REvil ransomware gang claims over $100 million profit in a year

bleepingcomputer.com/news/security/revil-ransomware-gang-claims-over-100-million-profit-in-a-year/

Ionut Ilascu

By
Ionut Ilascu

- October 29, 2020
- 02:02 AM
- 0

REvil ransomware developers say that they made more than $100 million in one year by extorting large businesses across the world from various sectors.

They are driven by profit and want to make $2 billion from their ransomware service, adopting the most lucrative trends in their pursuit of wealth.

Affiliates do the heavy lifting

A REvil representative that uses the aliases “UNKN” and “Unknown” on cybercriminal forums talked to tech blog Russian OSINT offering some details about the group’s activity and hints of what they have in store for the future.

Like almost all ransomware gangs today, REvil runs a ransomware-as-a-service (RaaS) operation. Per this model, developers supply file-encrypting malware to affiliates, who earn the lion’s share from the money extorted from victims.

With REvil, the developers take 20-30% and the rest of the paid ransom goes to affiliates, who run the attacks, steal data, and detonate the ransomware on corporate networks.

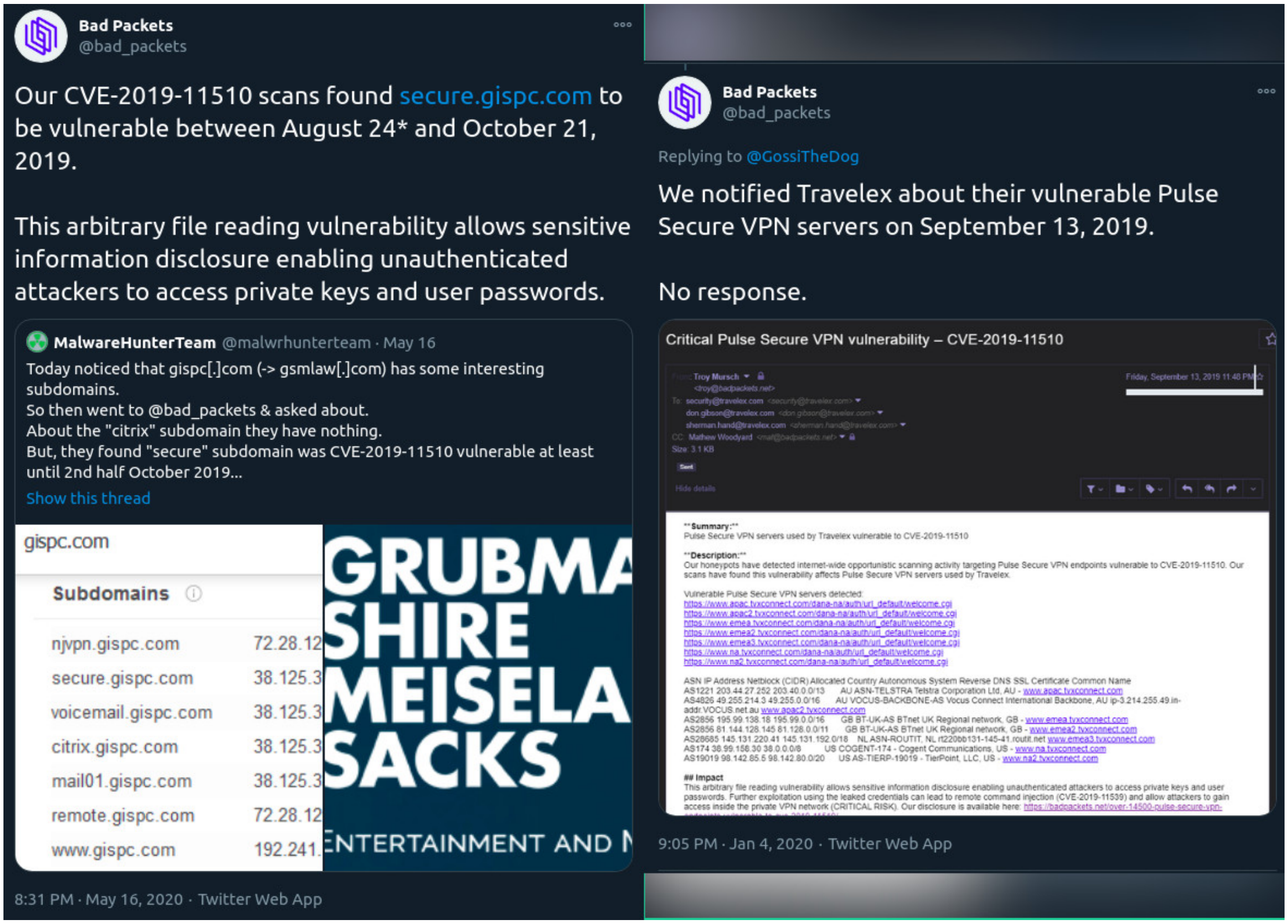
"Most work is done by distributors and ransomware is just a tool, so they think that's a fair split," REvil representative, Unknown, told Russian OSINT.

