HC3: Analyst Note

October 28, 2021 TLP: White Report: 202110281300

Threat Actor 'Orange' and Groove Data Leak Site Target US HPH Sector

Executive Summary

Russian-speaking threat actor 'Orange' a.k.a. TetyaSluha posted on the Ransomware Anonymous Marketplace (RAMP) cybercrime and ransomware forum seeking partners that could provide access to healthcare and public health (HPH) entities in the U.S. and some EU countries. The actor also specified the targeted entities must be small enough for a solo actor to target alone. 'Orange' recently resigned as RAMP site administrator, citing a major upcoming project as the reason. On October 22, the data leak group Groove posted a message encouraging other cybercriminals to target the U.S. HPH sector. U.S. HPH organizations should be aware of the threat posed by 'Orange' and the cybercriminal communities on RAMP and Groove.

Report

On October 19, 2021, Russian-speaking threat actor 'Orange' a.k.a. TetyaSluha posted on the RAMP cybercrime forum seeking network access credentials for hospitals, government, and medical institutions in the United States. 'Orange' also indicated interest in networks located in the European Union, although they cautioned that not every EU country was an acceptable target. The actor specifically mentioned a desire to target Italian HPH entities. As of October 21, 2021, a comment asking why Italy was mentioned as an example went unanswered. 'Orange' also specified that the network should be small enough that the actor could target it alone and referred partners with access to larger networks to another threat actor, 'steelman.'

