Ransomware gangs are running riot and paying them off doesn't help

February 17 2021, by Jan Lemnitzer

Credit: vitalina from Pexels

In the past five years, ransomware attacks have evolved from rare misfortunes into common and disruptive threats. Hijacking the IT systems of organizations and forcing them to pay a ransom in order to

reclaim them, cybercriminals are freely extorting millions of pounds from companies—and they're enjoying a remarkably low risk of arrest as they do it.

At the moment, there is no coordinated response to ransomware attacks, despite their ever-increasing prevalence and severity. Instead, states' intelligence services respond to cybercriminals on an ad-hoc basis, while cyber-insurance firms recommend their clients simply pay off the criminal gangs that extort them.

Neither of these strategies is sustainable. Instead, organizations need to redouble their cybersecurity efforts to stymie the flow of cash from blackmailed businesses to cybercriminal gangs. Failure to act means that cybercriminals will continue investing their growing loot in ransomware technologies, keeping them one step ahead of our protective capabilities.

Daylight robbery

Ransomware is a lucrative form of cybercrime. It works by encrypting the data of the organizations that cybercriminals hack. The cybercriminals then offer organizations a choice: pay a ransom to receive a decryption code that will return your IT systems to you, or lose those systems forever. The latter choice means that firms would have to rebuild their IT systems (and sometimes databases) from scratch.

Unsurprisingly, many companies choose to quietly pay the ransom, opting never to report the breach to the authorities. This means successful prosecutions of ransomware gangs are exceedingly rare.

In 2019, the successful prosecution of a lone cybercriminal in Nigeria was such a novelty that the US Department of Justice issued a celebratory press release. Meanwhile, in February 2021, French and Ukrainian prosecutors managed to arrest some affiliates Egregor, a gang

that rents powerful ransomware out for other cybercriminals to use. It appears that those arrested merely rented the ransomware, rather than creating or distributing it. Cybersecurity experts have little faith in the criminal justice system to address ransomware crimes.

The frequency of those crimes is increasing rapidly. An EU report published in 2020 found that ransomware attacks increased by 365% in 2019 compared to the previous year. Since then, the situation is likely to have become much worse. The US security company PurpleSec has suggested that overall business losses caused by ransomware attacks might have exceeded US$20 billion (£14.3 billion) in 2020, up from US$11.5 billion (£8.2 billion) in 2019.

Even hospitals have suffered attacks. Given the potential impact of a sustained IT shutdown on human lives, healthcare databases are in fact actively targeted by ransomware gangs, who know they'll pay their ransoms quickly and reliably. In 2017, the NHS fell foul of such an attack, forcing staff to cancel thousands of hospital appointments, relocate vulnerable patients, and conduct their administrative duties with a pen and paper for several days.

Waging war?

With ransomware spiraling out of control, radical proposals are now on the table. Chris Krebs, the former head of the US Cybersecurity and Infrastructure Security Agency, recently advocated using the capabilities of US Cyber Command and the intelligence services against ransomware gangs.

The US government and Microsoft coordinated over such a attack in 2020, targeting the "Trickbot botnet" malware infrastructure—often used by Russian ransomware gangs—to prevent potential disruption of the US election. Australia is the only country to have publicly admitted

to using offensive cyber capabilities to destroy foreign cybercriminals' infrastructure as part of a criminal investigation.

Sustained operations of this kind could have an effect on cybercriminals' ability to operate, especially if directed against the gangs' servers and the infrastructure they need to turn their bitcoin into cash. But unleashing offensive cyberwarfare tools against criminals also creates a worrying precedent.

Normalising the use of the armed forces or intelligence units against individuals residing in other countries is a slippery slope, especially if the idea is adopted by some of the less scrupulous regimes on this planet. Such offensive cyber operations could disrupt another state's carefully planned domestic intelligence operations. They could also negatively affect the innocent citizens of foreign states who unwittingly share web services with criminals.

Further, many cybercriminals in Russia and China enjoy de facto immunity from prosecution because they occasionally work for the intelligence services. Others are known to be state hackers moonlighting in cybercrime. Targeting these people might diminish the ransomware threat, but it might just as well provoke revenge from hackers with far more potent tools at their disposal than ordinary cybercriminals.

Paying up

So what is the alternative? Insurers, especially in the US, urge their clients to quickly and quietly pay the ransom to minimize the damage of disruption. Then insurers allow the company to claim back the ransom payment on their insurance, and raise their premiums for the following year. This payment is usually handled discreetly by a broker. In essence, the ransomware ecosystem functions like a protection racket, effectively supported by insurers who are set to pocket higher premiums as attacks

continue.

Aside from the moral objections we might have to routinely paying money to criminals, this practice causes two important practical problems. First, it encourages complacency in cybersecurity. This complacency was best exemplified when a hacked company paid a ransom, but never bothered to investigate how the hackers had breached their system. The company was promptly ransomed again, by the same group using the very same breach, just two weeks later.

Second, some ransomware gangs invest their ill-gotten gains into the research and development of better cyber-tools. Many cybersecurity researchers are concerned about the increasing sophistication of the malware used by leading cybercrime groups such as REvil or Ryuk, which are both thought to be based in Russia. Giving these ransomware groups more money will only enhance their ability to disrupt more and larger companies in the future.

Banned aid

In January 2021, the former head of the UK's National Cyber Security Centre called for cyber-insurance policies that cover ransom payments to be banned, arguing that such payments fund criminal organizations and only make ransomware attacks more common.

In response, the British Association of Insurers became the first European organization to publicly defend the practice, arguing that paying the ransom was the cheapest option for companies. Naturally, that also makes it the cheapest option for insurers. Ransom coverage also helps brokers sell cyber-insurance policies.

In the end, neither calling in the cavalry nor paying off cybercriminals are viable solutions to the growing ransomware problem. Instead, a

sustained effort must be made to build a more robust cybersecurity culture that stands a better chance of repelling ransomware gangs in the first place. This will demand commitment, not just from boards and CEOs, but from employees at every level of an organization.

Improving cybersecurity in all companies won't just protect them from extortion hackers: it's the next frontier in our battle to harden our defenses against state hackers, too. The sooner we start shouldering this pressing responsibility, the better.

Provided by The Conversation