BLEEPINGCOMPUTER

Hackers leak passwords for 500,000 Fortinet VPN accounts

A threat actor has leaked a list of almost 500,000 Fortinet VPN login names and passwords that were allegedly scraped from exploitable devices last summer.

While the threat actor states that the exploited Fortinet vulnerability has since been patched, they claim that many VPN credentials are still valid.

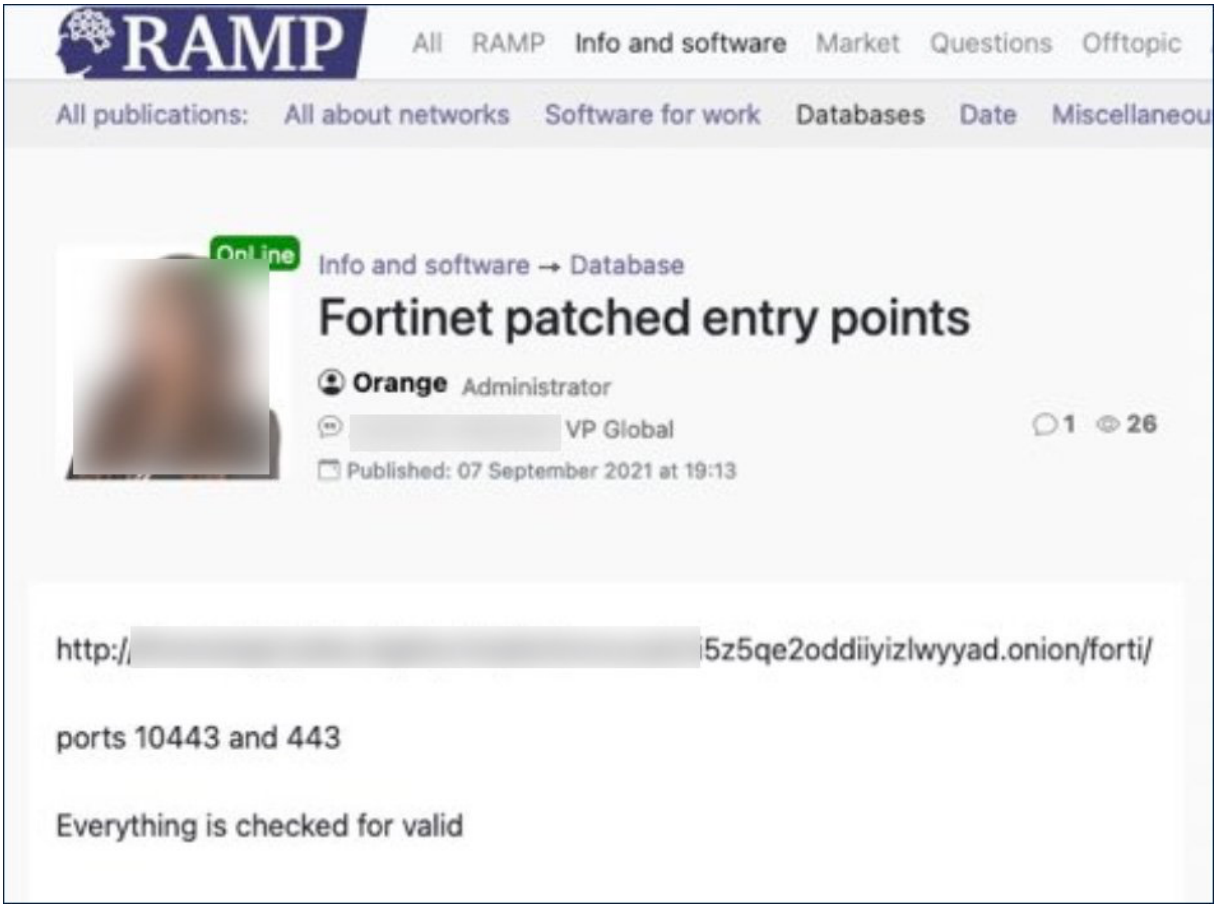
This leak is a serious incident as the VPN credentials could allow threat actors to access a network to perform data exfiltration, install malware, and perform ransomware attacks.

Fortinet credentials leaked on a hacking forum

The list of Fortinet credentials was leaked for free by a threat actor known as 'Orange,' who is the administrator of the newly launched RAMP hacking forum and a previous operator of the Babuk Ransomware operation.

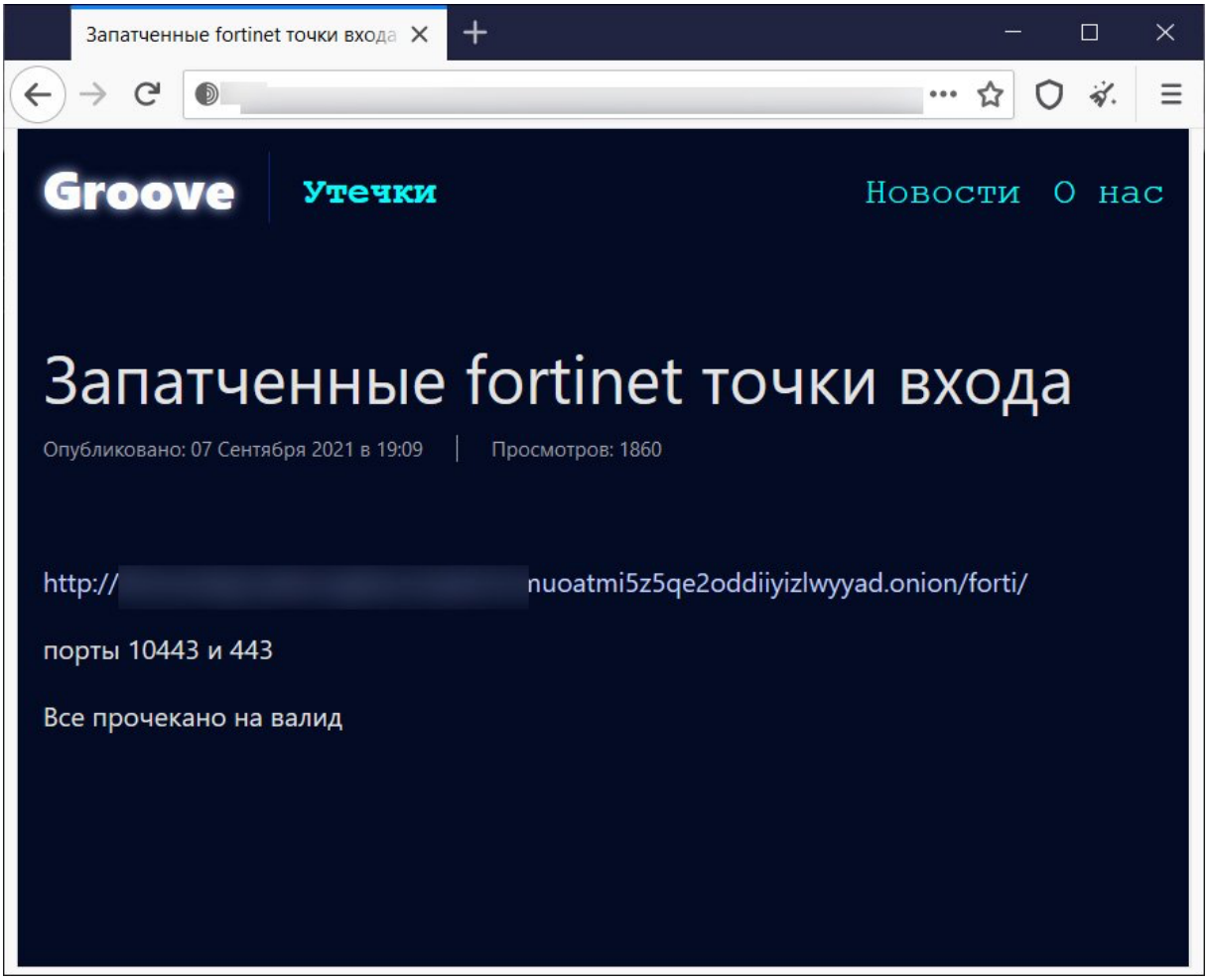
After disputes occurred between members of the Babuk gang, Orange split off to start RAMP and is now believed to be a representative of the new Groove ransomware operation.

Yesterday, the threat actor created a post on the RAMP forum with a link to a file that allegedly contains thousands of Fortinet VPN accounts.



Post on the RAMP hacking forum

At the same time, a post appeared on Groove ransomware's data leak site also promoting the Fortinet VPN leak.



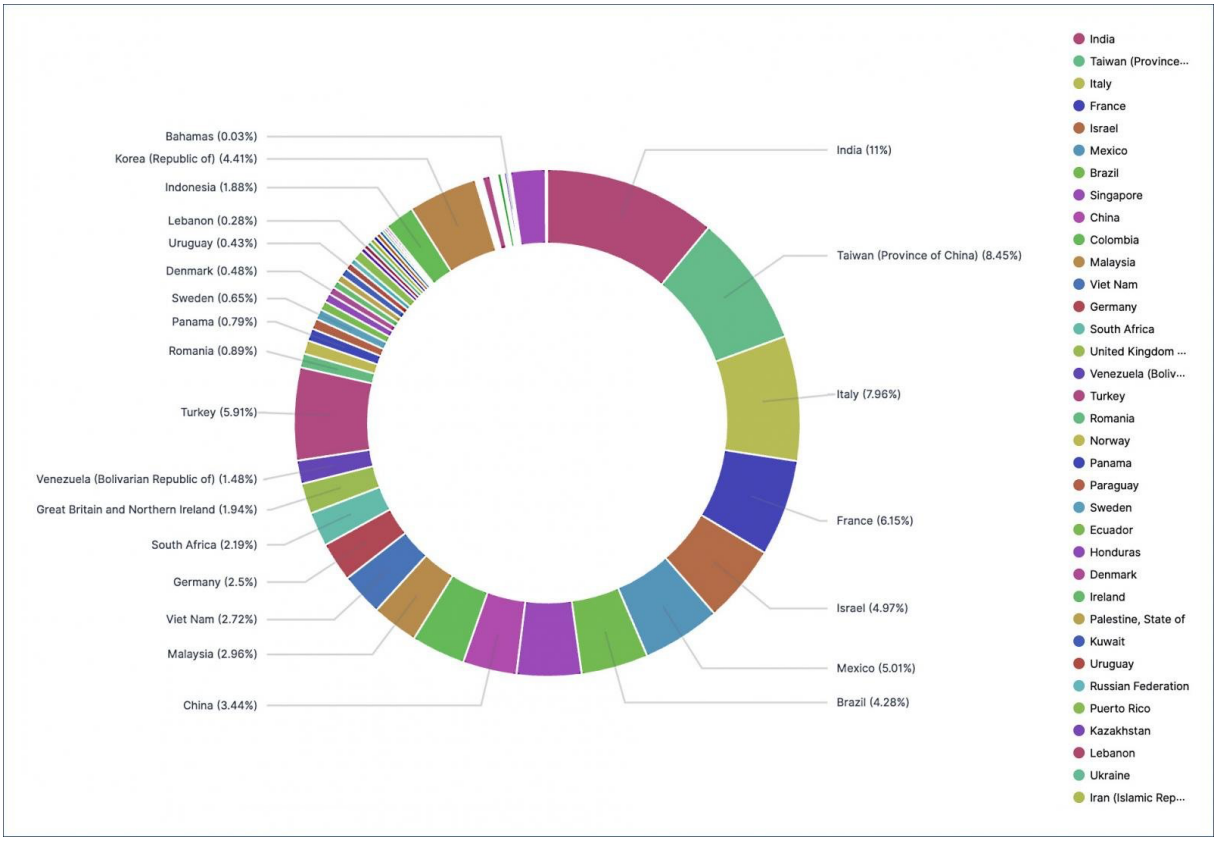
Post about the Fortinet leak on the Groove data leak site

Both posts lead to a file hosted on a Tor storage server used by the Groove gang to host stolen files leaked to pressure ransomware victims to pay.

BleepingComputer's analysis of this file shows that it contains VPN credentials for 498,908 users over 12,856 devices.

While we did not test if any of the leaked credentials were valid, BleepingComputer can confirm that all of the IP address we checked are Fortinet VPN servers.

Further analysis conducted by Advanced Intel shows that the IP addresses are for devices worldwide, with 2,959 devices located in the USA.



Geographic distribution of leaked Fortinet servers

Kremez told BleepingComputer that the Fortinet CVE-2018-13379 vulnerability was exploited to gather these credentials.

A source in the cybersecurity industry told BleepingComputer that they were able to legally verify that at least some of the leaked credentials were valid.

It is unclear why the threat actor released the credentials rather than using them for themselves, but it is believed to have been done to promote the RAMP hacking forum and the Groove ransomware-as-a-service operation.

"We believe with high confidence the VPN SSL leak was likely accomplished to promote the new RAMP ransomware forum offering a "freebie" for wannabe ransomware operators." Advanced Intel CTO Vitali Kremez told BleepingComputer.

Groove is a relatively new ransomware operation that only has one victim currently listed on their data leak site. However, by offering freebies to the cybercriminal community, they may be hoping to recruit other threat actors to their affiliate system.

What should Fortinet VPN server admins do?

While BleepingComputer cannot legally verify the list of credentials, if you are an administrator of Fortinet VPN servers, you should assume that many of the listed credentials are valid and take precautions.

These precautions include performing a forced reset of all user passwords to be safe and to check your logs for possible intrusions.

If you have Fortinet VPN, please go force reset all your user's passwords. Also, it's probably not a bad idea to check logs and potentially spin up an IR or two

— pancak3 (@pancak3lullz) September 7, 2021

If anything looks suspicious, you should immediately make sure that you have the latest patches installed, perform a more thorough investigation, and make sure that your user's passwords are reset.