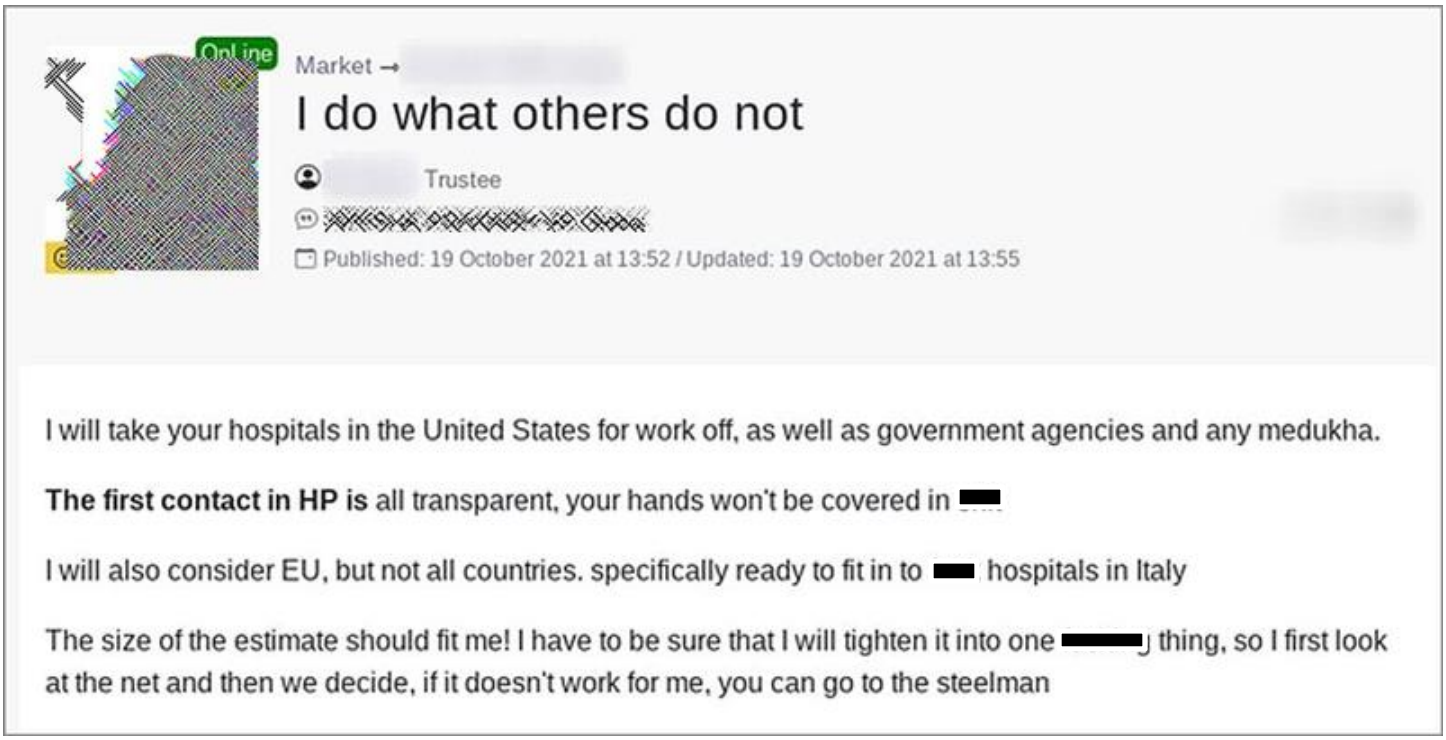

Fig. 1: a post on the RAMP ransomware forum

The post above appeared on RAMP, a ransomware discussion forum that appeared in July 2021. RAMP is unaffiliated with the defunct RAMP (Russian Anonymous Marketplace) dark web marketplace. Like many cybercrime forums, RAMP is Russian-affiliated and primarily in Russian. The site, formerly known as Payload[.]bin, was the home of the Babyk/Babuk ransomware blog prior to the rebrand and is currently affiliated with the Groove

cybercrime collective. The site's launch was a response to the decision by several high-profile cybercrime forums to ban discussion of and recruitment for ransomware attacks after the increased scrutiny following the Darkside ransomware attack on Colonial Pipeline in May 2021. An overwhelming volume of spam posts on the forum led to its relaunch in August 2021.

Threat actor 'Orange' stepped down as a RAMP site administrator on October 18, 2021. The threat actor made an announcement on the forum, adding that site moderators 'MRT' and '999' would be stepping down as well, and referenced an upcoming project as the reason for their resignation. All three actors had been affiliated with the site since its launch in July 2021 and with the Groove data leak operation. The threat actors had previously announced that their partner site, Groove data leak, would be retired once it had collected USD 30 million in ransom or donations.

On October 22, 2021, the Groove data leak gang issued a statement calling for attacks on the United States. The group's spokesperson stated that "at a difficult and troubled time when the United States is trying to fight us, I call on all affiliate programs to stop competing, to unite, and start attacking the US public sector, to show [expletive] the President of the United States who is boss on the Internet." The Groove spokesperson also called for attacks on cybersecurity firms that support state institutions of the United States and urged affiliates not to attack Chinese companies as they should be seen as allies and neighbors should the attackers' home countries turn against them.

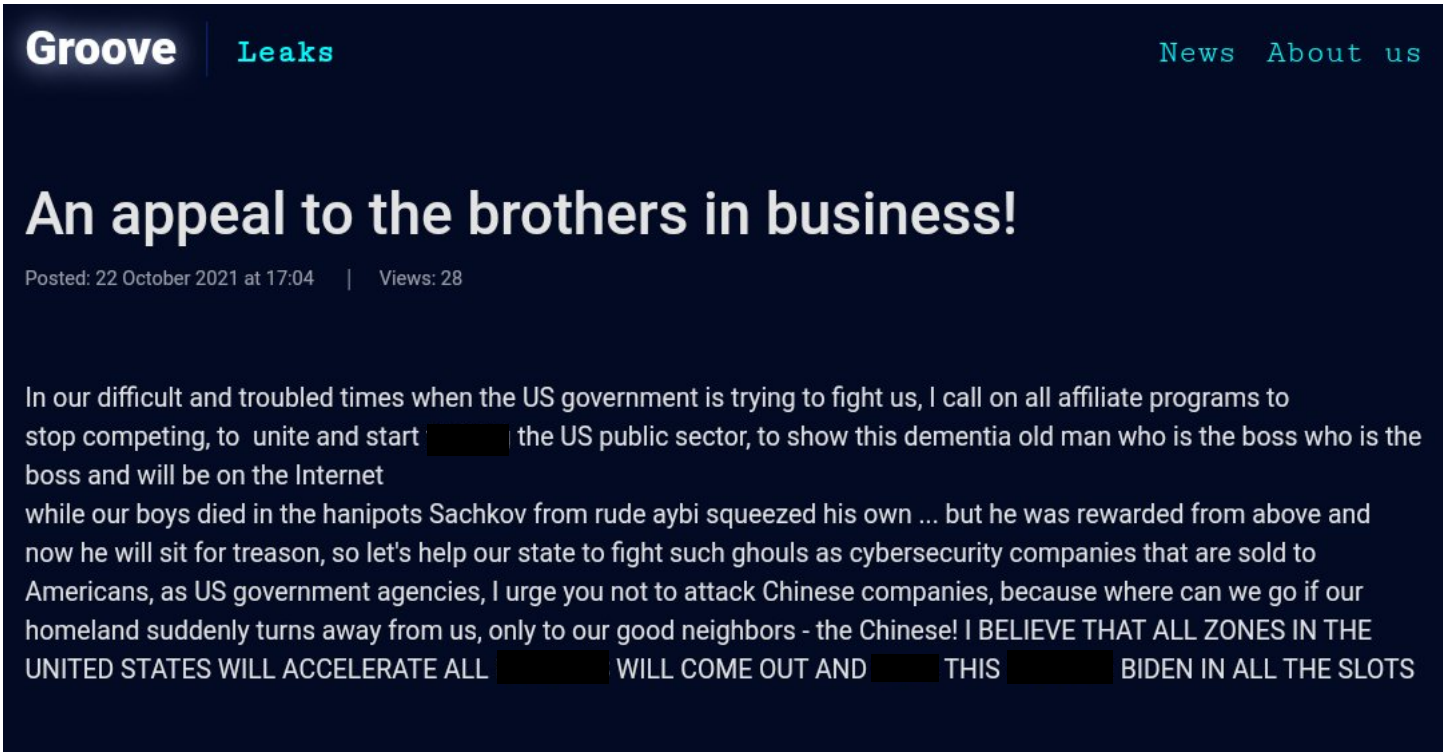

Fig. 2. A post from the Groove data leak blog, posted October 22, 2021.

The post above appeared on the Groove data leak blog. Groove is believed to be a rebrand of Babyk/Babuk ransomware but has announced on its site that it will not limit its activities to only ransomware, saying "Groove is first and foremost an aggressive financially motivated criminal organization dealing in industrial espionage for about two years." In September 2021, the group posted a list of 86,941 allegedly compromised Fortinet VPN connection credentials.

HC3: Analyst Note

October 28, 2021 TLP: White Report: 202110281300

On October 21, 2021, the Groove data leak blog posted a ransom note for a U.S. HPH entity. Groove threatened to expose allegedly stolen patient data, conduct distributed denial-of-service (DDoS) attacks and launch a call flooding attack if the victim organization refused to pay the ransom. It is unknown whether this attack on the U.S. HPH entity is connected to actor Orange's recent actions or was initiated before the October 18, 2021 RAMP post.

Analyst Comment

Security researchers assess 'Orange' as an experienced cybercriminal capable of targeting HPH entities in the U.S. and worldwide. It is not clear which EU countries are unacceptable to 'Orange' but one possibility is that countries affiliated with former-Soviet bloc countries are off-limits due to the actor and site's Russian-affiliation. Based on the stated preferred target organization size, small- to medium-sized HPH sector entities likely have increased risk of an attack by 'Orange.' HC3 analysts assess with high confidence that the Groove data leak group is likely to continue to target U.S. HPH entities.

References

Abrahms, Lawrence. "Groove ransomware calls on all extortion gangs to attack US interests," Bleeping Computer. October 22, 2021. https://www.bleepingcomputer.com/news/security/groove-ransomware-calls-on-all-extortion-gangs-to-attack-us-interests/

DarkTracer: DarkWeb Criminal Intelligence, @darktracer_int. "Groove ransomware gang issued a statement calling for attacks on the United States," Twitter. October 22, 2021. https://twitter.com/darktracer_int/status/1451556403324198921

Kersten, Max, John Fokker and Thibault Seret. "How Groove Gang is Shaking up the Ransomware-as-a-Service Market to Empower Affiliates," McAfee. September 8, 2021. https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/how-groove-gang-is-shaking-up-the-ransomware-as-a-service-market-to-empower-affiliates

"REvil Continues Its Reemergence, Joins Groove-led RAMP Forum," Flashpoint Intel. October 7, 2021. https://www.flashpoint-intel.com/blog/revil-continues-reemergence-on-ramp-forum/

Schwartz, Mathew. "Groove Promises Maximum Profits for Ransomware Affiliates," Data Breach Today. September 9, 2021. https://www.databreachtoday.com/groove-promises-maximum-profits-for-ransomware-affiliates-a-17496

"What the RAMP leadership change means for cybersecurity," Blue Liv. October 21, 2021. https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/what-the-ramp-leadership-change-means-for-cybersecurity/

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback