

国家信息中心主办

第6卷 第2期 2020年2月

Vol.6 No.2 Feb. 2020



QK2007461

信息安全研究

Journal of Information Security Research

瑞星 2019 年中国网络安全报告与趋势展望



基于汇编指令词向量特征的恶意软件检测研究
基于 SVM 的 ICMP 网络存储隐藏信道检测
一种基于暗网的威胁情报主动获取框架

ISSN 2096-1057



9 772096 105204

邮发代号: 2-41 定价: 38.00 元

万方数据

本刊全文已被《CNKI 中国期刊全文数据库》《中国核心期刊(遴选)数据库》《中文科技期刊数据库》《超星期刊域出版平台》《博视网》收录。

主管单位 国家发展和改革委员会
主办单位 国家信息中心

出版单位 《信息安全研究》杂志社
地址 北京市西城区三里河路 58 号
邮编 100045
电话 +86(10)68557385
网址 <http://www.sicris.cn>
电子信箱 ris@cei.cn

主编 李新友
社长 欧阳鹏
执行主编 崔传桢
副主编 吕欣 马修军
出版日期 每月 5 日

中国标准刊号 ISSN 2096-1057
CN 10-1345/TP

广告经营许可证 京西工商广登字 20170054 号
印刷单位 北京博海升彩色印刷有限公司
国内发行 北京市报刊发行局
订购处 全国各地邮电局(所)
邮发代号 2-41
定价 38.00 元

战略合作单位 北京龙象之本投资管理有限公司
协办单位 亚信网络安全产业技术研究院

稿件授权声明: 凡向本刊投稿并被录用, 由本刊支付稿酬的稿件, 均视为稿件作者同意以下条款:

1. 文责自负。作者保证其拥有该作品的完全著作权(版权), 该作品不侵犯任何他人的著作权。
2. 全权许可。本刊有权以任何形式(包括但不限于媒体、网络、光盘等介质)使用、编辑、修改该作品, 无须另行征得作者同意, 无须另行支付稿酬。
3. 独家使用。未经本刊书面许可, 作者不同意任何单位和个人以任何形式使用(包括但不限于通过媒体、网络、光盘等介质转载、张贴、集结、出版)该作品, 著作权法另有规定的除外。

版权声明: 未经本刊书面许可, 任何单位和个人不得以任何形式使用(包括但不限于通过媒体、网络、光盘等介质转载、张贴、集结、出版)该作品, 著作权法另有规定的除外。

» 特别策划

98 瑞星 2019 年中国网络安全报告与趋势展望
..... 北京瑞星网安技术股份有限公司

» 学术论文

- 108 一种可实用的量子保密查询方案
..... 徐鹏翔 贺振兴 张鑫 马鸿洋
- 113 基于汇编指令词向量特征的恶意软件检测研究
..... 杨频 潘岳镭 贾鹏 刘亮
- 122 基于 SVM 的 ICMP 网络存储隐蔽信道检测
..... 李抒霞 周安民 郑荣锋 胡星高
- 131 一种基于暗网的威胁情报主动获取框架
..... 黄莉峥 刘嘉勇 郑荣锋 李孟铭
- 139 基于行为的安全验证码生成及验证方案研究
..... 张艳 彭华燕 何申
- 145 万兆 IPSec 协议芯片关键技术研究
..... 桂祚勤 崔广财 林存花 陈浩涓
- 151 文件上传漏洞研究与实践
..... 黄志华 王子凯 徐玉华 李云龙 孙伟
- 159 数字化背景下网络贩毒的特点及侦查策略研究
..... 雷丹丽 黄相升 向大为
- 165 面向装备软件质量管理的系统工程建模方法研究
..... 王强 尚京威 李强

» 技术应用

- 171 “雪亮工程”中的公安视频网安全防护体系建设 宣耀
- 181 互联网企业 Web 系统易忽视漏洞分析 潘志岗
- 188 基于同态加密技术的实验室开放管理系统
..... 郭俊岭 侯红霞

CONTENTS

目次

Special Report

2019 China Cyber Security Report and Trend Outlook

..... Beijing Rising Network Security Technology Co., Ltd. (98)

Research Papers

A Practical Quantum Private Query Scheme..... Xu Pengao, et al (108)

Malware Detection Based on Word Embedding Features of

Assembly Instruction Yang Pin, et al (113)

