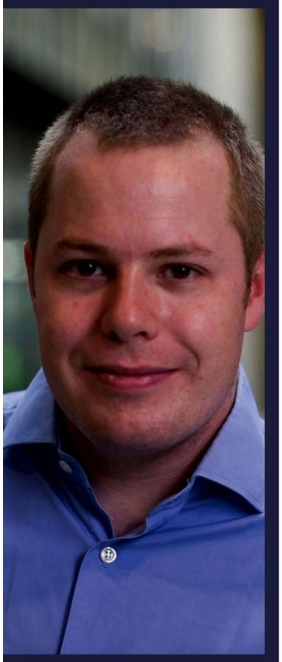
WED, 11 OCT 2017

Time to Bolster Defenses

Time to Bolster Defenses

PREVENT, CONTAIN, RESPOND– SYMANTEC TELLS US HOW ORGANIZATION SHOULD FOLLOW THE 3-STEP STRATEGY TO PREPARE FOR THE RANSOMWARE OF THREATS.



CANDID WUEEST,
SECURITY ANALYST AND RESEARCHER AT SYMANTEC

? How has the evolution of Ransomware been in 2017?

While ransomware has long been one of the main cyber threats to businesses, the past number of months have seen organizations more exposed than ever. Symantec's latest research paper on ransomware has found that businesses were the main victims of the WannaCry and Petya outbreaks, with corporate networks the ideal breeding ground for this new generation of self-propagating threats. Our research found that overall ransomware infection numbers have continued to trend upwards. During the first 6 months of 2017, Symantec blocked just over 319,000 ransomware infections. If this infection rate continued for the full year, 2017 would be a significant increase over 2016, when a total of 470,000 infections were blocked. Contributing to this increase was a spike in blocked infections during May and June 2017, the months when the WannaCry and Petya outbreaks occurred.

This year saw the arrival of a new generation of self-propagating ransomware. WannaCry, which was the first to appear, caused global panic due to its ability to spread itself across the networks of infected organizations and then spread to other organizations across the internet. Petya mimicked some of the techniques employed by WannaCry to spread itself across networks.

WannaCry and Petya's disproportionate impact on organizations can be seen in infection statistics. During 2015 and 2016, businesses accounted for between 29 and 30 percent of ransomware infections. That figure shot up to 42 percent in the first half of 2017, with a major spike in business infections during May and June, the months WannaCry and Petya spread.

? How should organizations safeguard themselves from attacks like Wannacry & Petya?

Building a multi-layered defense ensures that any point of failure is mitigated by other defensive practices. This should include not only regularly patching vulnerabilities and ensuring critical systems are backed up, but also employing multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method.

Tips for businesses and consumers

- Always keep your operating system & software updated.
- Do no open unknown links/attachments
- Do not enable macros.
- Always backup your files

? How will the concept of 'RoT' – Ransomware of Things change the course of security?

IoT devices are increasingly becoming a lucrative source for cybercriminals, notably devices such as smart TVs and smart watches, which could be a profitable attack scenario.

Ransomware is commonly used by attackers on expensive devices with a screen to clearly display the ransom message, hence we do not expect to see ransomware on all smart devices. However, we already see a shift in the security landscape when it comes to protecting our smart devices from RoT infections and it focuses on adopting a multi-layered approach.

Symantec's comprehensive 3-step strategy outlines how we can best prepare for the future of RoT:

1. **Prevent:** Email security, Intrusion Prevention, Download Insight, Browser Protection, Proactive Exploit Protection (PEP).
2. **Contain:** Advanced __ antivirus engine with machine learning heuristic technologies (SAPIENT) and behaviour based detection
3. **Respond:** Dedicated Incident Response team to help organizations respond and recover from a ransomware attack.