IEEE: artikel

Sophie Marien

Abstract

Recently the attacks on Belgacom and other high profile targeted attacks shows us that even the most secure companies can still be compromised. It also shows that these attacks are not immediately detected. FlipIt is a framework that can model these stealthy takeovers and is proposed by a group of researchers at RSA. It is a 2-players game composed of a single attacker, a single defender and a singe shared resource. These players will try to gain control over the shared resource and they do this in a stealthy way. In this paper we try to adapt FlipIt in a way that we can use it to model the game of defending a company network. This network will consist of multiple shared resources instead of one. Through analytic results we can provide useful information for the defender to defend his network.

1 REst

Not so long ago we discovered some high profile targeted attacks that infiltrated in a lot of systems without anyone noticing it. Belgacom [] has been the victim of a cyber security attack that has been uncovered for almost 2 years. The communication infrastructure of the Telecom company was infected with highly sophisticated malware making it possible to eavesdrop remotely. This means that even the most secure company can still be compromised without even noticing it. Such an attack can gain access to vulnerable data, credentials, cryptographic keys and many more. These kind of attacks that target organisations in a stealthy way and stay undetected for a long period are called APT (Advanced Persistent Threats).

uitleggen waarom we gametheorie gaan gebruiken om het spel te modelleren
The problem that we want to address in this article is how to react as a defender if our network system can be compromised by an attacker in a stealthy way. A research group at the RSA proposed a game to model the scenario where compromising the system is done stealthy and not immediately noticed by the system manager. In this FlipIt [1] game we have 2 players, the attacker and the defender, and a shared resource. Both players can gain at any time control of the shared resource, but this will always happen in a secretly manner. None of the players can observe who is in control of the resource. Every unit of time that a player is in control it gets utility. A player can 'flip' a resource which means that he is taking control over the resource. Each time the player flips the resource it has to pay a fixed cost. In this paper we want to model the problem of a corporate network that is under attack daily by viruses and worms. To do so we have to adapt the basic FlipIt game. Instead of one shared resource we have multiple resources that represent the nodes or devices in a corporate network. Each of these nodes are connected to other nodes by a graph. email systeem

.

The actions of the defender are. The actions of the attacker are. When system compromised

1.1 Basic model

In our basic model the defender can only 'flip' all the nodes in the network at the same time. The attacker will always drop his virus on the most woord vinden
node. The virus will then spread itself one time to all of his neighbours. Once infected again the virus will again spread itself to all of his neighbours. The network is compromised by the attacker when all of the nodes of the network are infected.

We can model the spreading of the virus through matrices. Google uses the same technique for page ranking. First the graph of the network is defined. Once the graph is known we can construct the first matrix for the calculation. If we have n nodes in our graph, the matrix will be of size nxn. The columns and rows correspond with the nodes. Every n_{ij} entry of the matrix will be set on 1 if there is a connection between node i and node j. The diagonal of the matrix will also be set on 1.

Now we know how we can model the spreading of the virus. If we want to set-up a gain function we have to know how ling it takes for the virus to compromise the whole system. This will be equal to the shortest path from the start infected node to the node that is the furthest away from this node. With this information we can calculate after how many steps this node is infected through our matrix calculation. We will end up with kind of a delayed FlipIT

2 References

- *FlipIt: Game of stealthy takeovers*