World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:14, No:12, 2020

The Underground Ecosystem of Credit Card Frauds

Authors : Abhinav Singh

Abstract : Point Of Sale (POS) malwares have been stealing the limelight this year. They have been the elemental factor in some of the biggest breaches uncovered in past couple of years. Some of them include • Target: A Retail Giant reported close to 40 million credit card data being stolen • Home Depot : A home product Retailer reported breach of close to 50 million credit records • Kmart: A US retailer recently announced breach of 800 thousand credit card details. Alone in 2014, there have been reports of over 15 major breaches of payment systems around the globe. Memory scrapping malwares infecting the point of sale devices have been the lethal weapon used in these attacks. These malwares are capable of reading the payment information from the payment device memory before they are being encrypted. Later on these malwares send the stolen details to its parent server. These malwares are capable of recording all the critical payment information like the card number, security number, owner etc. All these information are delivered in raw format. This Talk will cover the aspects of what happens after these details have been sent to the malware authors. The entire ecosystem of credit card frauds can be broadly classified into these three steps: • Purchase of raw details and dumps • Converting them to plastic cash/cards • Shop! Shop! Shop! The focus of this talk will be on the above mentioned points and how they form an organized network of cyber-crime. The first step involves buying and selling of the stolen details. The key point to emphasize are : • How is this raw information been sold in the underground market • The buyer and seller anatomy • Building your shopping cart and preferences • The importance of reputation and vouches • Customer support and replace/refunds These are some of the key points that will be discussed. But the story doesn't end here. As of now the buyer only has the raw card information. How will this raw information be converted to plastic cash? Now comes in picture the second part of this underground economy where-in these raw details are converted into actual cards. There are well organized services running underground that can help you in converting these details into plastic cards. We will discuss about this technique in detail. At last, the final step involves shopping with the stolen cards. The cards generated with the stolen details can be easily used to swipe-and-pay for purchased goods at different retail shops. Usually these purchases are of expensive items that have good resale value. Apart from using the cards at stores, there are underground services that lets you deliver online orders to their dummy addresses. Once the package is received it will be delivered to the original buyer. These services charge based on the value of item that is being delivered. The overall underground ecosystem of credit card fraud works in a bulletproof way and it involves people working in close groups and making heavy profits. This is a brief summary of what I plan to present at the talk. I have done an extensive research and have collected good deal of material to present as samples. Some of them include: • List of underground forums • Credit card dumps • IRC chats among these groups • Personal chat with big card sellers • Inside view of these forum owners. The talk will be concluded by throwing light on how these breaches are being tracked during investigation. How are credit card breaches tracked down and what steps can financial institutions can build an incidence response over it.

Keywords : POS mawalre, credit card frauds, enterprise security, underground ecosystem
Conference Title : ICSRD 2020 : International Conference on Scientific Research and Development
Conference Location : Chicago, United States
Conference Dates : December 12-13, 2020