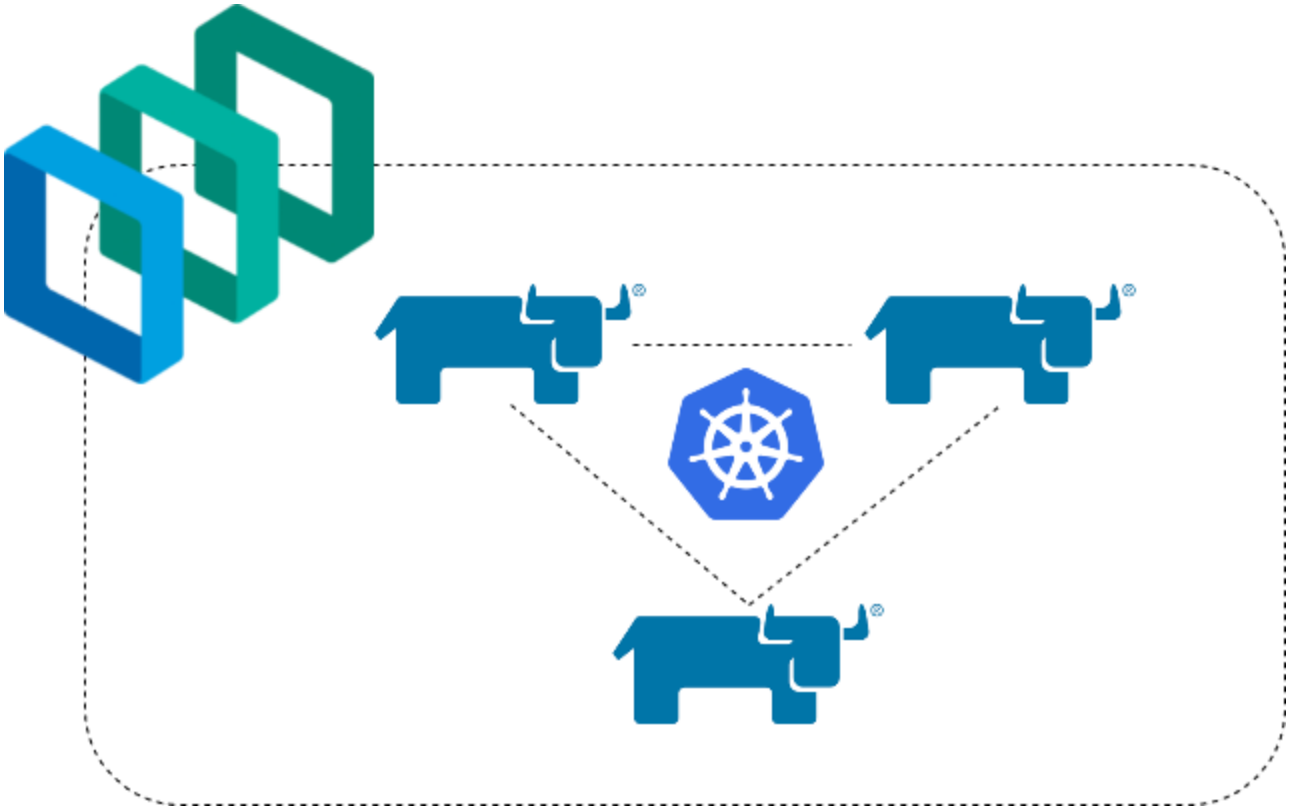
The Bvp47 - a Top-tier Backdoor of US NSA Equation Group

pangulab.cn/en/post/the_bvp47_a_top-tier_backdoor_of_us_nsa_equation_group/



Full Report Download: The Bvp47 Technical Paper (PDF)

In a certain month of 2013, during an in-depth forensic investigation of a host in a key domestic department, researchers from the Pangu Lab extracted a set of advanced backdoors on the Linux platform, which used advanced covert channel behavior based on TCP SYN packets, code obfuscation, system hiding, and self-destruction design. In case of failure to fully decrypt, It is further found that this backdoor needs the check code bound to the host to run normally. Then the researchers cracked the check code and successfully ran the backdoor. Judging from some behavioral functions, this is a top-tier APT backdoor, but further investigation requires the attacker's asymmetric encrypted private key to activate the remote control function. Based on the most common string "Bvp" in the sample and the numerical value 0x47 used in the encryption algorithm, the team named the corresponding malicious code "Bvp47" at the time.