This means that the developers set the ransom amount, run the negotiations, and collect the money that is later split with affiliates.

Long list of victims

The cybercriminal operation has encrypted computers at big-name companies, among them Travelex, Grubman Shire Meiselas & Sacks (GSMLaw), Brown-Forman, SeaChange International, CyrusOne, Artech Information Systems, Albany International Airport, Kenneth Cole, and GEDIA Automotive Group.

Unknown says that REvil affiliates were able to breach the networks of Travelex and GSMLaw in just three minutes by exploiting a vulnerability in Pulse Secure VPN left unpatched for months after the fix became available [1, 2].



Bad Packets
@bad_packets

Our CVE-2019-11510 scans found secure.gispc.com to be vulnerable between August 24* and October 21, 2019.

This arbitrary file reading vulnerability allows sensitive information disclosure enabling unauthenticated attackers to access private keys and user passwords.

MalwareHunterTeam @malwrhunterteam · May 16
Today noticed that gispc[.]com (-> gsmlaw[.]com) has some interesting subdomains.
So then went to @bad_packets & asked about.
About the "citrix" subdomain they have nothing.
But, they found "secure" subdomain was CVE-2019-11510 vulnerable at least until 2nd half October 2019...
Show this thread

gispc.com

Subdomains

njvpn.gispc.com	72.28.12
secure.gispc.com	38.125.3
voicemail.gispc.com	38.125.3
citrix.gispc.com	38.125.3
mail01.gispc.com	38.125.3
remote.gispc.com	72.28.12
www.gispc.com	192.241.

8:31 PM · May 16, 2020 · Twitter Web App

Bad Packets
@bad_packets

Replying to @GossiTheDog

We notified Travelex about their vulnerable Pulse Secure VPN servers on September 13, 2019.

No response.

Critical Pulse Secure VPN vulnerability – CVE-2019-11510

From: Troy Mursch <troy@badpackets.net>
To: security@travelex.com <security@travelex.com>
don.gibson@travelex.com <don.gibson@travelex.com>
sherman.hand@travelex.com <sherman.hand@travelex.com>
CC: Mathew Woodyard <mat@badpackets.net>
Size: 3.1 KB
Sent
Friday, September 13, 2019 11:48 PM
Hide details

Summary:
Pulse Secure VPN servers used by Travelex vulnerable to CVE-2019-11510

Description:
Our honeypots have detected internet-wide opportunistic scanning activity targeting Pulse Secure VPN endpoints vulnerable to CVE-2019-11510. Our scans have found this vulnerability affects Pulse Secure VPN servers used by Travelex.

