More than 60% of US office workers are unaware of the ransomware threat

Stu Sjouwerman

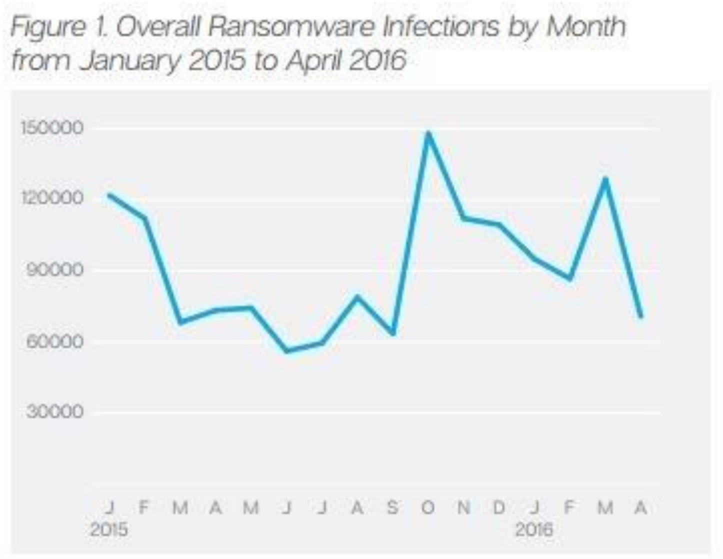


Figure 1. Overall Ransomware Infections by Month from January 2015 to April 2016

Nearly half of ransomware attacks are aimed at office workers, but almost two-thirds of those polled are unaware of the threat

More than 60% of US office workers are unaware of ransomware and the threat it poses to business, according to a survey of more than 1,000 employees commissioned by security firm Avecto.

Ransomware infections are typically triggered by people clicking on malicious links in legitimate-looking emails or opening attachments that have a malicious payload.

The survey also showed that 39% of respondents either have no confidence that their employer has measures in place to protect them against cyber threats or they are unaware of what their employer is doing to safeguard their online safety.

While 58% of those surveyed feel their employer regularly updates them on cyber threats, more than a quarter (28%) said security education is rare or only provided after something has gone wrong, when it is often too late.

Why does this matter?

More than 4,000 ransomware attacks occur every day, according to US government statistics, earning cyber criminals more than $208m in first three months of 2016 alone, projecting it to be a 1 billion dollar business for this year.

According to a report by security firm Symantec, ransomware attacks are becoming more targeted and a number of ransomware groups have begun using advanced attack techniques, displaying a level of expertise similar to that seen in many cyber espionage attacks.

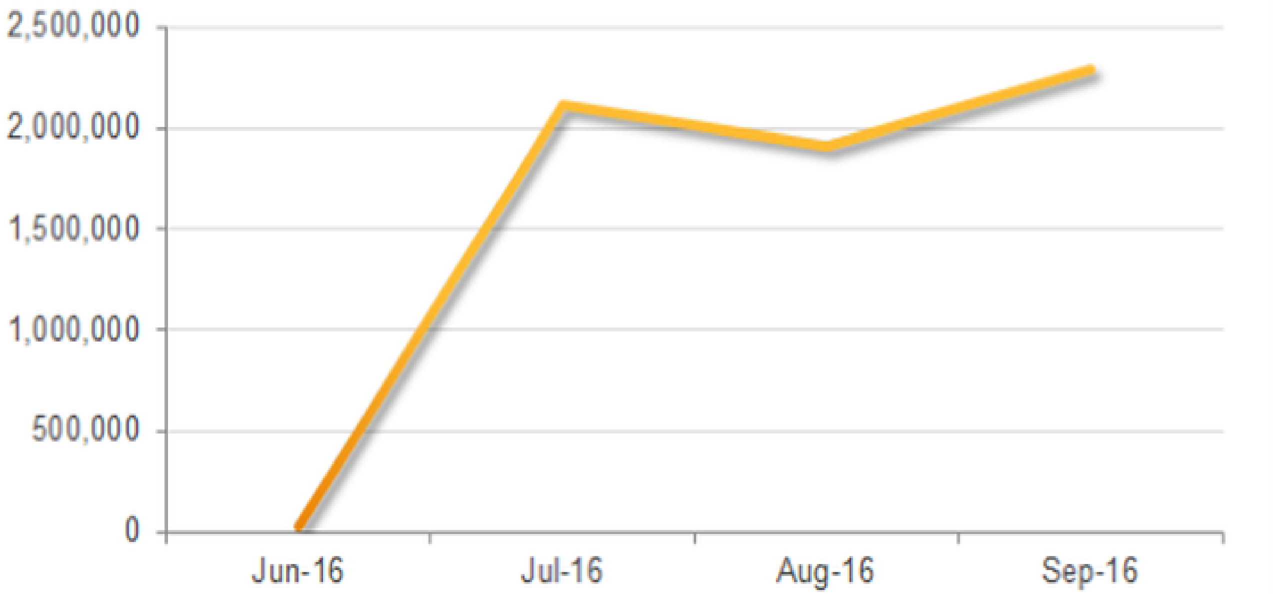
It gets worse...

Symantec also reported that organized cybercrime has evolved yet another new tactic to infect victims with ransomware, specifically the gang responsible for the notorious Locky campaign.

Email is the #1 delivery method of ransomware but over the last three months there's been a shift in tactics, with cybersecurity researchers at Symantec spotting a sudden surge in Windows Script Files (WSF) used to distribute ransomware. WSF files are opened by Windows Script Host (WSH) and are designed to allow a variety of scripting languages to mix within a single file.

What makes files with the .wsf extension appealing is that they're not automatically blocked by some email clients and can be launched like a standard executable file. Having realized that WSF files are less likely to be blocked by endpoint security, ransomware campaigns using that extension type have massively jumped in recent months.

Symantec researchers say 22,000 emails containing malicious .wsf files were blocked in June and that figure had multiplied by almost 100 times by July to 2 million. The figure has remained steady since then, with 2.2 million malicious .wsf files blocked in September.



The rise in ransomware emails using WSF. Image: Symantec