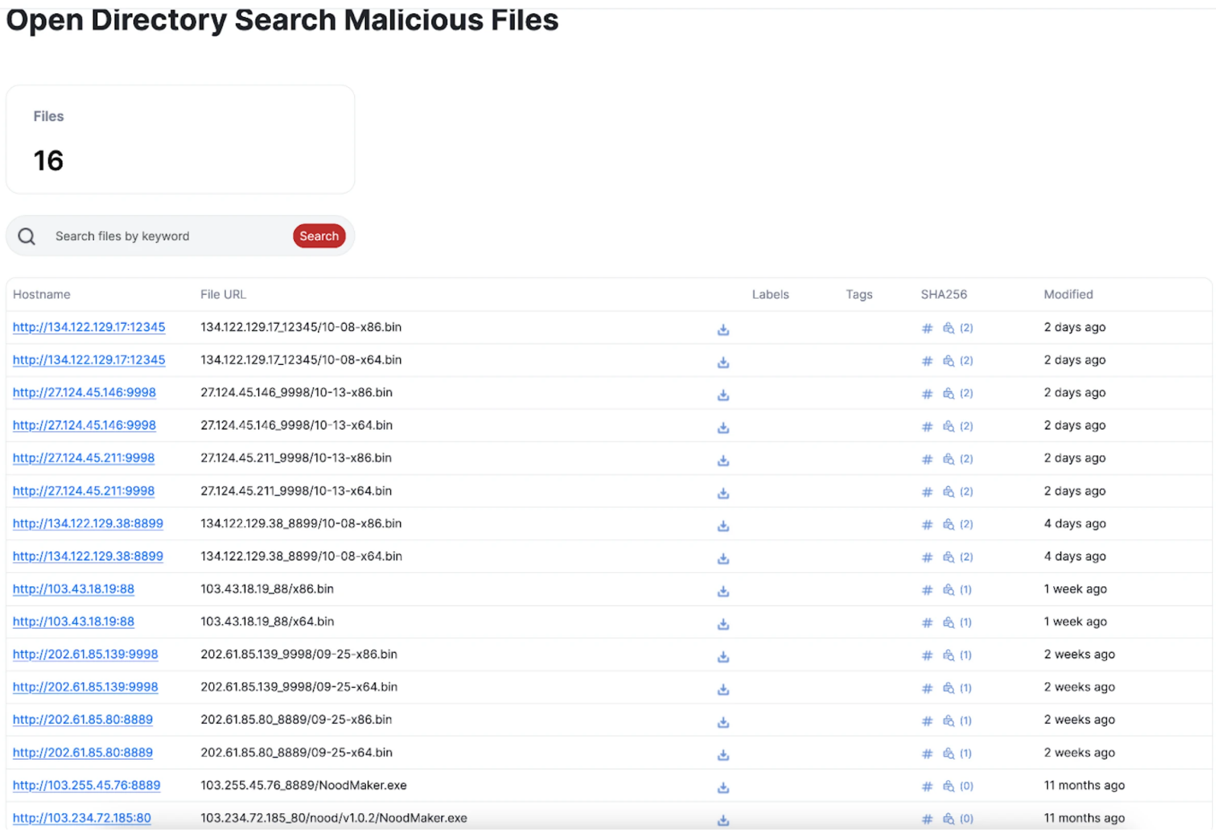
Processes

/tmp/na.elf
/tmp/na.elf
PID:2518

/tmp/CCCCCCCC
/tmp/CCCCCCCC
PID:2521

Figure 2: Triage analysis of na.elf processes

By clicking the 'Rekoobe' tag, users can easily find additional open directories hosting Rekoobe samples, as shown in Figure 1.



Open Directory Search Malicious Files

Files

16

Search files by keyword

Hostname	File URL	Labels	Tags	SHA256	Modified
http://134.122.129.17:12345	134.122.129.17_12345/10-08-x86.bin			# (2)	2 days ago
http://134.122.129.17:12345	134.122.129.17_12345/10-08-x64.bin			# (2)	2 days ago
http://27.124.45.146:9998	27.124.45.146_9998/10-13-x86.bin			# (2)	2 days ago
http://27.124.45.146:9998	27.124.45.146_9998/10-13-x64.bin			# (2)	2 days ago
http://27.124.45.211:9998	27.124.45.211_9998/10-13-x86.bin			# (2)	2 days ago
http://27.124.45.211:9998	27.124.45.211_9998/10-13-x64.bin			# (2)	2 days ago
http://134.122.129.38:8899	134.122.129.38_8899/10-08-x86.bin			# (2)	4 days ago
http://134.122.129.38:8899	134.122.129.38_8899/10-08-x64.bin			# (2)	4 days ago
http://103.43.18.19:88	103.43.18.19_88/x86.bin			# (1)	1 week ago
http://103.43.18.19:88	103.43.18.19_88/x64.bin			# (1)	1 week ago
http://202.61.85.139:9998	202.61.85.139_9998/09-25-x86.bin			# (1)	2 weeks ago
http://202.61.85.139:9998	202.61.85.139_9998/09-25-x64.bin			# (1)	2 weeks ago
http://202.61.85.80:8889	202.61.85.80_8889/09-25-x86.bin			# (1)	2 weeks ago
http://202.61.85.80:8889	202.61.85.80_8889/09-25-x64.bin			# (1)	2 weeks ago
http://103.255.45.76:8889	103.255.45.76_8889/NoodMaker.exe			# (0)	11 months ago
http://103.234.72.185:80	103.234.72.185_80/nood/v1.0.2/NoodMaker.exe			# (0)	11 months ago

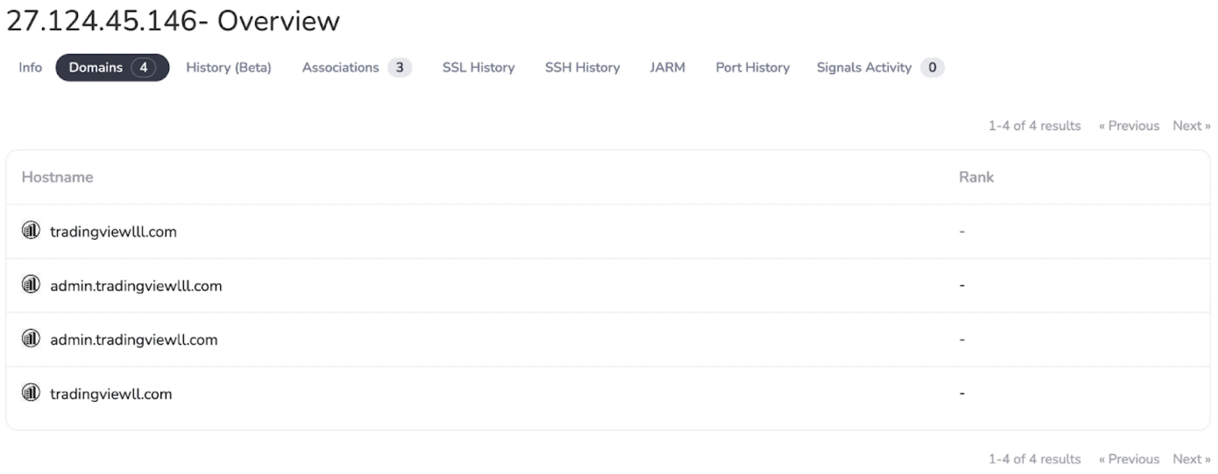
Figure 3: Results of clicking the Rekoobe tag to find additional open directories hosting the malware

