BLEEPINGCOMPUTER

FIN12 hits healthcare with quick and focused ransomware attacks

By Ionut Ilascu

While most ransomware actors spend time on the victim network looking for important data to steal, one group favors quick malware deployment against sensitive, high-value targets.

It can take less than two days for the FIN12 gang to execute on the target network a file-encrypting payload - most of the time Ryuk ransomware.

Fast-moving FIN12

FIN12 is a prolific threat actor with a strong focus on making money that executes ransomware attacks since at least October 2018.

The group is a close partner of the TrickBot gang and targets high-revenue victims (above $300 million) from various activity sectors and regions on the globe.

FIN12 is characterized by skipping the data exfiltration step that most ransomware gangs have adopted to increase their chances of getting paid.

This attribute allows the group to execute attacks at a much faster rate than other ransomware operations, taking them less than two days from the initial compromise to the file encryption stage.

According to data collected from investigations, most ransomware gangs that also steal data have a median dwell time of five days and the average value is 12.4 days.

With FIN12, the average time spent on the victim network dropped each year, getting to less than three days in the first half of 2021.

After getting initial access, the group did not waste any time hitting their victims and in most cases they started activity on the same day.

FIN12 are known for their preference for deploying Ryuk ransomware but the gang also used Conti, Ryuk's successor, in at least one attack investigated by Mandiant.

During the attack, FIN12 also exfiltrated about 90GB of data to multiple cloud storage providers and extorted the victim twice to keep the data off the public space.

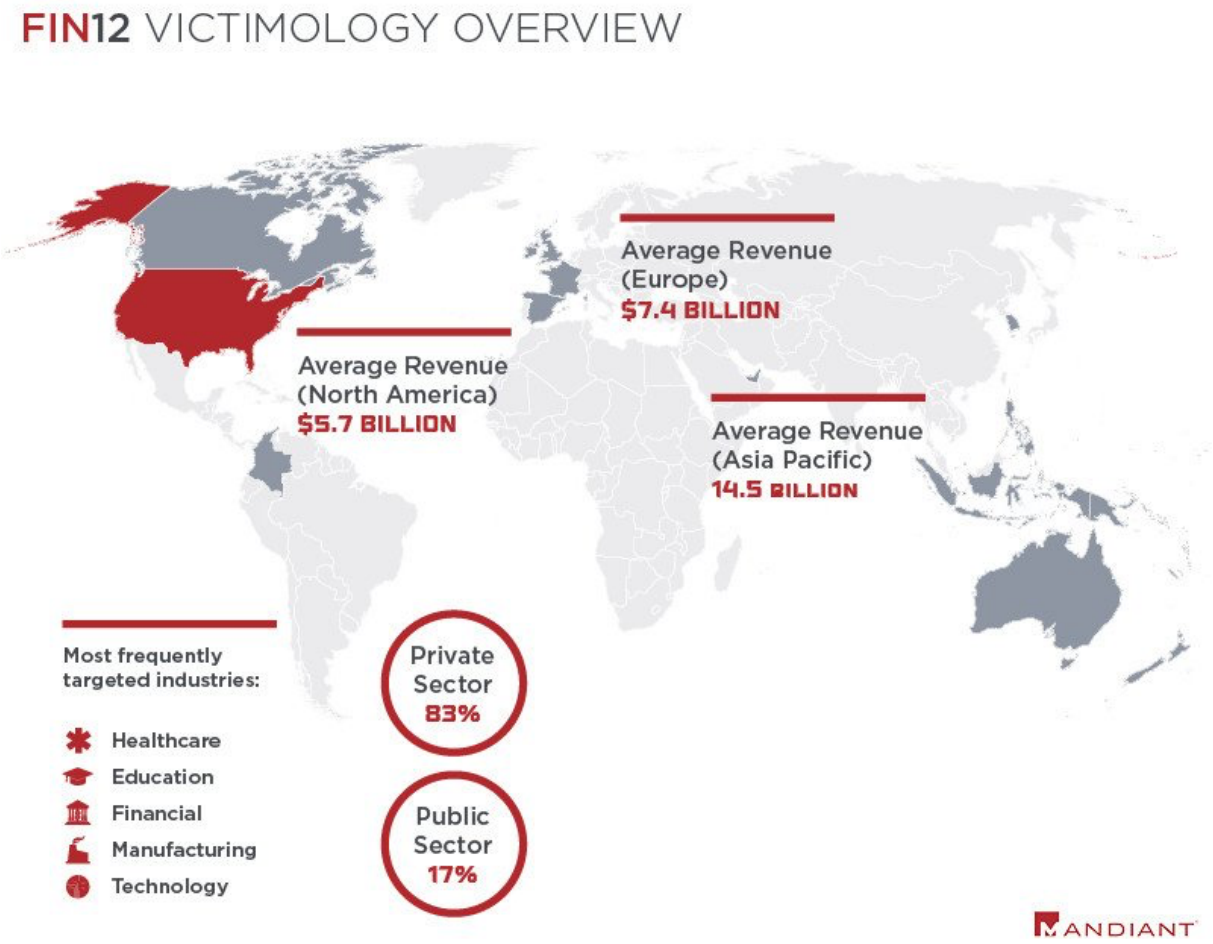
Conti ransomware appeared in isolated incidents at the end of 2019 and shares code with Ryuk. Conti activity picked up in July 2020 as Ryuk ransomware attacks started to become less frequent.

The researchers say that FIN12 also engaged in other ransomware incidents that involved data theft using Ryuk. In those cases, the information was exfiltrated to the attacker's machines and was not leveraged for extortion.

Mandiant says that nearly 20% of their incident response engagements since September 2020 are for FIN12 intrusions.

