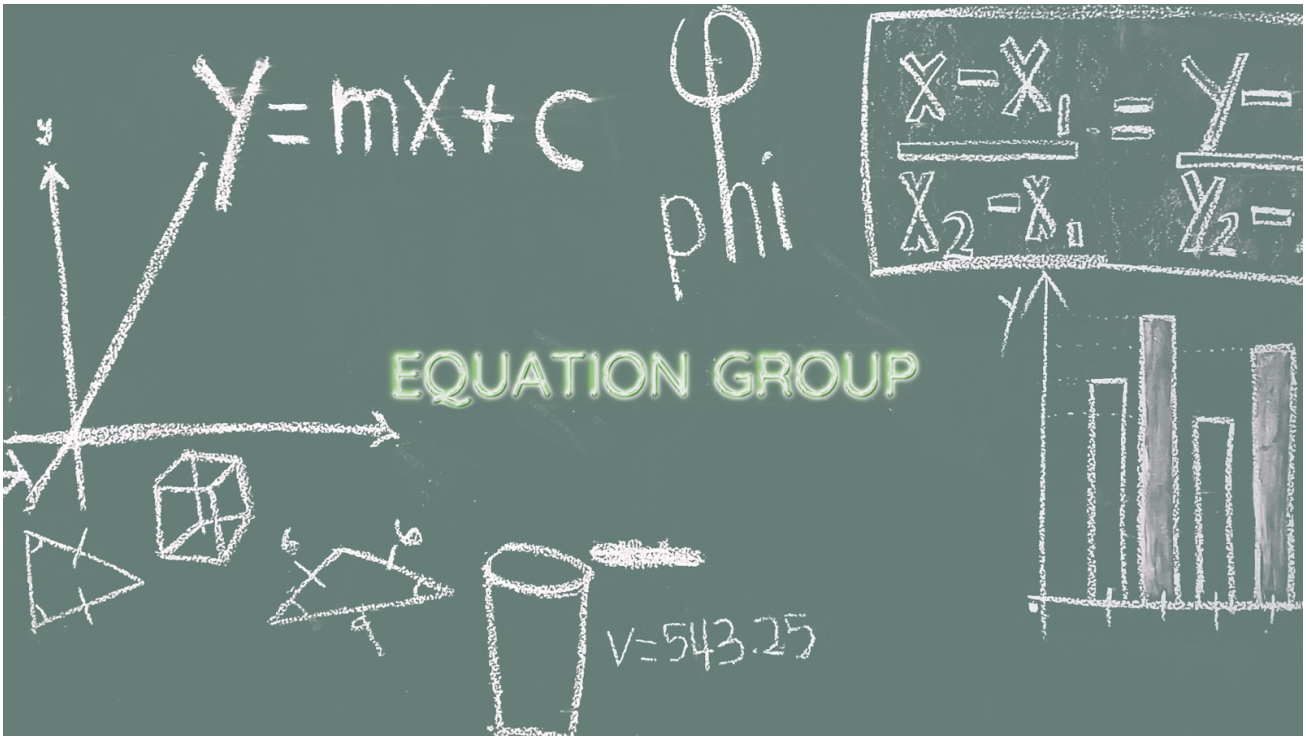
NSA-linked Bvp47 Linux backdoor widely undetected for 10 years

bleepingcomputer.com/news/security/nsa-linked-bvp47-linux-backdoor-widely-undetected-for-10-years/

