'Vaccine' created for huge cyber-attack

Dave Lee
North America technology reporter

28 June 2017 | Technology

Security researchers have discovered a "vaccine" for the huge cyber-attack that hit organisations across the world on Tuesday.

The creation of a single file can stop the attack from infecting a machine.

However, researchers have not been able to find a so-called kill switch that would prevent the crippling ransomware from spreading to other vulnerable computers.

Experts are still unsure about the attack's origins or its real purpose.

Given that the ransom amount - $300 - was relatively small, some are speculating that the attack may be a front for causing wider disruption or making a political statement.

Among the victims of the attack were the Ukrainian central bank, Russian oil giant Rosneft, British advertising firm WPP and the global law firm DLA Piper.

Also caught up in the attack was at least one hospital in the US city of Pittsburgh.

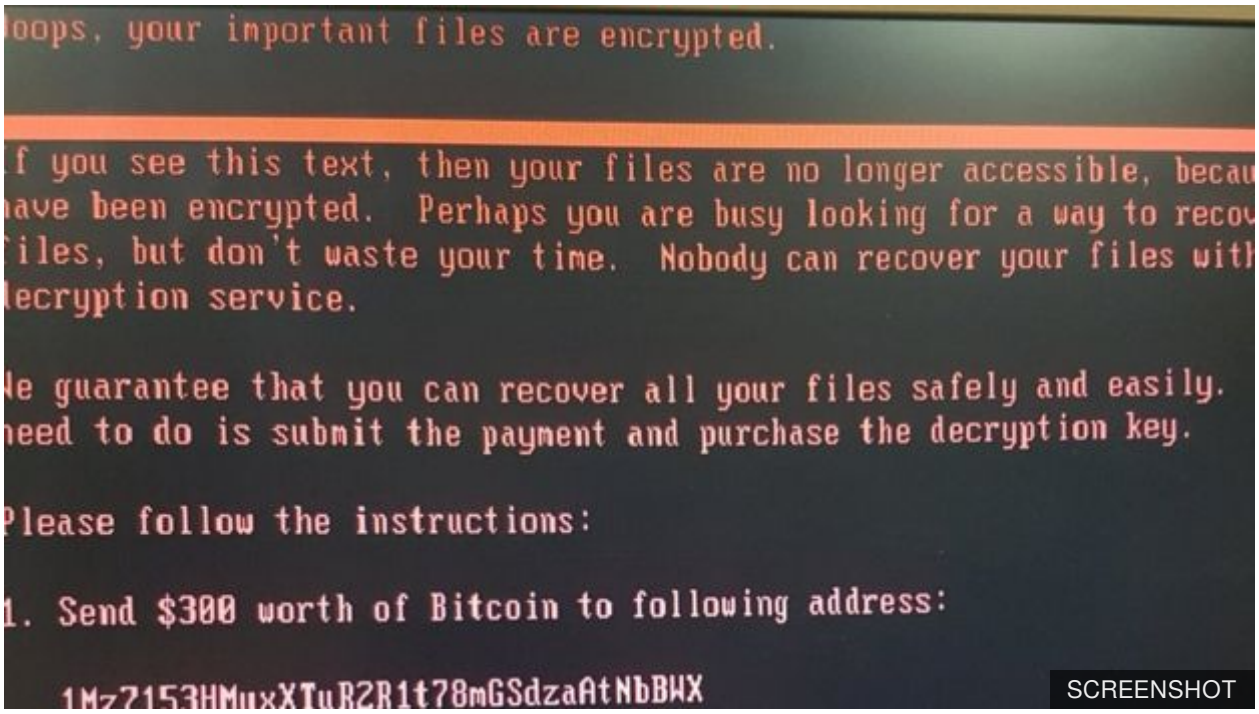
A perfc solution

But for those concerned about the attack there appears to be fix, albeit one with limited effectiveness.

By creating a read-only file - named perfc - and placing it within a computer's "C:\Windows" folder, the attack will be stopped in its tracks.

An explanation of how to do this has been **posted by security news website Bleeping Computer** and has been backed up by several other security experts.

However, while this method is effective, it only protects the individual computer the perfc file is placed on. Researchers have so far been unable to locate a kill switch that would disable the ransomware attack entirely.



"Even though it will make a machine 'immune'," explained computer scientist Prof Alan Woodward, "It is still a 'carrier' (to use the biological analogy).

"It will still act as a platform to spread the ransomware to other machines on the same network."

For the vast majority of users, simply running an up-to-date version of Windows will be sufficient to prevent the attack taking hold, were it to infect your PC.

The spread of this new ransomware is likely to be much slower than last month's WannaCry attack, researchers predict, as code analysis showed the new attack did not attempt to spread itself beyond the network it was placed on.

Because of this, several experts are predicting that the attack will not spread significantly further than it did on Tuesday, unless it is modified.

"There is low risk of new infections more than one hour after the attack," **suggested the MalwareTech blog**.

MeDoc fear

So how did it spread? Experts from Cisco's Talos intelligence unit said it believed the attack may have been carried out by exploiting vulnerable accounting software.

"We believe it is possible that some infections may be associated with software update systems for a Ukrainian tax accounting package called MeDoc," the company **said in a blog post**.

MeDoc initially posted an update to its website on Tuesday saying, in Russian, "Attention! Our server made a virus attack" - though this was later removed, and the company has since denied its software was exploited.

As reported on Tuesday, the method by which victims can pay the ransom fee has been rendered useless. An email address provided by the criminals has been shut down by the hosting provider, while the Bitcoin wallet - where ransoms are deposited - has not been touched.

At the time of writing, the wallet contains approximately $8,000-worth of Bitcoin, not a large return for such a significant and widespread attack.

These factors contribute to a now-prevailing theory that this was a politically motivated attack on Ukraine, coming as it did just as the country is set to celebrate its Constitution Day.

"This looks like a sophisticated attack aimed at generating chaos, not money," said Prof Woodward.

***Follow Dave Lee* on Twitter @DaveLeeBBC**

You can reach Dave securely through encrypted messaging app Signal on: +1 (628) 400-7370

View comments

Related Topics

Computer security

Share this story About sharing

More on this story

Global ransomware attack causes turmoil

28 June 2017

More Technology stories >

Samsung reuses Note 7 parts for new phone

1 hour ago

Silicon Valley's women have spoken. Now what?

1 July 2017

Drone causes Gatwick airport disruption

7 hours ago

Top Stories

Gulf states give Qatar 48-hour extension
Qatar gets two more days to meet a list of demands to lift a blockade by Saudi Arabia and its allies.
1 hour ago

China calls US warship 'a provocation'
35 minutes ago

Eight injured in France mosque shooting
3 hours ago

Most Read