



西安交通大学管理学院  
THE SCHOOL OF MANAGEMENT  
XI'AN JIAOTONG UNIVERSITY

# 第5部分——系统安全

## Part V: Management Information Systems Safety and Security

刘跃文 博士 Dr. LIU, Yuewen

教授、博士生导师 Professor

[liuyuewen@xjtu.edu.cn](mailto:liuyuewen@xjtu.edu.cn)

西安交通大学管理学院

School of Management, Xi'an Jiaotong University

V2.0, 2023-Oct

An iceberg floating in the ocean. The tip of the iceberg is above the water line, representing the Surface Web. The much larger part of the iceberg is submerged below the water line, representing the Deep Web and Dark Web. The background is a blue sky with white clouds.

## Surface Web 明网

YAHOO!  
Google  
reddit  
CNN.com  
bing

## Deep Web 深网

Academic databases  
Medical records  
Financial records  
Legal documents  
Some scientific reports  
Some government reports  
Subscription only information  
Some organization-specific repositories

## Dark Web 暗网

TOR  
Political protest  
Drug trafficking  
and other illegal activities

**96%**

of content on the  
Web (estimated)

# System Safety

---

- System Safety : It refers to the application of system safety engineering and system safety management methods in the system life cycle. It can identify the hidden dangers in the system, and adopt effective control measures to minimize the risk, so that the system can achieve the best degree of safety in the specified performance, time and cost range.
- The more functions the system can achieve, the greater the loss caused by a shutdown.

# Example: convenience and security challenges of 5G

When 5G breaks the network boundary and further realizes the integration of the network world and the physical world, attacks on the virtual world will become physical harm, and the influence of cyber attacks will skyrocket exponentially.

## eMBB

Large broadband: 10GB/s download rate, making 3D, ultra-high-definition video and other large traffic mobile broadband services possible;

Big broadband also makes it easy for hackers to quickly access data;

## uRLLC

High reliability and low delay: theoretical delay of 5G is 1ms, so that unmanned driving, industrial automation and other businesses no longer only realized in the movie;

When it is combined with important vertical industries such as the Internet of vehicles, telemedicine, industrial automation, and smart grid, the objects and rights of cyber attacks are further expanded;

## mMTC

Massive connection: The theoretical value of the number of IOT terminals which can be connected to 5G single communication cell has reached millions of levels.

When more critical infrastructure and important application architectures are on their 5Gs, these high-value targets will attract a greater attack force - national hackers.

# 提纲 Outline

---

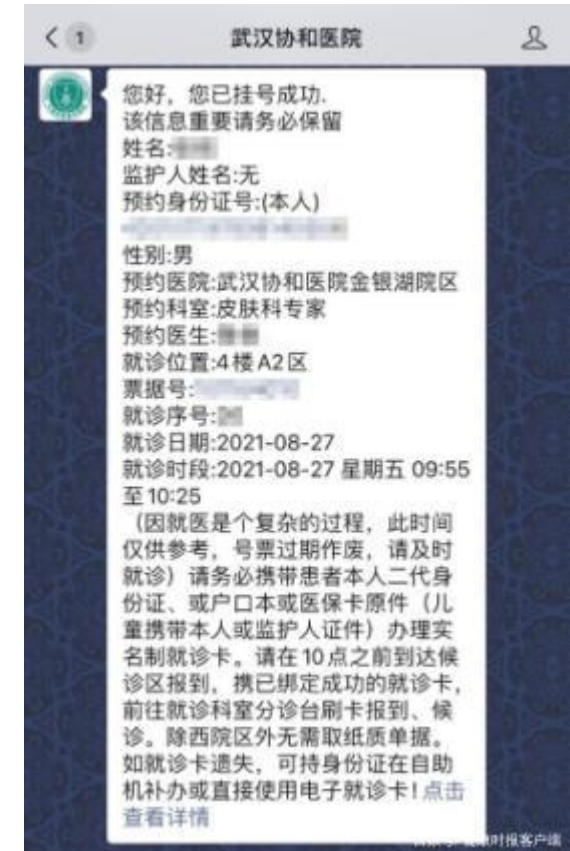
- 系统越强大 组织越脆弱 The stronger the system, the more vulnerable the organization
- 勒索与系统攻击 Extortion and system attacks
- 钻系统的漏洞 Exploit system vulnerabilities
- 将系统用于服务犯罪 Use the system to serve crimes

# 1. 系统越强大 组织越脆弱

## The stronger the system, the more vulnerable the organization

# 1. Case: Wuhan Union Jinyinhu hospital system collapsed

- " The hospital's information system broke down at around 8:30 in the morning, and now it is impossible to read the electronic medical card. The doctor's computer can not receive any patient information, and the doctors can not write checklists or prescriptions, and can not do treatment... Patients and their families have to wait in the lobby, and doctors don't know what to do. " On August 27th, Chen Lu (pseudonym), who lives in the Dongxihu district of Wuhan City, Hubei province, told reporters about his experience in Jinyinhu Hospital of Wuhan Union Medical College.



# The system is broken, nothing can be done

---

- "The registration system of this hospital is very convenient, after registering on the mobile phone and binding the medical card, relying on the registration information received on the mobile phone can report directly at the department triage table and wait for treatment." Chen said he arrived at the department floor 10 minutes earlier than the recommended time of 9:50 am.
- However, the nurse at the triage table told him that the hospital's information system had broken down at around 8:30, making it impossible for doctors to activate the electronic doctor's card, write prescriptions or do treatment. Waiting patients and their families had to wait in the lobby, and doctors did not know what to do. "One patient told me he had been waiting for over an hour." Chen Lu said.
- "There are waiting patients of the stomatology department and dermatology department in this area. Because the doctors can't see them, many patients and their families are stuck here. In order to prevent and control the epidemic, the hospital requires to sit in other seats, and the waiting area has dozens of people, so the seats are almost full." Chen Lu recalled, there were also doctors who came out of the consulting room to ask the nurse at the triage table how to do, but they were at a loss for each other.



# Manual registration

---

- Around 10:30, the system still did not recover, but doctors resumed diagnosis and treatment temporarily. The nurse at the triage desk called the waiting patients to manually register their information, and Chen Lu got his "call slip" with his serial number written in black pen.
- "I waited less than an hour for my turn to see a doctor. Because the system was not good, the doctor could only write the medical record by hand, but could not order a checklist." Chen Lu told reporters that his surgery way needs to be confirmed after B-ultrasound, but the doctor can not generate a checklist in the system. The doctor told Chen Lu that he has an outpatient clinic in another hospital area in the afternoon, so that he can go there to re-register for examination.
- That's a wasted trip and an extra two hours of waiting. "The system is broken, even the withdrawing registration cannot be finished. Withdrawing registration by mobile phone only can be done before 16:30 the day before the visit. On the day of the visit, withdrawing registration must be handled at the hospital window, so I can not finish the withdrawing registration." Chen Lu said helplessly. Later, the nurse began to manually register the withdrawal information, and promised that the withdrawing registration would be done after the system was restored.

