May 16, 2017

Security Awareness - Ransomware WannaCry

If you haven't come across a "ransomware," consider yourself lucky.

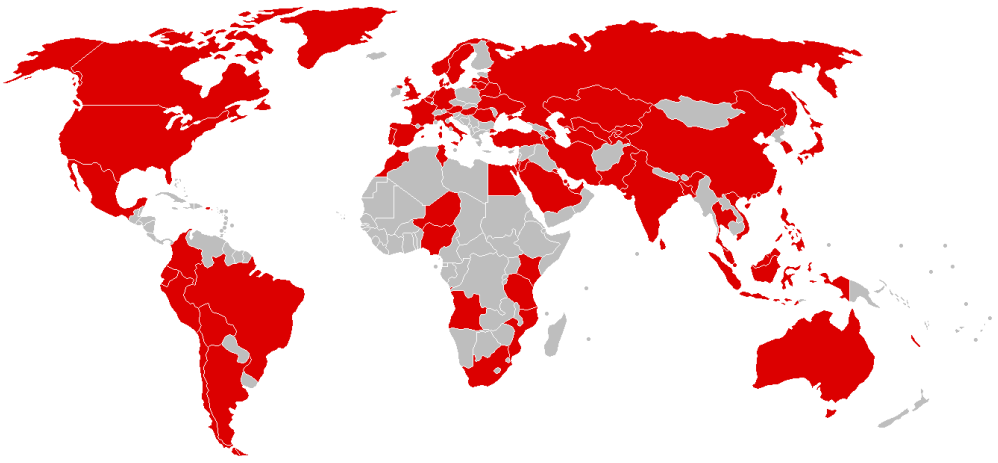
Ransomware is a sophisticated piece of malware that blocks you (the victim) from accessing your files, sometimes your computer, and the only way to regain access is by paying a ransom, usually between 300$ and 1000$.

Researchers saw more than 3.8 million ransomware attacks in the second quarter of 2015, that was a modest 19% rise from 2014. In 2016 ransomware attacks grew dramatically to reach 638 million with an estimate of nearly $1 billion dollar source of income for cyber criminals.

Ransomware attacks are typically carried out using a Trojan that is masqueraded as a legitimate file or drive-by downloading. 59% of ransomwares are being spread through well-worded phishing emails that appear to come from a legitimate email address and domain name, 24% through Websites and Web Applications and 4% through Social Media.

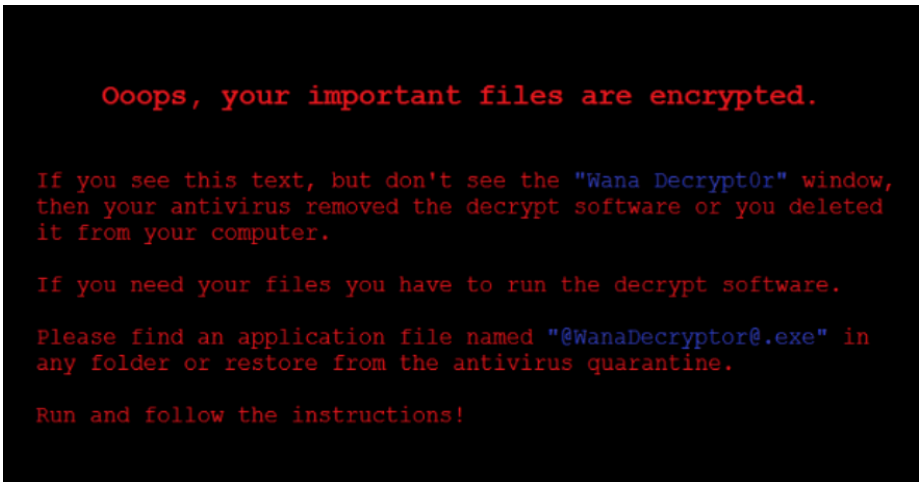
"*Drive-by downloading occurs when a user unknowingly visits an infected website and then malware is downloaded and installed without the user's knowledge.*"

A ransomware named **WannaCry** stormed through the web on Friday, May 12 infecting hundreds of thousands of computers in 150 countries. **WannaCry** is far more dangerous than other common ransomware types because of its ability to spread itself across an organization's network by exploiting a critical vulnerability in Windows computers.



Geographical target distribution for the first few hours of the attack

Once infected, the user will see something similar to the screenshots below:



Symantec announced that its Endpoint Protection technologies blocked 99.999% of the WannaCry Ransomware attacks. And computers who received the Microsoft security update MS17-010 are not vulnerable to this threat.

Guidelines to stay safe:

- Be careful to click on harmful attachments and links in your emails. Even if you have received this email from a friend or colleague, drop him/her a call to make sure the attachment or link is safe. Infected machines send infected messages masqueraded as legitimate but with harmful attachments and links
- Stay away of unsafe and unreliable sites and social media applications.
- Never click on a link that you do not trust on a web page or access to Facebook or messaging applications such as WhatsApp and other applications using your browser on your Work PC.
- Be aware of cracked softwares as they contain trojans and malicious codes.
- Keep your files backed up regularly and periodically, and make sure this backup is always offline.
- Be aware of fraudulent email messages that use names similar to popular services such as "PayePal" instead of PayPal or use popular service names without commas or excessive characters.
- Use Anti-Virus and Always make sure to have the latest update.
- Make sure your Windows have the latest security updates.
- Don't stay logged in with a privileged user such as administrator. Always use an ordinary user, with limited privileges, to access your computers.

If you feel that you may be a victim of this attack, please unplug your network cable immediately, turn off your PC and contact EXEO IT support team right away.

We will continue to monitor the situation as it evolves and keep you informed.

Employee awareness is key to halting Ransomware attacks, so please spread the message.

To always stay up-to-date with the latest news and get tips & tricks that will help you boost your efficiency at work, you can subscribe to our Blog

Support Team

T +961 1 699799 Ext. 911

Mkalles 2001 Center, 2nd Floor

PO Box 16-5005 Beirut, Lebanon

www.exeo.me