'Ransomware' wave seemed aimed at old flaw and Ukraine

June 28 2017

Ukraine's central bank says a cyberattack hit several lenders in the country, hindering operations and leading the regulator to warn other financial institutions to tighten security measures

A global wave of cyberattacks exploited an already patched vulnerability in Windows software and appeared to have Ukraine as a primary target, according to computer security specialists.

The first reports of trouble came from Ukrainian banks, Kiev's main airport and Rosneft, in a major incident reminiscent of the recent WannaCry virus.

WannaCry was a version of ransomware that, once in a computer, locked away data from users who were then told to pay to have access returned to their own files.

The bedeviling onslaught Tuesday was also being referred to as ransomware by US software titan Microsoft and security specialists.

"Our initial analysis found that the ransomware uses multiple techniques to spread, including one which was addressed by a security update previously provided for all platforms from Windows XP to Windows 10 (MS17-010)," a Microsoft spokesperson told AFP.

After the WannaCry scourge in May, Microsoft called on people to protect machines with the MS17-010 patch.

The flaw—and the means to exploit it—had previously been disclosed in pirated documents about cyber weapons at the US National Security Agency.

Microsoft said that its anti-virus software detects and removes the ransomware used in the latest attack.

Microsoft is continuing to investigate the latest cyberattack and will take necessary steps to protect customers, the spokesperson said.

People were also urged to be wary of clicking on email attachments or shared links, since that is a common trick used to unleash malicious code on computers.

"As ransomware also typically spreads via email, customers should exercise caution when opening unknown files," the Microsoft spokesperson said.

Identification of the way the latest ransomware initially got into machines was proving challenging, and the use of email was not confirmed, according to a post by Cisco Talos threat intelligence.

"Based on observed in-the-wild behaviors, the lack of a known, viable external spreading mechanism and other research we believe it is possible that some infections may be associated with software update systems for a Ukrainian tax accounting package called MeDoc," Cisco Talos wrote.

Ukraine's central bank said several lenders had been hit in the country, hindering operations and leading the regulator to warn other financial institutions to tighten security measures.

The virus is "spreading around the world, a large number of countries are affected," Costin Raiu, a researcher at the Moscow-based Kaspersky Lab said in a Twitter post.

The cryptolocker demands $300 in bitcoins and does not name the encrypting program, which makes finding a solution difficult, Group IB spokesman Evgeny Gukov said.