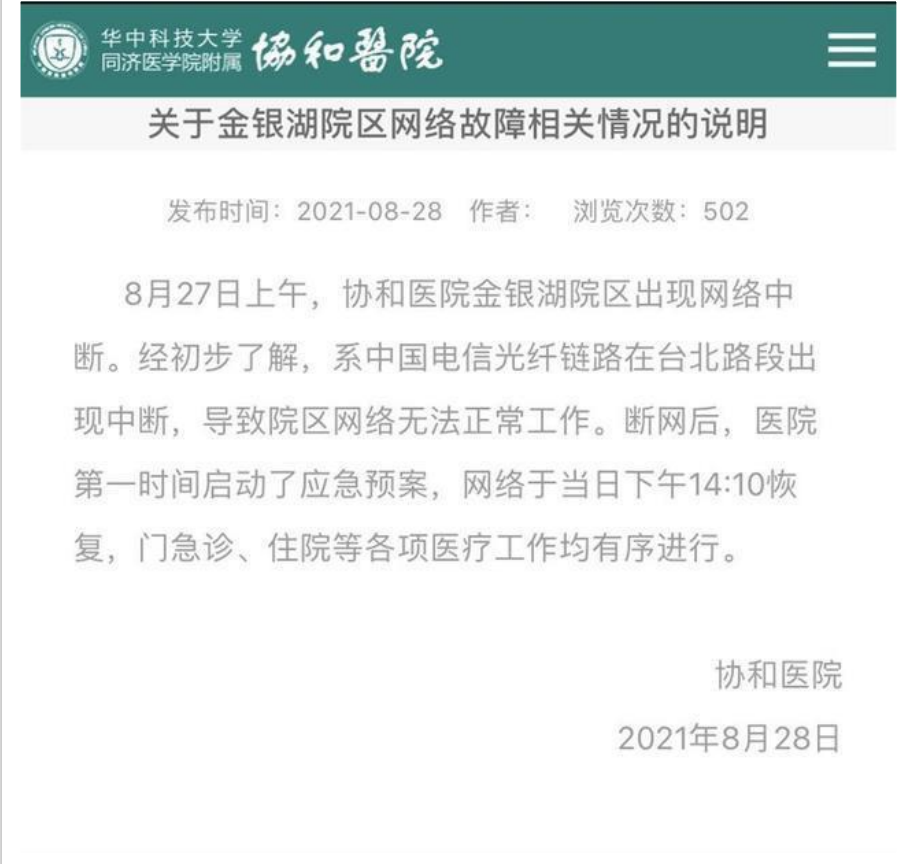
# Emergency preparedness

---

- "The system is down, can't we see a clinic? Is it true that in the past, when there were no computers and the Internet, medical treatment was not possible?" Chen Lu helplessly said that the hospital's various processes are electronic, including online registration, reading card and waiting for treatment, electronic medical records, electronic prescriptions... Once the electronics fail, the hospital goes into shutdown mode. In the face of power outage, network shutdown and other emergencies, the hospital should have some preparations to ensure the stability of medical order.

# Cause of system shutdown

- On the morning of August 27th, there was a network interruption in the Jinyinhu Hospital area of the Union Hospital. After preliminary understanding, it is the interruption of the optical fiber link of China Telecom in Taipei Road, which causes the network of the hospital to not work normally. After the network was disconnected, the hospital launched an emergency plan for the first time. The network was restored at 14:10 p.m. on the same day. Various medical work such as outpatient and emergency care, and hospitalization were carried out in an orderly manner.
- The relevant person in charge of the hospital said that the hospital launched the emergency plan and manual process at the first time, and opened a green channel for emergency patients. The implementation of the manual process has brought inconvenience to some outpatient patients, but the treatment and surgery of emergency and inpatient are normal and have not been affected.



华中科技大学 同济医学院附属 协和医院

### 关于金银湖院区网络故障相关情况的说明

发布时间: 2021-08-28 作者: 浏览次数: 502

8月27日上午, 协和医院金银湖院区出现网络中断。经初步了解, 系中国电信光纤链路在台北路段出现中断, 导致院区网络无法正常工作。断网后, 医院第一时间启动了应急预案, 网络于当日下午14:10恢复, 门急诊、住院等各项医疗工作均有序进行。

协和医院  
2021年8月28日

# Other cases

---

- In 2006, approximately 350,000 pacemakers and 123,000 IDCs (Implantable cardiac defibrillators) were implanted in patients in the United States. 2006 was a particularly significant year, as it was the year that the FDA approved the clinical use of medical devices based entirely on wireless connection control. 3 million pacemakers and 1.7 million defibrillators are in use today.
- At a computer security conference in Melbourne, Australia, in October 2012, Jack showed a video demonstrating how he could use a laptop to control a pacemaker from 15.2 meters away, causing it to instantly generate 830 volts, enough to kill a person. He also said that it might be possible to design "worms" that target a particular brand of pacemaker and defibrillator to spread from one device to another over a certain distance, taking control of one patient after another.

- In 2013, Jack, as a "star hacker", reemerged and planned to show a more amazing "hacker trick" at the "Black Hat" hacker conference that opened on July 31 — to invade wireless medical devices such as implantable cardiac pacemakers 9 meters away, and then send a series of 830V high-voltage electric shocks to it, so that "remote control killing" becomes a reality! Jack claims to have discovered security flaws in pacemakers made by several manufacturers.
- 《Implantable Medical Devices: Hacking Humans》  
*" This talk will focus on the safety of wireless implanted medical devices. I will discuss how these devices operate and communicate, as well as security vulnerabilities in communication protocols. Our research will reveal how an ordinary data transceiver can search for and hack into nearby medical devices. I will also discuss how these designs can be improved to enhance their security. "*



**IOActive, Inc**  
@IOActive

Follow

Lost but never forgotten our beloved pirate, Barnaby Jack has passed. He was a master hacker and dear friend. Here's to you Barnes!

