

Cerber ransomware targeted to Office 365 users - blueAPACHE

Canonical: <https://www.blueapache.com/blog/cerber-ransomware-attack-on-microsoft-office-365-users>

Details:

Historical article: 5 July 2016. Campaign descriptions and figures below relate to that period.

Hackers target Microsoft's built-in security to distribute ransomware to Office 365 users

Last week, a massive zero-day attack was launched against Microsoft Office 365 users with a cryptolocker virus called Cerber. According to industry estimates, over 57 percent of companies that use Office 365 received at least one copy of the malware hidden in emails, which is no mean feat. The ransomware was able to bypass Office 365's built-in security tools for a short period of time (Microsoft quickly blocked the attack). During this window, the ransomware targeted Office 365 users with spam and phishing emails that contained the malicious malware hidden in attached Word documents. Recipients of the emails were encouraged to open the attachment in Edit mode and Enable Content in order to view the file. Enabling Content activates the macros in the document, invoking a background download of Cerber ransomware. The 2016 article described Cerber encrypting local and networked files and demanding 1.24 bitcoins (then approximately US\$500) for decryption software. Its later technical description specifies AES-256; the earlier AES-265 reference was a typographical error. The article's statement that free decryption was unavailable describes the position reported at the time. Macros in Word documents (also referred to as Weaponised Office Documents) are not new. Locky ransomware used them, and over \$22 million was pilfered from banks using macros with Dridex in 2015. Cerber was first seen in March this year and is now the third largest threat in the ransomware segment with 24 percent market share. According to Fortinet, only CryptoWall (41 percent) and Locky (34 percent) are greater threats. The rapid expansion of Cerber may be due, at least in part, to the delivery model. Cerber is offered 'as a Service' through a closed underground Russian forum according to cyber intelligence analysts, SenseCy. Branded as Ransomware as a Service (RaaS), affiliates can rent the malware instead of building their own – and developers are further rewarded with bonus commissions from each successful ransom payment. This model reduces the barrier to entry for criminal entrepreneurs, and encourages Cerber developers to continually refine the malware to avoid detection and improve encryption rates.

Avoiding Detection

Malware developers are always exploring different techniques to evade detection, and those behind Cerber are now employing a server-side 'hash factory', say Invincea researchers. This means that the server morphs the Cerber payload very frequently to generate unique hashes. In this instance, a new hash is generated every 15 seconds. As signature-based security solutions often rely on the identification of hashes of known malware for detection, the changing payload helps Cerber circumvent security software and reach the target. The concept of changing hashes is not new, but the 15 second frequency makes Cerber stand out from others. Researchers were unable to determine whether the payloads on the server were being programmatically generated locally, or were being generated remotely and uploaded by a script.

Targeted Deployment

After the macros are enabled and Cerber activated, it will check which country the computer is registered as. If registered as Armenia, Azerbaijan, Belarus, Georgia, Kyrgyzstan, Kazakhstan, Moldova, Russia, Turkmenistan, Tajikistan, Ukraine or Uzbekistan, the process will stop and the computer will not be encrypted. If the computer is registered as any other country, Cerber will then install in the Application Data directory and name itself as a random Windows executable. It is most active in the United States (nearly 50 percent of infections), but also targets Taiwan, Japan, Australia, Brazil, Canada, Portugal, Spain, Malaysia, and Germany.

Current Attack

The current Cerber campaign began targeting Microsoft Office 365 users on June 22. Cloud security company Avanan identified that the attack was widely distributed very quickly after the originator confirmed that they could bypass the Office 365 built-in security tools through a private Office 365 mail account. Microsoft quickly identified the problem, circumvented the issue and successfully started blocking the malicious email attachment around the world within hours. The attack used macros in Word documents to activate the ransomware on victims' machines. The macros leverage PowerShell, which in turn invoke commands encoded in Base64. Whilst this campaign targeted Office 365 users, it was not restricted to the online version – it had the same impact when using desktop versions of the software. Once triggered, Cerber configured itself to start automatically when the user logs into windows, execute as a screensaver when the computer is idle, and set a task to execute itself once every minute. It will also show fake system alerts and begin a restart process. The initial restart will be problematic, and a second restart will follow. Researchers are unsure what happens during this multiple restart phase. When the restart process is complete, the encryption process of the victim's computer using AES-256 encryption starts. Cerber creates three ransom notes (TXT, HTML and VBS) named 'DECRYPT MY FILES' in every folder as it is encrypted. The TXT and HTML notes contain the same content. They explain the encryption has occurred, and provide links to Tor and a dedicated Cerber decryption site where ransom payment can be made and the decryption files potentially accessed. Included is the Latin quote "Quod me non necat me fortorem facit" that translates to "That which does not kill me makes me stronger". The VBS note is a script that uses the Microsoft Speech API that is built into Windows to talk directly to the victim. When the script is executed, the victim's computer will explain the computer's files have been encrypted, repeating the message five times. This message can be listened to below: <https://www.blueapache.com/wp-content/uploads/2016/06/Cerber.mp3>

The Cerber Decryptor

The ransom notes contain a link to the decrypttozybarc.onion Tor site. Titled Cerber Decryptor, the site can be accessed in 12 different languages. The site provides information on the ransom amount, an explanation highlighting the ransom will double if not paid within 7 days, and details on how to pay the ransom. Once a victim makes the bitcoin payment, they are supposedly provided with a download link for their unique decryption files.

