


# Palo Alto Networks Unit 42's Post



Palo Alto Networks Unit 42

52,967 followers

1w

2024-02-08 (Thursday): #TA577 #Pikabot activity — IOCs from an infection run available at <https://bit.ly/3OAfdqw>

#Unit42ThreatIntel #TimelyThreatIntel #Wireshark #MalwareTraffic #Cybercrime

email

link from email

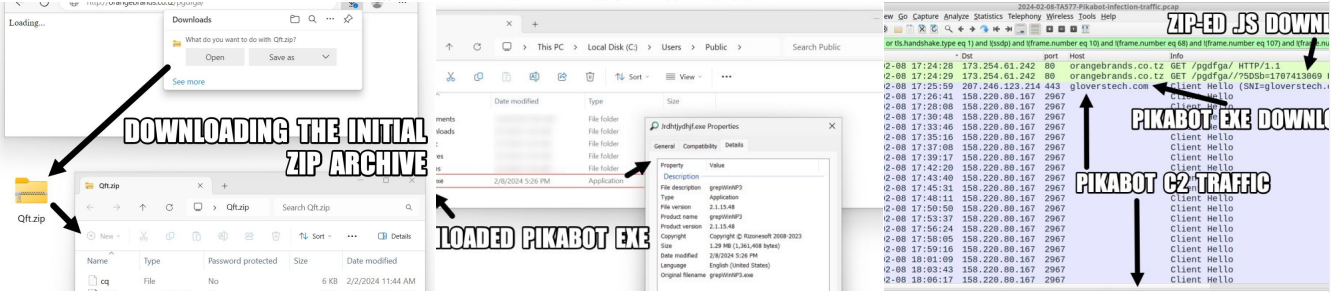
downloaded zip archive

extracted JavaScript file

web traffic for Pikabot installer EXE

Pikabot

Pikabot



DOWNLOADING THE INITIAL ZIP ARCHIVE

LOADED PIKABOT EXE

PIKABOT EXE DOWNLOADED


PIKABOT C2 TRAFFIC

119 · 1 Comment

Like

Comment

Share



Bradley Duncan

1w

A #pcap of the #Pikabot infection traffic and the associated malware samples are now available at <https://www.malware-traffic-analysis.net/2024/02/08/index.html>

[https://www.linkedin.com/posts/unit42\\_ta577-pikabot-unit42threatintel-activity-7161507003310231552-ufq1](https://www.linkedin.com/posts/unit42_ta577-pikabot-unit42threatintel-activity-7161507003310231552-ufq1)

1/6

MALWARE-TRAFFIC-ANALYSIS.NET

2024-02-08 (THURSDAY): TA577 PIKABOT INFECTION

NOTES:

- Zip files are password-protected. Of note, this site has a new password scheme. For the password, see the "about" page of this website.

REFERENCES:

- [https://www.linkedin.com/posts/unit42\\_ta577-pikabot-unit42threatintel-activity-7161507003310231552-ufq1](https://www.linkedin.com/posts/unit42_ta577-pikabot-unit42threatintel-activity-7161507003310231552-ufq1)
- [https://twitter.com/Unit42\\_intel/status/1755741384982581175](https://twitter.com/Unit42_intel/status/1755741384982581175)

ASSOCIATED FILES:

- 2024-02-08-IOCs-from-TA577-Pikabot-infection.txt.zip 1.7 kB (1,890 bytes)
- 2024-02-08-TA577-Pikabot-infection-traffic.pcap.zip 3.5 MB (3,525,620 bytes)
- 2024-02-08-TA577-Pikabot-malware-and-artifacts.zip 796 kB (796,593 bytes)

[Click here to return to the main page.](#)

Copyright © 2024 | [Malware-Traffic-Analysis.net](#)

Like · Reply | 3 Reactions

To view or add a comment, [sign in](#)

More Relevant Posts

**Palo Alto Networks Unit 42**  
52,967 followers  
3d

Sneak Peak! We've got [Michael Sikorski](#), aka "Siko," CTO and VP of Engineering at Unit 42, on the next episode of the Threat Vector podcast.

Siko will break down the key findings from the 2024 Incident Response Report and offers his call-to-action for businesses. Follow Threat Vector and never miss an episode: [https://lnkd.in/g-43pH\\_K](https://lnkd.in/g-43pH_K)

52

Like                      Comment                      Share

To view or add a comment, [sign in](#)