Vulnerable Pulse Secure VPN servers detected:
https://www.apac.tvxconnect.com/dana-na/auth/url_default/welcome.cgi
https://www.apac2.tvxconnect.com/dana-na/auth/url_default/welcome.cgi
https://www.emea.tvxconnect.com/dana-na/auth/url_default/welcome.cgi
https://www.emea2.tvxconnect.com/dana-na/auth/url_default/welcome.cgi
https://www.emea3.tvxconnect.com/dana-na/auth/url_default/welcome.cgi
https://www.na.tvxconnect.com/dana-na/auth/url_default/welcome.cgi
https://www.na2.tvxconnect.com/dana-na/auth/url_default/welcome.cgi

```
ASN IP Address Netblock (CIDR) Allocated Country Autonomous System Reverse DNS SSL Certificate Common Name
AS1221 203.44.27.252 203.40.0.0/13      AU ASN-TELSTRA Telstra Corporation Ltd, AU - www.apac.tvxconnect.com
AS4826 49.255.214.3 49.255.0.0/16      AU VOCUS-BACKBONE-AS Vocus Connect International Backbone, AU ip-3.214.255.49.in-
addr.VOCUS.net.au www.apac2.tvxconnect.com
AS2856 195.99.138.18 195.99.0.0/16      GB BT-UK-AS BTnet UK Regional network, GB - www.emea.tvxconnect.com
AS2856 81.144.128.145 81.128.0.0/11      GB BT-UK-AS BTnet UK Regional network, GB - www.emea2.tvxconnect.com
AS28685 145.131.220.41 145.131.192.0/18    NL ASN-ROUTIT, NL rt220bb131-145-41.routit.net www.emea3.tvxconnect.com
AS174 38.99.158.30 38.0.0.0/8         US COGENT-174 - Cogent Communications, US - www.na.tvxconnect.com
AS19019 98.142.85.5 98.142.80.0/20      US AS-TIERP-19019 - TierPoint, LLC, US - www.na2.tvxconnect.com
```

## Impact
This arbitrary file reading vulnerability allows sensitive information disclosure enabling unauthenticated attackers to access private keys and user passwords. Further exploitation using the leaked credentials can lead to remote command injection (CVE-2019-11539) and allow attackers to gain access inside the private VPN network (CRITICAL RISK). Our disclosure is available here: https://badpackets.net/over-14500-pulse-secure-vpn-

9:05 PM · Jan 4, 2020 · Twitter Web App

source: Bad Packets

REvil's public-facing representative says that the syndicate has hit the network of a "major gaming company" and will soon announce the attack.

They also say that REvil was responsible for the attack in September against Chile's public bank, BancoEstado. The incident prompted the bank to close all its branches for a day but did not affect online banking, apps, and ATMs.

Along with managed services providers (MSPs) that have access to networks of multiple organizations, the most profitable targets for REvil are companies in the insurance, legal, and agriculture sectors

As for initial access, Unknown mentioned brute-force attacks as well as remote desktop protocol (RDP) combined with new vulnerabilities.

One example are vulnerabilities tracked as CVE-2020-0609 and CVE-2020-0610 bugs and known as BlueGate. These allow remote code execution on systems running Windows Server (2012, 2012 R2, 2016, and 2019).

New money-making avenues

REvil initially made its profit from victims paying the ransom to unlock encrypted files. Since the attackers also locked backup servers, victims had few options to recover, and paying was the quickest way.

The ransomware business changed last year when operators saw an opportunity in stealing data from breached networks and started to threaten victims with damaging leaks that could have a much worse impact on the company.

Even if it takes longer and causes a significant setback, large businesses can recover encrypted files from offline backups. Having sensitive data in the public space or sold to interested parties, though, can be synonymous with losing the competitive advantage and reputation damage that is difficult to rebuild.

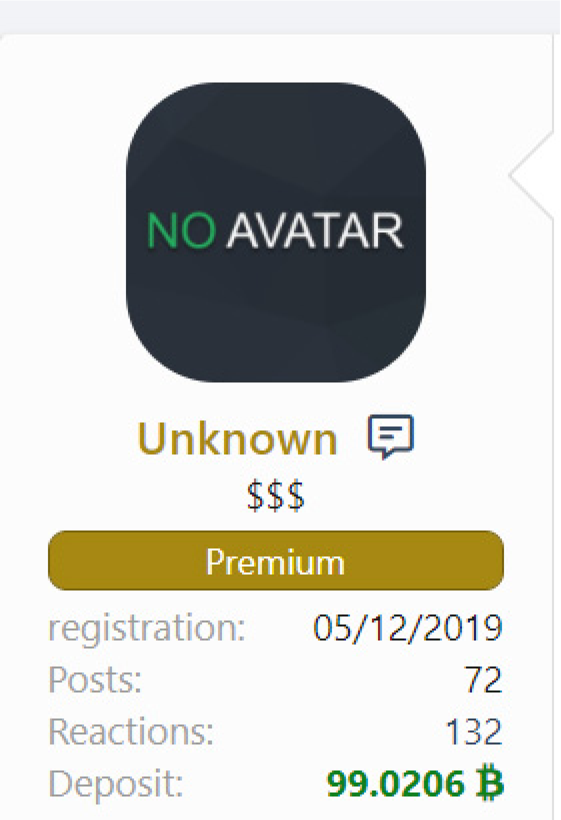
This method proved to be so lucrative that REvil now makes more money from not publishing stolen data than from decryption ransom.

Unknown says that one in three victims are currently willing to pay the ransom to prevent the leaking of company data. This could be the next step in the ransomware business.

REvil is also thinking to adopt another tactic designed to increase their odds of getting paid: hitting the victim with distributed denial-of-service (DDoS) attacks to force them to at least (re)start negotiating a payment.

SunCrypt ransomware used this tactic recently on a company that had stopped negotiations. The attackers made it clear that they launched the DDoS attack and terminated it when negotiations resumed. REvil plans to implement this idea.

REvil's model for making money is working and the gang already has plenty in their coffers. In their search for new affiliates, they deposited $1 million in bitcoins on a Russian-speaking forum.


NO AVATAR

Unknown

$$$

Premium

registration: 05/12/2019

Posts: 72

Reactions: 132

Deposit: 99.0206 ₿

The move was designed to show that their operation generates plenty of profit. According to Unknown, this step is to recruit new blood to distribute the malware, as the ransomware scene is full to the brim with professional cybercriminals.

Although they have truckloads of money, REvil developers are confined to the borders of the Commonwealth of Independent States (CIS, countries in the former Soviet Union) region.

A reason for this is attacking a large number of high-profile victims that prompted investigations from law enforcement agencies from all over the world. As such, traveling is a risk REvil developers are not willing to take.

REvil built on older code

This ransomware syndicate is also referred to as Sodin or Sodinokibi but the name REvil is inspired by the Resident Evil movie and stands for Ransomware Evil.

Their malware was first spotted in April 2019 and the group started looking for skilled hackers (elite penetration testers) shortly after GandCrab ransomware closed shop.

Unknown says that the group did not create the file-encrypting malware from scratch but bought the source code and developed on top of it to make it more effective.

It uses elliptic curve cryptography (ECC) that has a smaller key size than the RSA-based public-key system, with no compromise on security. Unknown says that this is one reason affiliates choose REvil over other RaaS operations like Maze or LockBit.

Before shutting their business, GandCrab developers said they made $150 million, while the entire operation collected more than $2 billion in ransom payments.

Clearly, REvil developer’s ambitions are greater.

BleepingComputer was told that Unknown confirmed that the interview (in Russian) was real.

Watch Video At:

https://youtu.be/ZyQCQ1VZp8s

Related Articles:

Industrial Spy data extortion market gets into the ransomware game

New RansomHouse group sets up extortion market, adds first victims

The Week in Ransomware - May 6th 2022 - An evolving landscape

Conti, REvil, LockBit ransomware bugs exploited to block encryption

REvil ransomware returns: New malware sample confirms gang is back

- Extortion
- Ransomware
- REvil
- Sodinokibi

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

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: