Monitoring of Malware Communication Channels

Radovan Holík, Roman Jašek
Department of Informatics and Artificial Intelligence
Tomas Bata University in Zlín
Zlín, Czech Republic
{rholik, jasek}@fai.utb.cz

***Abstract*—One of the trends in the security world of the 21st century has been a massive growth in malware. Anti-virus vendors make efforts to respond to the malware growth with constant development of anti-virus software and its updating signatures. In spite of this fact, there is a chance that even secured systems may be infected. Analysis of malware of Command and Control (C&C) servers is a technique for detecting unknown malware in anti-virus software. It allows for detailed understanding of the important aspects of malware and plays a key part in any forensic analysis. This paper is an initial work for future research and describes possible usage of this technique for a malware detection.**

Keywords-HTTP; DNS; C&C; malware detection

I. INTRODUCTION

The amount of malware has rapidly increased since the beginning of the twenty-first century, especially when compared to the end of the twentieth century [1][13]. In the years preceding the twenty-first century, malware used to be created to experiment with systems and also for authors of such malicious programs to rise to fame. Modern malware, however, is built for one purpose only – to make money. In particular, it aims at stealing and re-selling personal or company's data (e.g., user names, passwords, etc.) or resources (e.g., for botnets, etc.)[2][14]. In terms of their development, advanced techniques and methods are used to conceal attacks against modern security systems and anti-viruses, even though the general acceptance in Information Technology security is that all systems are bound to once fail. When a computer system is successfully attacked, it is necessary to prepare it for system recovery, screen it for a range of penetration threats, identify weak points in the system which enabled the penetration, and to provide steps to prevent similar penetrations in the future [15]. One of the possible ways to detect malware attacks is to monitor the malware communication channels. In the following, several basic methods for analyzing these channels are described. It is demonstrated that, although it is possible to get a lot of interesting information about the malware behavior in the network, the performance of the analysis does not require an advance knowledge of a systems analyst. Input data are easy to collect and many organizations follow this standard practice (e.g., for analyzing the network traffic). These are primarily records of domain names translation by Domain Name Server (DNS) protocol and records of computer accesses from a local network to Uniform Resource Locator (URL) in Internet (including heads of Hypertext Transfer Protocol (HTTP)). These records may be collected on clients and also on systems for a network monitoring.

The rest of the paper is organized as follows: command & control channels are described in Section 2; common obfuscation techniques are presented in Section 3; and Section 4 presents web services for analysis. Methods of C&C channels are discussed in Section 5, and conclusion will wrap up the paper.

II. COMMAND AND CONTROL CHANNELS

The analysis of communication channels of malware is inestimable in big organizations to detect penetrations. In small organizations, it is recommended that analysts respond when such incidents are discovered. Especially, it is important to focus on the inspection of the range of penetration and execution of the attack. In the following subsections, we focus in particular on analysis of HTTP and DNS protocols because these protocols are largely used by modern malware.

Monitoring of malware communication channels is a technique capable of revealing successfully attacked computers communicating to the world. This method is also effective if these computers have already been infected by malware for which no anti-virus signatures have been created. The analysis contains monitoring of used protocols, communicating sides and transmitted data. Variability of communication channels is lower than the variability of polymorphic malware, which allows grouping of malware into related families. In the case of targeted attacks, it also allows linking attacks between different organizations. Identification, blocking and disconnection of control servers are important weapon against malware worldwide as well. In certain cases, the monitoring of communication channels may be used also for detection of a range of targeted attacks. If an attacker is able to successfully crack a protected network, his next steps within the network are often done by already obtained credentials of ordinary users; therefore, without further use of malware. By identifying the primary communication channel and subsequent searching similar links, it is possible to detect an effort of the attacker using obtained data from the protected area [10].

ISBN: 978-1-61208-427-5

The role of control servers traditionally perform computers controlled by malware. These computers have been successfully attacked during a previous attack. They are usually located in the same country as target of the attack (see Figure 1), in order to decrease the probability of successful detection. It is very difficult to track the people that perpetrate attacks, as they communicate with control server through several links distributed worldwide.

At the same time, the amount of the malware that resort to administration legitimate Internet services, such as network storage (Google Disk, One Drive, DropBox, etc.), social networks (Twitter, Facebook) and/or discussion forums, increases. For instance, in 2009 was detected Trojan.Grups, which used published messages on Google Groups for command distribution towards to control machines [4]. Similarly, Flashback malware receives commands via Twitter messages that contain specific hashtags [5], whereas network storage may be used as transship point for stolen data that the attacker tries to send quietly out of the targeted network. Moreover, network storage might be used for malware updates on infected computers [6]. The motivation for the usage of existing users' infrastructure is hiding in common data traffic and thus avoid detection mechanisms based for example on monitoring of communication with other than predefined servers. Basically, network services themselves decrease the effectiveness of detecting mechanisms. For instance, systems based on assigning a reputation to each Internet Protocol (IP) address have a limited use for cloud services with a risk of high number of false positives.

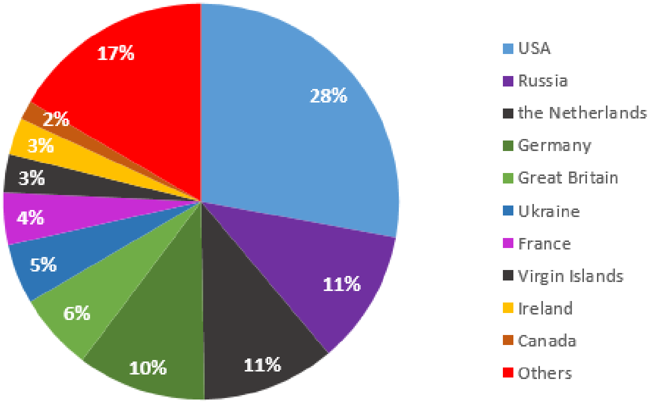

Figure 1. Distribution of main countries hosting malware C&C servers [3]

A. HTTP

Contemporary malware overwhelmingly uses HTTP protocol as a communication channel. It is very pleasant for malware creators because HTTP protocol is enabled on firewalls almost in every organization. The heterogeneity of communication via this protocol facilitates in hiding in common network traffic. A common phenomenon is the use of modified headers of HTTP protocol [17]. Modifications may be expressed by missing field of header, by changed order of header fields and/or by unexpected values of these fields [16].

A typical call from an infected machine to the control server is a HTTP request, usually GET or POST request with specific structure. The call may contain a status code or other information about infected computer (e.g., for example Media Access Control (MAC) address, used character set, etc.). Malware usually attempts to call several different domains while using the same or different URL (see Figure 2).

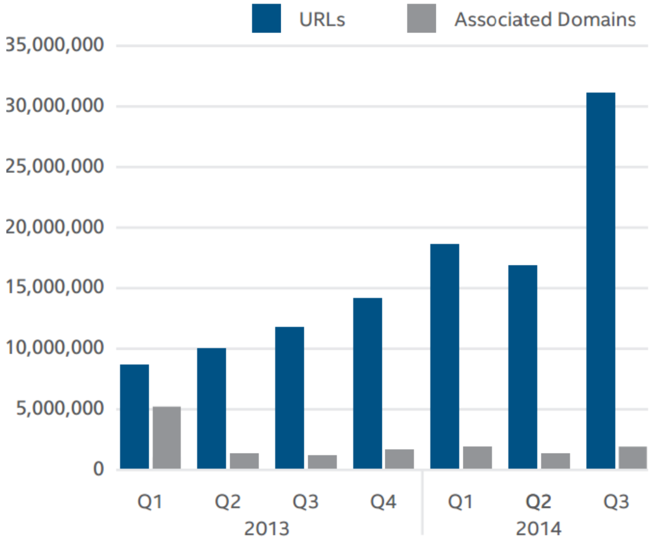

Figure 2. Number of newly discovered suspicious URLs and domains [7]

In this way, it is possible to avoid a blocking at level of domain names and alternatively of IP addresses as well. On the other hand, detection of the same Uniform Resource Identifier (URI) in outgoing calls to reach different domains is very good indicator of anomalies and does not matter if calls are conducted at different times (more often) or in a short period. In the following example, there are HTTP requests of Zeus botnet matched in type, URI and even at 3^{rd} level domain.

- POST hxxp://ix.kasprsky.org/cynic/gate.php
- POST hxxp://ix.dwonkistr.org/cynic/gate.php

Next of possible methods for malware detection is the analysis of values of User-Agent field. This field contains identification data about application that communicates to a server, and it is primarily intended for the server to provide a content to the client applications in various form. In case of malware is often used value which imitates a common browser [17]. In some cases the malware sets this field to its own specific string. It is possible to detect a malware within secured network by evaluating User-Agent values and monitoring where the malware tries to connect. For example, this method may be combined with IP reputation systems. Subsequently, those values of User-Agent that are used for communication with low-reputation IP addresses field are identified as suspicious. In the following example, it can be seen that malware does not try to hide but proudly indicates its presence:

- GET hxxp://www.ody.cc
  HTTP/1.0
  User-Agent: STORMDDOS

In the next example, there is User-Agent field used for a message transfer encoded in Base64 from infected computer to the control server:

- POST hxxp://www.gougle.com
  HTTP/1.1
  User-Agent: UGFzc3dvcmRVc2VybmFtZQ==

B. DNS

It is possible to detect malware actions by collecting and by analyzing DNS requests and their relevant responses. The basic element of detection is pairing domain names and corresponding IP addresses on time. Such information is inestimable for searching the primary cause when investigating of security incident, but it also may help to identify infected computers [8].

Malware tries to contact control servers on IP address obtained from DNS server. A domain name is either permanently written into the malware code or it is generated by pseudo-random algorithm from initial value. Most of control servers exist under several different domain names. A reason for that is an effort to protect a communication channel against common block techniques. If in computer network reveals some computer trying to connect to the control server, it is a good practice to block the targeted IP address and domain to prevent taking out of sensitive data and at the same time prevent receiving next commands from malware operators. However, other infected computers in the computer network may still communicate if are not identified all IP addresses and domain names. Modern fast flux botnets are able to fast change IP address for given domain name for the purpose of increasing robustness. Infected computers contacting control servers in various times are routed to different control servers [10][16].

Database that stores records of DNS translations in time may be very useful. When revealing some domain name, the database can be used to track down IP addresses of several control servers. By reverse procedure, it is possible to identify domains that indicate tracked IP address. For instance, when we put domain *ix.dwonkistrz.org* into the search box on service VirusTotal, we can find that the given domain name corresponds to IP address *195.22.26.231*. We can get a dubious list of domains by searching this IP address at the same website. In addition, we also can find a list of malware which has been spreading in last days.

Malware domains last relatively for a little time. Most of them are registered only a few days before they are used for the first time. Dynamic DNS services are also often used. Domain names are usually created as seemingly legitimate looking (e.g., gmailboxes.com, google.eu) or are generated by pseudo-random algorithm from predefined group of keywords (e.g., startftp.com, meown.eu), and/or are generated randomly with limiting conditions (e.g., run30.org, fdms.edu). The first group is primarily intended for confusing users (e.g., may be used in phishing campaign), whereas the other groups prevent simple blocking of domains by security organizations because the percentage of potentially large number of registered domains is very small [11].

By analysis of DNS records, it is possible to detect a range of the incident, but it also enables to reveal incidents which have not been detected yet. It is advisable to investigate those computers which have high failure rates of DNS translations. By this way, the malware may be detected by using generated domain names. An alternative is a calculation of the entropy of a domain name because fully random generated domain names consist of unexpected strings for people [9].

III. Obfuscation

A communication between malware and control servers is rarely realized in open form. An encryption may be used, but obfuscation is used more often. The encryption prevents understanding of transferred messages. From the perspective of malware creators, the encryption is limited because of possible recognition of encrypted channel on systems for a detection of range penetration. For example, one of possible techniques for detecting of encrypted data is a calculation of the binary entropy. Encrypted channels to control servers can be found mainly at APT malware. The malware often uses self-signed certificates representing itself as signed certificate by trusted CA [10].

On the contrary, obfuscation typically resorts to simple transformation or a combination of several transformations [9]. The advantage is an easy implementation and resistance against manual inspection. In contrast, performing automatic analysis is relatively simple [12]. It is possible to use brute force and test all commonly performed operations. Afterwards, search expected strings in decrypted data (MAC address, computer name, credentials). Between the most common obfuscations belong:

XOR operations with short key (typically 1-2 bytes)

- To each substring of message of relevant length the XOR function is always applied.

Bitwise or char shift

- A bitwise shift is applied on the message a few positions left or right. Bit writing of message is shifted a few positions left or right. An alternative is a char shifting within a predefined alphabet.

Unique encoding

- A common feature of obfuscation is a conversion of message to Base64 encoding. The encoding is in basic form relatively easily recognizable (e.g., by the end padding). Because of this, in some cases malware creators modify this encoding and change the order of the characters of the coded alphabet.

For example, username *"admin"* has after XOR operation with key *AA* shape *cbcec7c3c4*. After bitwise shift by one bit to the right, it has shape *30b236b4b7* and in Base64 encoding it is *NjE2NDZkNjk2ZQ==* or *YWR-Taw4=*. A similar string may occur everywhere in transferred data.

In addition to these classical obfuscation techniques, there are also used targeted modifications distracting an attention of security analytics. Common is e.g., file transfer with JPG extension, but in fact it is executable file. There are also known cases when malware inserts data into legitimate files. When opening the file an expected content is shown to the user. Everything works and seems to be fine but without detailed analysis it is not possible to reveal these data.

IV. INTERNET SERVICES

There exist many free available web services that can facilitate the analysis of outgoing malware calls. It is not necessary to build an extensive support infrastructure within the organization. Here are several representatives:

VirusTotal (virustotal.com)

- Provides not just a cloud system for analysis of binary files, but also provides services of passive DNS. When searching IP address, it is capable of returning a list of observed domains, which route to the same IP address, and with timestamps of their detection as well. There are also provided information about reputation and trustworthiness. In a similar way works also a query at domain name.

URLQuery (urlquery.net)

- URLQuery (urlquery.net)
  Enables malware control of given URL without a risk of infection of analyst´s computer. It also provides a screenshot of the webpage with an access by a common web browser.

UserAgentString (user-agent-string.info)

- Maintains a list of observed values of HTTP User-Agent field. Enables basic screening of trustworthiness of observed value.

TextMechanic (textmechanic.com)

- Offers a web interface for performing basic transformations with given strings. Enables easy manipulation with the string when there is a suspicion on using obfuscation techniques.

Reputation systems

- A lot of antiviruses and also other security software provide a system for checking up the reputation of the domain name or IP address. When detecting a suspicious calling, a verification of the reputation of a target is a fast indicator if it is necessary to continue the analysis.

Whois

- Provides information about domain registration. From the perspective of malware detection, there are particularly interesting information about recently registered domains or domains with obviously wrong details of responsible person. There are known cases when it was possible to interconnect seemingly unrelated targeted attacks on various organizations on the basis of data in whois.

DISCUSSION

As is shown in Table 1, there are two protocols that are described in Section II. The first protocol is HTTP that, nowadays, is overwhelmingly used by malware as a communication channel in order to merge with standard traffic data because it is a commonly open port in the majority of networks. However, it is possible that a malware to be detected within secure network by evaluating anomalies in HTTP requests, especially by monitoring the User-Agent field and URLs which are used by malware to connect the server. These methods may be combined with IP reputation systems. Subsequently, the values of User-Agent field which are used for communication particularly with understanding the low reputation of IP addresses can be identified as suspicious.

TABLE I. KEY FEATURES OF C&C CHANNELS

Protocol name	**Key features**
HTTP	• URL monitoring • modified User-Agent field in header
DNS	• pairing domain names and corresponding IP address • database of DNS translations

The second protocol is DNS, which can help to detect symptoms of malware by collecting and analyzing of DNS requests and their relevant responses. The basic element of detection is pairing domain names and corresponding IP addresses on time. By analyzing DNS records, it is possible to detect a range of incidents and also reveal incidents, which have not been detected yet. It is recommended to investigate those computers that have high failure rates of DNS translations. By this way, the malware may be detected by using generated domain names. Another possibility is a calculation of the entropy of domain names because fully random generated domain names consist of unexpected strings for people.

CONCLUSION

The analysis of calls between malware and their C&C servers is an effective method of detection of infected computers. The method can be classified on boundary between anomalous and signature systems. The advantage is revealing of indicators (URI tracks, IP addresses, domain names, values of User-Agent fields, etc.) that subsequently can be searched as common signatures, detecting in this way repeating infections in protected network. The disadvantage is the possibility of false positives. This situation requires at least a basic screening of detected anomalies and subsequent confirmation if it is a manifestation of malware behavior. A seeking of patterns of common malware does not require specialized knowledge. The analysis can be even more facilitated by a range of free available services.

ACKNOWLEDGMENT

This work was supported by grant No. IGA/FAI/2015/037 from Internal Grant Agency of Thomas Bata University in Zlin.

REFERENCES

[1] P. Szor, “The Art of Computer Virus Research and Defense,” Addison-Wesley Professional, February 2005.

[2] E. Skoudis and L. Zeltser, ”Malware: Fighting Malicious Code,” Prentice-Hall, November 2003.

[3] V. Chebyshev, D. Emm, M. Garnaeva, R. Unuchek, D. Makrushin, and A. Ivanov, “IT threat evolution Q3 2014,” November 2014. [Online]. Available from: https://securelist.com/analysis/67637/it-threat-evolution-q3-2014/ [retrieved: 7, 2015]

[4] G. O. Gorman, “Google Groups Trojan,” 2009. [Online]. Available from: http://www.symantec.com/connect/blogs/google-groups-trojan [retrieved: 7, 2015]

[5] P. James, “Flashback Mac Malware Uses Twitter as Command and Control Center,” March 2012. [Online]. Available from: http://www.intego.com/mac-security-blog/flashback-mac-malware-uses-twitter-as-command-and-control-center/ [retrieved: 7, 2015]

[6] D. Talbot, “Dropbox and Similar Services Can Sync Malware,” August 2013. [Online]. Available from: http://www.technologyreview.com/news/518506/dropbox-and-similar-services-can-sync-malware/ [retrieved: 7, 2015]

[7] McAfee Labs, “McAfee Threats Report: Q3,” November 2014. [Online]. Available from: http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2014.pdf [retrieved: 7, 2015]

[8] L. Bilge, E. Kirda, C. Kruegel, M. Balduzzi, and M. Exposure, “Finding Malicious Domains Using Passive DNS Analysis” Network and Distributed System Security Symposium, 2011, pp. 14–42, doi: 10.1145/2584679

[9] Y. He, Z. Zhong, S. Krasser, and Y. Tang, “Mining DNS for Malicious Domain Registrations,” Proc. of The 6th International Conference on Collaborative Computing, 2010. [Online]. Available from: http://www.trustedsource.org/download/research_publications/domain_registration.pdf [retrieved: 7, 2015]

[10] Centre for the Protection of National Infrastracture, “Command & Control: Understanding, denying, detecting,” 2014. [Online]. Available from: http://www.cpni.gov.uk/documents/publications/2014/2014-04-11-cc_qinetiq_report.pdf [retrieved: 7, 2015]

[11] H. Shulman and M. Waidner, “Towards Forensic Analysis of Attack with DNSSEC,” IEEE Security and Privacy Workshops, 2014. [Online]. Available from: http://www.ieee-security.org/TC/SPW2014/papers/5103a069.PDF [retrieved: 7, 2015

[12] S. Shamid, R. N. Horspool, I. Traore, and I. Sogukpinar, “A framework for metamorphic malware analysis and real-time detection,” Elsevier: Computers & Security 48, February 2015, pp. 212-233, doi:10.1016/j.cose.2014.10.011

[13] M. Fredrikson, S. Jha, M. Christodorescu, R. Sailer, and X. Yan, “Synthesizing, near-optimal malware specifications from suspicious behaviors,” IEEE, Berkeley, CA, USA, April 2010, pp. 45-60.

[14] J. Soryal and T. Saadawi, “Dos attack detection and mitigation utilizing Cross Layer Design,” ACM, Ad Hoc Networks, Volume 14, March 2014, pp. 71-83, doi: 10.1016/j.adhoc.2013.11.006

[15] G. Dondossola, F. Garrone, and J. Szanto, “Cyber Risk Assessment of Power Control Systems – A Metrics weighed by Attack Experiments,” IEEE, Berkeley, CA, USA, July 2011, pp. 1-9, doi: 10.1109/PES.2011.6039589

[16] K. Aoki, T. Yagi, M. Iwamura, and M. Itoh, “Controlling Malware HTTP Communications in Dynamic Analysis System using Search Engine,” IEEE, September 2011, [Cyberspace Safety and Security (CSS), Milan, p. 1-6]

[17] M. Grill and M. Rehák, “Malware Detection Using HTTP User-Agent Discrepancy Identification,” IEEE, Atlanta, GA, USA, December 2014, pp. 221-226, doi: 10.1109/WIFS.2014.7084331