Ransomware Hits Office365

On June 22 at 6:44 a.m. UTC, Avanan's Cloud Security Platform detected a massive ransomware attack against customers using Office 365 for email. The attack, identified as *Cerber*, encrypts users' files like other ransomware, but tauntingly, also demands $500 payment via an audio file. Microsoft was eventually able to block the malware later that day, but in that time, Avanan estimates that over 57% of customers were sent at least one version of the file.

This attack was a variant of a ransomware virus released in March of this year. While earlier versions were spread via infected websites and zero-day vulnerabilities, this attack was successful because it was delivered via a benign-looking Office document that had been designed to bypass Offices 365's Advanced Persistent Threat email security filters.

THE BASICS

- Cerber spread via phishing emails with a macro-enabled Microsoft Word document.
- Once infected, a victim's files became encrypted using the AES-265 and RSA encryption method, which is currently unbreakable.
- Victims are given a message saying they need to pay a ransom of ~$500 USD to decrypt their files.
- Victims are further taunted by an audio message that repeats "Attention! Attention! Attention! Your documents, photos, databases and other important files have been encrypted!"
- Currently, there is no way to recover files except by restoring from backup or paying the ransom.

SAAS MALWARE ON THE RISE

As more enterprises are moving to SaaS-based email, malware attackers have followed. "Many users of cloud email programs believe they 'outsourced' everything to Microsoft or Google, including security," explains Gil Friedrich, CEO of Avanan. "The reality is that hackers first make sure their malware bypasses major cloud email providers' security measures, so most new malware reaches SaaS-email inboxes undetected. This is why the majority of the users of Avanan's Cloud Security Platform activate advanced sandboxing protection such as Check Point SandBlast—a best practice that proved very effective in this incident. It is the minimum required to protect against the most sophisticated and evasive attacks."

ZERO-DAY DEFENSE

After it was reported, Microsoft acknowledged the attack and noted that its internal security tools were updated to respond later the same day. During the window of opportunity, Avanan customers were protected by the many security partners available on its platform. In this case, Check Point.

Avanan email-protection suite immediately discovered the virus using Check Point's SandBlast malware sandboxing solution. SandBlast identified the attack as a sophisticated zero-day version of ransomware virus so that Avanan was able to remove and quarantine the file before it reached users' inboxes. Traditional antivirus tools were not able to detect this attack at the time it occurred so users had no desktop defense, should they have opened the file.

"We are seeing a significant increase in the complexity of malware targeting business users, and this attack is an excellent example. By utilizing several exploit kits, it was able to bypass Microsoft's APT sandboxes. It speaks to the effort hackers are putting into creating targeted zero-day attacks," said Nathan Shuchami, head of threat prevention, Check Point. "Our SandBlast Zero-Day Protection product provides organizations the advanced threat prevention they need to stop malware at the pre-infection stage to ensure they are effectively secured against the latest threats."

As attackers become more sophisticated, email security must keep up. Only Avanan offers the most advanced technology from the industry's most trusted names.