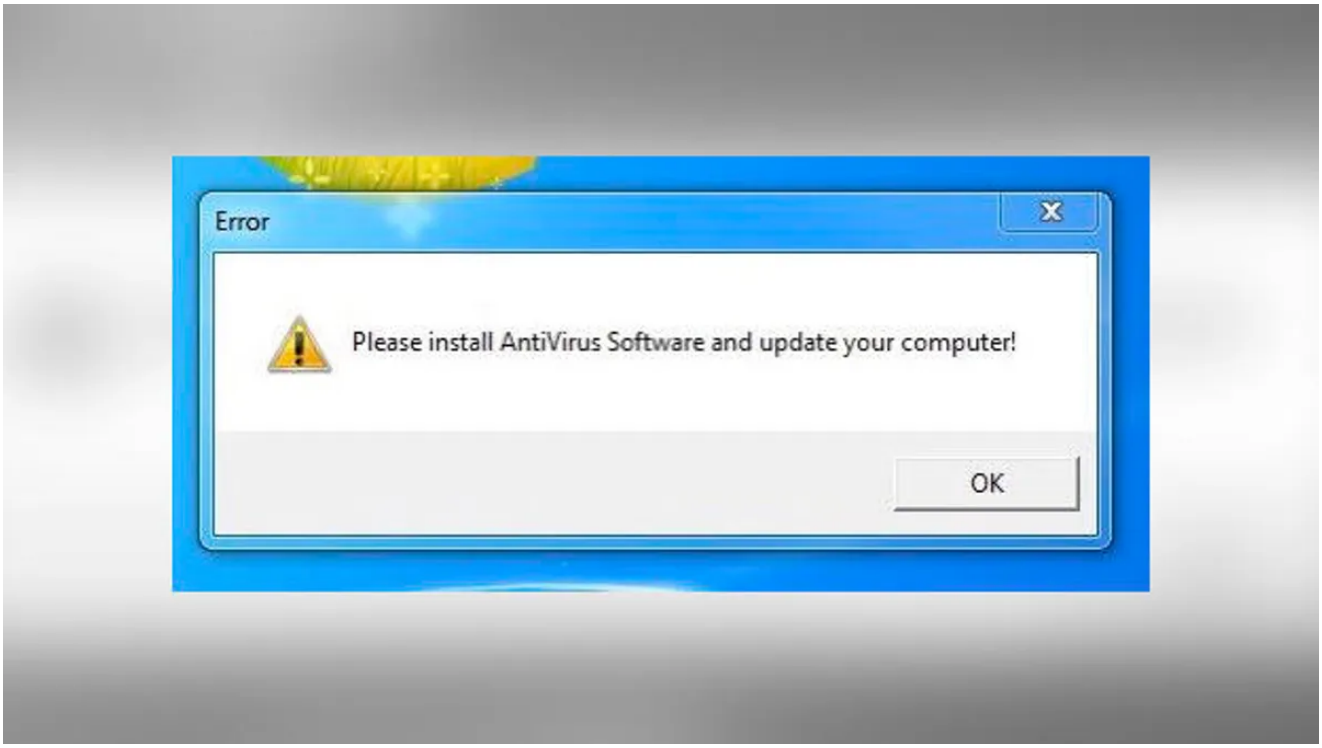
Someone is uninstalling the Phorpiex malware from infected PCs and telling users to install an antivirus