Infrastructure Analysis: TradingView Lookalike Domains and Hosting Connections

During our investigation into the IP address hosting the two backdoor files, we discovered several domains closely mimicking the legitimate TradingView site. These domains show slight variations in spelling that are indicative of typosquatting attacks:

- tradingviewlll[.]com
- admin.tradingviewlll[.]com
- tradingviewll[.]com
- admin.tradingviewll[.].com

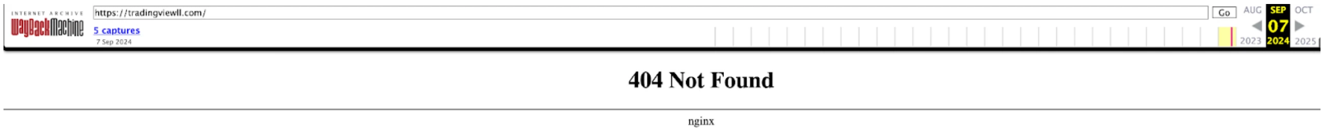
These minor changes, such as the addition of an extra "l" in **tradingviewll[.]com** and **tradingviewlll[.]com**, could easily be missed by users, making them practical for phishing or other social engineering operations.


27.124.45.146- Overview

Hostname	Rank
tradingviewlll.com	-
admin.tradingviewlll.com	-
admin.tradingviewll.com	-
tradingviewll.com	-

Figure 4: Domain overview showing typosquatting domains targeting TradingView

Unfortunately, we could not capture any active web pages associated with these domains created earlier this year. According to the Wayback Machine, both domains returned a standard 404 Not Found Nginx response on 07 September this year. This means any web page may not have been fully deployed or is in a consistently inactive state.



404 Not Found

nginx

Figure 5: Wayback machine results for tradingviewll.com

While we can't be sure these domains were used in this campaign, they represent an interesting infrastructure overlap when viewed alongside the presence of the Rekoobe backdoor. This could suggest an attempt to exploit financial platforms and their user base, as many of these systems rely on Linux.

Expanded Network Findings

Continuing our deep dive into **27.124.45[.]146**, we found three IP addresses linked by shared SSH keys, suggesting a connection to our original server. This relationship was uncovered using the Hunt's Association tab, as shown in Figure 6.

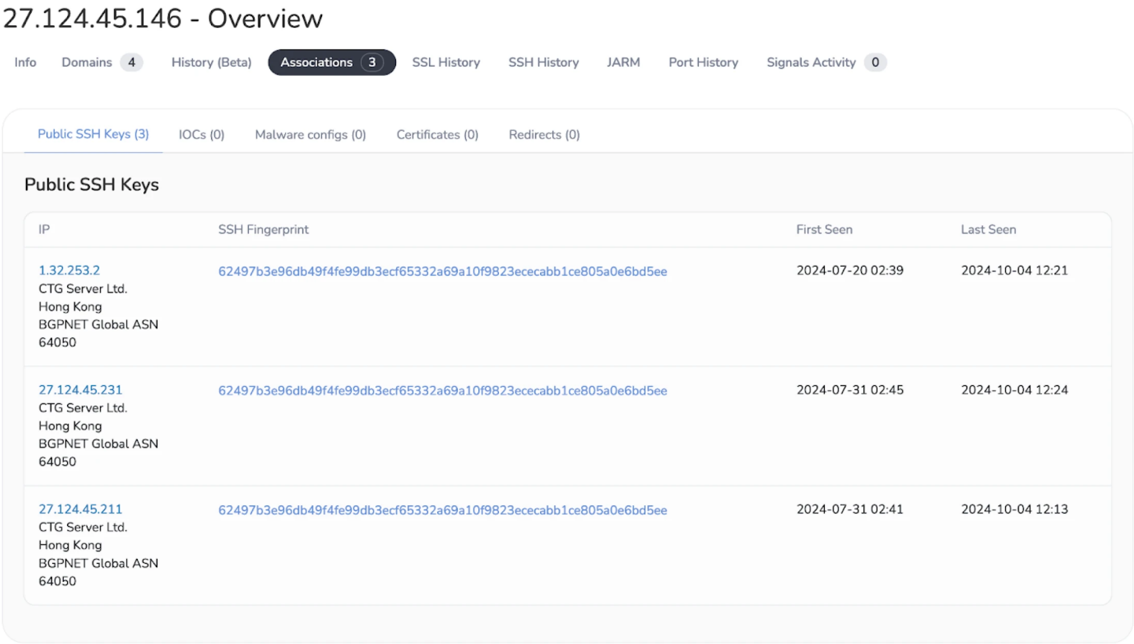
The IPs include:

- 27.124.45[.]231
- 1.32.253[.]2

- 27.124.45[.]211

The SSH key (fingerprint: **62497b3e96db49f4fe99db3ecf65332a69a10f9823ececabb1ce805a0e6bd5ee**) for all three was first observed by our scanners between late July and early August, and were last active on 04 October.

Like the original open directory, these servers are also hosted in Hong Kong, indicating they are likely part of the same operational setup.