Way Forward

According to Kaspersky Security Network, ransomware attacks increased five fold between 2014 and 2016, and are showing no signs of abating. The attacks are also shifting their target from individuals to enterprises with a significant increase in the complexity of malware targeting business networks. Organisations can no longer rely just on built-in security tools – attackers spend considerable time testing and refining malware to ensure it can bypass security before launching full attacks (as we saw in the 2013 Target attack). Organisations should be investigating in a layered defence, augmenting built-in security with additional online tools, next generation firewalls with live sandboxes, and stringent

endpoint protection. Equally important is the continued investment in staff education on social engineering and how to identify potential malware threats. If staff can spot malware rather than inadvertently activating it, organisations can mitigate the risks and save days, if not weeks in remediation time and costs. Ransomware threats continue reaching the desktops of the most poorly trained employees within your company. To discuss ways you can easily improve your organisation's security posture through staff education programs and IT as a Service solutions, contact our account team .

What is Cerber ransomware and when did the major attack on Office 365 users occur?

Our article dated 5 July 2016 describes Cerber ransomware targeting Microsoft Office 365 users. Its 'Current Attack' section dates the campaign's start to 22 June 2016.

How many Office 365 companies were affected by the Cerber attack?

According to industry estimates cited in the article, over 57 percent of companies that use Office 365 received at least one copy of the Cerber malware hidden in emails.

How did the Cerber ransomware infect victims' computers?

The ransomware bypassed Office 365's built-in security tools briefly and spread via spam and phishing emails containing malicious Word document attachments. Recipients were encouraged to open the attachment in Edit mode and Enable Content, which activated macros that invoked a background download of Cerber ransomware. The macros leveraged PowerShell, which in turn invoked commands encoded in Base64.

What encryption method does Cerber use and what ransom does it demand?

The July 2016 article describes AES-256 and RSA encryption and a demand for 1.24 bitcoins, then approximately US\$500. It reported no free decryption option at that time; this is historical reporting, not a statement about current decryption tools or every Cerber variant.

How does the Cerber Ransomware as a Service (RaaS) model work?

Cerber is offered 'as a Service' through a closed underground Russian forum, according to cyber intelligence analysts SenseCy. Under this Ransomware as a Service (RaaS) model, affiliates can rent the malware instead of building their own, and developers earn bonus commissions from each successful ransom payment. This reduces the barrier to entry for criminal entrepreneurs and encourages continual refinement of the malware to avoid detection and improve encryption rates.

How does Cerber avoid detection by security software?

According to Invincea researchers, those behind Cerber use a server-side 'hash factory' that morphs the Cerber payload very frequently to generate unique hashes—a new hash is generated every 15 seconds. Since signature-based security solutions often rely on identifying hashes of known malware, this changing payload helps Cerber circumvent security software.

Which countries does Cerber avoid targeting, and which are most affected?

If a computer is registered in Armenia, Azerbaijan, Belarus, Georgia, Kyrgyzstan, Kazakhstan, Moldova, Russia, Turkmenistan, Tajikistan, Ukraine, or Uzbekistan, Cerber stops and does not encrypt the computer. It is most active in the United States (nearly 50 percent of infections), and also targets Taiwan, Japan, Australia, Brazil, Canada, Portugal, Spain, Malaysia, and Germany.

What market share does Cerber hold among ransomware threats, according to Fortinet?

In the July 2016 article, Fortinet was cited as placing Cerber third with 24 percent, behind CryptoWall at 41 percent and Locky at 34 percent. These are historical figures for the period discussed.

What happens after Cerber encrypts a victim's files?

Cerber creates three ransom notes (TXT, HTML, and VBS) named 'DECRYPT MY FILES' in every folder as it encrypts. The TXT and HTML notes explain that encryption has occurred and provide links to Tor and a dedicated Cerber decryption site, including the Latin quote 'Quod me non necat me fortiolem facit' ('That which does not kill me makes me stronger'). The VBS note uses the Microsoft Speech API to verbally tell the victim that their files have been encrypted, repeating the message five times.

What is the Cerber Decryptor site and how does the ransom payment process work?

The ransom notes contain a link to the decrypttozxybarc.onion Tor site, titled Cerber Decryptor, accessible in 12 different languages. The site provides information on the ransom amount, explains that the ransom will double if not paid within 7 days, and gives details on how to pay. Once a victim makes the bitcoin payment, they are supposedly provided with a download link for their unique decryption files.