Ransomware’s Apparent Overture to Chinese Threat Actors

flashpoint-intel.com/blog/ramp-ransomware-chinese-threat-actors/

November 16, 2021

Blogs

Blog

RAMP Ransomware’s Apparent Overture to Chinese Threat Actors

Flashpoint has observed an increase in recent weeks of Mandarin and Chinese-speaking threat actors on RAMP as well as other illicit communities across the deep and dark web.

RAMP forum returns—but to what end?

Flashpoint has observed an increase in recent weeks of Mandarin and Chinese-speaking threat actors on RAMP as well as other illicit communities across the deep and dark web.

There are indications that the Russian-language ransomware forum is warming to English- and Mandarin-speaking threat actors. However, these clues, outlined below, may represent a social engineering experiment aimed at manipulating the media, à la Groove.

RAMP is now in multiple languages

In October, RAMP administrators made changes to the forum's interface that make it more accessible to Chinese-speaking and English-speaking threat actors. Forum sections are now in Russian, English, and Mandarin; the main administrator is addressing members in English more often than before; and there is noticeably more English content and comments—and even coming from some Russian-speaking actors.

Furthermore, the RAMP authorization form (for account verification) now includes a domain for a Chinese forum among the others.

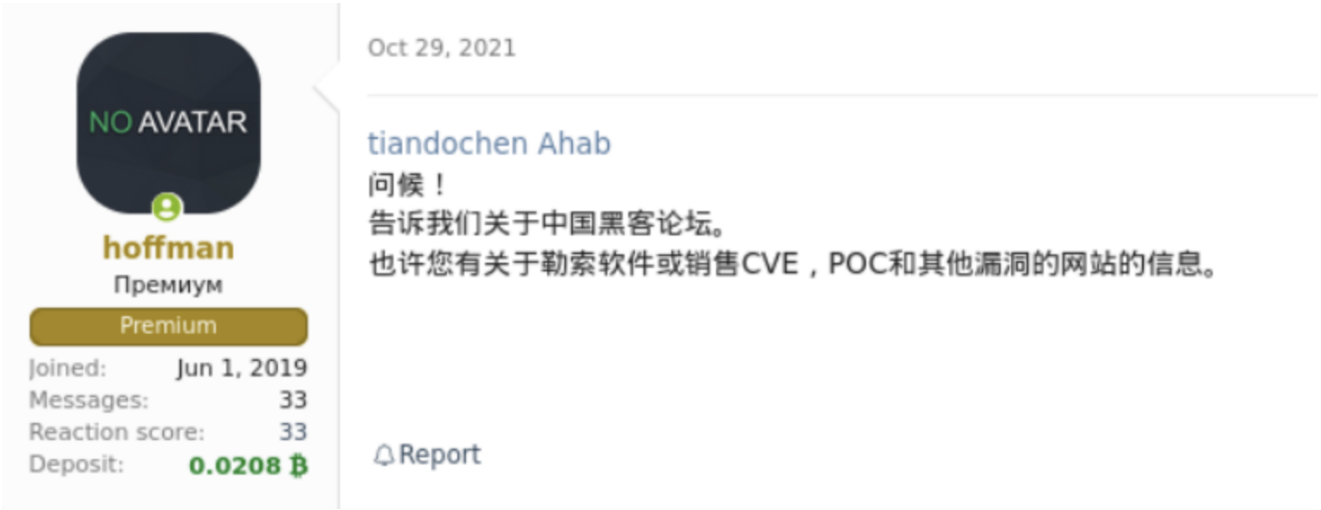
Previously, RAMP was a mainly Russian-speaking forum, although English-speaking members were tolerated.

Founded this summer year in response to top-tier Russian-speaking forums banning ads by ransomware gangs, and now in its third iteration, RAMP now appears under a new .onion domain and requires former users to re-register.

Mandarin on illicit communities

In October, an XSS user replied to a thread with a Chinese-language ad looking for partners in a ransomware operation. Furthermore, in the wake of BlackMatter's shutdown, the spokesperson of LockBit invited BlackMatter's affiliates to move to China where the LockBit spokesperson claimed to be residing.

In the screenshot below, XSS user "hoffman" greets two forum members who revealed themselves as Chinese. The threat actor asks them if they could provide information about ransomware and purchasing various kinds of system vulnerabilities. The language seems to be machine-translated Chinese.



According to RAMP administrators, there are about 30 users of Chinese origin on the forum thus far. However, apart from the Chinese-language forum headings, there is no notable presence from Chinese-language threat actors. Admins promised to add content for Chinese users soon.

Notably, RAMP administrators no longer require proof of membership on Exploit and XSS—two other top-tier Russian-language illicit forums—to approve registration.

Flashpoint analysis

While it is possible that Russian-speaking ransomware operators may be seeking alliances outside of Russia—cooperative cybersecurity talks with the U.S. are currently underway—it remains unclear whether RAMP efforts to woo Chinese-speaking threat actors are in fact legitimate or simply a smokescreen.

In late October 2021, the "Groove" ransomware gang called on other ransomware operators to jointly attack US entities; once this generated media attention, the operator of Groove's public blog claimed that it was a media hack. It is certainly possible that RAMP's overture to Chinese-speaking threat actors is part of a similar strategy.

Prepare for Ransomware and Cyber Extortion with Flashpoint

Data and analysis for this article was discovered directly through analyst research in the Flashpoint platform. **Request a demo** or **sign up for a free trial** and see firsthand how Flashpoint cybersecurity technology can help your organization access critical information and insight into ransomware actors and their tactics, techniques, and procedures (TTPs).