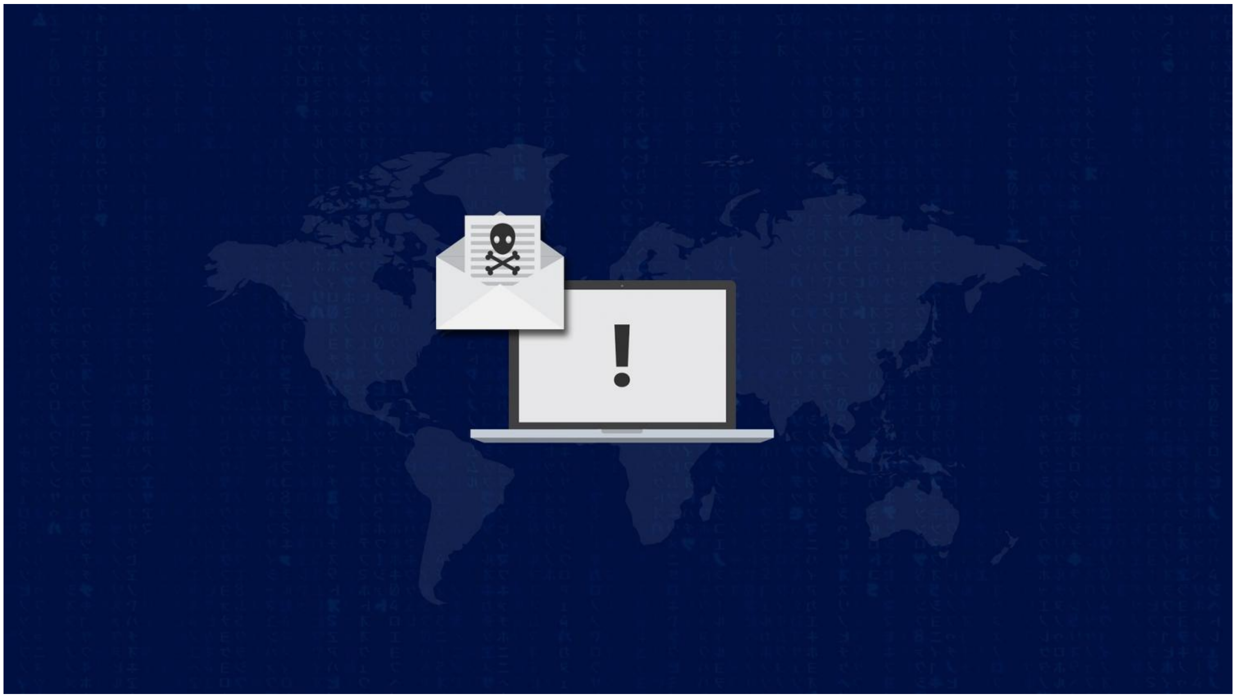
PHYS.ORG

Hackers are making personalised ransomware to target the most profitable and vulnerable

March 18 2019, by Lena Connolly



Credit: CC0 Public Domain

Once a piece of ransomware has got hold of your valuable information, there is very little you can do to get it back other than accede to the attacker's demands. Ransomware, a type of malware that holds a computer to ransom, has become particularly prevalent in the past few years and virtually unbreakable encryption has made it an even more powerful force.

Ransomware is typically delivered by powerful botnets used to send out millions of malicious emails to randomly targeted victims. These aim to extort relatively small amounts of money (normally £300-£500, but more in recent times) from as many victims as possible. But according to police officers we have interviewed from UK cybercrime units, ransomware attacks are becoming increasingly targeted at high-value victims. These are usually businesses that can afford to pay very large sums of money, up to £1,000,000 to get their data back.

In 2017 and 2018 there was a rise in such targeted ransomware attacks on UK businesses. Attackers increasingly use software to search for vulnerable computers and servers and then use various techniques to penetrate them. Most commonly, perpetrators use brute force attacks (using software to repeatedly try different passwords to find the right one), often on systems that let you operate computers remotely.

If the attackers gain access, they will try to infect other machines on the network and gather essential information about the company's business operations, IT infrastructure and further potential vulnerabilities. These vulnerabilities can include when networks are not effectively segregated into different parts, or are not designed in a way that makes them easy to monitor (network visibility), or have weak administration passwords.

They then upload the ransomware, which encrypts valuable data and sends a ransom note. Using information such as the firm's size, turnover and profits, the attackers will then estimate the amount the company can afford and tailor their ransom demand accordingly. Payment is typically requested in cryptocurrency and usually between 35 and 100 bitcoins (value at time of publication £100,000–£288,000).

According to the police officers we spoke to, another popular attack method is "spear phishing" or "big game hunting". This involves researching specific people who handle finances in a company and sending them an email that pretends to be from another employee. The email will fabricate a story that encourages the recipient to open an attachment, normally a Word or Excel document containing malicious code.

These kind of targeted attacks are typically carried out by professional groups solely motivated by profit, though some attacks seek to disrupt businesses or infrastructure. These criminal groups are highly organised and their activities constantly evolve. They are methodical, meticulous and creative in extorting money.

For example, traditional ransomware attacks ask for a fixed amount as part of an initial intimidating message, sometimes accompanied by a countdown clock. But in more targeted attacks, perpetrators typically drop a "proof of life" file onto the victim's computer to demonstrate that they control the data. They will also send contact and payment details for release of the data, but also open up a tough negotiation process, which is sometimes automated, to extract as much money as possible.

According to the police, the criminals usually prefer to target fully-digitised businesses that rely highly on IT and data. They tend to favour small and medium-sized companies and avoid large corporations that have more advanced security. Big firms are also more likely to attract media attention, which could lead to increased police interest and significant disruptions to the criminal operations.

How to protect yourself

So what can be done to fight back against these attacks? Our work is part of the multi-university research project EMPHASIS, which studies the economic, social and psychological impact of ransomware. (As yet unpublished) data collected by EMPHASIS indicates that weak cybersecurity in the affected organisations is the main reason why cybercriminals have been so successful in extorting money from them.

One way to improve this situation would be to better protect remote computer access. This could be done by disabling the system when it's not in use, and using stronger passwords and two-step authentication (when a second, specially generated code is needed to login alongside a password). Or alternatively switching to a virtual private network, which connects machines via the internet as if they were in a private network.

When we interviewed cybercrime researcher Bob McArdle from IT security firm Trend Micro, he advised that email filters and anti-virus software containing dedicated ransomware protection are vital. Companies should also regularly backup their data so it doesn't matter if someone seizes the original. Backups must be tested and stored in locations that are inaccessible to ransomware.

These kind of controls are crucial because ransomware attacks tend to leave very little evidence and so are inherently difficult to investigate. As such, targeted ransomware attacks are not going to stop any time soon, and attackers are only likely to get more sophisticated in their methods. Attackers are highly adaptive so companies will have to respond just as smartly.

This article is republished from The Conversation under a Creative Commons license. Read the original articl

Provided by The Conversation

Citation: Hackers are making personalised ransomware to target the most profitable and vulnerable (2019, March 18) retrieved 27 April 2024 from https://phys.org/news/2019-03-hackers-personalised-ransomware-profitable-vulnerable.html