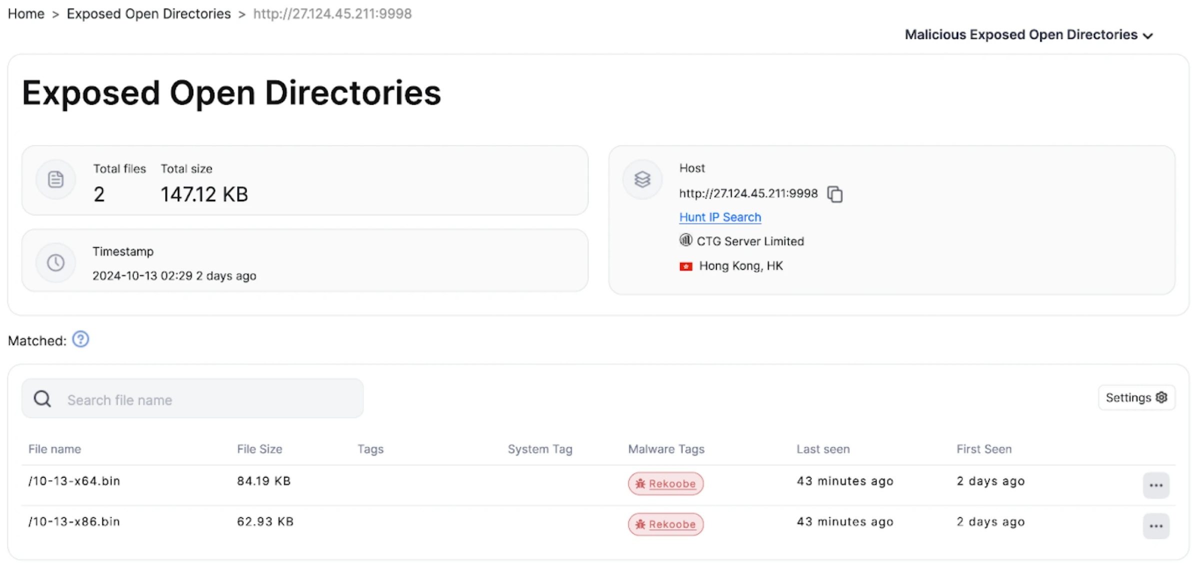
27.124.45.146 - Overview

Public SSH Keys

IP	SSH Fingerprint	First Seen	Last Seen
1.32.253.2 CTG Server Ltd. Hong Kong BGPNET Global ASN 64050	62497b3e96db49f4fe99db3ecf65332a69a10f9823ececabb1ce805a0e6bd5ee	2024-07-20 02:39	2024-10-04 12:21
27.124.45.231 CTG Server Ltd. Hong Kong BGPNET Global ASN 64050	62497b3e96db49f4fe99db3ecf65332a69a10f9823ececabb1ce805a0e6bd5ee	2024-07-31 02:45	2024-10-04 12:24
27.124.45.211 CTG Server Ltd. Hong Kong BGPNET Global ASN 64050	62497b3e96db49f4fe99db3ecf65332a69a10f9823ececabb1ce805a0e6bd5ee	2024-07-31 02:41	2024-10-04 12:13

Figure 6: The Associations Tab in Hunt displays associated IPs that can be pivoted to enhance investigations

Among the IPs identified, **27.124.45[.]211** stood out as it also hosts an open directory (on the same port) running the same Python and SimpleHTTP versions and the duplicate Rekoobe-detected files as the original server ending in .146.


Home > Exposed Open Directories > http://27.124.45.211:9998
Malicious Exposed Open Directories
Hunt IP Search
Search file name
Settings

Exposed Open Directories

Total files: 2

Total size: 147.12 KB

Timestamp: 2024-10-13 02:29 2 days ago

Host: http://27.124.45.211:9998

CTG Server Limited

Hong Kong, HK

Matched:

File name	File Size	Tags	System Tag	Malware Tags	Last seen	First Seen
/10-13-x64.bin	84.19 KB			Rekoobe	43 minutes ago	2 days ago
/10-13-x86.bin	62.93 KB			Rekoobe	43 minutes ago	2 days ago

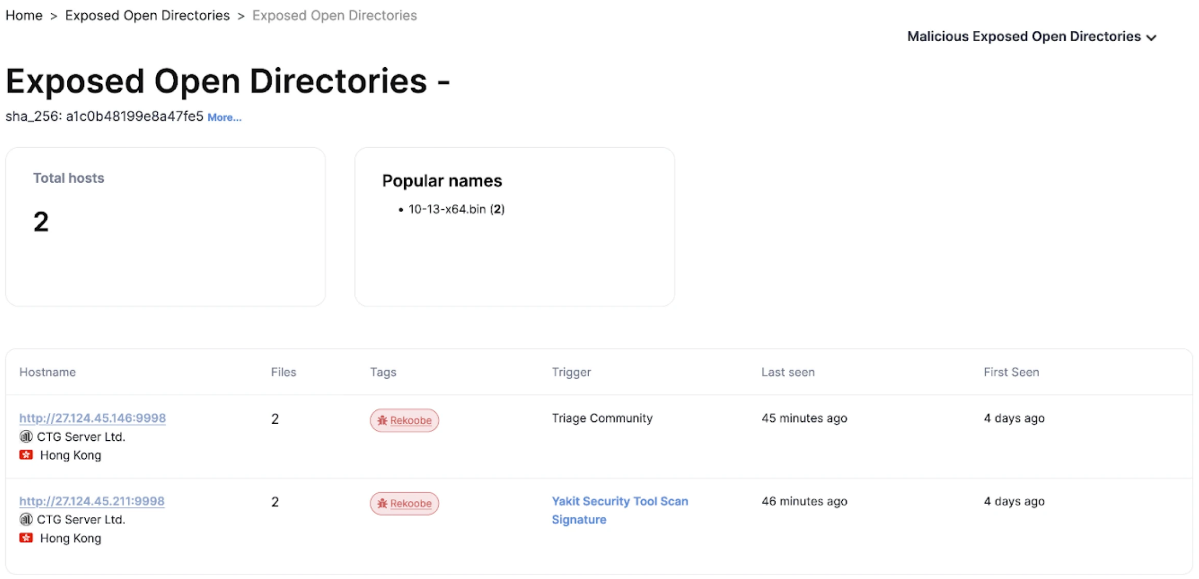
Figure 7: Open directory contents for 27.124.45[.]211:9998

Clicking on the button containing the three dots next to the files opens a menu for further actions, including searching by SHA-256 to identify other locations where the file is hosted. As shown in Figure 8, this search confirms that the two IPs--.146 and .211--are the only servers hosting these Rekoobe samples. Interestingly, our scanners also detected the **Yakit Security Tool** on 27.124.45[.]211

We previously wrote about Yakit, an all-in-one cybersecurity application that integrates tools like Nuclei and includes features such as man-in-the-middle (MiTM) interception and web fuzzing.

Primarily designed for legitimate security work by red teamers and researchers, Yakit's presence alongside Rekoobe and the typosquatting domains raises concerns about how this setup could be leveraged for malicious purposes.

Combining these elements points to activity that merits further investigation to understand the potential risks involved fully.



Home > Exposed Open Directories > Exposed Open Directories
Malicious Exposed Open Directories

Exposed Open Directories -

sha_256: a1c0b48199e8a47fe5 More...

