GTI

Classification of Malicious Links for Vertical Industries

Version:	V1.0.0
Deliverable Type	□ **Procedural Document** ☑ **Working Document**
Confidential Level	□ **Open to GTI Operator Members** □ **Open to GTI Partners** ☑ **Open to Public**
Working Group	
Task	**PM3-PJ9-task5: Classification of malicious links for vertical industries**
Source members	CMCC
Support members	NSFOCUS
Editor	Bangling Li(CMCC), Huaxi Peng(CMCC)
Last Edit Date	（11-08-2022）
Approval Date	

Document History

Date	Meeting #	Version #	Revision Contents

Table of Contents

1 Introduction

With the advent of the network information era, the rapid development of industries such as the Internet, mobile Internet, and smart mobile terminals has promoted the rapid rise of e-commerce. The rapid development of Internet technology has undoubtedly greatly facilitated people's lives and accelerated the dissemination of information, but at the same time, it has also provided criminals with the possibility of illegal profit. In recent years, malicious links have been widely used by criminals to carry out illegal activities throughout the Internet, with serious harm. Some criminals use malicious links to spread obscenity, pornography, gambling, violence, homicide, terror, or instigate crimes of unlawful illegal information. Some attackers often use malicious links as phishing, Trojan horses and malware and other types of network attacks, stealing user information, and even transferring funds, which has a bad impact on network security. At present, different vendors have different definitions of malicious link types. It is not conducive to subsequent risk analysis and unified management, and information exchange and sharing among vendors. Different classification will also affect the subsequent disposal of the responsible website management department.

In view of the inconsistency in the definition and type of malicious links between different vendors, the project aims to unify the malicious links classification framework and standardize the type and name of malicious links. This is conducive to the design, development, construction and evaluation of the malicious links monitoring system. At the same time, it provides basic support for different vendors to realize information sharing and exchange. It also provides strong support for Internet governance.

2 Definition

Malicious Links

Malicious links, also known as malicious URLs, mean that the network resources pointed to by the URL address provide illegal and insecure network services.

3 Abbreviations

URL	Uniform Resource Locator
SQL	Structured Query Language
XSS	Cross-Site Scripting
MWL	Malware Links
WHHL	Website Hanging Horses Links
MDL	Malicious Download Links
OMWL	Other Malware Links
WAL	Web Attacks Links
SQLIAL	SQL Injection Attacks Links
XSSAL	XSS Attacks Links
XPIAL	XPath Injection Attacks Links
DTAL	Directory Traversal Attack Links
RAL	Redirect Attack Links
FIAL	File Inclusion Attack Links
OWAL	Other Web Attacks Links
IFL	Internet Fraud Links
PHL	Phishing Links
FWL	Fake Winning Links
FRRL	Fake Recruitment Links
FCSL	Fake Customer Service Links
FRHL	Fake Recharge Links
FAL	False Advertising Links
FIFML	Fake Investment And Financial Management Links

FLL	Fake Loan Links
FNL	Fake Number Links
BSRL	Brush Single Rebate Links
CCALL	Credit Card Agent Links
OIFL	Other Internet Fraud Links
JIL	Junk Information Links
SL	Spam Links
JML	Junk Messages Links
HISL	Harassment Information Spread Links HISL
OJIL	Other Junk Information Links
ILL	Information Leakage Links
NILL	National Information Leakage Links
CILL	Corporate Information Leakage Links
PILL	Personal Information Leakage Links
OILL	Other Information Leakage Links
ICL	Illegal Content Links
GL	Gambling Links
POL	Pornographic Links
DRL	Drug Links
IL	Illegal links
DIL	Discrimination Links
TL	Terrorism Links
ISL	Illegal Software Links
OICL	Other Illegal Content Links
OML	Other Malicious Links

4 Malicious Links Classification

4.1 Consider Elements And Basic Classification

Classify malicious links based on the cause, performance, and results of malicious links. Malicious links are divided into 7 basic categories: malware links (MWL), web attack links (WAL), internet fraud links (IFL), junk information links (JIL), information leakage links (ILL), illegal content links (ICL), and other malicious links (OML). And each level category includes several sub-categories.

4.2 Detailed Classification

4.2.1 Malware Links

MWL refer to that the websites the links point to contain malware, or the webpage are hanged with a Trojan horse to spread malware, or the sites hosts a large number of other malicious resources for spreading or injection.

MWL include website hanging horses links (WHHL), malicious download links (MDL), and other malware links (OMWL). The specific descriptions are shown in the following table.

Sub-Categories	Description
WHHL	The websites that the WHHL points to were broken by hackers using site vulnerabilities, and the Trojan horse code was implanted on the Web servers or the Trojan horse program was deliberately placed on the malicious sites. When a user clicks on WHHL, the hackers take advantage of the loopholes in the user's machine to steal links, increase the amount of visits to their websites, steal user information, and damage the websites database to achieve the purpose of attacking the servers and paralyzing the servers.
MDL	MDL refer to links that provide download services such as viruses, Trojan horses, worm programs, botnet programs, ransomware, mining software, etc.
OMWL	OMWL refer to other MWL that cannot be included in the above 2 subcategories

4.2.2 Web Attacks Links

WAL refer to links used by attackers to attack network information systems or steal sensitive information.

WAL include SQL injection attack links (SQLIAL) , XSS attack links (XSSAL), XPath injection attack links (XPIAL), directory traversal attack links (DTAL), redirect attack links (RAL), file inclusion attack links (FIAL) and other Web attack links (OWAL).

Sub-Categories	Description
SQLIAL	SQLIAL refer to the URLs constructed after inserting malicious SQL statements into the URL, which is executed by the attacker to attack the WEB server, causing any data in the database to be leaked or tampered with.
XSSAL	XSSAL refer to the URLs constructed after inserting XSS script program into the URL. After clicked by the user, the attacker's script will be executed to steal the user's personal data such as cookies.
XPIAL	XPIAL refer to the URLs constructed by using the loose input and fault-tolerant features of the XPath parser to attach malicious XPath query code to the URL, which is executed to gain access to permission information and attack the website.
DTAL	DTAL refer to the URLs that can be used by an attacker to carry out directory traversal attack.
RAL	RAL refer to the URLs that can be redirected to another domain sites without the user's knowledge to lure the user to a malicious page, often used for phishing.
FIAL	FIAL refer to the URLs constructed for the pages with file inclusion vulnerability to carry out file inclusion attack, resulting in file information disclosure or illegal operations.
OWAL	OWAL refer to WAL that cannot be included in the above 6 subcategories.

4.2.3 Internet Fraud Links

IFL refer to the links pointing to the network resources to provide some false information, deceiving users into property transactions, resulting in potential property losses of users.

IFL include phishing links (PHL), fake winning links (FWL), fake recruitment links (FRRL), fake customer service links (FCSL), fake recharge links (FRHL), fake advertising links (FAL), fake investment and financial management links (FIFML), fake loan links (FLL), fake number links (FNL), brush single rebate links (BSRL), credit card agent links (CCAL) and other internet fraud links (OIFL).

Sub-Categories	Description
PHL	PHL refer to links that provide phishing services. Phishing means that criminals use various methods to imitate the URL address and page content of the real website, or use loopholes in the server program of the real website to insert dangerous HTML codes into certain pages of the site to defraud users of bank or credit card account number, password and other private information.
FWL	FWL refer to links that provide fake winning information. Fake winning refers to pretending to be various official activities in the name of giving back to users without official authorization, such as product anniversary celebrations of major companies, sweepstakes, variety show out lottery, etc., spreading fake user winning news in order to collect Handling fees, deposits, postage, taxes and fees are used to deceive users into entering account numbers or to induce users to engage in remittance fraud before receiving prizes.
FRRL	FRRL refer to the links that provide services for publishing fake recruitment information.
FCSL	FCSL refer to the links that provide services for publishing fake customer information.
FRHL	FRHL refer to the links that provide fake recharge services. Fake recharge refers to the unauthorized imitation of official websites to sell all kinds of fake famous business recharge cards at low prices or to provide fake recharge service of recharge cards.
FAL	FAL refer to links that provide fake advertising services. Fake advertising means that the content of the advertisement is fake or misleading. One refers to that the content of the product promotion does not match the actual quality of the product or service provided, and the other refers to the object that may be promoted or affected by the promotion. People have wrong associations with the real situation of the goods, which affects the promotion of the goods in

