THE CRYPTOLOCKER VIRUS

RYAN DOCKSTADER

WHAT IS THE CRYPTOLOCKER VIRUS

Computers, while complex, are made up of several “simple” components. A simplified run down of the critical components would look something like:

- The Central Processing Unit (CPU)
- Ram
- mass data storage (a hard drive)
- a Power Supply Unit (PSU)
- a motherboard to connect everything together

Take away one of these components, and your computer will not function at all, or at minimum not the way you want it to. The CryptoLocker virus targeted the mass data storage of the modern computer.

OVERVIEW

The virus itself was a clever piece of malware. It would take all the files on the drives in your computer and simply encrypt them (something that is a good practice when you’re the one encrypting your files). This would cause the computer to no longer function correctly. The virus would then display to the user that their files had been encrypted and they would need to pay a ransom to get the key to unencrypt them.

DISTRIBUTION OF THE CRYPTOLOCKER VIRUS

The virus itself couldn’t jump from computer to computer, so it needed to be sent to the victims. To accomplish this the attackers used what is known as the Gameover ZeuS botnet. This botnet would propagate the virus via an attachment to an email message, that was disguised as a PDF, but was really a .exe.

OPERATION OF THE VIRUS

Once the user “opened” the “PDF”, the virus would install itself on the machine and add a registry key to run on startup. Once the computer restarted, the payload would encrypt every drive it could access, including any network drives. This is one of the worst problems for corporations, as just a single user with mapped network drives could cripple their entire data stores.

FALLOUT

The United States Department of Justice was able to take down the botnet distributing the software in an operation called Operation Tovar. However, according to a study by the University of Kent, 41% of people paid to have their information unlocked. This is estimated to be 41,928 Bitcoin which was equivalent to roughly $27 million dollars at that time.

CITATIONS

- "U.S. Leads Multi-National Action Against 'Gameover Zeus' Botnet and 'Cryptolocker' Ransomware, Charges Botnet Administrator." The United States Department of Justice, 16 Sept. 2014, https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware.
- Hernandez-Castro, Julio, et al. "University of Kent Survey." University of Kent Computing, University of Kent, 30 Apr. 2014, https://web.archive.org/web/20140308080430/http://www.cybersec.kent.ac.uk/Survey2.pdf.
- "Krebs on Security." Brian Krebs, https://krebsonsecurity.com/2014/06/operation-tovar-targets-gameover-zeus-botnet-cryptolocker-scourge/.