6:58 PM - 26 Jul 2013

267 RETWEETS 52 FAVORITES



- At the same time that the Ford Kuga and Toyota Prius were found by hackers to control the sudden acceleration, braking, and steering wheel of the driving system, a number of Volkswagen car models were also found by cryptographers to have vulnerabilities, which can be easily unlocked by hackers to ignite and go away, just like the car keys were taken away. In addition, most navigators on the market can be remotely hacked, which means that the security issue of cars with smart devices such as electronic locks, ignition systems, and GPS will become increasingly serious.



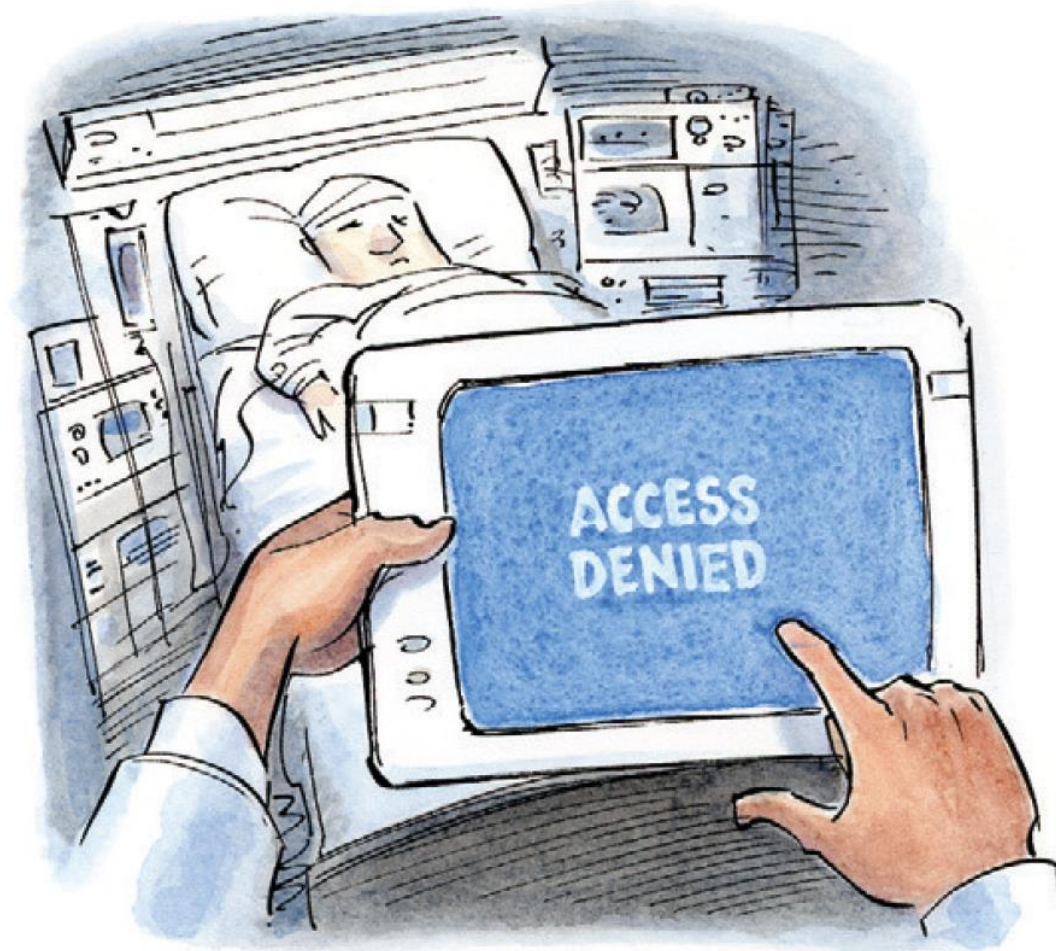
## 2. 勒索与系统攻击 Extortion and system attacks



# 1. 案例：Sunnylake医院

## Case: Sunnylake Hospital

---



# Background Information

---

- Paul is the CEO of Sunnyslake Hospital, and he has been in office for 5 years.
- One of Paul's first goals at the beginning of taking office was to convert the hospital's records system from paper to electronic.
- Paul hired Jacob Dale as the head of the hospital's IT department. IT department implemented the goal of electronization successfully and built the Electronic Medical Records (EMRs) system.
  - Initially, some doctors resisted the system.
  - In the late era, the most stubborn old doctors admit that the system can automatically check medical affairs and drug reactions.
- This move catapulted Sunnyslake Hospital from a stagnant rural hospital to a nationally renowned model of small hospitals.
- Paul was worried about patient data privacy at first. Three years have passed and nothing has happened. As a result, Paul began to have confidence in the system and felt that security was not a big issue.

# 第一封邮件 The first mail

---

- 星期五下午，CEO Paul收到一封匿名邮件：  
On Friday afternoon, CEO Paul received an anonymous email:

*Ur network security sucks.  
But we can help u.  
for 100K cash well insure your little  
hospital dont suffer any disasters.*

*你的网络安全太烂了！  
但是我们能帮助你！  
只需要10万美元，  
就能让你的医院不遭受任何的灾难！*

# 第二封邮件 The second mail

---

- 星期一上午8:00,  
Monday 8:00 a.m.

*We warned u.*  
*我们警告过你哦*

# Access Denied (访问被拒)

- The hospital is busy as usual!
- The medical records system is inaccessible!
- Hackers have taken down the entire EMR system, and they're taking it offline!
- Anyone who tries to access the system will see the same content: "Access Denied"
- Doctors are crowding the doors of the IT department...



# 第三封邮件 The third mail

---

- Jacob去找Paul，此时第三封邮件寄到：  
Jacob goes looking for Paul, and the third email arrives:

*We bet u want your stuff back.  
probably shud have protected it better.  
for the small price of 100K well  
make this go away.*

*我们觉得你肯定希望你的员工回到工作岗位上  
也许你现在后悔，系统应该保护得更好！  
只需要10万美元这么一丢丢钱  
我们就能让所有的事情正常。*

# What's going on?

---

- Hackers used a system-based ransomware that demanded a ransom of \$100,000 in exchange for decryption tools.
- The ransomware prevents access to electronic medical records, even by system administrators.
- Safety technology has evolved rapidly over the past three years, but hospitals have not kept up to date. It may be that an employee thinks that while downloading "anti-virus software" or updating software, hackers took the opportunity to break in.
- The data is backed up on the network, so it can't be lost. However, at this moment, the hospital cannot access the data and is forced to go into a "standstill" state!

# IT department

- IT department felt they definitely could take back control of the system.
  - We can't pay hackers the money because hackers can't be trusted!
  - We know the system better, and hackers just win on surprise!
  - But it will take some time to win this battle!
- IT department did their best to fix the system twice!
- The Hackers immediately fought back and hacked the system again!

