WHAT IS RANSOMWARE?

Ransomware generally stops applications from running, or prevents you from accessing data. Instead, you receive a message stating your computer has been hacked and in order to remove the hack, you must pay to do so, generally in untraceable digital currency called bitcoins.

HOW DO I GET IT?

Ransomware can infect your computer through several sources including, but not limited to, clicking on advertising on legitimate websites, malicious websites, or the most popular method – social engineering by luring the victim to click on a malicious link in their email.

HOW LONG HAS THIS BEEN GOING ON?

Ransomware originated in the late 80s with a version aptly named “AIDS” because it was spread through diskettes that were distributed at an AIDS conference. The latest version is called WannaCry and as of May 16th, 2017, it has affected tens of thousands of computers and has been spread to over 100 countries. It originated in Russia, and spread to China and the EU and US.
WHAT IS WANNACRY?

WannaCry is the latest variant of ransomware that is primarily spread through a method called “phishing.”

WHAT IS PHISHING?

Phishing is the process of sending out email blasts with malicious links in hopes that the email recipient will click on the link which opens the door for the computer to get attacked.

WHAT IS SPEAR PHISHING?

Spear phishing is a targeted phishing attack against one individual, normally a high ranking employee in the company or one who normally has high levels of network access like a network engineer or network administrator.

HOW DO YOU PREVENT PHISHING ATTACKS?

Most companies prevent phishing attacks like WannaCry, which targets Microsoft Windows, by continuously updating Windows patches. They also employ SIEM (Security Information and Event Management) software and IDS/IPS (Intrusion Detection & Prevention Systems) to detect and block the unique signatures of the ransomware. However, the best way to prevent the attacks is to delete email from unknown sources and avoid clicking unreliable links.

“THE BEST WAY TO PREVENT THE ATTACKS IS TO DELETE EMAIL FROM UNKNOWN SOURCES... “
The initial infection vector employs EternalBlue and DoublePulsar to spread (spy software reportedly stolen from the NSA). Once it infects a host, it attempts to replicate itself to other systems by connecting to its Command and Control (C2) domain, encrypts files (wrcy extension), and attempts cross infection via SMB service running on port 445. A ‘Kill switch’ was found by a UK researcher, who found it would not execute if the domain answered it’s query. WannaCry uses SSL via TOR for communication with attackers and payment. I initially and primarily affected Russia and EU and just started affecting US.
There have been reports of 200,000 to 300,000 detections and possible links to “Lazarus” (North Korean group) have been found. There are no guarantees of decryption if you pay the ransom, however there have been reports of successful transactions. The encryption process takes some time and can be stopped during the process by disconnecting from the internet.

The most common defenses are: OS patching, anti-virus, anti-Malware, FWs, file integrity monitoring, IDS/IPS, website security scans, network isolation, SIEM OTX and threat intelligence, and phishing awareness training. Cisco Umbrella (internet gateway, MS Azure, AWS, and G Suite have current compromise fixes.

ARTICLE LINKS

Phishing is the process of sending out email blasts with malicious links in hopes that the email recipient will click on the link which opens the door for the computer to get attacked.


[https://www.nytimes.com/2017/05/15/business/china-ransomware-wannacry-hacking.html?_r=0](https://www.nytimes.com/2017/05/15/business/china-ransomware-wannacry-hacking.html?_r=0)