Ionut Ilascu

By
Ionut Ilascu

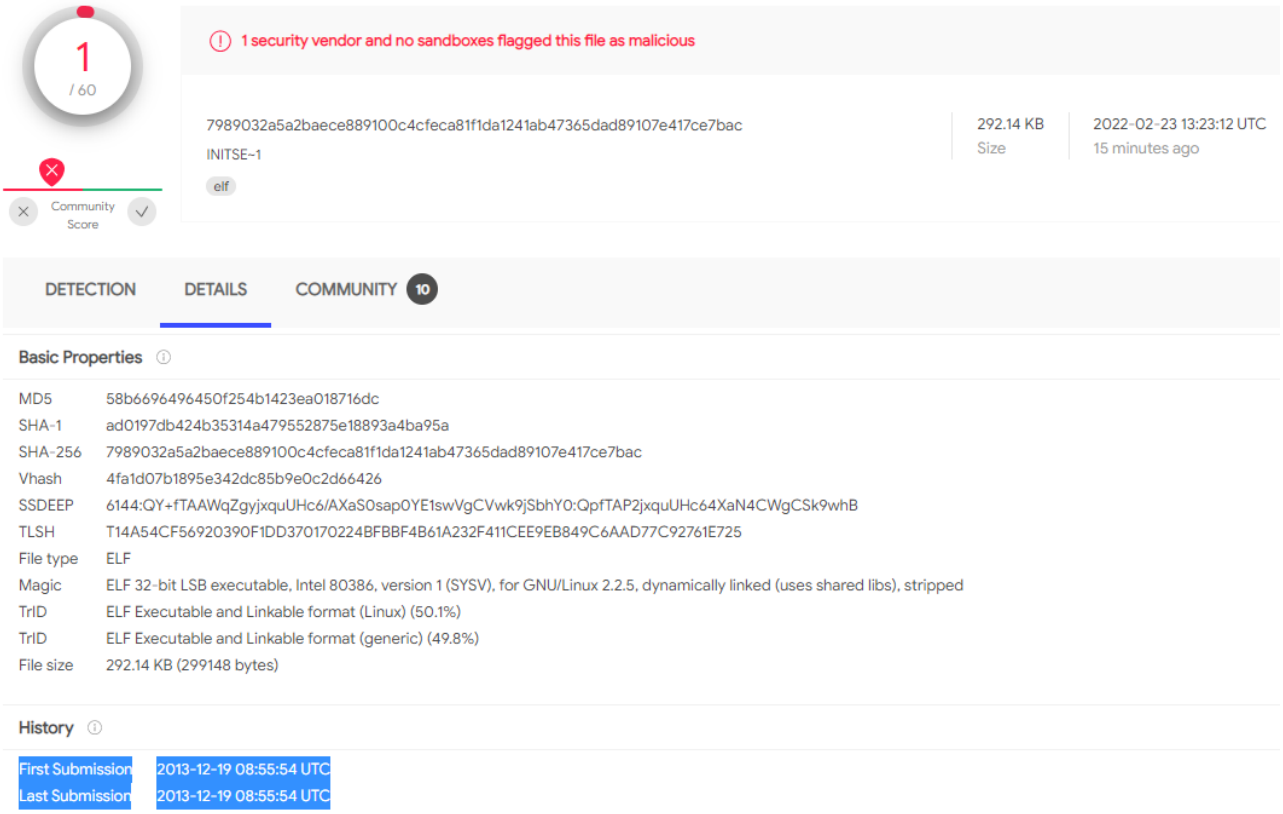
- February 23, 2022
- 07:21 PM
- 5



A report released today dives deep into technical aspects of a Linux backdoor now tracked as Bvp47 that is linked to the Equation Group, the advanced persistent threat actor tied to the U.S. National Security Agency.

Bvp47 survived until today almost undetected, despite being submitted to the Virus Total antivirus database for the first time close to a decade ago, in late 2013.

Until this morning, only one antivirus engine on Virus Total detected the Bvp47 sample. As the report spread in the infosec community, detection started to improve, being flagged by six engines at the moment of writing.



source: BleepingComputer

The Equation Group connection

The Advanced Cyber Security Research team at Pangu Lab, a Chinese cybersecurity company, says that it found the elusive malware in 2013, during a “forensic investigation of a host in a key domestic department.”

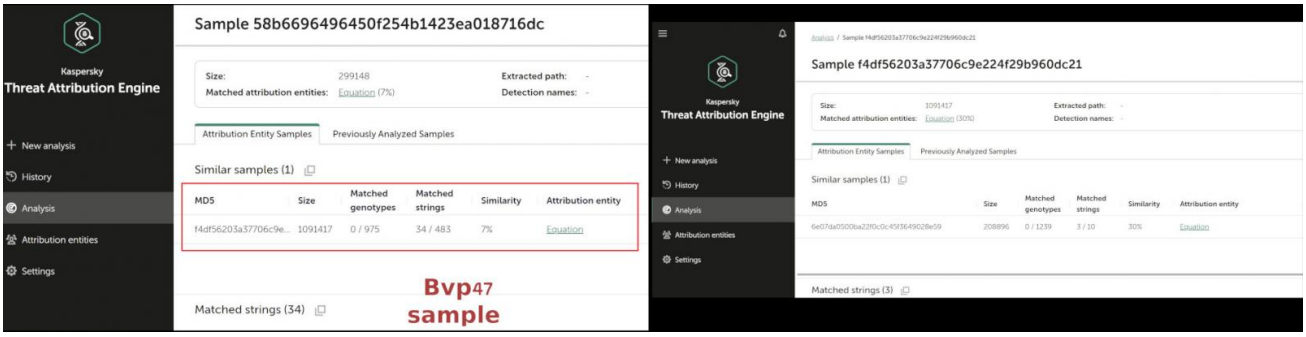
The Bvp47 sample obtained from the forensic investigation proved to be an advanced backdoor for Linux with a remote control function protected through the RSA asymmetric cryptography algorithm, which requires a private key to enable.

