The 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications
15-17 September 2011, Prague, Czech Republic

Detecting Network Attacks Using Behavioural Models

Jiří Schäfer , Michal Drozd
Brno University of Technology, Božetěchova 1/2, Brno 612 66, Czech Republic, www.fit.vutbr.cz
schafer@fit.vutbr.cz, idrozd@fit.vutbr.cz

***Abstract* – In this paper we're dealing with the problem of detecting malware using behaviour model. For better malware description we have divided this model into two parts - malware spreading model and malware statistical behavioural model. Spreading models are typical epidemiological models like SI model, advanced SIR and SEIR models and empiric file spreading model. In statistical behavioural model we're describing characteristics of malware trojan communication and communication characteristics of a typical user, we're describing basic detection for both models (behavioural statistic and spreading), we're proposing some standard and specific countermeasures based on these models as same as possibility of detection of malware communication, attacks like DoS and Network scanning detection and detection of Malware propagation.**

***Keywords* – network attacks; denial of service; malware; malware behaviour; spreading models; statistic behavioural models; trojan horse; user behaviour**

I. Introduction

In this paper we're working with small groups of active users, for example a company with a few hundred users; within this environment we're trying to deal with some network attacks and malware network behaviour [1] using mathematical and empirical spreading models [2].

We're presuming that we have access to the network infrastructure, which have few a hundred active users and appropriate number of active devices, like routers, firewalls, IDS and so on. In this environment we have access to all network devices, so we have access to all syslogs, routers and all network information. We're correlating this information and gathering netflow information, information about specific packets and similar information.

In first part of this paper we're describing some attacks like network attacks and malware network communication and in next section we're going to detect these attacks. We're proposing how easy is to carry out these attacks and how necessary is to defend against them. Then we're describing spreading models under which we're going to detect these attacks and last section is describing how we can detect these attacks using models mentioned above. At the final section we're describing our conclusion and notes for future work in this area.

Detecting these attack is partly solved by NBA, ADS and NBAD systems. These systems are able to detect clearly definable and predictable attacks, but for detecting non-standard, unknown attacks, or otherwise deliberately modified attack, for example attacks communication, are results from these systems inconclusive. It is because all these detections (using systems above) are done by evaluating simple facts and limited groups of rules, and for detecting of more "sophisticated" attacks is a human interaction mandatory. Without security analyst these systems are not able to detect more that simple attacks [3].

On the other hand, our system can detect anomalies on basis of the spreading models and based on model behaviour patterns in network communication which proceeds from infected workstations and based on attacks from these workstations.

Primary goal of our research is to find a model that could detect specific type of attack, or type of malware (even malware using obfuscation of communication)just based on its behaviour and on ongoing communication.

II. Attacks detectable by netflow

We will briefly describe some of most common used networks attacks and malware behaviour as well as its description in this section; afterwards we will describe how to detect these attacks.

A. DoS attacks

A denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers. The term is generally used with regards to computer networks, but is not limited to this field; for example, it is also used in reference to CPU resource management. For example see few attacks, which was carried out last year [4] [5] [6].

This work was partially supported by the BUT FIT grant FIT-10-S-1 and the research plan MSM0021630528. Thank you all, especially you Veronika.

1) DDoS attack: This kind of attack is very well known, because there is no defence against it yet. In flooded DDoS (Distributed Denial of Service) attacker abuse lot of networks users, often noted as zombies.

These zombies send bogus packets to dedicated target. The main goal of this attack is to exhaust victim resources so that victim is not able to provide services any more. The key resources are network bandwidth, network latency or TCP resources. From the attacker point of view successful attack isn't just to exhaust resources, but to use large amount of zombies too. This last characteristic makes very difficult to defend against this attack.

2) UDP flood: UDP is a connectionless protocol, which does not require any connection set up procedure for transferring data. A UDP Flood Attack is possible when an attacker sends a UDP packet to a random port on the victim system. When the victim system receives a UDP packet and there is no application waiting for this packet then two things can happen, first: victim is behind firewall and firewall will drop this packet and second: there is no firewall dropping this packet so system will generate ICMP packet with destination unreachable and sends it to the forged source address (address of victim). Using massive amount of UDP packet can an attacker carry out a DDoS attack.

3) ICMP attack: ICMP is used by the IP layer to send one-way informational messages to a host, and the important think is that there is no authentication, therefore ICMP can be used to carry out many attacks such as DoS (Denial of Service) or allowing the attacker to intercept packets. An attacker can make use of this by simply forging one of these ICMP messages and sending it to one or both of the communicating hosts. Their connection will then be broken. The ICMP "Redirect" message is commonly used by gateways when a host has mistakenly assumed the destination is not on the local network. If an attacker forges an ICMP "Redirect" message, it can cause another host to send packets for certain connections through the attacker's host. [7]

4) Land Attack: In this attack an attacker sends a forged stream of TCP-SYN packets with the same source and destination IP address and TCP port numbers. This attack may lead on some OS to a system crash. [8]

B. Port scan

A Port Scan is one of the most popular reconnaissance techniques that attackers use to discover services they can break into. All machines connected to a network providing many services that use TCP or UDP ports. A port scan helps the attacker find which ports are available and open.

Detecting port scan isn't very complicated, unless an attacker uses advanced techniques to cover his actions. Few of these techniques are communication obfuscation, bigger time-outs, random targets, random ports, skipping ports and so on. For example when an attacker use random ports scanning, that means, he is not scanning victims ports in order, but randomly chooses ports (or small group of ports)and using these pseudo-random port choosing he scans all ports on victim station. Same strategy can attacker use when choosing targets inside scanned network and also he can combine these two strategies.

Here are few variants of port scanning and few obfuscation techniques how to cover their detections.

1) Horizontal scan: Horizontal scan means that an attacker scans all ports(0-65535) on victims station. This scan can by covered by randomly choosing ports from all available group of ports. For example scan first 50 ports, than wait time T and then scans ports from the middle range, or scans another machine and then come back to the first one.

2) Vertical scan: When an vertical port scan is carried out then an attacker scans for example all port 80 in whole sub-network.

Covering these actions is also very easy, an attacker can scans for example just few targets, than wait time T1, scan few another targets, wait different time T2 and so on, an attacker can also use slower scanning for not being detected (something like parameter -T3 when using nmap application).

C. Peer-to-peer networks

Peer-to-peer (P2P) network can be defined as sharing of computer resources and services among participants using direct exchange. P2P client can ensure direct information exchange, computing time and data sharing. Participant in P2P network acts as client and server simultaneously.

Peer-to-peer networks are nowadays very widely used and their usage is not limited to the legal purposes only, most of P2P users uses their clients for unauthorized file distribution, like movies, music and non-free applications. Peer-to-peer networks are logical sub-networks of internet and their special environment is vulnerable for special types of attacks, like modified DoS, password cracking and so on [1].

D. Malware - Trojan horse's network communication

Most malware, trojan, backdoor, etc. has its communication based on a client-server model in which a client reaches the server and creates communications, this communication commonly proceeds at http/https and it is independent on victim's will.

III. SPREADING MODELS

Most of next few spreading models are based on biological epidemiology and in most cases they are very useful in computer epidemiology. With these model we can predicts basic malware behaviour and possible impact on victims.

A. SI Model

The Susceptible-Infectious (SI) model is the simplest model of the dynamics of viral epidemics. In the given model the individual is both healthy and vulnerable to infection or infected and thus infecting others. The size of the population is constant and equals N = S(t) + I(t) where in the moment of time t there are S(t) vulnerable and I(t) infected individuals.

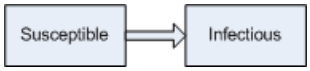

Figure 1. SI Model

B. SIR Model

SIR model is epidemiological model, which uses three states: S – susceptible, I – infectious, R – recovered. Subject can be only in one and only in this one group [9] [10]. This epidemiological model is very simple and suits for most of the biological diseases. Each state can be described as a triple (S, I, R) each letter indicates the number of subjects in appropriate state.

