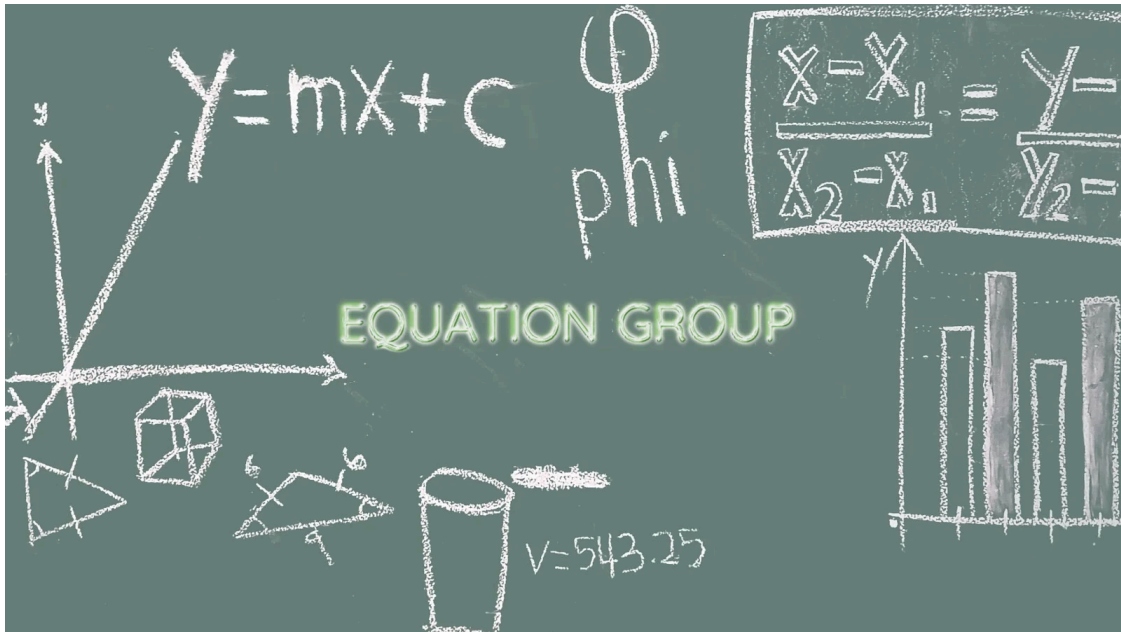


## NSA-linked Bvp47 Linux backdoor widely undetected for 10 years

By Ionut Ilascu

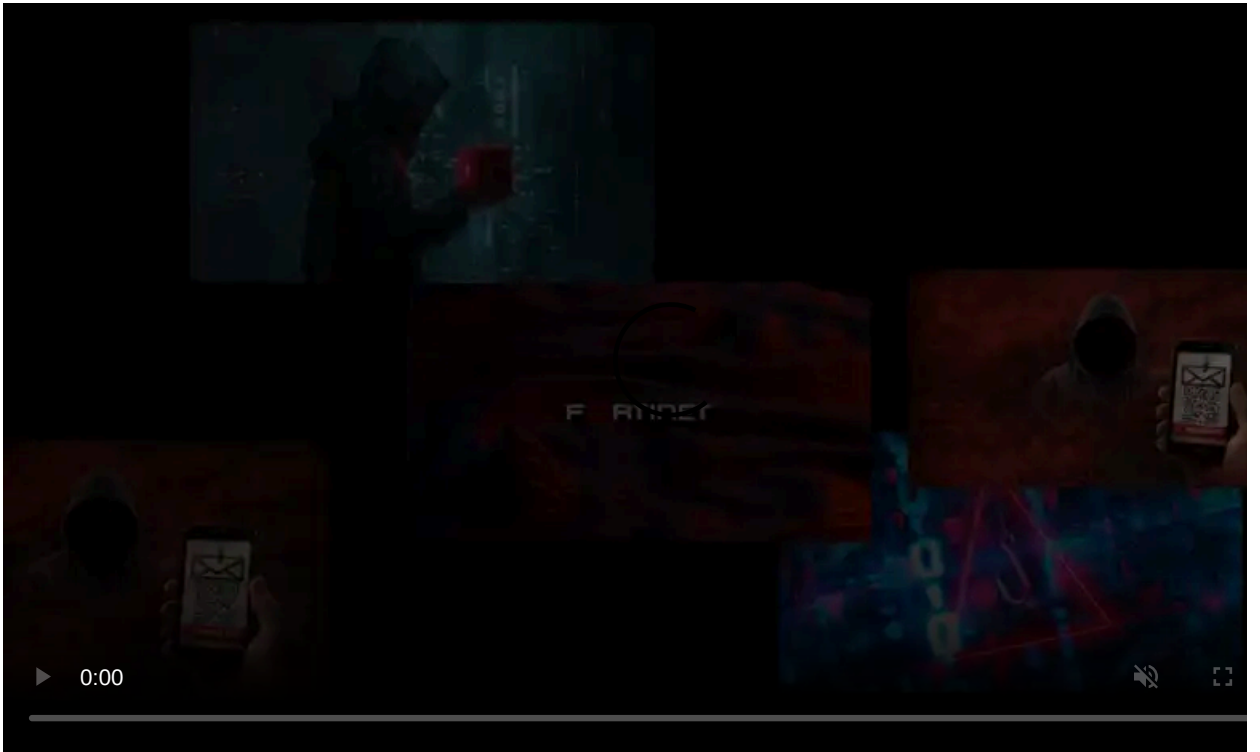
Published: 2022-02-24 · Archived: 2026-04-06 01:05:07 UTC



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.