They found the private key in the leaks published by the Shadow Brokers hacker group between 2016-2017, which contained hacking tools and zero-day exploits used by NSA’s cyberattack team, the Equation Group.

Some components in the Shadow Brokers leaks were integrated into the Bvp47 framework - “dewdrop” and “solutionchar_agents” - indicating that the implant covered Unix-based operating systems like mainstream Linux distributions, Juniper’s JunOS, FreeBSD, and Solaris.

Apart from Pangu Lab attributing the Bvp47 malware to the Equation Group, automated analysis of the backdoor also shows similarities with another sample from the same actor.

Kaspersky's Threat Attribution Engine (KTAE) shows that 34 out of 483 strings match those from another Equation-related sample for Solaris SPARC systems, which had a 30% similarity with yet another Equation malware submitted to Virus Total in 2018 and posted by threat intel researcher Deresz on January 24, 2022.



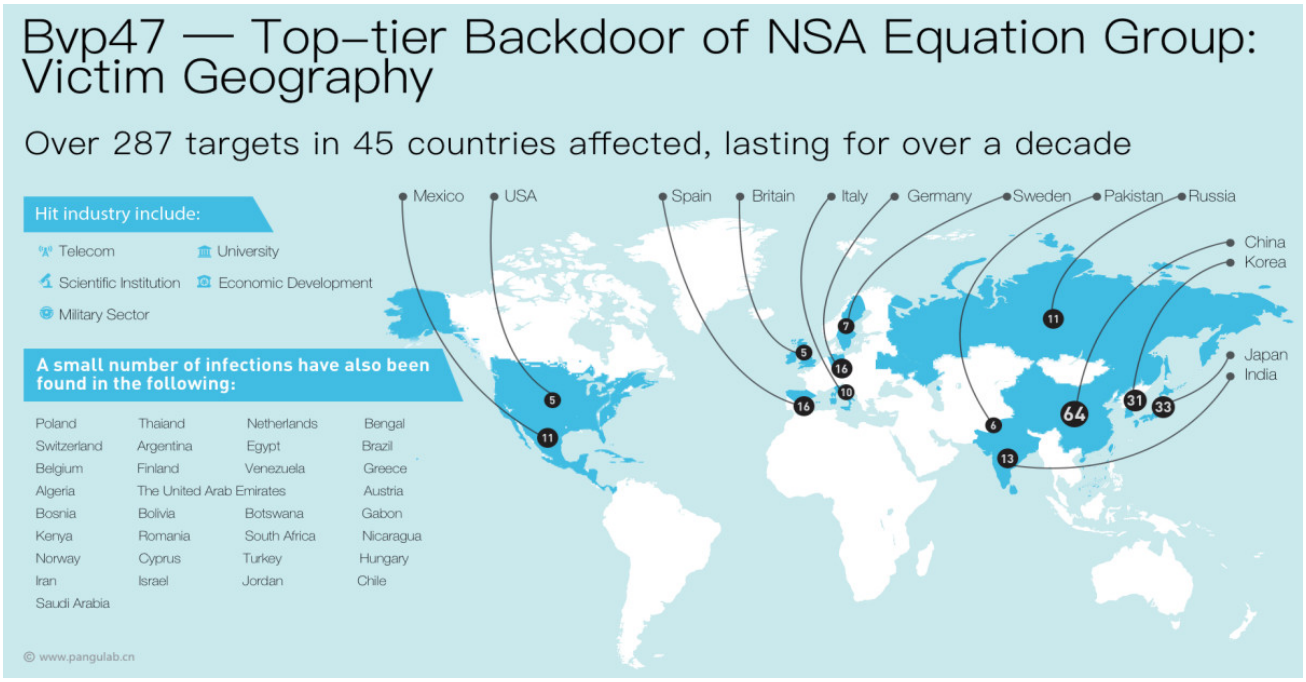
source: Kaspersky

Costin Raiu, director of Global Research and Analysis Team at Kaspersky, told BleepingComputer that Bvp47's code-level similarities match a single sample in the company's current malware collection.