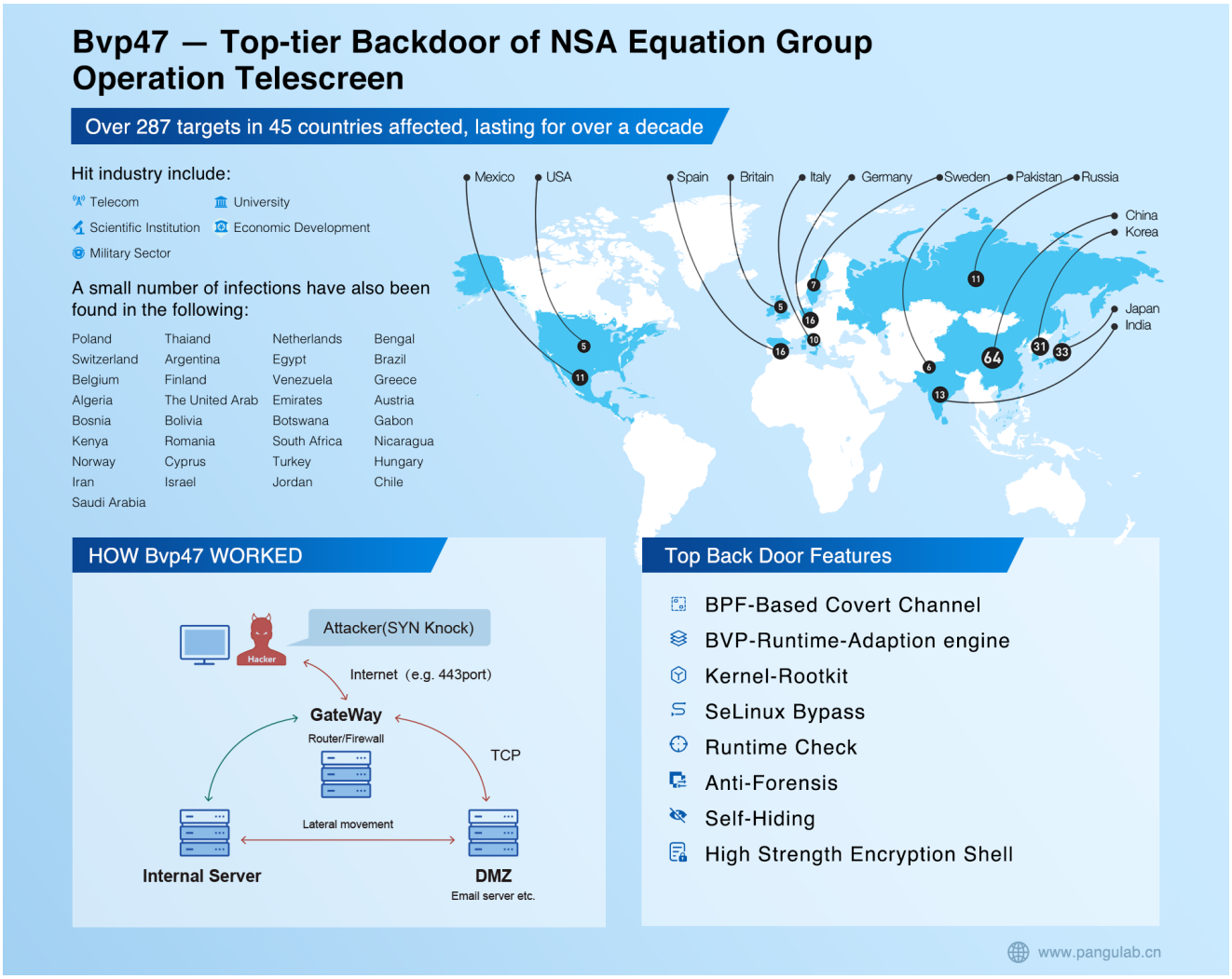
In 2016 and 2017, “The Shadow Brokers” published two batches of hacking files claimed to be used by "The Equation Group". In these hacking files, researchers form Pangu Lab found the private key that can be used to remotely trigger the backdoor Bvp47. Therefor, It can be concluded that Bvp47 is a hacker tool belonging to "The Equation Group".

Through further research, the researchers found that the multiple procedures and attack operation manuals disclosed by "The Shadow Broker" are completely consistent with the only identifier used in the NSA network attack platform operation manual [References 3 and 4] exposed by CIA analyst Snowden in the "Prism" incident in 2013.

In view of the US government's prosecution of Snowden on three charges of "spreading national defense information without permission and deliberately spreading confidential information", it can be determined that the documents published by "The Shadow Brokers" are indeed NSA, which can fully prove that "The Equation Group" belongs to NSA, that is, Bvp47 is the top-tier backdoor of NSA. Besides the files of "The Shadow Brokers" revealed that the scope of victims exceeded 287 targets in 45 countries, including Russia, Japan, Spain, Germany, Italy, etc. The attack lasted for over 10 years. Moreover, one victim in Japan is used as a jump server for further attack.

Pangu Lab has a code named "Operation Telescreen" for several Bvp47 incidents. Telescreen is a device imagined by British writer George Orwell in his novel "1984". It can be used to remotely monitor the person or organization deploying the telescreen, and the "thought police" can arbitrarily monitor the information and behavior of any telescreen.

The Equation Group is the world's leading cyber-attack group and is generally believed to be affiliated with the National Security Agency of the United States. Judging from the attack tools related to the organization, including Bvp47, Equation group is indeed a first-class hacking group. The tool is well-designed, powerful, and widely adapted. Its network attack capability equipped by 0day vulnerabilities was unstoppable, and its data acquisition under covert control was with little effort. The Equation Group is in a dominant position in national-level cyberspace confrontation.



Translations:

"中文"|