World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:11, No:03, 2017

Lessons Learned from Ransomware-as-a-Service (RaaS) Organized Campaigns

Authors : Vitali Kremez

Abstract : The researcher monitored an organized ransomware campaign in order to gain significant visibility into the tactics, techniques, and procedures employed by a campaign boss operating a ransomware scheme out of Russia. As the Russian hacking community lowered the access requirements for unsophisticated Russian cybercriminals to engage in ransomware campaigns, corporations and individuals face a commensurately greater challenge of effectively protecting their data and operations from being held ransom. This report discusses two notorious ransomware campaigns. Though the loss of data can be devastating, the findings demonstrate that sending ransom payments does not always help obtain data. Key learnings: 1. From the ransomware affiliate perspective, such campaigns have significantly lowered the barriers for entry for low-tier cybercriminals. 2. Ransomware revenue amounts are not as glamorous and fruitful as they are often publicly reported. Average ransomware crime bosses make only $90K per year on average. 3. Data gathered indicates that sending ransom payments does not always help obtain data. 4. The talk provides the complete payout structure and Bitcoin laundering operation related to the ransomware-as-a-service campaign.

Keywords : bitcoin, cybercrime, ransomware, Russia
Conference Title : ICCNS 2017 : International Conference on Cryptography and Network Security
Conference Location : Miami, United States
Conference Dates : March 09-10, 2017