Total hosts

2

Popular names

- 10-13-x64.bin (2)

Hostname	Files	Tags	Trigger	Last seen	First Seen
http://27.124.45.146:9998 CTG Server Ltd. Hong Kong	2	Rekoobe	Triage Community	45 minutes ago	4 days ago
http://27.124.45.211:9998 CTG Server Ltd. Hong Kong	2	Rekoobe	Yakit Security Tool Scan Signature	46 minutes ago	4 days ago

Figure 8: Results of SHA-256 search across all open directories for similar files

Conclusion

In this blog post, we explored how the discovery of the Rekoobe backdoor in an open directory revealed a broader network of potentially malicious infrastructure, lookalike domains mimicking TradingView, and additional servers linked via shared SSH keys.

Hunting for malware in open directories can yield valuable insights into the servers behind attack campaigns. By leveraging tools like Hunt, security teams can uncover hidden threats and expand their visibility into attacker infrastructure.

Network Observables

IP Address	ASN	Domain(s)	Host Country	Notes
27.124.45[.]146	CTG Server Limited	tradingviewlll[.]com admin.tradingviewlll[.]]com tradingviewll[.]com admin.tradingviewll[.]]com	HK	Open directory containing two (2) Rekoobe samples.

IP Address	ASN	Domain(s)	Host Country	Notes
1.32.253[.]2	BGPNET Global ASN	70332[.]club 390698[.]ru 953388[.]cc 836833[.]cc 734439[.]com 56204[.]sx 49246[.]sx 836833[.]cc 94783[.]club 734439[.]com 963388[.]cc	HK	IP seen sharing SSH keys with 27.124.45[.]146 from 2024-07-20 - 2024-10-04
27.124.45[.]231	CTG Server Limited	N/A	HK	Shared SSH keys from 2024-07-31 - 2024-10-04
27.124.45[.]211	CTG Server Limited	N/A	HK	Shared SSH keys from 2024-07-31 - 2024-10-04

File Information

File Name	SHA-256
10-13-x64.bin	a1c0b48199e8a47fe50c4097d86e5f43a1a1c9a9c1f7f3606ffa0d45bb4a2eb3
10-13-x86.bin	28382231cbfe3bf7827c1a874b3d7f18717020ced516b747a2a1bb7598eabe0b

TABLE OF CONTENTS

Introduction

Rekoobe is a versatile backdoor previously deployed by **APT31**, also known as Zirconium, amongst other adversaries involved in cyber espionage and data theft. With code partially based on the publicly available Tiny SHell, the malware has evolved to use enhanced encryption techniques and unique command-and-control configurations to hinder analysis and evade detection.

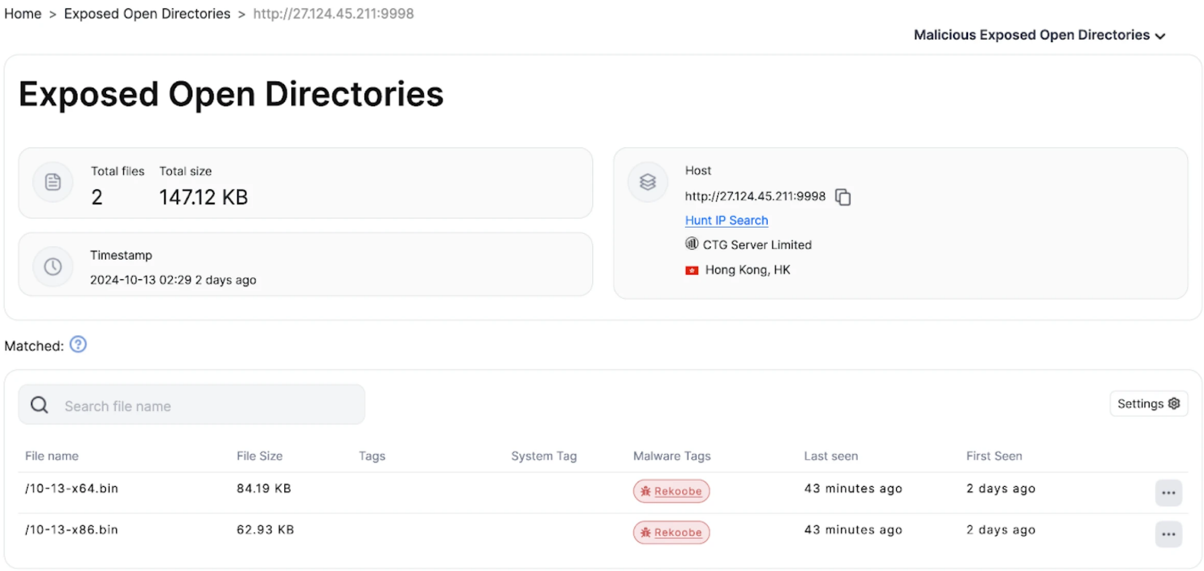
While researching open directories, we uncovered two Rekoobe samples, prompting a deeper investigation into the hosting IP. Upon further analysis, we discovered a handful of domains resembling TradingView, a widely used platform for worldwide charting, trading, and sharing financial insights traders use.

These suspicious domains suggest a potential interest in targeting the site's community. By pivoting on shared SSH keys, we identified additional infrastructure potentially linked to this campaign and another open directory.

Discovery of the Open Directory & Malware

We found an open directory at **27.124.45[.]146:9998** running Python version 3.12.4, SimpleHTTP 0.6, which exposed two binaries: 10-13-x64.bin and 10-13x86.bin. Both files were identified as Rekoobe by Hatching Triage, and their SHA-256 hashes are as follows:

- **10-13-x64.bin**: a1c0b48199e8a47fe50c4097d86e5f43a1a1c9a9c1f7f3606ffa0d45bb4a2eb3 (renamed na.elf in Triage)
- **10-13-x86.bin**: 28382231cbfe3bf7827c1a874b3d7f18717020ced516b747a2a1bb7598eabe0b



Home > Exposed Open Directories > http://27.124.45.211:9998

Malicious Exposed Open Directories

Exposed Open Directories

Total files: 2
Total size: 147.12 KB

Timestamp: 2024-10-13 02:29 2 days ago

Host: http://27.124.45.211:9998
Hunt IP Search
CTG Server Limited
Hong Kong, HK

Matched:

Search file name

Settings

File name	File Size	Tags	System Tag	Malware Tags	Last seen	First Seen
/10-13-x64.bin	84.19 KB			Rekoobe	43 minutes ago	2 days ago
/10-13-x86.bin	62.93 KB			Rekoobe	43 minutes ago	2 days ago