Healthcare sector most targeted

In a profile of the group published today by cybersecurity company Mandiant, researchers note that many FIN12 victims are in the healthcare sector.



In 2019 and 2020 most of FIN12's victims were located in North America - 71% in the United States and 12% in Canada.

Starting this year, the group appears to have shifted focus to organizations outside this region, targeting companies in Australia, Colombia, France, Indonesia, Ireland, the Philippines, South Korea, Spain, the United Arab Emirates, and the United Kingdom.

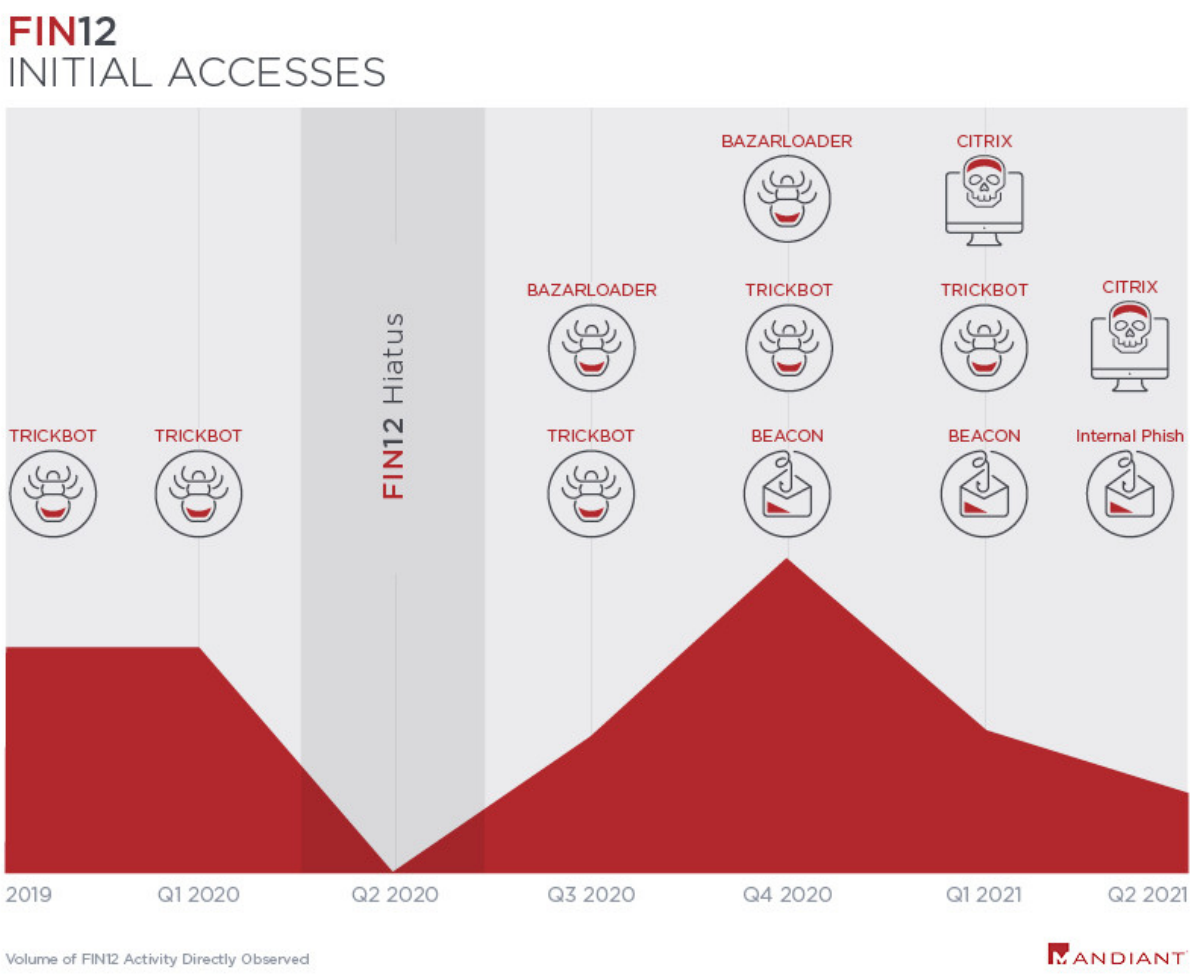
Organizations in the healthcare sector have been a constant target for FIN12, even during the Covid-19 pandemic, as almost 20% of the FIN12 attacks that Mandiant observed were against entities in this industry.

TrickBot's initial access

The researchers note that FIN12 did not breach the networks themselves but obtained initial access from their partners, via TrickBot and BazarLoader in particular; other initial access vectors were observed.

Mandiant says that despite FIN12's use of "overlapping toolsets and services including backdoors, droppers, and codesigning certificates," they track the group as a distinct threat actor because they showed they can work independently of the two malware families.

The set of initial access vectors that the researchers observed includes phishing emails and compromised remote logins to Citrix environments.



The researchers believe that one option FIN12 has in choosing their victims is through a TrickBot administration panel that allows them to interact with compromised machines.

In their choice for post-exploitation tools, the gang is keeping up with the trends, constantly evolving their tactics, techniques, and procedures.

Since February 2020, one constant in the group's intrusions was the use of the Cobalt Strike Beacon. Before that, until mid-2019, they used the PowerShell-based Empire post-exploitation framework.

Mandiant says that after the break from 2020 the group tried other tools (e.g. Convenant/Grunt, the GRIMAGENT and Anchor backdoors) by they returned to Beacon by November 2020.

FIN12 is believed to be a group of Russian-speaking individuals that may be located in the Commonwealth of Independent States (CIS) region.

The gang is likely to further evolve and expand their operations to include data theft as a more common stage of an attack as they start collaborating

with a more diverse assortment of cybercriminals (e.g. ransomware operations with a leak site).