ANTIY | Antiy Labs

Specification of Malicious URL

Antiy Labs

Contents

Scope

The specification sets the related information about computer malicious URL, such as definition, attribute, nomenclature and so on.

The specification is applied to be used for identifying malicious URL and information data exchange.

Normative References

The terms of the following files become the ones of this specification by quoting them. All the subsequent amendments (not including corrections) or revisions of the files with date marks are not applied to this specification. The latest version of all the quoted files with no date marks applies to this specification.

Terms and Definitions

Terms and definitions

The following terms and definitions apply to this specification.

Malicious URL

It refers to the transmission carrier of malware or malicious controlling instructions; the URL information source is malicious.

Information source and information sink

Information Source refers to the source of sending message, Information Sink refers to the object that receives and uses information. The Information Sink in this specification refers to the endpoint user; the Information Source refers to the object that communicates directly with the Information Sink.

For example, user C accesses the B file on the A website, then A website is the information source and user C is the information sink. Supposing that there is malware X in user’s system, malware X accesses the B file of the A website, user C positively accepts the B file of the A website, then malware X is the information source during the whole process and user C is the information sink.

Attribute Categories of Malicious URL

This part will introduce the signature attributes of internet malicious URL, the URL can be defined as malicious when it possesses one or some of the following attributes.

You should pay attention to the following aspects in this specification:

- The URL examples use “hXXp” instead of “http” in order to avoid people mistakenly clicking that leads to potential threats and avoid the capture of search engine and web crawler which will result in improving the URL ranking illegally.
- The key and commonly-used modes in HTTP protocol are POSE and GET; we can find the data transmission through GET mode in the following URL examples, such as privacy steal, information passing back, updating key words and so on. In this way, we can know the URL actions intuitively, but it is also applied to the data transmission through POST mode.
- In the following specification, when the condition that “under the situation that the URL is unknown to and unauthorized by users” is not specially emphasized, it will make that situation as precondition.
- The combination of italic percent sign and lower-case letter “s” of the malicious URL in all the examples represents the wildcard character.

Remote

- Outline: It can be used as the transmission carrier of controlling instructions between the controlled end and the C&C server, and also as the transmission carrier of webshell file shape.
- As the transmission carrier of controlling instructions between the controlled end and the C&C server, the controlled end sends requests to the controlling ends.

  For example:

  hXXp://flashupdates.info

  hXXp://nvidiasoft.info

  hXXp://nvidiadrivers.info
- As the transmission carrier of webshell file shape, the controlling end sends instructions to the controlled end.

  For example:

  hXXp://filebin.ca/xxptk/c99.php

  hXXp://ergoswiss.ch/documents/images/108.jpg

  hXXp://fileden.com/files/2013/3/30/3431486/zurikipbot.txt

Privacy

- Outline: it is used as a transmission carrier of the stolen privacy user information.

Users' privacy information includes user systems, equipment information; variety accounts and passwords; other privacy information.

- Pass the user system and equipment information back;

  For example:

  hXXp://vvww-baidu.com/updata.asp?f=sta&ip=192.168.122.242&mac=00-24-81-C4-29-67&pid=147186DF1E50BDDE4B2941AC293620F9&jc=[SYSTEM%20PROCESS]SYSTEMSMSS.EXECSRSS.EXEWINLOGON.EXESERVICES.EXELSASS.EXESVCHOST.EXESVCHOST.EXESVCHOST.EXESVCHOST.EXEEXPLORER.EXESVCHOST.EXEALG.EXECTFMON.EXEPYTHON.EXECONIME.EXEPYTHONW.EXECMD.EXEHOOKANAAPP.EXE147186DF1E50BDDE4B2941AC293620F9.358F55C0WMIPRVSE.EXE&time=2011-4-2811:22:10

  hXXp://114.200.199.251/b1aliveins.php?mac=00-24-81-A3-2B-54&ip=192.168.122.124&pid=ares&app=savitaro.exe%3B

- Pass users' various accounts and passwords information back;

  For example:

  hXXp://168.cn.am78.nb118.com/9/mail.asp?qqnumber=%s&qqpassword=%s

  hXXp://222.73.85.222:81/zhongzhong/zhongzhong/qq.asp

- Pass back other users' privacy information.

Spread

- Outline: it is the transmission carrier of malware or malware update configuration file. Here mainly refers to the transmission with file shape. The threat levels posed to users are divided into the following kinds: the binary executable malware that can execute directly at users' systems and brings direct threats to users' systems, such as sabotaging, stealing information; script (or other binary) malware, of which the main function is transmission carrier, it normally might not pose direct threats to users, such as sabotaging, stealing information; other update configuration file that is not the executable program itself.

- As the transmission carrier of binary executable malware.

  For example:

  hXXp://60.190.216.166:800/2/Game.exe

  hXXp://www.tssgdam.com/qishow.exe

- As the transmission carrier of script (or other binary) malware.

  For example:

hXXp://www.dbslj.com/images/images../index.htm

hXXp://122.228.204.135/web/1.htm

- As the transmission carrier of malware update configuration file.

  For example:

  hXXp://60.190.216.166:800/1/5566.txt

  hXXp://ad.ittz.net:72/hosts.txt

Fraud

- Outline: it is the transmission carrier of files with fraud information, which means that the web file that URL points at contains fraud information. The final goal of the fraud information we focus on is to steal user information. Fraud information involves the following categories: payment transaction, financial security, media communication, instant communication and so on.

- Fraud information of payment transaction type.

  For example:

  hXXp://www.iphone.obcsc.com

  hXXp://taobao.com-item.com

- Fraud information of financial security type.

  For example:

  hXXp://1cbc.com.cn

  hXXp://www.858danbao.com/bank/ccb/bank_ccb.asp

- Fraud information of media communication type.

  For example:

  hXXp://www.cctv-29.com

  hXXp://www.qqsk3.cn

- Fraud information of instant communication type.

  For example:

  hXXp://www.zhuoh.com/index.php?URL=http://?www.qq.com/

  hXXp://www.hntv898.com

Rogue

- Outline: the files are requested directly by the binary executable malware, which have no malware and will not pose threats to users' systems. This kind of URL is the transmission carrier of these files. The files are divided into binary executable programs, texts and binary files.

- The transmission files are binary executive programs.

  For example:

  hXXp://down.360safe.com/p/360safe_oemwwq.exe

  hXXp://rsdownload.rising.com.cn/rsfree/20119/ravf20101020.exe

- The transmission files are scripts, texts or other binary files, which is requested directly by malware, in other words, they have no referrer (There are some flaws, such as the forged referrer.).

  For example:

  hXXp://0y31wjcn578o65y0k92dizp738cxo0.ipcheker.com

  hXXp://youword.cn/mycomputer/hx_sina_qi.asp?7

Potential

- Outline: the files or data may bring threats to users through the information carriers transmitted due to the threats posed by information source or information sink.

- The files, which are requested directly by the binary executable malware, contain no malware and will not pose threats to users' systems; then this kind of files requests other files directly, the final transmitted files are mostly the media resource ones with no malware and threats.

  For example:

  hXXp://js.users.51.la/12197600.js

  hXXp://img.blamcity.com/uci/software/logo/xvid.jpg

  hXXp://js.lxchyl.com/rt/tree/dtree.css

- The files in transmission contains the data information that is unknown to or unauthorized by the information source, but the information doesn't pose direct threats to users, for example, the government websites are implanted with black chain.

  For example:

hXXp://www.hcccp.gov.cn/news/yjdt/2011/621/1162116434352H249J62D3BKF19E754.html

hXXp://www.zsds.gov.cn/download/jianmianshuilei/2010-05-12/1125.html

- The URL carrier, as data, is transmitted by other carriers. Here, the carriers mainly refer to emails with trustless junk information, IM, SNS and so on.

  For example:

  hXXp://fashionengineering.com.ua/slave.html

  hXXp://www.dombrovskaya.com/dataach_proc.html

Other

- Outline: this kind of URL refers to the ones as data that are transmitted by other carriers. This kind of URL will not pose threats to users, but they will force or trap users to access webpage or record information and so on when users are unknown of it. However, both the information source and the transmitted information data of the URLs will not bring obvious threats to users, so they are made as a separate category.

- Request the corresponding files when users know, this kind of files contain no malware and will not pose threats to users; the files will then request other files, the final transmitted files are mostly media resource ones with no malware and threats; but these files will be pop-up to force users to access and click, which will affect user' experience and consume users' resource, for example: website pop ads.

  For example:

  hXXp://nl.tg.laolinow.com/yjlc62_2011229614.htm?ths=5179&uksid=sunqing&ukuid=3239&ulinkstr=MjUxfDU4NDB8c3VucWluZ3wxfGh0dHA6Ly93d3cuYnRzY2cuY29tL3RyYWNrZXItMjA3MTAtMS0xLmh0bWw=

  hXXp://se7vena1.r.arpg2.com/jlcp324-0x58900326372938.htm?ths=5453

- Request the corresponding files when users know, this kind of files contain no malware and will not pose threats to users; this kind of files will then request other files, the final transmitted files are mostly media resource ones with no malware and they will not bring threats to users' systems.

  For example:

  hXXp://pcookie.cnzz.com/app.gif?&cna=h13TCAhnFiMCAXL2n3lEyxZY

  hXXp://drmcmm.baidu.com/media/id=rH6dPHmLP1D&gp=402&time=nHndPj04n1nsP0.jpg

Cross-attribute Classification of Malicious URL

When classifying the attribute of malicious URL, we find that some malicious URL may possess one or more attributes, for example, a malicious URL have both remote control and privacy steal (information passing back) attributes, we can classify the malicious URL according to the hazard level of “the main classification codes of malicious URL attribute”; if the hazard levels are equal, we can classify according to the sequence (from top to bottom) of “the main classification codes of malicious URL attribute”, the principle is that let the attribute with high risk level be defined as the main attribute of current malicious URL, which will be decided by the actual situation.

Nomenclature Criteria of Malicious URL

Nomenclature criteria of Malicious URL

The malicious URL uses segmented format nomenclature, of which the first four fields are required options using English (case-insensitive) or numbers as marks; the fifth field is the extend one which is optional with bracket “[]” as mark, the primary user mark information source, the extend fields can be added to be more.

The main classification code of malicious URL. The detail attribute code of malicious URL. The family name of malicious URL. The variants’ names [information source].

Such as:

- remote.C&C.Dorgam.un
- privacy.Password.Generic.a
- spread.Payload.Unknown[Spam]
- spread.Config.Tiny.cqt
- potential.Unknown.Jorik.bod

The main classification code of malicious URL

The specification plays the malicious URL attributes in sequence according to the risk levels and marks with correspondent colors to make it easy to be descript and identified. If the URL possesses several attributes, then it will make the one in the top sequence as the main classification.

The main classification codes and sequences of malicious URL attribute are as follows:

Sequence	Main Classification of	Risk Level	Threshold Interval	Color	RGB Color Code

	Attribute				
1	remote	High	7--9	Red	#FF0000
2	privacy	High	7--9	Red	#FF0000
3	spread	High	7--9	Red	#FF0000
4	fraud	Middle	4--6	Orange	#FF8C00
5	rogue	Middle	4--6	Orange	#FF8C00
6	potential	Low	0--3	Yellow	#FFFF00
7	other	Low	0--3	Yellow	#FFFF00

The detail attribute classification code of malicious URL

The specification divided the main classification of malicious URL's attributes carefully according to the information source, information sink and the differences of actions, so that it can be descript in detail and identified by the public.

Information source: as the name suggests, it refers mainly to the way how the malicious URL sparks, such as sample self-generating, user operation, junk mails and so on.

Data format: the contents that the malicious URL points at, such as PE files, media resources, script and so on.

Main Classification of Attribute	Information Source	Data Format	Detail Attribute	Family Name	Variant
remote			C&C		
remote			Webshell		
remote			Unknown		
privacy			System		
privacy			Password		
privacy			Unknown		
spread		PE	Payload		
spread		Script	Exploit		
spread		Config	Config		
spread			Unknown		
fraud		Site	Media		

fraud		Site	IM		
fraud			Unknown		
rogue	Malicious	PE	PE		
rogue	Malicious	Site	Site		
Rogue			Unknown		
potential	*Malicious*	*Resource*	*Malicious*		
potential	Hack		Hack		
potential	Spam		Spam		
potential			Unknown		
other	*Normal*		*pop*		
other	*Normal*	*Resource*	*Resource*		

Note: the italics above are not involved in the practical application temperately.

Any technical information that is made available by Antiy Labs is the copyrighted work of Antiy Labs and is owned by Antiy Labs.

NO WARRANTY. Antiy Labs makes no warranty as to this document's accuracy or use. The information in this document may include typographical errors or inaccuracies, and may not reflect the most current developments; and Antiy Labs does not represent, warrant or guarantee that it is complete, accurate, or up-to-date, nor does Antiy Labs offer any certification or guarantee with respect to any opinions expressed herein or any references provided. Changing circumstances may change the accuracy of the content herein. Opinions presented in this document reflect judgment at the time of publication and are subject to change. Any use of the information contained in this document is at the risk of the user. Antiy Labs assumes no responsibility for errors, omissions, or damages resulting from the use of or reliance on the information herein. Antiy Labs reserves the right to make changes at any time without prior notice.

About Antiy Labs

Antiy Labs is an antivirus vendor which makes advanced research and technology contributions to the field. Currently, there are tens of thousands of firewalls, UTM and security devices deployed with our antivirus engine. More information is available at www.antiy.net.

ANTIY | Antiy Labs