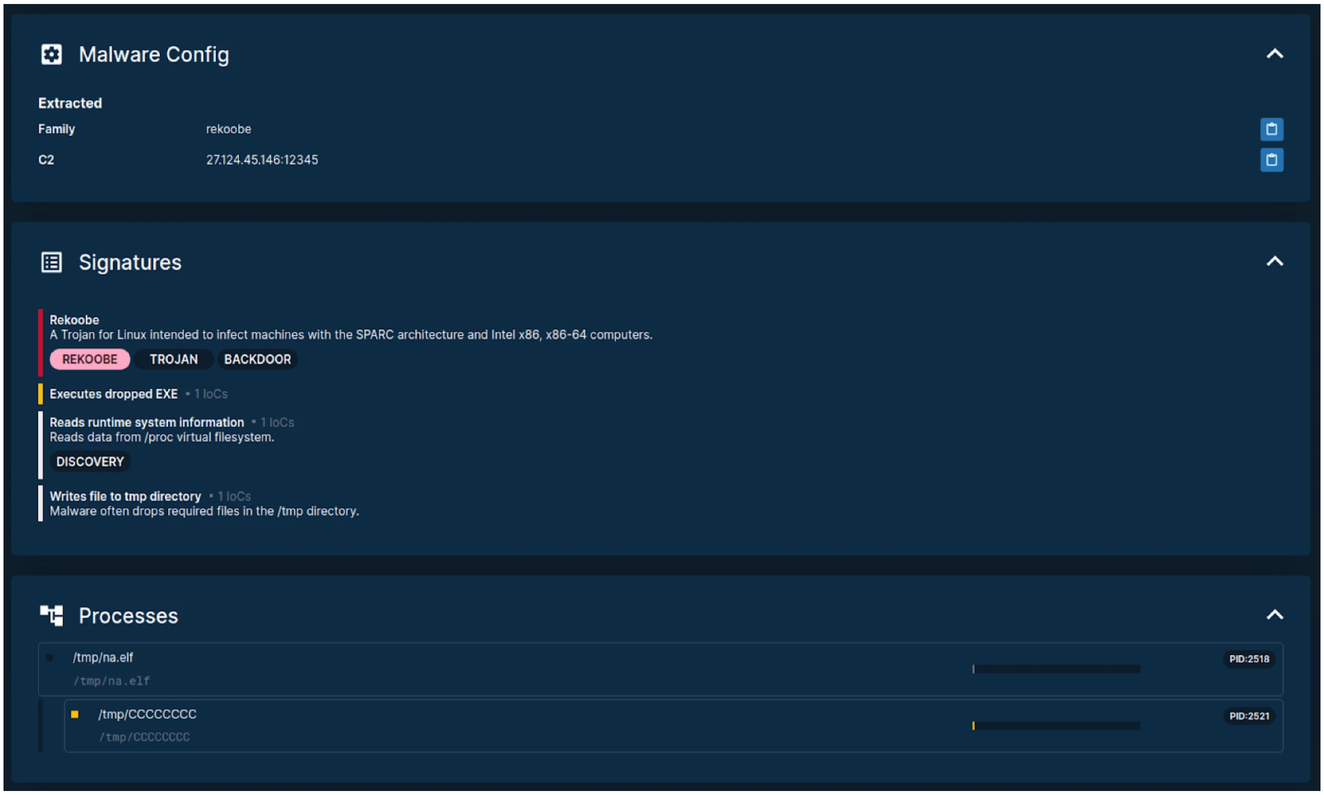
Figure 1: Open directory page for 27.124.45[.]146

During dynamic analysis, both binaries attempted to communicate with the same IP address hosting the open directory, specifically targeting port **12345**. The naming convention of the files, which follows a month-day-architecture format, is consistent with other Rekoobe samples we've seen in open directories.

In our analysis of na.elf, we observed behavior closely resembling that identified by AhnLab as "NoodRAT" and Trend Micro as "Noodle RAT." Specifically, the file changes its process name and copies itself to the **/tmp/CCCCCCCC** directory, where it executes from.

However, it's important to note that this alone does not definitively confirm that the binaries in this case are NoodRAT or Noodle RAT. The similarities in behavior could indicate the work of a copycat, but additional analysis would be required to make a conclusive attribution.

Figure 2 depicts the process tree of na.elf as seen in the Hatching Triage analysis.



Malware Config

Extracted

Family	rekoobe
C2	27.124.45.146:12345

Signatures

Rekoobe
A Trojan for Linux intended to infect machines with the SPARC architecture and Intel x86, x86-64 computers.
REKOOBE TROJAN BACKDOOR

Executes dropped EXE • 1 IoCs

Reads runtime system information • 1 IoCs
Reads data from /proc virtual filesystem.
DISCOVERY

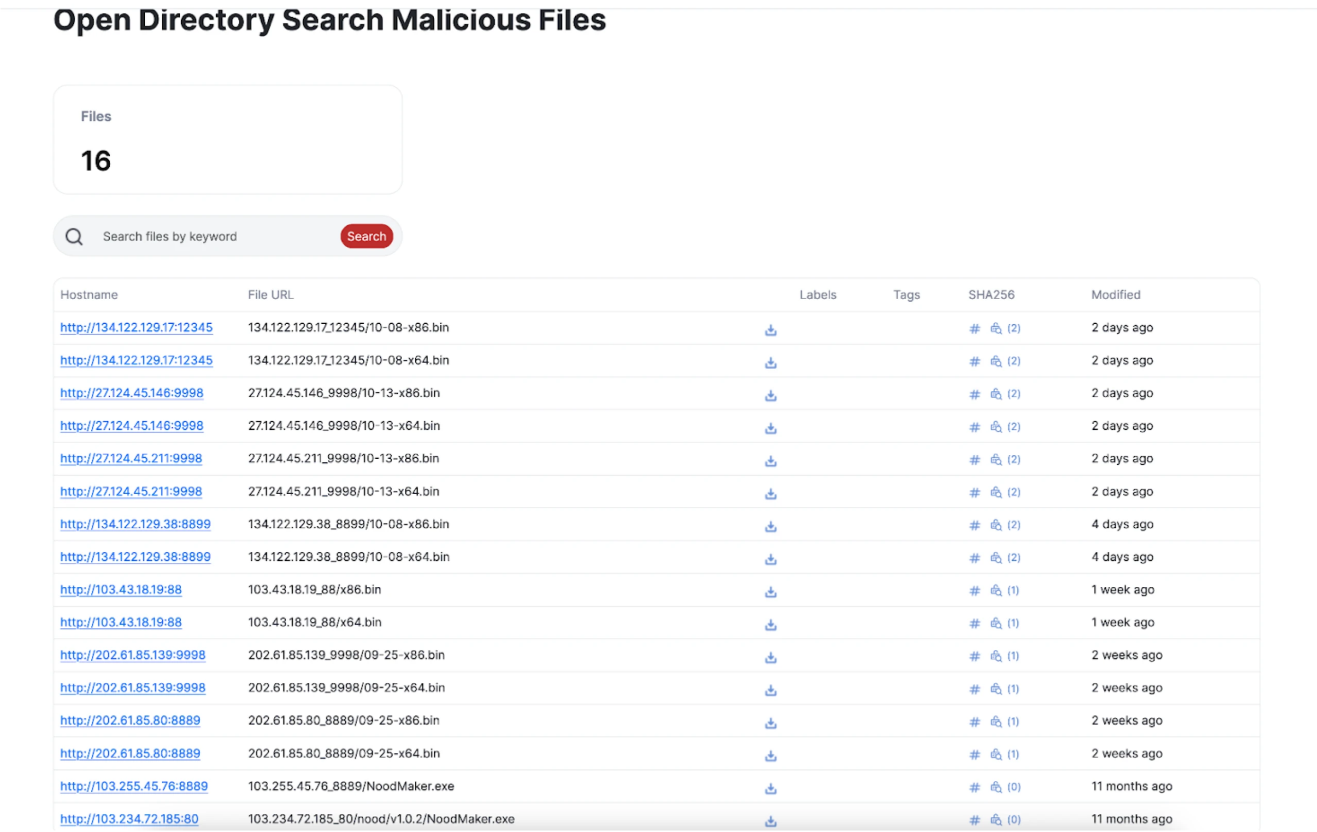
Writes file to tmp directory • 1 IoCs
Malware often drops required files in the /tmp directory.

