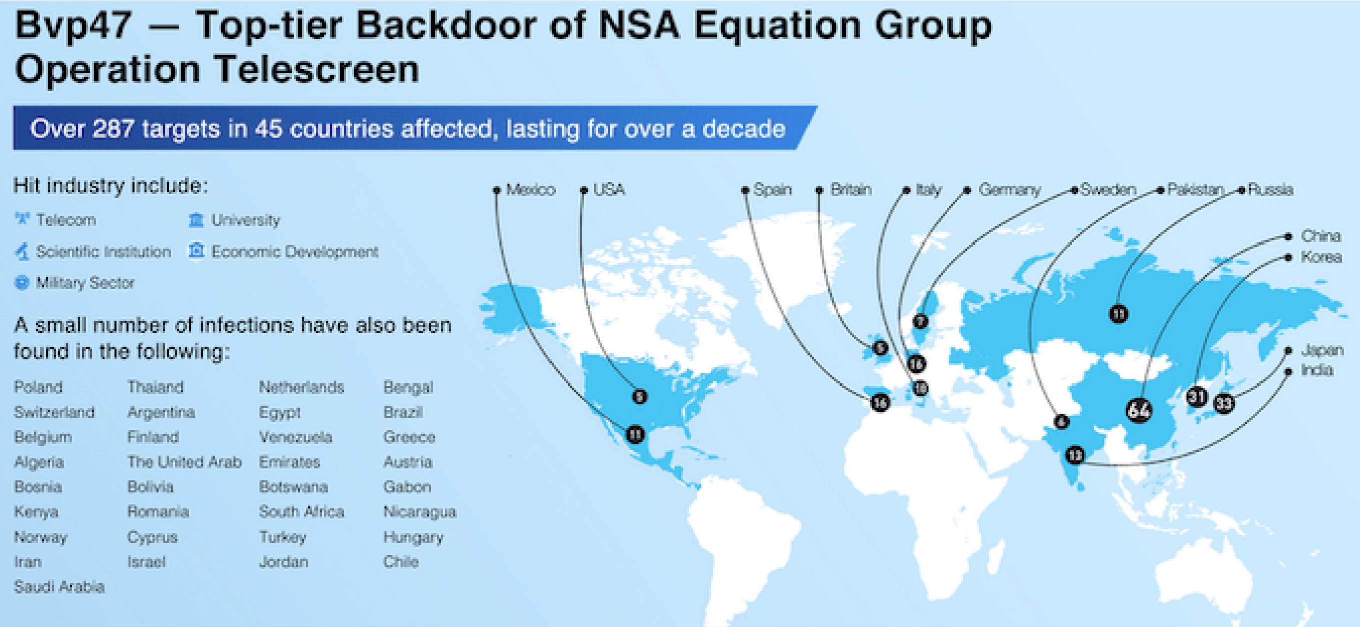

Bvp47 — Top-tier Backdoor of NSA Equation Group
Operation Telescreen

Over 287 targets in 45 countries affected, lasting for over a decade

Hit industry include:

- Telecom
- Scientific Institution
- Military Sector
- University
- Economic Development

A small number of infections have also been found in the following:

Poland
Switzerland
Belgium
Algeria
Bosnia
Kenya
Norway
Iran
Saudi Arabia
Thailand
Argentina
Finland
The United Arab Emirates
Bolivia
Romania
Cyprus
Israel
Netherlands
Egypt
Venezuela
Botswana
South Africa
Turkey
Jordan
Bengal
Brazil
Greece
Austria
Gabon
Nicaragua
Hungary
Chile

Cyber Security

Researchers shared technical details of NSA Equation Group’s Bvp47 backdoor

February 23, 2022 3 min read

Pangu Lab researchers disclosed details of the Bvp47 backdoor that was used by the US NSA Equation Group.

Researchers from The China's Pangu Lab have disclosed details of a Linux top-tier APT backdoor, tracked as Bvp47, which is associated with the U.S. National Security Agency (NSA) Equation Group.

The name "Bvp47" comes form numerous references to the string "Bvp" and the numerical value "0x47" used in the encryption algorithm.

The Bvp47 backdoor was first discovered in 2013 while conducting a forensic investigation into a security breach suffered by a Chinese government organization.

The experts extracted the backdoor from Linux systems "during an in-depth forensic investigation of a host in a key domestic department."

The malware appeared as a top-tier APT backdoor, but in order to further investigate the malicious code required the attacker's asymmetric encrypted private key to activate the remote control function.

In 2016 and 2017, the hacking group The Shadow Brokers leaked a bunch of data allegedly stolen from the Equation Group, including many hacking tools and exploits.

At the end of October 2016, the hackers leaked a fresh dump containing a list of servers that were hacked by the NSA-linked group known as Equation Group.

Pangu Lab researchers discovered the Bvp47 backdoor within the data leaked by The Shadow Brokers.

