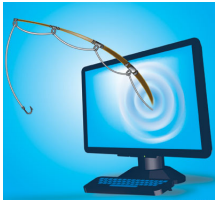


6 September 2008

By: Lucian Constantin, Web News Editor



Phishing attacks will increase
HowStuffWorks

[Phishers Update Their Infrastructure](#)

The notorious Rock Phish gang is uniting its forces with the Asprox botnet

The RSA FraudAction Research Labs [claims](#) that the Eastern European Rock Phish team is preparing for something big and that it is upgrading its infrastructure to integrate the Asprox botnet. According to their report, this upgrade might be the reason why its phishing activity has decreased for the past several months, but once finished a new wave of more powerful attacks is likely to hit.

The Rock Phish gang operates in Eastern Europe and, according to statistics, it is behind nearly half of the worldwide phishing attacks, the fraud it is responsible for being of several millions of dollars. This is no ordinary gang of cyber crooks, but a professional cybercrime organization with enough resources to pay third-party malware developers for their services.

According to RSA's observations the Zeus Trojan launched by Rock Phish in April was quickly replaced by "custom-made and more sophisticated crimeware." It was at that time that an interesting discovery was made. The control server of the gang started infecting users with a new independent botnet client. This marked a change in Rock Phish's MO and classic attacks.

Upon further investigation of the botnet client it was noticed that it was using the Neosploit infection kit and that the structure of its control server, part of the Rock Phish network, was identical to the structure of the control servers for the infamous fast-flux Asprox botnet, which has been the source of recent major SQL injection attacks on legit servers. Due to these attacks it successfully infected a massive number of computers and increased its zombie army. Even more, the team suggests that it is very likely for the Rock Phish botnet and the Asprox botnet to be using at least one common control server.

The RSA team speculates that the overlapping of a decrease in classic Rock Phish attacks and an increase in Asprox activity can only mean one thing - that the two groups are collaborating and that Rock Phish is adopting Asprox infrastructure. Not only that, but it seems Asprox has adopted classic attack techniques specific to Rock Phish. There is also the possibility of Rock Phish buying usage rights over the entire Asprox botnet. Either way, the RSA strongly suggests that a spike in phishing activity will follow and that the attacks will be a lot more complex than before because of the fast-flux nature of Asprox.