Visit Advertiser website [GO TO PAGE](#)

1 security vendor and no sandboxes flagged this file as malicious

7989032a5a2baece889100c4cfeca81f1da1241ab47365dad89107e417ce7bac

292.14 KB Size | 2022-02-23 13:23:12 UTC | 15 minutes ago

elf

Community Score

DETECTION | DETAILS | COMMUNITY 10

**Basic Properties**

MD5 58b6696496450f254b1423ea018716dc  
 SHA-1 ad0197db424b35314a479552875e18893a4ba95a  
 SHA-256 7989032a5a2baece889100c4cfeca81f1da1241ab47365dad89107e417ce7bac  
 Vhash 4fa1d07b1895e342dc85b9e0c2d6642e  
 SSDEEP 6144:QY+ftAAWqZgyjxquUHc6/AXaSOsap0YE1swWgCVwk9j\$bhY0:GpFTAF2jxquUHc64XaN4CWgCSk9whB  
 TLSH T14A54CF5692039F1DD3701702248FBBF4B61A232F411CEE9EB849C6AAD77C92761E725  
 File type ELF  
 Magic ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), for GNU/Linux 2.2.5, dynamically linked (uses shared libs), stripped  
 TrID ELF Executable and Linkable format (Linux) (50.1%)  
 TrID ELF Executable and Linkable format (generic) (49.8%)  
 File size 292.14 KB (299148 bytes)

**History**

First Submission 2013-12-19 08:55:54 UTC  
 Last Submission 2013-12-19 08:55:54 UTC

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 Derez on January 24, 2022.

Sample 58b6696496450f254b1423ea018716dc

Size: 299148 | Extracted path: | Matched attribution entities: Evident (73) | Detection names: | Attribution Entity Samples | Previously Analyzed Samples

Similar samples (1)

MD5	Size	Matched genotypes	Matched strings	Similarity	Attribution entity
f4df56203a37706c9e224f29b960dc21	109417	9 / 975	34 / 483	7%	Evident

Matched strings (34)

**Bvp47 sample**

Sample f4df56203a37706c9e224f29b960dc21

Size: 109417 | Extracted path: | Matched attribution entities: Evident (30) | Detection names: | Attribution Entity Samples | Previously Analyzed Samples

Similar samples (1)

MD5	Size	Matched genotypes	Matched strings	Similarity	Attribution entity
6dc7ba05050a37706c9e224f29b960dc21	208908	9 / 1209	3 / 10	30%	Evident

Matched strings (3)

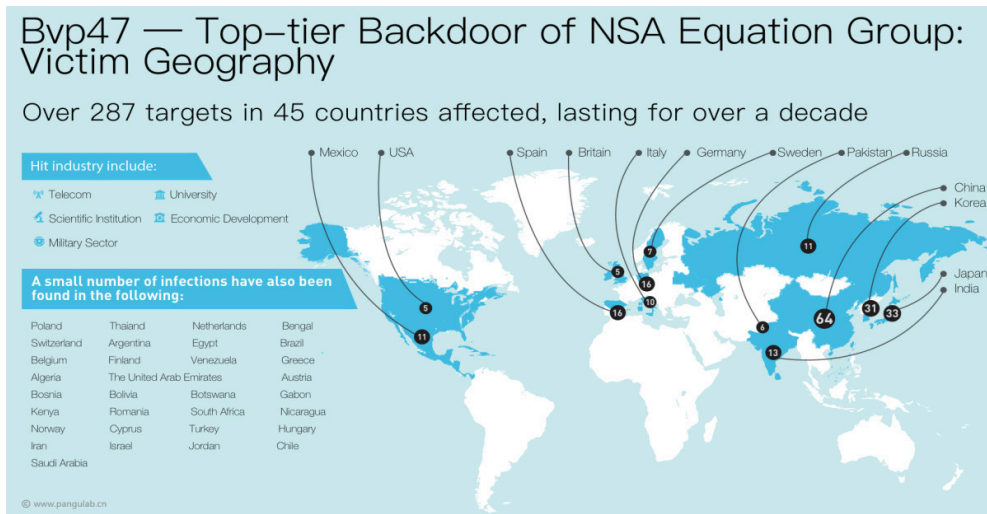
source: Kaspersky

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.

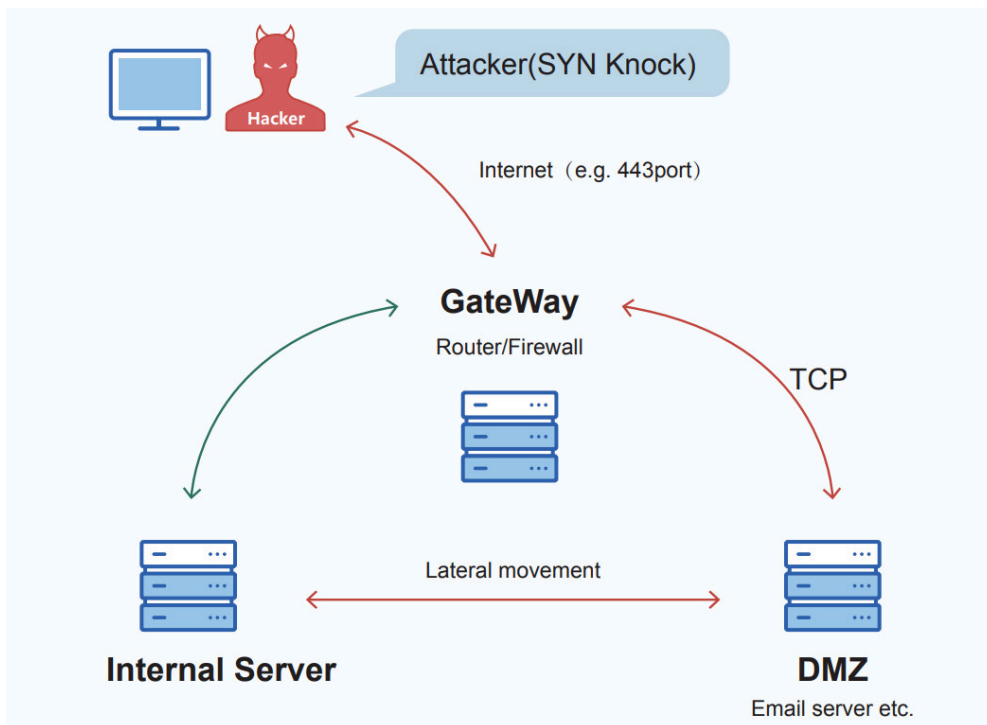
They note that the malware hit more than 287 organizations in 45 countries and went largely undetected for over 10 years.



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.”

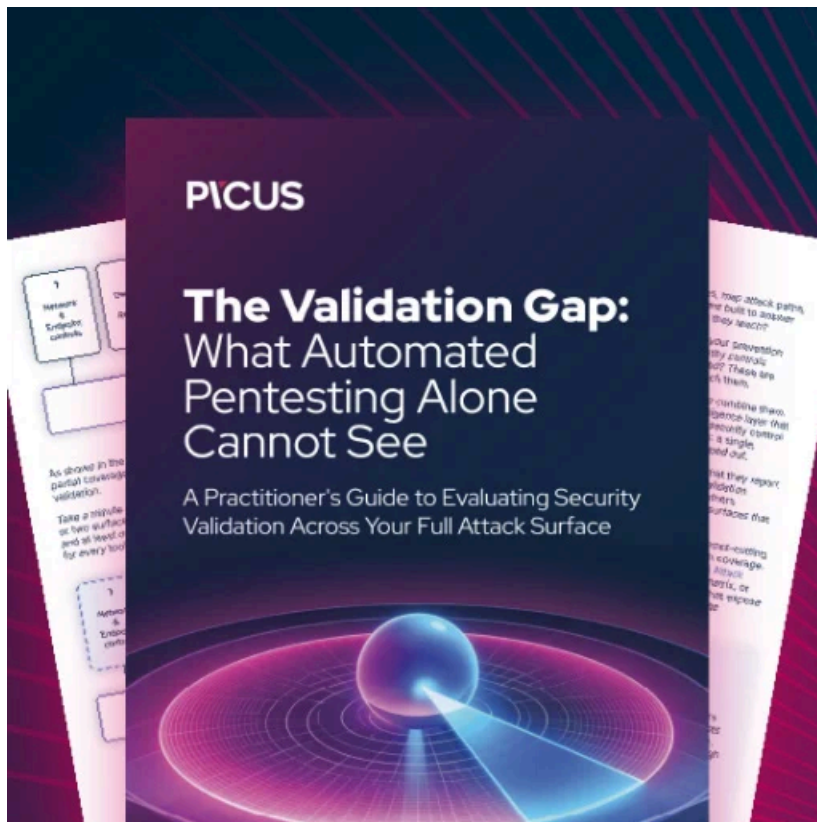
An HTTP server is started on one of the two compromised machines, serving two HTML files to the other. One of the files was a base64-encoded PowerShell script that downloads “index.htm,” which contains asymmetrically encrypted data.

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.”



**[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)**

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---

Source: <https://www.bleepingcomputer.com/news/security/nsa-linked-bvp47-linux-backdoor-widely-undetected-for-10-years/>