DATA PRIVACY AND SECURITY

# GDPR-based extortion could be the next cybercrime trend

Posted by Dan Swinhoe on August 06 2018

Ransomware is so 2017. The popularity of cryptojacking malware ebbs and flows depending on the price of the currencies they mine. Even DDoS attacks are flat after a memcache-based spike earlier in the year. A new report from Malwarebytes said the last few months have been a "slow quarter" due to a "lull" in cybercrime activity.

But now that the World Cup is over and criminals are going back to work, could the recently-enacted General Data Protection Regulation (GDPR) offer up new potential scareware revenue streams? With many companies yet to achieve full compliance the EU's GDPR and the threat of large fines looming, some cyber-experts predict criminals could earn money in exchange for their silence.

## GDPR extortion campaigns could be on the horizon

GDPR came into force on 25th May 2018. In the run-up to the new regulations going into force, phishing emails pretending to be from the likes of Apple, Airbnb, and Natwest hoovered up details of customers clicking through to fake links, proving that criminals are well aware of the new legislation.

But now that the regulations have come into force and most consumers have largely forgotten about GDPR (if they ever cared in the first place), the opportunity is ripe to move onto businesses who will be all too aware of the risks.

A June survey of 600 IT and legal professionals in the UK, US, and EU found 20% of companies surveyed believe they are GDPR compliant. The survey found just over half are in the implementation phase while a quarter have not yet started compliance efforts. Amongst smaller businesses and regions such as the Middle East, Latin America, and APAC, the percentage of compliant companies is even lower. This offers a huge number of potential companies to target.

A number of companies have predicted that the regulations could lead to a rise in cyber-extortion; criminals breaching a company or discovering they are not GDPR complaint – and demanding money in return for not reporting them to the Information Commissioner's Officer (ICO) or equivalent data regulator.

"With the arrival of the GDPR, data that was once considered to be 'boring' or 'worthless', residential addresses etc., can now be used as a source of revenue via GDPR extorsion," says Tom B, Red Team Leader at Thinkmarble.

## How will criminals exploit GDPR and who is a target?

72% of CIOs have already named corporate extortion and ransomware as the most significant risks to businesses, according to a global survey of 900 CIOs by Logicalis.

David Emm, Principal Security Researcher, Kaspersky Lab, predicts that before any extortion attempt is made, criminals will penetrate a company's defenses in the same way they do today. Once they have found a way in, then comes the demand for money.

"They'd have to find a way into a company's system and reveal how they did it – thereby essentially proving that the organization is vulnerable to attack – and that the information they hold can be stolen and used by threat actors."

To prove the breach is real and not just a ruse, hackers would need to show proof that the breach -- and therefore the threat of a large fine – is real.

"They could provide an example of the stolen data as evidence that they've exploited a vulnerability in the system, and thus demonstrate that the right measures haven't put in place by that company to stop breaches happening."

However, even if no evidence is provided, companies would probably need to investigate internally to search to sign of a breach, using up a security team's time and resources.

Rather than report directly to the local data regulator, criminals would publish the information online and making it available to the generic public, making it accessible to the likes of the ICO without the danger of exposing themselves.

Trend Micro is another security company which predicts GDPR-based extortion attacks could become popular.

"I don't think they'll target large enterprises but certainly the small to medium, and maybe not UK ones or European ones but certainly outside of EU borders," says Bharat Mistry, Trend Micro's Principal Security Strategist.

He also predicts that criminals may combine extortion with crypto-ransomware, leading to a catch-22 "double-whammy" where failing to pay the ransom leads to loss of data and someone informing a data regulator that they have breached your organization, but paying the fee and possibly getting access to data still means your company is legally obligated to admit the breach (assuming the criminals don't inform them either way).

The GDPR legalization gives individuals and groups the right to compensation for infringement, and Julie Evans, COO at Exonar, predicts criminals could threaten a company with class action from multiple consumers who have been impacted by a GDPR failure.

"The perpetrator could threaten to expose the GDPR failure to thousands or even millions of consumers, even handling the Data Subject Access Requests (SARs) alone could be crippling for a company, especially if they are still doing that manually, let alone the cost of compensation that could come from such a class action – it would not be capped at 4%."

## When will criminals start exploiting GDPR, and much could the demand?

The fines attached to GDPR -- €20 million or 4% of global turnover – are well-publicized, but how much could a criminal using the threat of telling a data regulator ask for?

F-Secure's chief research officer Mikko Hypponen last year predicted demands could go as high 2% or 3% of the targeted organization's global annual turnover because criminals could easily work out the size of the maximum fine, and many organizations will be willing to pay to keep the fine secret and pay as little as they can.

The actual figure criminals will ask for however, will all depend on what kind of precedent data regulators set and the size of the fines they issue.

"Big fines might be few and far between, and hackers might therefore not know what value an organization would place on a 'hush job'. However, the $100,000 that Uber paid speaks volumes: they thought the breach was worth that amount."

"It's always going to come down to the differential value, for a company to either risk a fine or pay the hush money that the criminal demands."

While we have seen several companies such as Telefonica and Ticketmaster admit data breaches in recent months as well as several GDPR-based lawsuits filed by consumer rights groups, none have resulted in a fine at the time of writing.

Emm predicts that until we've seen an actual headline-grabbing fine issued, there will be few such attempts.

"If the ICO hands out lots of tiny fines, rather than demanding crippling payments, hackers may decide it's not worth their time to hold companies to ransom."

## What to do

While being GDPR compliant is obviously the best way to avoid such attacks, many companies are still on the journey to reach that point. So, what should an organization do if it becomes a victim of a GDPR extortion attempt?

Whether real or merely a 'scareware' attack, you should report it to law enforcement and conduct an internal investigation to access the veracity of the threats. And if they have legitimately compromised your systems, go to the ICO or local equivalent; lying to a regulator only creates more trouble in the long run. Though you may be hit with a fine of some sort, the whole point of GDPR is to encourage companies to be better, so showing you did the right things and acted responsibly will look better than trying to sweep things under the carpet.

When it comes to paying criminals, the advice is the same as ransomware attacks; do not pay, ever. It only enables and encourages more attacks and there's no guarantee they will act honestly after they've received the monies.

"As long as you have a process and plan that shows you are working towards compliance, regulators have said that resultant GDPR fines will be proportionate and context-dependent and theoretically you should only have to pay it once, if at all," says Bas Alberts, VP of Security Projects, Cyxtera. "Ransoms, on the other hand, are at the whim of random attackers."