Game Over Zeus

Evgeniy Mikhailovich Bogachev or lucky12345 is one of the world’s most infamous bank robbers who is charged for the loss of upwards of 100 million dollars of money stolen from banks, major corporations and even individuals. He is one of the 21st century’s most notorious hackers and is responsible for the creation of the Zeus malware, which is some of the most sophisticated and damaging malware ever to be used in cybercrime. He is also suspected of collecting sensitive information on behalf of the Russian government and has one of the highest cyber most wanted bounties. Bogachev is the most elite cyber criminal of this time and his actions usher in a new era of organized crime.

One of Bogachev’s most notorious pieces of malware is GameOver Zeus, a peer to peer botnet, this is the botnet that is responsible for the majority of the 100 million dollars of losses. What made Bogachev’s botnet so trying for the FBI to take down is that it used peer to peer communication. Unlike a regular botnet where computers are infected and controlled from a single server and have no communication between each other in a peer to peer botnet though, all of the computers communicate with each other so if the command server is disabled the administrator can just hijack another computer in the botnet and start issuing commands from that computer. Once a computer is infected with GameOver Zeus the hacker can siphon off bank accounts, install software like Cryptolocker, or a plethora of other malicious things. One of the major things that
Bogachev and his allies used GameOver Zeus for bank theft, and the way that they would do that is a bank’s webpage opened the botnet would create a shell of the webpage and then record passwords and usernames and then use them to siphon away the money from that account and as long as that computer was infected with GameOver Zeus the user would never notice that the money had been withdrawn. What Bogachev’s organization would then do is employ a money mule to go into a bank open an account into which the botnet would dump the money and then the mule would later withdraw the 10,000 or so dollars.

Another thing that they would do with infected computers is they would install a software called Cryptolocker which would go through and encrypt all of the files and then tell the user that they must pay up 100 or so dollars to get the key to turn their files back to plain text. Bogachev’s organization that he used to run GOZ was called the Business Club was a group of about 50 criminals that paid an access fee use and access GOZ control panels, this whole network was run through two British websites that were called Work.businessclub.so, and Visitcoastweekend.co. This is how Bogachev and the Business Club used GOZ to steal money.

Once the FBI, botnet fighters, and cybersecurity firms discovered Game Over Zeus plans were immediately made to disable the botnet. In January of 2013 two botnet fighters, Tillmann Werner a researcher at CrowdStrike and Stone-Gross who just graduated from grad school mounted their attack on GOZ using a technique called “sinkholing”. What the two did was they rerouted the network and then redirected the traffic to servers under their control, in the beginning, everything was running smoothly
and Bogachev wasn’t resisting. With no resistance from Bogachev and the Business Club, they were able to direct 99% of the network to their servers and it was around this time that Bogachev responded to the capture of his network. Using the computers that were still controlled by his server he made a connection with the computers in the sinkhole and pushed through an update to his computers that wrestled control of the network back to his servers.

For the second attack, Werner and Stone-Gross teamed up with the FBI’s cyber security unit in Pittsburg and international authorities. When the attack began international authorities shut down GOZ’s command servers and then Werner and Stone-Gross brought their improved sinkhole online but as the attack wore on the sinkhole was bringing in very few computers as the two scrambled to debug their code. When the sinkhole was running smoothly Bogachev came online and began fighting for control of his network but once they disabled his Turkish based proxy server Bogachev knew it was game over for his botnet and he went silent.

Evgeniy Mikhailovich Bogachev was a highly skilled hacker who made a malicious botnet called Game Over Zeus that he with the help of his secret criminal organization the Business Club was able to silently rob over 100 million dollars from banks, companies and everyday people. Eventually, thanks to the tenacious efforts of the FBI and two botnet fighters named Werner and Stone-Gross the botnet was contained and removed from the infected computers. In conclusion Bogachev and Game Over Zeus were one of the most devastating cyber attacks that at the time were
ever to hit the USA and served as a wake-up call for law enforcement, alerting them of the dangers and prominence of cybercrime.