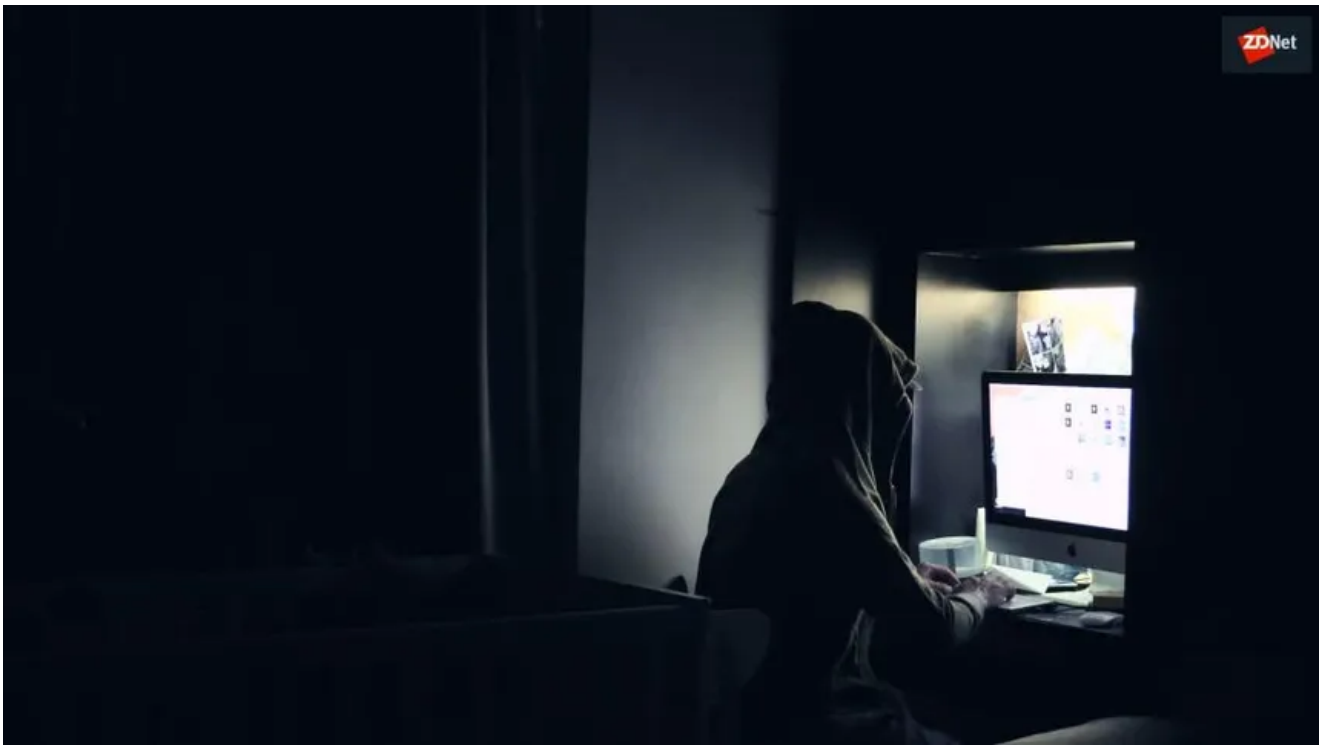
zdnet.com/article/someone-is-uninstalling-the-phorpiex-malware-from-infected-pcs-and-telling-users-to-install-an-antivirus/



Home Innovation Security

Malware analysts believe someone has hijacked the Phorpiex botnet from its creator and is sabotaging its operations by alerting users they've been infected.

Written by Catalin Cimpanu, Contributor on Jan. 23, 2020



A mysterious entity appears to have hijacked the backend infrastructure of the Phorpiex (Trik) botnet and is uninstalling the spam-bot malware from infected hosts, while also showing a popup telling users to install an antivirus and update their computers, ZDNet has learned.

The popups have started appearing on users' screens today, early morning, US Eastern time, and have been spotted by the research team at antivirus vendor Check Point.

Initially, ZDNet and others thought this was a prank coded inside the malware by the Phorpiex team for the purpose of trolling security researchers analyzing the malware.

However, as the hours passed, it became clear that this was actually taking place on customer systems, in the real world, and was not just a popup that was appearing in virtual machines used as malware analysis sandboxes.

"This is truly happening," Yaniv Balmas, Head of Cyber Research at Check Point, told ZDNet. "We are closely monitoring this malware family and have noticed this behavior started just a few hours ago."

Balmas listed several theories as what could have happened -- such as the malware operators deciding to quit and shut down the botnet on their own terms, a law enforcement action, a vigilante security researcher taking matters into his own hands, or a rival malware gang sabotaging the Phorpiex crew by destroying their botnet.

Most likely a hijack

"Hijack seems likely based on the track record for the Phorpiex developer," said a second malware analyst, who declined to have his name used in this article because he was not authorized to speak in his company's name -- another antivirus vendor.

"The Phorpiex developer has some pretty nasty rivals in the botnet game so it wouldn't surprise me if this is an attack motivated by jealousy or something along those lines," he added.

"The developer for the Phorpiex botnet is extremely lazy and careless," the malware analyst said, claiming that he could have also hijacked the botnet in the past due to its simplistic IRC-based command and control mechanism.

Same botnet suffered a data breach in 2018

The Phorpiex malware, which has been active for more than a decade, has suffered security breaches in the past, also due to the malware developer's carelessness.

In 2018, the Phorpiex developer left one of the botnet's command and control backend servers exposed online, and security researchers were able to retrieve a list of 43.5 million email addresses that the Phorpiex crew was targeting with spam campaigns.

Phorpiex is one of today's most active spam botnets. The Phorpiex team operates by infecting Windows computers and using these systems as spam bots to send out massive spam campaigns.

These spam campaigns keep the spam botnet alive, by infecting new PCs with Phorpiex, but they also send out custom spam campaigns on behalf of other cybercrime groups -- the method through which the Phorpiex crew makes its money.

Whoever hijacked the botnet today and instructed bots to uninstall themselves has put a serious dent in the Phorpiex gang's future profits and operations. To give an idea about the size of the profits the Phorpiex crew lost, Check Point previously reported that the same botnet made $115,000 in five months just from mass-spamming sextortion emails.

The FBI's most wanted cybercriminals