Processes

```
/tmp/na.elf                                   PID:2518
/tmp/na.elf
    /tmp/CCCCCCCC                             PID:2521
    /tmp/CCCCCCCC
```

Figure 2: Triage analysis of na.elf processes

By clicking the 'Rekoobe' tag, users can easily find additional open directories hosting Rekoobe samples, as shown in Figure 1.



Open Directory Search Malicious Files

Files

16

Hostname	File URL	Labels	Tags	SHA256	Modified
http://134.122.129.17:12345	134.122.129.17_12345/10-08-x86.bin			# (2)	2 days ago
http://134.122.129.17:12345	134.122.129.17_12345/10-08-x64.bin			# (2)	2 days ago
http://27.124.45.146:9998	27.124.45.146_9998/10-13-x86.bin			# (2)	2 days ago
http://27.124.45.146:9998	27.124.45.146_9998/10-13-x64.bin			# (2)	2 days ago
http://27.124.45.211:9998	27.124.45.211_9998/10-13-x86.bin			# (2)	2 days ago
http://27.124.45.211:9998	27.124.45.211_9998/10-13-x64.bin			# (2)	2 days ago
http://134.122.129.38:8899	134.122.129.38_8899/10-08-x86.bin			# (2)	4 days ago
http://134.122.129.38:8899	134.122.129.38_8899/10-08-x64.bin			# (2)	4 days ago
http://103.43.18.19:88	103.43.18.19_88/x86.bin			# (1)	1 week ago
http://103.43.18.19:88	103.43.18.19_88/x64.bin			# (1)	1 week ago
http://202.61.85.139:9998	202.61.85.139_9998/09-25-x86.bin			# (1)	2 weeks ago
http://202.61.85.139:9998	202.61.85.139_9998/09-25-x64.bin			# (1)	2 weeks ago
http://202.61.85.80:8889	202.61.85.80_8889/09-25-x86.bin			# (1)	2 weeks ago
http://202.61.85.80:8889	202.61.85.80_8889/09-25-x64.bin			# (1)	2 weeks ago
http://103.255.45.76:8889	103.255.45.76_8889/NoodMaker.exe			# (0)	11 months ago
http://103.234.72.185:80	103.234.72.185_80/nood/v1.0.2/NoodMaker.exe			# (0)	11 months ago

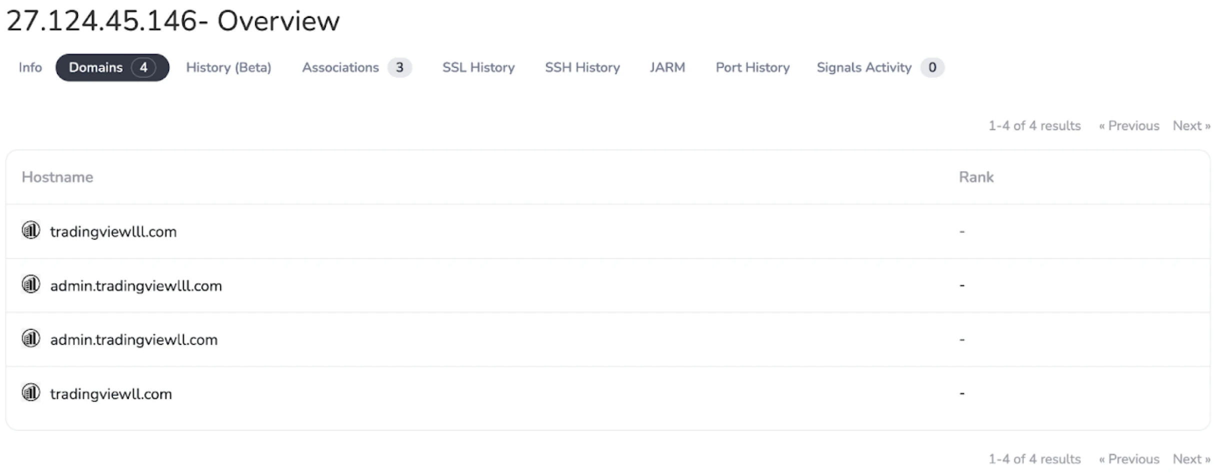
Figure 3: Results of clicking the Rekoobe tag to find additional open directories hosting the malware

Infrastructure Analysis: TradingView Lookalike Domains and Hosting Connections

During our investigation into the IP address hosting the two backdoor files, we discovered several domains closely mimicking the legitimate TradingView site. These domains show slight variations in spelling that are indicative of typosquatting attacks:

- tradingviewlll[.]com
- admin.tradingviewlll[.]com
- tradingviewll[.]com
- admin.tradingviewll[.].com

These minor changes, such as the addition of an extra "l" in **tradingviewll[.]com** and **tradingviewlll[.]com**, could easily be missed by users, making them practical for phishing or other social engineering operations.

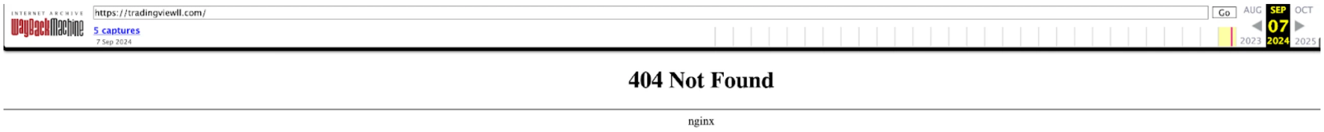


27.124.45.146- Overview

Hostname	Rank
tradingviewlll.com	-
admin.tradingviewlll.com	-
admin.tradingviewll.com	-
tradingviewll.com	-

Figure 4: Domain overview showing typosquatting domains targeting TradingView

Unfortunately, we could not capture any active web pages associated with these domains created earlier this year. According to the Wayback Machine, both domains returned a standard 404 Not Found Nginx response on 07 September this year. This means any web page may not have been fully deployed or is in a consistently inactive state.



404 Not Found

nginx

Figure 5: Wayback machine results for tradingviewll.com

While we can't be sure these domains were used in this campaign, they represent an interesting infrastructure overlap when viewed alongside the presence of the Rekoobe backdoor. This could suggest an attempt to exploit financial platforms and their user base, as many of these systems rely on Linux.

Expanded Network Findings

Continuing our deep dive into **27.124.45[.]146**, we found three IP addresses linked by shared SSH keys, suggesting a connection to our original server. This relationship was uncovered using the Hunt's Association tab, as shown in Figure 6.

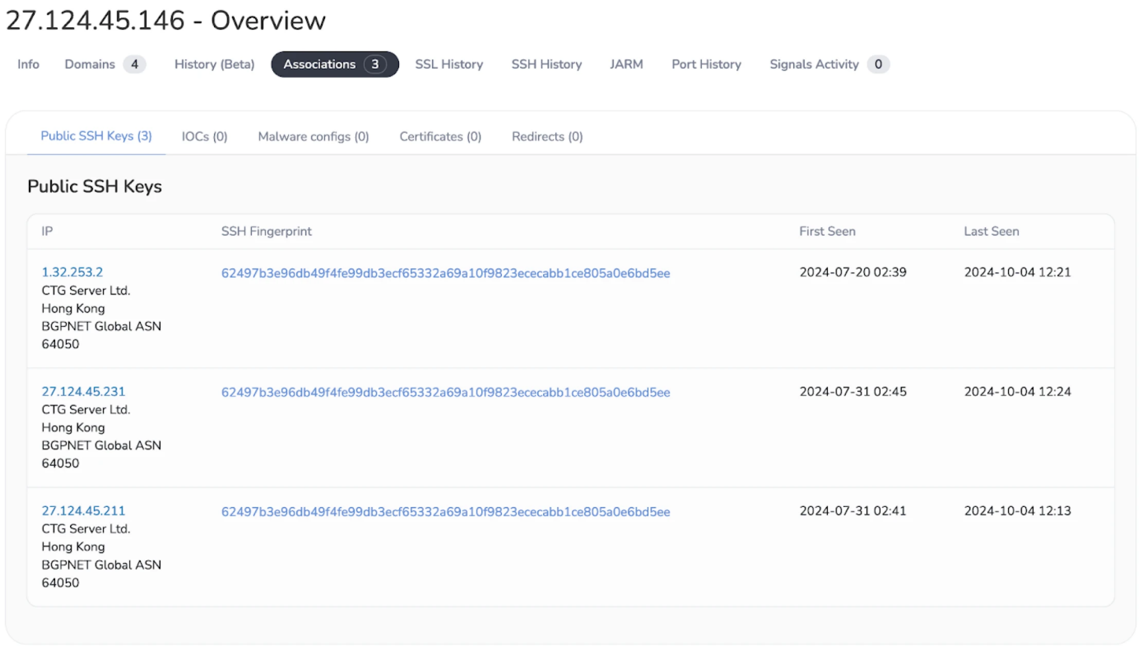
The IPs include:

- 27.124.45[.]231
- 1.32.253[.]2

- 27.124.45[.]211

The SSH key (fingerprint: **62497b3e96db49f4fe99db3ecf65332a69a10f9823ececabb1ce805a0e6bd5ee**) for all three was first observed by our scanners between late July and early August, and were last active on 04 October.

Like the original open directory, these servers are also hosted in Hong Kong, indicating they are likely part of the same operational setup.

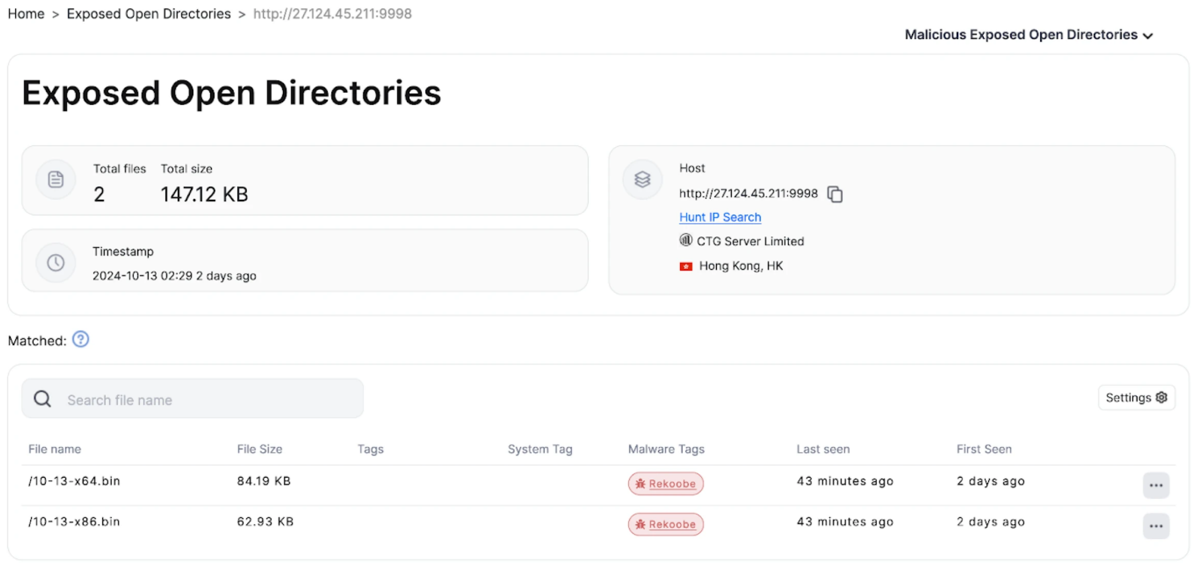


Public SSH Keys

IP	SSH Fingerprint	First Seen	Last Seen
1.32.253.2 CTG Server Ltd. Hong Kong BGPNET Global ASN 64050	62497b3e96db49f4fe99db3ecf65332a69a10f9823ececabb1ce805a0e6bd5ee	2024-07-20 02:39	2024-10-04 12:21
27.124.45.231 CTG Server Ltd. Hong Kong BGPNET Global ASN 64050	62497b3e96db49f4fe99db3ecf65332a69a10f9823ececabb1ce805a0e6bd5ee	2024-07-31 02:45	2024-10-04 12:24
27.124.45.211 CTG Server Ltd. Hong Kong BGPNET Global ASN 64050	62497b3e96db49f4fe99db3ecf65332a69a10f9823ececabb1ce805a0e6bd5ee	2024-07-31 02:41	2024-10-04 12:13

Figure 6: The Associations Tab in Hunt displays associated IPs that can be pivoted to enhance investigations

Among the IPs identified, **27.124.45[.]211** stood out as it also hosts an open directory (on the same port) running the same Python and SimpleHTTP versions and the duplicate Rekoobe-detected files as the original server ending in .146.