Figure 2. SIR Model

Time function manages triggering the subjects between the states. This function changes with different diseases and with different populations. In this model, healed subjects can't be infected any more.

C. SEIR Model

Model SEIR is an extension of SIR model by group of exposed subjects (E). In this model, Infected individuals move into the Exposed (not infectious) state after an average incubation period and subsequently through the infectious state after an average time. This deterministic approximation assumes an exponential distribution of incubation and infectious periods. Also this model assumes that recovered individuals are immune from infection (strictly to the ability to retransmit) for life.

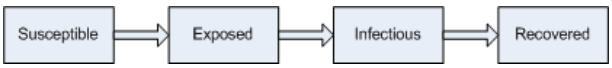

Figure 3. SEIR Model

D. SIRS Model

This model is simply an extension of the SIR model as we will see from its construction.

The only difference is that it allows members of the recovered class to be free of infection and rejoin the susceptible class.

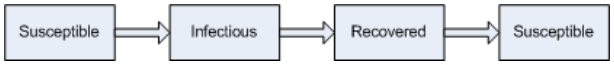

Figure 4. SIRS Model

E. SIS Model

The SIS model can be easily derived from the SIR model by simply considering that the individuals recover with no immunity to the disease, that is, individuals are immediately susceptible once they have recovered.

Figure 5. SIS Model

Removing the equation representing the recovered population from the SIR model and adding those removed from the infected population into the susceptible population gives the following differential equations:

F. Spreading process

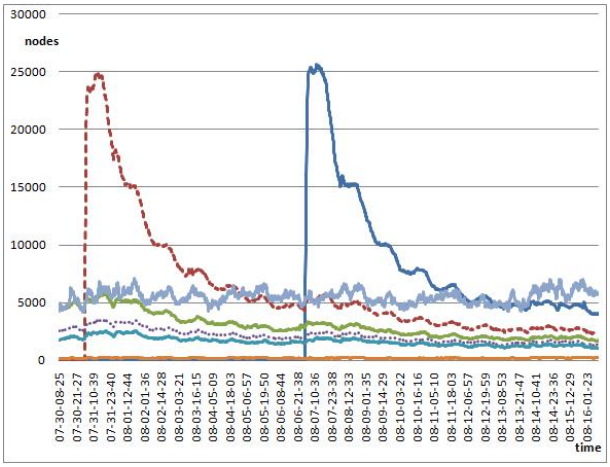

Figure 6. Real spreading process

These following graphs describe process of sharing some files in peer-to-peer network BitTorrent for a few months. X axis describes the time line (samples were taken about every 10 minutes) and on Y axis we have total number of participating users, who shares the same package. We can see process of sharing weekly distributed files in figure 6. Each line is process of sharing one file.

As we can see right after 8 hours of sharing the peak appears and this peak can reach up to 25000 users. This behaviour can be very dangerous because if someone is able to infect this file or spread similar file then he can exploit 25000 users in no time.

IV. Statistic behavioural model

For detecting malware behaviour we can not use basic epidemiological spreading model, but we need to use more precise model of statistic behaviour. Statistic behaviour analysis is based on statistic description of communication protocol between two communication nodes. Its fundamentals are described here [11]. In our system is this statistic model based on data gathered from communication netflow.

This model is useful mostly for detection malware such as viruses and Trojan horses. At the present time this malware communicates foremost through http (or https, to avoid anti-malware perimeter check at the border) and passed through the firewall.

A. User behaviour

Normal user's behaviour is from statistic behavioural model partly unpredictable. As described in [12] [13] user's communication creates (in terms of statistical analysis) certain clusters and voids, which are characteristic for specific user. On figure 7 we can see part of this statistical analysis.