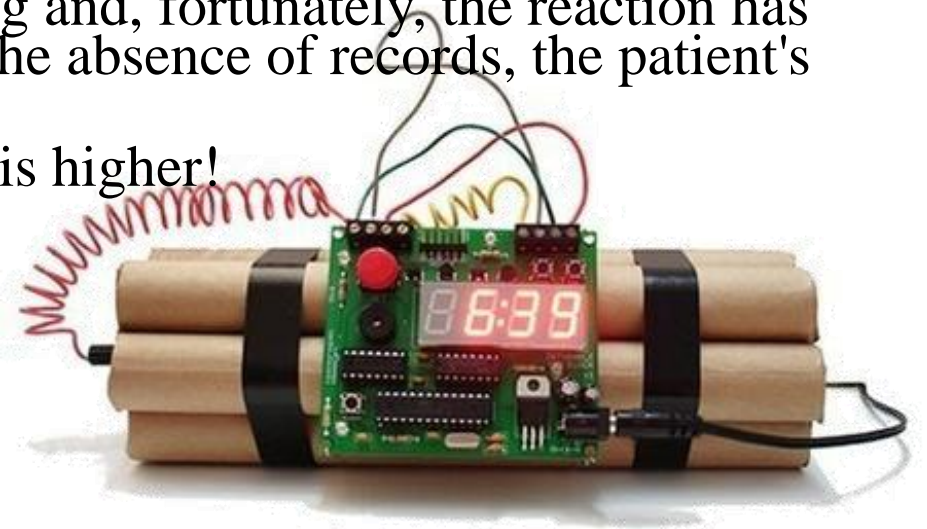




# Legal adviser

---

- Lisa Mankins, the hospital's general counsel, wants this resolved immediately, even if the ransom is paid!
  - Young doctors are at a loss, and old doctors have forgotten how to prescribe medicine!
  - Relying on outdated records for the most urgent cases is risky!
  - One patient has already been given the wrong drug and, fortunately, the reaction has been mild. If the hospital makes any mistakes in the absence of records, the patient's life could be lost!
  - We don't have time! Every hour we wait, the risk is higher!
  - The hospital has insurance to pay the ransom for the damage.
  - The loss is only a small budget!



# 办公室主任（Chief of Staff）

---

- 你知不知道这事儿后果有多严重？  
Do you have any idea how serious this could be?
- 你要是不能立即搞定这件事，我们就回到用纸记录信息的方式！  
If you don't get this done right away, we'll go back to paper records!

*Paul, I'm never touching one of those damn devices again.  
And I know plenty of others here who will feel the same way.*

*Paul, 我再也不会碰那些该死的设备了。我知道在座的很多人也会有同样的感觉。*

A close-up photograph of a middle-aged man with grey hair, wearing a dark pinstriped suit jacket, a light blue shirt, and a red tie. He is shown in profile, leaning forward with his head bowed and his hands covering his face, conveying a sense of despair, stress, or being overwhelmed. The background is a plain, dark grey.

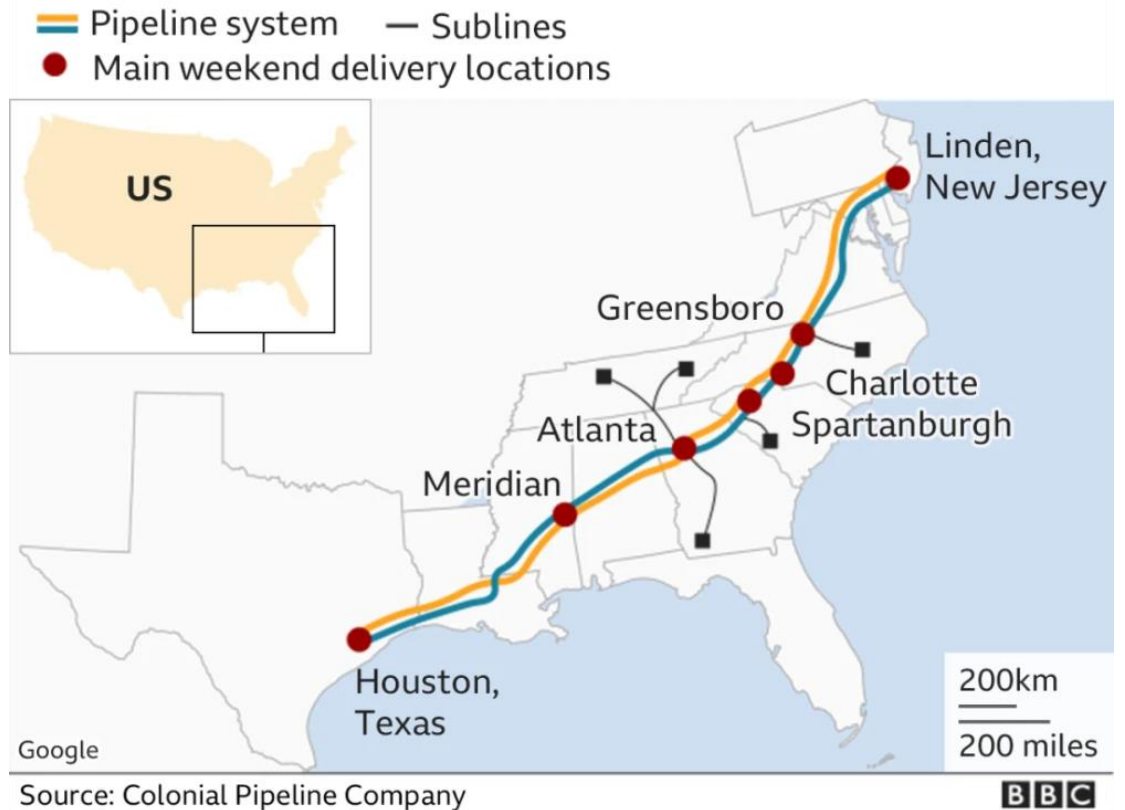
如果你是Paul  
你该怎么办？

If you're Paul,  
what should you do?