This indicates that the malware was not used extensively, as it usually happens with hacking tools from high-level threat actors, who use them in highly targeted attacks.

In the case of the Bvp47 Linux backdoor, Pangu Lab researchers say that it was used on targets in the telecom, military, higher-education, economic, and science sectors.

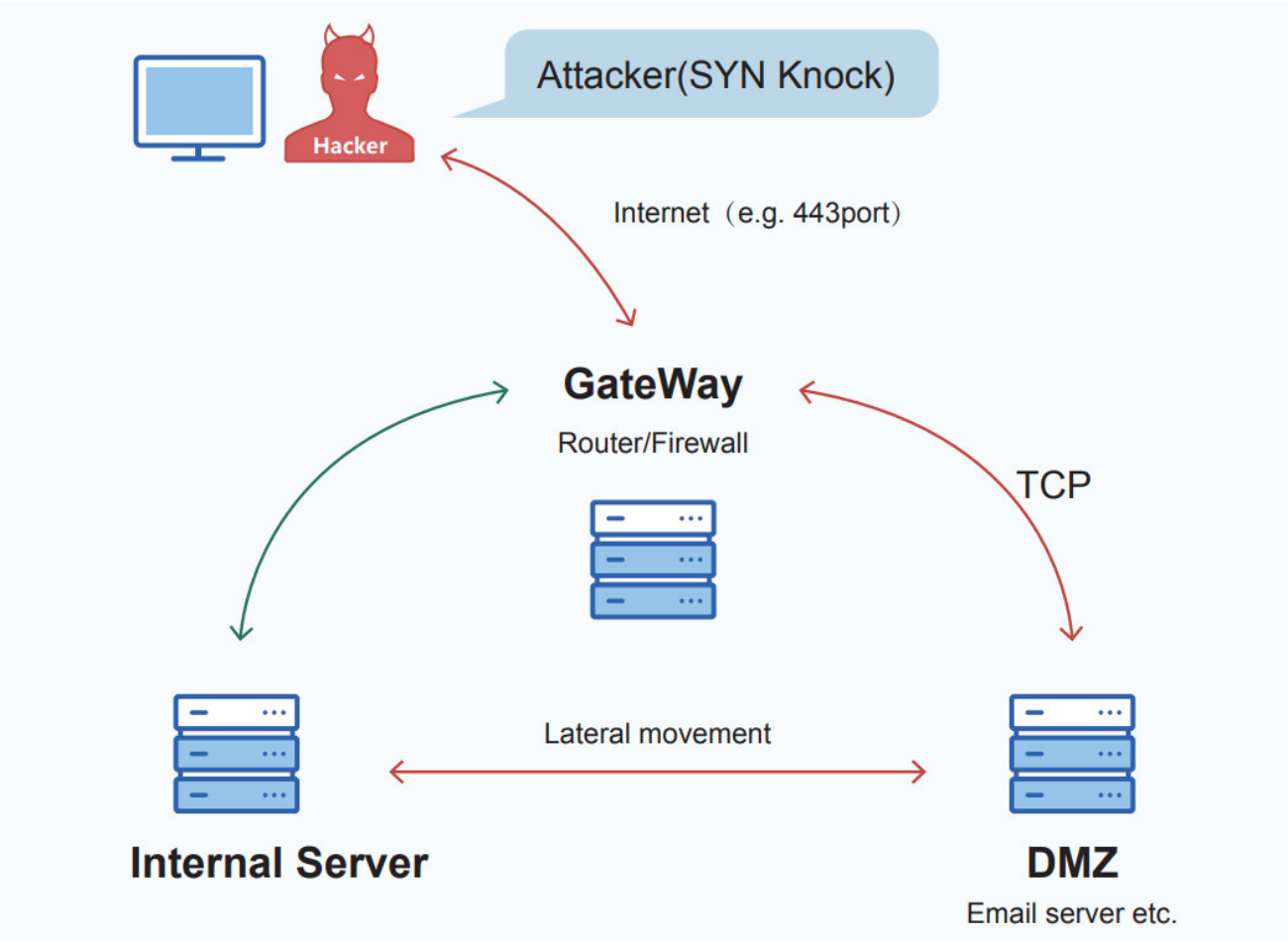
They note that the malware hit more than 287 organizations in 45 countries and went largely undetected for over 10 years.



source: Pangu Lab

Attack stages

Pangu Lab's incident analysis involved three servers, one being the target of an external attack and two other internal machines - an email server and a business server.



source: Pangu Lab

According to the researchers, the threat actor pivoted established a connection between the external server and the email server via a TCP SYN packet with a 264-byte payload.

