Ransomware: Attacks could be about to get even more dangerous and disruptive

zdnet.com/article/ransomware-why-these-attacks-could-get-even-more-dangerous-and-disruptive

Danny Palmer

Ransomware and hospitals: Why cyber criminals are targeting healthcare during coronavirus and how to stop them

Watch Now

Ransomware is one of the biggest threats facing businesses. An organisation that falls victim to a ransomware attack – which sees cyber criminals use malware to encrypt the network, rendering it inoperable – will quickly find itself unable to do business at all.

Cyber criminals lock down networks like this for one simple reason: it's the quickest and easiest way to make money from a compromised organisation and they're unlikely to get caught.

The attackers demand a ransom payment in exchange for the decryption key for the files – and throughout 2020 the extortion demands have risen, with ransomware gangs now regularly demanding millions of dollars in bitcoin from victims.

The unfortunate reality is that ransomware continues to be successful because a significant number of victims give in to extortion demands of the criminals by paying the ransom. While the police and cybersecurity companies say organisations shouldn't pay criminals, many feel as if it's the quickest and easiest way to restore their network and prevent long-term economic damage – although it still creates plenty of ongoing problems.

And ransomware gangs have increasingly added a new tactic in an attempt to force victims to pay up; they threaten to leak stolen data from the victim, meaning that sensitive corporate data or personal information of customers and clients ends up being made available to other criminals.

"From a financially motivated criminal's perspective, ransomware remains the most lucrative type of cyberattack, especially when the victims are high-value enterprises. In late 2020, cyber criminals are intensifying their attacks to maximise their financial gains and increase

the odds of getting paid," says Anna Chung, cybersecurity threat research analyst for Unit 42 at Palo Alto Networks.

Ransomware attacks have become more powerful and lucrative than ever before – to such an extent that advanced cyber-criminal groups have switched to using it over their traditional forms of crime – and it's very likely that they're just going to become even more potent in 2021.

For example, what if ransomware gangs could hit many different organisations at once in a coordinated attack? This would offer an opportunity to illicitly make a large amount of money in a very short amount of time – and one way malicious hackers could attempt to do this is by compromising cloud services with ransomware.

"The next thing we're going to see is probably more of a focus on cloud. Because everyone is moving to cloud, COVID-19 has accelerated many organisations cloud deployments, so most organisations have data stored in the cloud," says Andrew Rose, resident CISO at Proofpoint.

We saw a taster of the extent of the widespread disruption that can be caused when cyber criminals targeted smartwatch and wearable manufacturer Garmin with ransomware. The attack left users around the world without access to its services for days.

If criminals could gain access to cloud services used by multiple organisations and encrypt those it would cause widespread disruption to many organisations at once. And it's entirely possible that in this scenario ransomware gangs would demand tens of millions of dollars in extortion fees due to what's at stake.

The destructive nature of ransomware could also see it exploited by hacking operations that aren't purely motivated by money.

The first example of this was in 2017 when NotPetya took down networks of organisations around the world and cost billions in damages. While the attack was designed to look like ransomware, in reality the malware was designed for pure destruction as there wasn't even a way of paying the ransom demand.

NotPetya was attributed to the Russian military and it's likely that the idea of using ransomware as a purely destructive cyberattack hasn't gone unnoticed by other nation states. For a government or military force that doesn't want it's enemy to know who is behind a destructive malware attack, posing as cyber criminals could become a useful means of subterfuge.

"We've already seen a precedent that's been set by nation-state actors who have used this, but what if they take it to the next step? The destructive capabilities of ransomware are certainly appealing to malicious espionage actors and they may use it to cause disruption," says Sandra Joyce, senior vice president and head of global intelligence at FireEye.

"So as we continue to see ransomware in the criminal underground continue to rise, we need to be mindful of the fact that nation states are watching and could take this on as their weapon of choice," she adds.

Ransomware will continue to be a major threat, but businesses can help protect themselves from it by applying a small number of relatively simple cybersecurity practices.

Organisations should should ensure they have a well-managed plan around applying cybersecurity patches and other updates. These patches are often released because software companies have become aware of known vulnerabilities in their product, which cyber criminals could be exploiting – by applying the patch in a swift and timely manner, it prevents malicious hackers using these as means of breaking into the network.

One of the other methods cyber criminals use to gain entry to networks is taking advantage of weak passwords, either buy buying them on dark web forums or simply guessing common or default passwords.

To prevent this, organisations should encourage employees to use more complex passwords and accounts should have the additional security of multi-factor authentication, so if an intruder does manage to crack login credentials to gain access to a network, it's harder for them to move around it.

Businesses should also make sure they're prepared for what could happen should they end up falling victim to a ransomware attack. Regularly creating backups of the network and storing them offline means that if the worst happens and ransomware encrypts the network, it's possible to restore it from a relatively recent point – and without giving into the demands of cyber criminals.

Because ultimately, if hacking gangs stop making money from ransomware, they won't be interested in conducting campaigns any more.

MORE ON CYBERSECURITY