Issued 6/15/17

Ransomware Uses Pics of Sick Kids to Lure in Victims

Ransomware can be incredibly lucrative for cybercriminals. Older forms of fraud, such as the 419 Nigerian spam emails of the late ’90s and early aughts, required a large workforce to continue to string along the unwitting into sending actual money. Even breaking into the databases of large companies and swiping customers’ credit-card info is a bit of work — once a hacker has possession of the credit-card number, they need to sell them either to a middleman broker or directly to the black market. It’s a complicated ecosystem that requires management. You can still make money, but it takes a bit of effort to navigate an underground economy.

The ransomware then claims, “Congradulations! [sic] Now you are a member of GPAA (Global Poverty Aid Agency).” Unsurprisingly, there is no such agency — doing a search for it only turns up reports of the GPAA ransomware.

Most experts warn against paying up unless your circumstances are truly dire. And even if you do pay off the ransomware authors, there’s never any guarantee that you’ll actually receive the decryption code. Finally, if you actually want to help fight global poverty, donate money of your own accord. (This list is a great place to start.) Not only will you actually be helping people in need, but we’re pretty sure you can’t write off ransom paid via crypto-currency to hackers as charitable giving on your taxes.