"At almost the same time, the [email] server connects to the [business] server's SMB service and performs some sensitive operations, including logging in to the [business] server with an administrator account, trying to open terminal services, enumerating directories, and executing Powershell scripts through scheduled tasks" - Pangu Lab

The business server then connected to the email machine to download additional files, "including the Powershell script and the encrypted data of the second stage."

An HTTP server is started on one of the two compromised machines, serving two HTML files to the other. One of the files was a base64-encoded PowerShell script that downloads "index.htm," which contains asymmetrically encrypted data.

A connection between the two internal machines is used to communicate encrypted data via "its own protocol," Pangu Lab researchers say in their report.

The researchers were able to restore the communication between the servers and summarized it into the following steps, where machine A is the external system and V1/V2 are the email and business server, respectively:

1. Machine A connects to port 80 of the V1 server to send a knock request and start the backdoor program on the V1 server
2. The V1 server reversely connects the high-end port of machine A to establish a data pipeline
3. The V2 server connects to the backdoor web service opened on the V1 server, and obtains PowerShell execution from the V1 server
4. The V1 server connects to the SMB service port of the V2 server to perform command operations
5. The V2 server establishes a connection with the V1 server on the high-end port and uses its own encryption protocol for data exchange
6. The V1 server synchronizes data interaction with the A machine, and the V1 server acts as a data transfer between the A machine and the V2 server

Referring to the above communication technology between the three servers, the researchers assess that the backdoor is the creation of “an organization with strong technical capabilities.”

Related Articles:

BPFDoor malware uses Solaris vulnerability to get root privileges

BPFDoor: Stealthy Linux malware bypasses firewalls for remote access

Malicious PyPI package opens backdoors on Windows, Linux, and Macs

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

Gain foundational skills in Linux and IT with this course bundle deal

- Backdoor
- Equation Group
- Linux
- NSA

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

Comments

- 
  blitz120 - 3 months ago
  -
  -

  A great followup would be an investigation of WHY the backdoor was not addressed for so long. Did the NSA strong arm malware detection companies and researchers? If that turns out to be the case, then extreme pressure needs to be put on the US government to expose and expel those who did so from any government work going forward, including consultation.

- 

h_b_s - 3 months ago

"A great followup would be an investigation of WHY the backdoor was not addressed for so long. Did the NSA strong arm malware detection companies and researchers? If that turns out to be the case, then extreme pressure needs to be put on the US government to expose and expel those who did so from any government work going forward, including consultation."

Probably because nearly all anti-malware vendors concentrate on Windows malware and Linux malware is not their concern. Very few even have Linux native products, and those that have are concentrated on preventing malware from getting through to Windows clients (and Windows servers which lack some of Unix's robust security tools) rather than scanning the system area on Linux servers.

A highly alert Linux admin shouldn't need a separate proprietary malware scanner for Linux servers because they're schooled in how to manage Unix security. There are built in tools to alert to unknown file alterations along with monitoring for abnormal network traffic (tripwire, throw-away VMs, aggregate & deep packet network analysis, clamscan, account security, etc). Obviously, not everyone managing Linux servers is that educated or they may be hamstrung by budgets, or both. If that's the case, no malware scanner is going to help, because they won't buy it anyway because they're also ignorant of the tools already available for free.

Not that I'm going to convince the tin hat brigade, but no, there's no government conspiracy here. Just the market at work. There's no market for *Linux* malware scanners either for the server or desktop. The only real market for malware scanners is to protect client endpoints which are nearly always Windows. Linux native malware will nearly always drop through the cracks except perhaps for the ClamAV team which is FOSS.

- 
  lonegull - 3 months ago
  -
  -
  Burn Linux, burn!!
- 
  bbbaldie - 3 months ago
  -
  -
  Well aren't you special. I hereby sentence you to a world without Linux. Good luck.
- 
  nintendo1889 - 3 months ago
  -
  -
  link is fuxored
  try https://archive.is/tDcNQ

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: