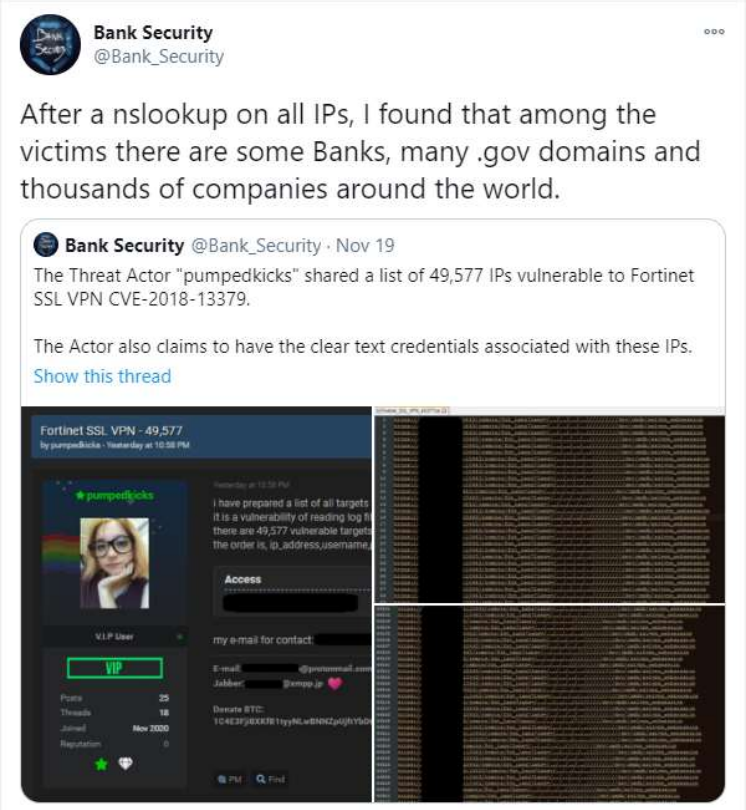
FortiOS - Path Traversal vulnerability exploited



A "Path Traversal" vulnerability allows malicious actors to access resources outside a web-servers' root folder. Such a vulnerability ("CVE-2018-13379") was previously discovered at FortiOS and patched by Fortinet and was seen used by state backed hackers, when combined with other Windows OS vulnerabilities to disrupt the support systems of the US government elections (BleepingComputers.com).

Unfortunately the vulnerability remains unattended and unpatched by many users. This concern has risen as a new threat actor published a 6.7 GB list including credentials and IP addresses of vulnerable, internet exposed FortiOS Servers. In a tweet shared by a threat intelligence analyst "Bank_Security" the list of credentials were first discovered and then checked for validity and confirmed by "Bank_Security" to be related to Banks, Government domains and other high profile FortiOS users around the world.

We recommend you Read more about the vulnerability at FortiGaurds Labs, where you'll find information about upgrading FortiOS, enabling 2FA for new connections which will help prevent exploitation of the vulnerability.