Pulse Report:
Continued Rise in Ransomware Attacks Against Healthcare Providers

It seems almost trite to write a report about ransomware attacks against healthcare providers. After all, organizations as diverse as INTERPOL, Microsoft, and the Cybersecurity Infrastructure and Security Agency (CISA) have all written about the rise in ransomware attacks targeting healthcare providers during the COVID-19 pandemic. What more is there to say?

Last year, Recorded Future wrote about the rise in ransomware attacks against healthcare providers, looking only at publicly reported incidents. Through the end of 2019, Recorded Future had catalogued 134 publicly reported ransomware attacks against healthcare providers, with 38 of those attacks occurring in 2019. This number is much smaller than numbers reported by other security vendors, but the incidents Recorded Future listed were confirmed through open-source reporting, which is always going to be a fraction of the real number.

Security incident reporting for the healthcare industry in the United States is unique because whenever the data of more than 500 patients is exposed in a breach, the provider must file a report with Health and Human Services, which often provides a good starting point for investigating potential ransomware attacks.

However, the aforementioned reporting can lag by several months, so even though this report is being written in June 2020, there will probably be breach notifications for June released well into August and September 2020. In short, the numbers collected so far will likely continue to grow.

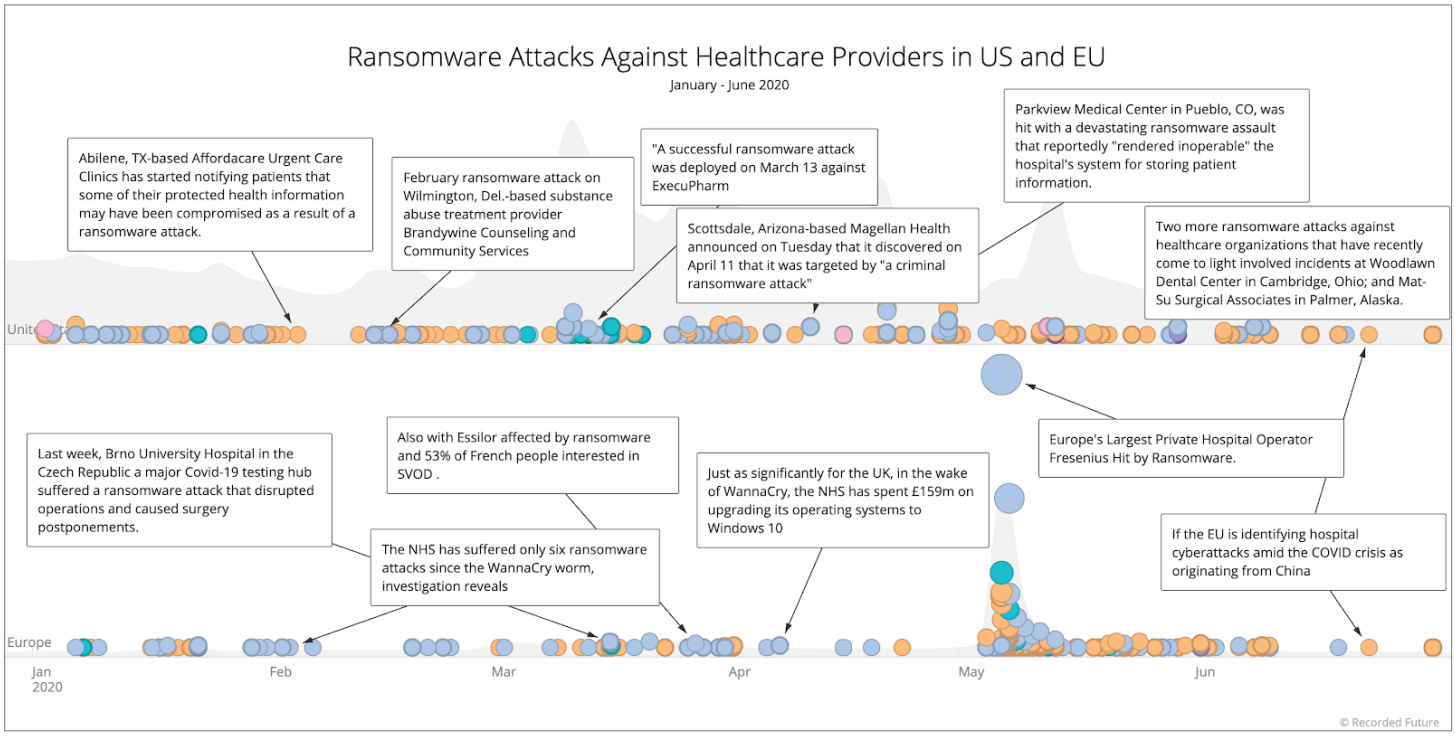

Figure 1: Ransomware Attacks Against Healthcare Providers in the U.S. and Europe

How do the numbers look? So far, in 2020, Recorded Future has catalogued 26 ransomware attacks against healthcare providers in the U.S. While there is no central reporting requirement for ransomware attacks against healthcare providers in Europe, anecdotally, those numbers appear to be on the rise as well.

Breaking the numbers down by month, compared to last year, this is what we have seen through May 2020:

	2019	2020
January	**4**	**4**
February	**1**	**5**
March	**2**	**4**
April	**5**	**6**
May	**3**	**6**

Attacks are up for every month so far this year, and there will undoubtedly be more disclosures for April and May 2020. Also, as shown in the chart above, the "pledge" from ransomware cybercriminals to not attack healthcare providers during the pandemic was a lie.

While it is a small sample size to work with, the ransomware groups that seem to be most focused on attacking healthcare providers are those behind Maze (six confirmed attacks) and Netwalker (four confirmed attacks).

One research angle that makes this year different from previous years is the availability of the extortion websites favored by many ransomware cybercriminals, which Recorded Future scrapes. These websites add an additional collection point to uncover attacks, especially for healthcare providers who are hesitant to report.

Unfortunately, healthcare providers will continue to be heavily targeted by ransomware threat actors. If these criminals didn't slow down attacks during the height of the pandemic, there is no reason to think that they will suddenly find a conscience. Healthcare providers need to take steps to improve their security, while managing reduced security budgets, layoffs of IT and security staff, and in many cases, increased hospitalizations due to COVID-19.

Full dataset available upon request