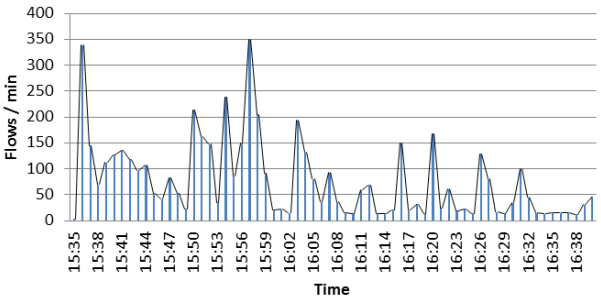

Figure 7. Normal user's behaviour - web browsing http/s communication

B. Trojan & Zombie behaviour

Trojan horses and infected victims in general uses http/https communication with master. In terms of statistical analysis of netflow data is this communication predictable because it takes place in identical, or similar intervals and most of the packets has roughly similar size. Figure 8 shows us statistical analysis of Trojan horse communication.

On next figure 9 we can see how is malware hiding inside users ongoing communication.

V. Detection based on network patterns

Each network communication is specific in a different way, for example network scan attack generates completely different network traffic than malware behaviour communication and it is the same form P2P spreading and for DDoS attack. Accessing and analysing network netflow data [14] and correlating them can be very useful

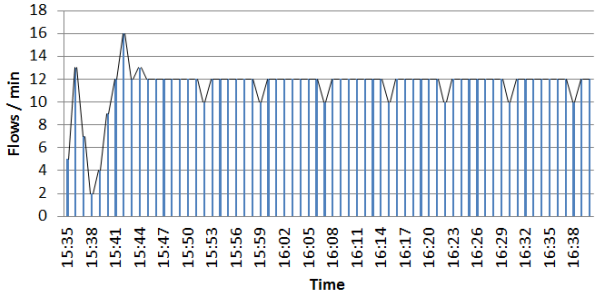

Figure 8. Trojan horse's behaviour - master-slave http/s communication

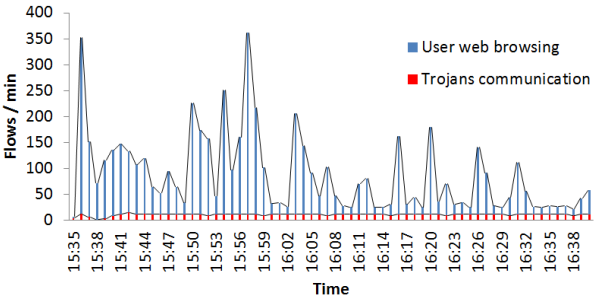

Figure 9. All communication at http/s

for helping detecting some networks attack, but more useful can be automatic correlation of this information with behaviour models of network communication.

A. Detecting malware

Malware symptoms can be divided into two categories.

1) Symptoms associated with malware's dissemination: Detecting malware using spreading model is no entirely trivial, because of malware network behaviour; malware, for example worm or virus, is using network communication for spreading itself amongst other possible victims. They are using vulnerable services with the usage of so-called zero day exploits [15] or trying to invade surrounding computers over exposed network services. Easily detectable symptoms are for example password cracking or port scans.

Its network communication will be easily predicted, when we correlate netflow from routers we will see increase of communication between computers (between infected ones and possible victims). When we take absolute value from this communication, it behaves exactly as spreading model [16]. In this case we can count differences between change of amount of communication through routers and absolute value of communication and then we can predict in which part of spreading model we are, and thanks to this knowledge we can estimate the future behaviour, we can raise security incident, contact security operator, or write down when spreading part is over.

2) Symptoms associated with botnet communication: Detecting malware based solely on communication within the botnet is also not trivial. As malware we understood foremost harmful code such as Trojans, rootkits or backdoors, which tries to connect to their Master and after connecting is malware listening and executing master's commands.

In this case the communication between Master and slave is concealed using http/https protocol because this protocol is allowed at border routers. Master-Slave communication can be labelled as predictable because slave contacts master periodically and uses similar size.