	their purchasing decisions. The content of this type of advertisement is often exaggerated, untrue, vague, and misleading.
FIFML	FIFML refer to links that provide fake investment and financial management services. Fake investment and financial management often mislead users into transactions by propagating investment information that contains high returns and low risks. Once investors are deceived, it is difficult to recover their losses.
FLL	FLL refer to the websites that the links points to are not qualified to provide loans and publish loan information services.
FNL	FNL refer to the links that provide fake mobile phone number services; Fake number refers to a mobile phone number without real-name system used to accept verification code information on behalf of others.
BSRL	BSRL refer to the links that provide rebate services.
CCAL	CCAL refer to the websites that the links points to provide online credit card agency service, requiring users to input their contact information, ID card and other personal privacy information.
OIFL	OIFL refer to IFL that cannot be included in the above 11 subcategories.

4.2.4 Junk Information Links

JIL refer to links that provide a large number of information services that induce users to spread.

JIL include spam links (SL), junk messages links (JML), harassment information spread links (HISL) and other junk information links (OJIL).

Sub-Categories	Description
SL	SL refer to the links that are found in spam emails.
JWL	JWL refer to the links that are found in junk messages.
HISL	HISL refer to the links that provide information services such as harassment, fraud, spam, attention, downloading, sharing, vulgar content, etc.
OJIL	OJIL refer to JIL that cannot be included in the above 3 subcategories.

4.2.5 Information Leakage Links

ILL refer to links that engaged in dissemination and trading of information leakage points.

ILL include national information leakage links (NILL), corporate information leakage links (CILL), personal information leakage links (PILL), and other information leakage links (OILL).

Sub-Categories	Description
NILL	NILL refer to the website links engaged in the dissemination and trading of national information disclosure.
CILL	CILL refer to the website links engaged in the dissemination and trading of corporate information disclosure.
PILL	PILL refer to the website links engaged in the dissemination and trading of personal information disclosure.
OILL	OILL refer to ILL that cannot be included in the above 3 subcategories.

4.2.6 Illegal Content Links

ICL refer to the web resources that the links pointed to provide illegal web services or content in violation of relevant Chinese laws or regulations.

ICL include gambling links (GL), pornographic links (POL), drug links (DRL), reactionary links (RL), discriminatory links (DL), terrorism links (TL), illegal software links (ISL), and other illegal content links (OICL).

Sub-Categories	Description
GL	GL refer to the links that provide gambling and related business services or disseminating gambling content.
POL	POL refer to the links that provide pornography and related business services or spreading obscene or pornographic content.
DRL	DRL refer to links that provide drug dealing and related services.
RL	RL refer to links that spread reactionary speech.
DL	DIL refer to links that spread discriminatory speech.
TL	TL refer to links that spread and operate involving terrorism.
ISL	ISL refer to links that provide illegal software trading and related services.
OICL	OICL refer to ICL that cannot be included in the above 7 subcategories.

4.2.7 Other Malicious Links

OML refer to malicious links that cannot be classified into the above 6 basic categories.

5 Terms of Use

Notwithstanding anything set out herein, the fact that the GTI makes this document available and performs certain tasks hereunder, does not constitute a service rendered by the GTI to any third party.

The GTI disclaims any and all liability for any mistakes, faults, incorrect information/instructions, variations, inconsistencies, actions or omissions; any information provided by a third party; any -assessment declaration; or any other activities, associated with this document.