

Forum: [Hack Forums](#)

Thread: [Hacking Group TeamPCP Arrested - Accounts linked to HackForums](#)

Respect - August 27, 2026, 5:35 am

Source: <https://flare.io/learn/resources/blog/teampcp-software-supply-chain-attacks>

TWO ALLEGED TeamPCP MEMBERS ARRESTED IN GLOBAL SOFTWARE SUPPLY-CHAIN CYBERCRIME OPERATION

Australian authorities have charged two Western Australian men, aged 21 and 23, following a joint AFP and Western Australia Police investigation conducted in parallel with the FBI.

The FBI identified the alleged cybercriminal group as TeamPCP.

Authorities allege the syndicate inserted malicious code into software hosted on an open-source repository, which was then unknowingly used by other developers and propagated into government, academic and private-sector environments.

The scale alleged by investigators is significant:

- More than 1,000 organizations potentially compromised worldwide

- More than 500,000 credentials and authentication materials stolen At least 300 GB of data exfiltrated

- Global remediation costs estimated in the hundreds of millions of dollars Data intrusion, identity crime and cryptocurrency-based money laundering allegedly involved

- The two suspects allegedly received cryptocurrency payments for their roles 14 criminal charges filed between the two men

- Additional arrests and charges have not been ruled out

Search warrants were executed on August 26 at properties in Cottesloe, Hamilton Hill and Mandurah, with electronic devices and other evidence seized for forensic examination.

? Analyst Note:

The particularly important element here is the supply-chain methodology.

Rather than attacking every victim directly, the alleged operators compromised trusted open-source software components and allowed downstream adoption to distribute the malicious code into potentially more than 1,000 organizations.

The case also highlights the value of private-sector intelligence: AFP says the investigation began after AFP and FBI received information from multiple cyber threat assessment companies.

<https://www.afp.gov.au/news-centre/media-release/two-wa-men-charged-following-afp-fbi-wapf-disruption-alleged-global>

P??sonl?af - August 27, 2026, 1:23 pm

And where do you see the connection with them and Hackforums?

Respect - August 27, 2026, 1:30 pm

(Aug 27, 2026 01:23 PM)P??sonl?af Wrote: [\[CITE\]](#) And where do you see the connection with them and Hackforums?

About midway through the article, they use Osint to connect his email and alias with any registered accounts, one of which links back to the user therealshookie -

<https://hackforums.net/member.php?action=profile&uid=4278417>

? loading encrypted image...

Hes only 21 today, so that means he registered when he was 14.

_VOX - August 27, 2026, 1:32 pm

(Aug 27, 2026 01:30 PM)Respect Wrote: [\[CITE\]](#) About midway through the article, they use Osint to connect his email and alias with any registered accounts, one of which links back to the user

therealshookie - <https://hackforums.net/member.php?action=profile&uid=4278417>

? loading encrypted image...

Hes only 21 today, so that means he registered when he was 14.

Skype in 2019 is crazy. What's next, using ts3 in 2026 and logmeinhamachi?

P??sonl?af - August 27, 2026, 1:38 pm

(Aug 27, 2026 01:30 PM)Respect Wrote: [\[CITE\]](#) About midway through the article, they use Osint to connect his email and alias with any registered accounts, one of which links back to the user

therealshookie - <https://hackforums.net/member.php?action=profile&uid=4278417>

? loading encrypted image...

Hes only 21 today, so that means he registered when he was 14.

Ah, I didn't see that diagram. Last seen 2023 & 1 post so burner account though.

Respect - August 27, 2026, 1:39 pm

(Aug 27, 2026 01:38 PM)P??sonl?af Wrote: [\[CITE\]](#) Ah, I didn't see that diagram. Last seen 2023 & 1 post so burner account though.

Yeah, wonder if admin can see other accounts linked to his IP

Sift - September 5, 2026, 8:49 am

What a genius posting his email on a forum.

elghub - September 23, 2026, 6:25 pm

if the osint chain is solid, that is a classic mistake. reusing the same email or alias across platforms makes correlation easy, even if the forum account only has one post.

the bigger story is the alleged supply chain method. compromising a trusted dependency and letting downstream projects pull it in is way more efficient than attacking victims directly. also, a burner account is not that burnery if it ties back to the same identity, payments, or infrastructure.