This process is showed on Figure 8. The picture shows a communication scheme based on netflow data, that shows that communication is done in periodical intervals, the size of transmitted data is approximately the same and the destination address is fixed. In contrast to the common user communications over http/https, which is in principle unpredictable, it is fully dependent on user behaviour.

We can see that each netflow data are in different time frames and in short term communication we can see certain clusters and delays, which doesn't appears in Trojan horse communication. On the basis of these behavioural stigmas we can evaluate each communication whether if it is a communication of potentially malware (trojan horse, backdoor, generally victim malware) or a communication of legitimate system's user.

To eliminate false positive detection rate is needed to evaluate more factors of ongoing communication such as the credibility of the destination address, it's DNS record or general information relating to the credibility of the target system.

With these information we can operate very flexible and we can easily solve if a computer is infected or not and defends against these types of thread, we can detect beginning of infection, we can monitor the process of infection spreading itself and we know when there is a maximum users infected (when infection is after it's peek).

The main benefit is that this way we can detect even one infected computer on a large network, infected computer, which has almost no any surrounding symptoms and is almost benign, the computer that do nothing but only communicates with his master.

B. Detecting DoS attack

DoS or DDoS is currently very effectively Detectable attack, both commercial and open source tools can detected these attacks at multiple levels, the principle of detection is based on statistical assessment of the number of established connections.

Very interesting is process of ongoing attack, its leading edge and attacks timing, there are DoS attacks that last from a few seconds to a few weeks and all these information can be used for detection.

A major drawback is that against effective DoS and DDoS attack is no defence (if we want preserving the availability of that services).

For detecting this type of attack we can use spreading model and we need to observe all amount of network communication and detect ongoing edge of spreading model, because process of this model will be similar to process of malware infection but with more sharper edges and quicker peak, and of course with more steeper ongoing edge will be more steeper descending edge too. So we're looking for differences between samples bigger than with malware spreading, but no so big as with network scan or UDP flood. Clarification rule can be limitation of network flow to one target, or small group of targets.

1) Detecting DDoS: Distributed Denial of service is specific in a few ways, it is type of attack where attacker is trying to deny access to some service and for this he's using some tools, like botnets, clouds or so on. Basically attacker sends command to all bots under his control and these bots are trying to shut down some service or computer.

Detecting DDoS is quite similar as detecting DoS, but instead of one source of attack there are many sources from whom the attacks comes.

And same as DoS, against DDoS there is no defence.

2) Detecting UDP flood: For UDP flood attack we can use spreading model too, for correlating we're using rule for detecting leading edge of SIR epidemiological model, so from part when an attacker starts sending UPD packet to the part that he stops sending or finally "destroys" victims machine.

We can also use rule clarification, that when the packets are from different source and for specified one, differences between amounts of communication is high at first and then zero and absolute value of communication is at stable level. Confirmation of this attack can be packet analysis that shows different destination UDP port.

C. Detecting P2P spreading

Detecting P2P spreading can be done in a few ways. By observing netflow and comparing to spreading models we can recognize file spreading by detecting ongoing shape of all-amount traffic. Then afterwards by comparing network protocols and ports we can detect which type of P2P network it is.

D. Detecting ports scan

Detecting port scan is very similar to the previous attack detection in that way that we're looking for same type of communication amount, we're looking for leading edge of SIR epidemiological model, for beginning of network recognition, after that the difference between two samples will be low, or zero and total amount of communication will be at constant level. Clarification of this rule will be little more complex, because when

someone is scanning network our network he can scan one sub network at time, or two networks simultaneously or so on, so basically we must rely on detection from our epidemiological model.

V. Conclusion

This paper proposed usage of spreading model for detecting some of networks attack and statistic behaviour model for detecting malware communication in overall system http/https communication.

We have focused on increasing level of security for each model. And both models can use data directly from netflow. On examples mentioned in previous chapters we showed functionality of both approaches and we have discussed the possibility of detection of each type of incident or attack.