Detection of Network Storage Covert Channel over ICMP Protocol

Based on SVM Li Shuxia, et al (122)

A Framework for Proactive Acquisition of Threat Intelligence

Based on Darknet Huang Lizheng, et al (131)

The Research of Secure CAPTCHA Generation and Verification

Scheme Based on Behavior Zhang Yan, et al (139)

The Key Techniques Research of 10 Gbps IPsec Protocol Chip

.....Gui Zuoqin, et al (145)

Research and Practice of File Upload Vulnerability

..... Huang Zhihua, et al (151)

Characteristics and Investigation Strategies of Internet Drug

Trafficking Under Digital BackgroundLei Danli, et al (159)

Research on System Engineering Modeling Method for Equipment

Software Quality Management Wang Qiang, et al (165)

Technical Applications

Discussion of Security Protection System of Public Security Video

Network in Xueliang ProjectXuan Yao (171)

Analysis on the Vulnerability of Internet Enterprise Web System to

Being Easily Ignored Pan Zhigang (181)

Laboratory Open Management System Based on Homomorphic

Encryption Technology Guo Junling, et al (188)

Journal of Information Security Research

Vol.6 No.2 Feb. 2020

Publishing Period: Monthly

Date of Publication: 5th day of each month

International Standard Serial Number:

ISSN 2096-1057

Issues of Domestic Unit: CN 10-1345/TP

Editor-in-Chief: Li Xinyou

Directed by: National Development and Reform
Commission

Sponsored by: The State Information Center

Published by: Journal of Information Security
Research

Address: No.58 Sanlihe Road, Xicheng District,
Beijing

Zip Code: 100045

Website: <http://www.sicris.cn>

E-mail: ris@cei.cn

AD Permit: BAIC XBB Ad. No.0410

Distributor: Beijing Press and Publication Bureau

Domestic Issue Code: 2-41

Price: 38.00RMB

编委会顾问

蔡吉人 崔书昆 杜虹 方滨兴 冯登国
顾建国 何德全 吕述望 倪光南 沈昌祥
严明 杨学山 赵战生

编委会主任 王小云

编委会委员

安德智 陈钟 陈嘉兴 陈尚义 陈晓桦
陈兴蜀 程学旗 丁珂 丁丽萍 杜彦辉
杜跃进 段海新 方勇 封化民 谷大武
顾健 郭莉 郭艳卿 何政 胡爱群
胡昌振 胡红钢 胡红升 贾焰 荆继武
康海燕 孔祥维 李晖 李剑 李涛
李建彬 李建华 李京春 李守鹏 李小勇
李欲晓 李舟军 林鹏 林东岱 林家骏
刘云 刘宝旭 刘吉强 罗森林 马智
马民虎 孟丹 孟小峰 闵京华 潘泉
潘柱廷 秦玉海 任卫红 孙伟 孙德刚
谭晓生 田俊峰 王标 王军 王楠
王智 王宝生 王丽娜 温巧燕 翁健
吴文玲 吴志军 肖新光 徐立臻 许光全
杨庚 杨义先 叶红 俞能海 云晓春
张健 张兴 张功萱 张宏莉 张焕国
张建标 张建军 张仕斌 张玉清 赵波
赵粮 赵淦森 赵有健 钟力 周民
周文 周琳娜 周世杰 朱岩 朱建明
祝烈煌 邹维 邹德清

蔡季良先生画作选



国画：万象更新

文化自信系列：新水墨写意创新探索

蔡季良，男，1962 年生于北京，毕业于中央美术学院壁画系。现为中国国家画院孔紫工作室画家、同泽书画研究院画家。他一贯坚持秉承中国传统文化绘画艺术精神，寻觅中国原创艺术元素，积极汲取中国书画同道艺术营养，不懈探寻和广汲“羊文化”内容，专注于以羊为内容的书画道路并积极探索创新，作品被诸多机构收藏。

《万象更新》这幅作品，表现了冬去春来、吉祥如意。作品以传统笔墨来表现中国文化独特性，歌颂热爱和平，崇尚温良的民族特质。通过三羊开泰传统题材，展现出一原复始、万象更新的美好景象。从物质到精神的憧憬，简淡随心，洋溢着幸福与美好。作品寻觅着健康向上的美好心境，表现了作者对中国文化的坚定自信。