The leaked data revealed that the Equation Group hit more than 287 targets in 45 countries, including Russia, Japan, Spain, Germany, Italy in a time span of ten years.

The group targeted multiple industries, including governments, telecom, aerospace, energy, financial institutions, nuclear research, oil and gas, military, transportation, and companies developing encryption technologies.

Pangu Lab has tracked the attacks involving the Bvp47 backdoor as "Operation Telescreen," the malicious code was developed to allow operators to achieve long-term control over infected devices.

"The implementation of Bvp47 includes complex code, segment encryption and decryption, Linux multi-version platform adaptation, rich rootkit anti-tracking techniques, and most importantly, it integrates advanced BPF engine used in advanced covert channels, as well as cumbersome communication encryption and decryption process" reads the report published by the experts.

The experts believe that there were no defense against the network attack capability of the backdoor that is equipped by zero-day vulnerabilities.

Technical details of the backdoor are included in the Pangu Lab's report, it also provides insights on the link between the Equation Group and the US NSA.

The attribution to the Equation Group is based on overlaps with exploits contained in the encrypted archive file "eqgrp-auction-file.tar.xz.gpg" published by the Shadow Brokers after the 2016 failed auction.

Follow me on Twitter: **@securityaffairs** and **Facebook**

Pierluigi Paganini

(SecurityAffairs – hacking, backdoor)

Share On

SHARE

Facebook Twitter Pinterest Linkedin

« Apple AirTag anti-stalking protection bypassed by researchers

Deadbolt Ransomware targets Asustor and QNap NAS Devices »

RELATED POSTS

Russia Sanctions May Spark Escalating Cyber Conflict

📅 February 25, 2022

Did we learn nothing from Y2K? Why are some coders still stuck on two digit numbers?

📅 February 25, 2022

Conti ransomware gang: You attack Russia, we'll hack you back

📅 February 25, 2022

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

Website

□ Save my name, email, and website in this browser for the next time I comment.

Post Comment

Search ... Search

GRID POSTS NEWS

Cyber Security

RUSSIA SANCTIONS MAY SPARK ESCALATING CYBER CONFLICT

February 25, 2022 8 min read

President Biden joined European leaders this week in enacting economic sanctions against Russia in response...

Cyber Security

DID WE LEARN NOTHING FROM Y2K? WHY ARE SOME CODERS STILL STUCK ON TWO DIGIT NUMBERS?

February 25, 2022 9 min read

If you use Mozilla Firefox or any Chromium-based browser, notably Google Chrome or Microsoft Edge,...

Cyber Security

CONTI RANSOMWARE GANG: YOU ATTACK RUSSIA, WE'LL HACK YOU BACK

📅 February 25, 2022 🕘 2 min read

The Conti ransomware gang says that it supports the Russian government's invasion of Ukraine… and…

Cyber Security

UKRAINE: BELARUSIAN APT GROUP UNC1151 TARGETS MILITARY PERSONNEL WITH SPEAR PHISHING

📅 February 25, 2022 🕘 2 min read

The CERT of Ukraine (CERT-UA) warned of a spear-phishing campaign targeting Ukrainian armed forces personnel.…

Cyber Security

DATA WIPER ATTACKS ON UKRAINE WERE PLANNED AT LEAST IN NOVEMBER AND USED RANSOMWARE AS DECOY

February 24, 2022 3 min read

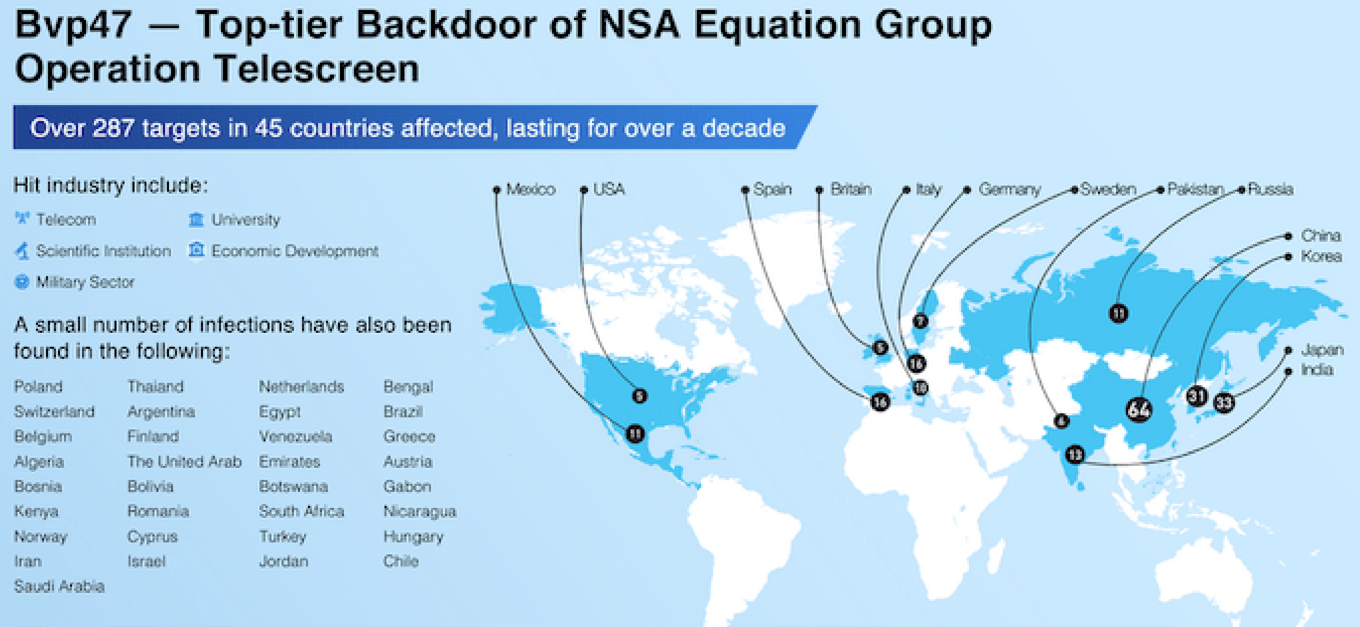
Experts reported that the wiper attacks that yesterday hit hundreds of systems in Ukraine used…

Cyber Security

DEADBOLT RANSOMWARE TARGETS ASUSTOR AND QNAP NAS DEVICES

February 24, 2022 3 min read

Deadbolt ransomware operators are targeting Asustor NAS (network-attached storage) appliances. Storage solutions provider Asustor is...



Bvp47 — Top-tier Backdoor of NSA Equation Group Operation Telescreen

Over 287 targets in 45 countries affected, lasting for over a decade

Hit industry include:

- Telecom
- University
- Scientific Institution
- Economic Development
- Military Sector

A small number of infections have also been found in the following:

Poland
Switzerland
Belgium
Algeria
Bosnia
Kenya
Norway
Iran
Saudi Arabia
Thaiand
Argentina
Finland
The United Arab Emirates
Bolivia
Romania
Cyprus
Israel
Netherlands
Egypt
Venezuela
Botswana
South Africa
Turkey
Jordan
Bengal
Brazil
Greece
Austria
Gabon
Nicaragua
Hungary
Chile

Cyber Security

RESEARCHERS SHARED TECHNICAL DETAILS OF NSA EQUATION GROUP’S BVP47 BACKDOOR

February 23, 2022 3 min read

Pangu Lab researchers disclosed details of the Bvp47 backdoor that was used by the US...

Cyber Security

APPLE AIRTAG ANTI-STALKING PROTECTION BYPASSED BY RESEARCHERS

February 23, 2022 9 min read

When the Apple AirTag hit the market in 2021, it immediately attracted the attention of...

Cyber Security

SOPHOS LINKED ENTROPY RANSOMWARE TO DRIDEX MALWARE. ARE BOTH LINKED TO EVIL CORP?

February 23, 2022 4 min read

The code of the recently-emerged Entropy ransomware has similarities with the one of the infamous...

Cyber Security

HORDE WEBMAIL SOFTWARE IS AFFECTED BY A DANGEROUS BUG SINCE 2012

February 23, 2022 2 min read

Experts found a nine-year-old unpatched flaw in the Horde Webmail software that could allow access...

Cyber Security

IRANIAN BROADCASTER IRIB HIT BY WIPER MALWARE

February 23, 2022 3 min read

Iranian national media corporation, Islamic Republic of Iran Broadcasting (IRIB), was hit by a wiper...

Cyber Security

THREAT ACTORS TARGET POORLY PROTECTED MICROSOFT SQL SERVERS

February 22, 2022 2 min read

Researchers from Ahn Lab’s ASEC spotted a new wave of attacks deploying Cobalt Strike beacons…

Cyber Security

THREAT ACTORS TARGET POORLY PROTECTED MICROSOFT SQL SERVER INSTALLS

February 22, 2022 2 min read

Researchers from Ahn Lab’s ASEC spotted a new wave of attacks deploying Cobalt Strike beacons…

Cyber Security

IRS: SELFIES NOW OPTIONAL, BIOMETRIC DATA TO BE DELETED

February 22, 2022 3 min read

The U.S. Internal Revenue Service (IRS) said Monday that taxpayers are no longer required to…

Cyber Security

REPORT: MISSOURI GOVERNOR'S OFFICE RESPONSIBLE FOR TEACHER DATA LEAK

📅 February 22, 2022 🕘 4 min read

Missouri Governor Mike Parson made headlines last year when he vowed to criminally prosecute a...