On the other side we must say that detection using statistical behavioural model can be abused by modification their detection model, for example abusing statistical behavioural model it is randomization of ongoing communication and for spreading model it is changing angle of rising and falling edges of communication. In future work we want to focus on improvement of detection techniques so they will be resists against these types of obfuscation.

References

[1] J. Schäfer, K. Malinka, and P. Hanáček, "Peer-topeer networks security," in *The Third International Conference on Internet Monitoring and Protection*. IEEE Computer Society, 2008, pp. 13–13. [Online]. Available: http://www.fit.vutbr.cz/research/view_ pub.php?id=8654

[2] J. Schäfer and K. Malinka, "Security in peer-to-peer networks: Empiric model of file diffusion in bittorrent," in *The Fourth International Conference on Internet Monitoring and Protection*. IEEE Computer Society, 2009, p. 6. [Online]. Available: http://www.fit.vutbr.cz/research/view_pub.php?id=8962

[3] M. Rehák, M. Pechoucek, M. Grill, J. Stiborek, K. Bartos, and P. Celeda, "Adaptive multiagent system for network traffic monitoring," *IEEE Intelligent Systems*, vol. 24, no. 3, pp. 16–25, 2009.

[4] D. Pauli, "Paypal hit by ddos attack after dropping wikileaks." [Online]. Available: http://www.zdnet.com/news/paypal-hit-byddos-attack-after-dropping-wikileaks/489237

[5] G. Keizer, "Dos attacks hammer wikileaks for second day running." [Online]. Available: http://www.computerworld.com/ s/article/9198679/DoS_attacks _hammer WikiLeaks for second day running

[6] S. Musil, "Wikileaks: We are under denial-of-service attack." [Online]. Available: http://news.cnet.com/8301-1023 3-20023932-93.html

[7] www.NetworkDictionary.com, "Network security at the network layer (layer 3: Ip)." [Online]. Available: http://www.networkdictionary.com/security/ NetworkSecurityLayer3.php

[8] NetworkDictionary.com, "Network security at the transport layer (layer 4: Tcp and udp)." [Online]. Available: http://www.networkdictionary.com/security/ NetworkSecu-rityLayer4. php

[9] Z. Chen, L. Gao, and K. Kwiat, "Modeling the spread of active worms," in INFOCOM 2003. IEEE INFOCOM, 2003, pp. 1890–1900.

[10] W. Yu, C. Boyer, S. Chellappan, and D. Xuan, "Peer-to-peer system-based active worm attacks: Modeling and analysis," in *IEEE International Conference on Communications*, 2005.

[11] H.-K. Choi and J. O. Limb, "A behavioral model of web traffic," in *Proceedings of the Seventh Annual International Conference on Network Protocols*, ser. ICNP '99. Washington, DC, USA: IEEE Computer Society, 1999, pp. 327–. [Online]. Available: http://portal.acm.org/citation.cfm?id=850936.852479

[12] J. J. Lee and M. Gupta, "A new traffic model for current user web browsing behavior." [Online]. Available: http://blogs.intel.com/research/HTTP0paper.pdf

[13] G. Serban, A. Tarta, and G. S. Moldovan, "A learning interface agent for user behavior prediction," in *Human-Computer Interaction*, 2007, pp. 508–517.

[14] I. Wikimedia Foundation, "Netflow." [Online]. Available: http://en.wikipedia.org/wiki/Netflow

[15] P. Porras, "An analysis of conficker." [Online]. Available: https://365.rsaconference.com/servlet/JiveServlet/download/2192-2-1627/FEA-402 FINAL.pdf

[16] F. Wang, Y. Zhang, C. Wang, J. Ma, and S. Moon, "Stability analysis of a seiqv epidemic model for rapid spreading worms," *Computers and Security*, vol. 29, no. 4, pp. 410 – 418, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/ B6V8G-4XFGJ76-2/2/adc8a8d4430df29b0821da3c199ae372