Home > Exposed Open Directories > http://27.124.45.211:9998

Exposed Open Directories

Total files: 2
Total size: 147.12 KB

Timestamp: 2024-10-13 02:29 2 days ago

Host: http://27.124.45.211:9998
Hunt IP Search
CTG Server Limited
Hong Kong, HK

Matched:

File name	File Size	Tags	System Tag	Malware Tags	Last seen	First Seen
/10-13-x64.bin	84.19 KB			Rekoobe	43 minutes ago	2 days ago
/10-13-x86.bin	62.93 KB			Rekoobe	43 minutes ago	2 days ago

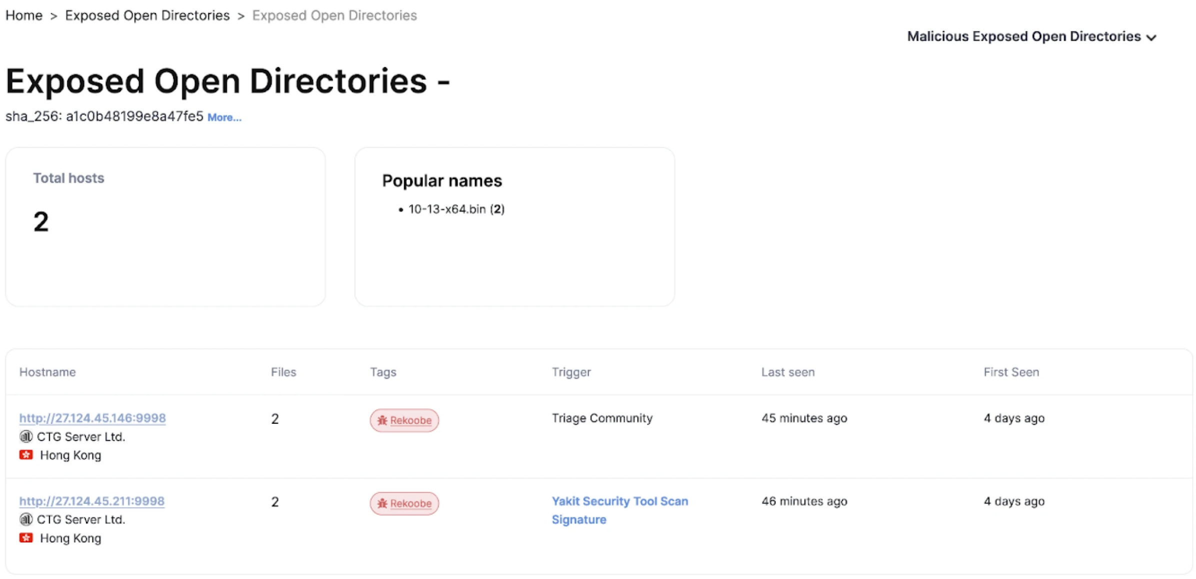
Figure 7: Open directory contents for 27.124.45[.]211:9998

Clicking on the button containing the three dots next to the files opens a menu for further actions, including searching by SHA-256 to identify other locations where the file is hosted. As shown in Figure 8, this search confirms that the two IPs--.146 and .211--are the only servers hosting these Rekoobe samples. Interestingly, our scanners also detected the **Yakit Security Tool** on 27.124.45[.]211

We previously wrote about Yakit, an all-in-one cybersecurity application that integrates tools like Nuclei and includes features such as man-in-the-middle (MiTM) interception and web fuzzing.

Primarily designed for legitimate security work by red teamers and researchers, Yakit's presence alongside Rekoobe and the typosquatting domains raises concerns about how this setup could be leveraged for malicious purposes.

Combining these elements points to activity that merits further investigation to understand the potential risks involved fully.



Home > Exposed Open Directories > Exposed Open Directories
Malicious Exposed Open Directories

Exposed Open Directories -

sha_256: a1c0b48199e8a47fe5 More...

Total hosts

2

Popular names

- 10-13-x64.bin (2)

Hostname	Files	Tags	Trigger	Last seen	First Seen
http://27.124.45.146:9998 CTG Server Ltd. Hong Kong	2	Rekoobe	Triage Community	45 minutes ago	4 days ago
http://27.124.45.211:9998 CTG Server Ltd. Hong Kong	2	Rekoobe	Yakit Security Tool Scan Signature	46 minutes ago	4 days ago

Figure 8: Results of SHA-256 search across all open directories for similar files

Conclusion

In this blog post, we explored how the discovery of the Rekoobe backdoor in an open directory revealed a broader network of potentially malicious infrastructure, lookalike domains mimicking TradingView, and additional servers linked via shared SSH keys.

Hunting for malware in open directories can yield valuable insights into the servers behind attack campaigns. By leveraging tools like Hunt, security teams can uncover hidden threats and expand their visibility into attacker infrastructure.

Network Observables

IP Address	ASN	Domain(s)	Host Country	Notes
27.124.45[.]146	CTG Server Limited	tradingviewlll[.]com admin.tradingviewlll[.]]com tradingviewll[.]com admin.tradingviewll[.]]com	HK	Open directory containing two (2) Rekoobe samples.

IP Address	ASN	Domain(s)	Host Country	Notes
1.32.253[.]2	BGPNET Global ASN	70332[.]club 390698[.]ru 953388[.]cc 836833[.]cc 734439[.]com 56204[.]sx 49246[.]sx 836833[.]cc 94783[.]club 734439[.]com 963388[.]cc	HK	IP seen sharing SSH keys with 27.124.45[.]146 from 2024-07-20 - 2024-10-04
27.124.45[.]231	CTG Server Limited	N/A	HK	Shared SSH keys from 2024-07-31 - 2024-10-04
27.124.45[.]211	CTG Server Limited	N/A	HK	Shared SSH keys from 2024-07-31 - 2024-10-04

File Information

File Name	SHA-256
10-13-x64.bin	a1c0b48199e8a47fe50c4097d86e5f43a1a1c9a9c1f7f3606ffa0d45bb4a2eb3
10-13-x86.bin	28382231cbfe3bf7827c1a874b3d7f18717020ced516b747a2a1bb7598eabe0b