## 2. Case: America's largest fuel pipeline hit by extortion attack

- Colonial Pipeline is the largest refined oil pipeline in the United States, moving more than 100 million gallons of fuel per day through the pipeline system.
- The pipeline system connects Houston, Texas, to Linden, New Jersey, and spans more than 5,500 miles.
- The Pipeline system supplies 45 percent of the fuel on the East Coast of the United States, and Colonial Pipeline also supplies refined petroleum products such as gasoline, diesel, and jet fuel to the U.S. military.

Colonial Pipeline system map



- 
- Friday, May 7th, 2021, Colonial Pipeline Company Statement:
  - On May 7th, Colonial Pipeline discovered a cyberattack. We have since determined that ransomware was involved in the incident. In response, we proactively took certain systems offline to contain the threat. The attack temporarily stopped the operation of all pipelines and affected certain of our IT systems. Upon learning of the issue, a leading third-party cybersecurity firm was engaged. They have conducted an investigation into the nature and scope of the incident, and that investigation is ongoing. We've reached out to law enforcement and other federal agencies.
  - Colonial Pipeline is taking steps to address the issue. At this time, our main focus is on safely and efficiently restoring services and working to restore normal operations. This process is already underway and we are working to resolve this issue and minimize disruption to our customers, as well as those who rely on Colonial Pipeline.

- On May 9th (Sunday), the United States declared a national emergency, due to a ransomware attack launched by a criminal gang in Eastern Europe against Colonial Pipeline, the most important fuel pipeline operator in the United States, on May 7, causing Colonial Pipeline to shut down its critical fuel network that supplies oil to the East Coast states of the United States.
- The U.S. Department of Transportation issued an emergency declaration for 17 states and the District of Columbia, announcing the easing of restrictions for road transportation fuel.
- It is believed to be the largest cyberattack on U.S. energy infrastructure in history, and if it continues, it could send gasoline prices soaring.



- On May 10th (Monday), FBI named Darkside as black hand.
- DarkSide responds that its purpose is only to collect money and has no political intention or intention to destroy society;
- Colonial expects to substantially restore service by the end of the week; Shortages and long lines at gas stations have been reported in Atlanta, North Carolina and elsewhere;
- On May 11st (Tuesday), Colonial Pipeline website was down.

The FBI confirms that the Darkside ransomware is responsible for the compromise of the Colonial Pipeline networks. We continue to work with the company and our government partners on the investigation.



S T A T E M E N T

- According to an April 2021 report provided by security firm Cybereason, DarkSide has been active since August 2020, operating in a RaaS (ransomware-as-a-service) model that is good at moving sideways and attacking to get the domain controller (DC) and bringing the whole network environment down.
- The group has now released "unredeemed" data of more than 40 victims (the actual number of victims is believed to be higher) and demanded ransom payments of between \$200,000 and \$2 million.





- 
- 世界经济论坛网络安全中心的网络战略负责人阿尔吉德·皮皮凯特针对本次事件发表了自己的见解：“安全脆弱性已成为系统性问题，除非将网络安全嵌入开发阶段，从源头解决安全问题，否则针对石油和天然气管道或水处理厂等工业系统的攻击事件只会越来越多。”
  - "Security vulnerabilities have become a systemic issue, and unless cybersecurity is embedded in the development phase to address security at the source, attacks on industrial systems such as oil, gas pipelines or water treatment plants will only increase," said Aljid Pipikett, head of cyber strategy at the World Economic Forum's Cyber Security Center.

- The company had to pay a \$4.4 million ransom to the hackers to restore the attacked systems.
- In an interview with The Wall Street Journal last month, Blunt, Colonial Pipeline's CEO, said the company complied with the \$4.4 million ransom demand because they did not know the extent of the hack and the time it would take to recover. But privately, the company had taken early steps to notify FBI and followed instructions to help investigators track down the cryptocurrency wallet used by the hackers.



- On June 7th, 2021, U.S. Deputy Attorney General Lisa Mona said that U.S. investigators had recovered 63.7 Bitcoins worth \$2.3 million—the “majority” of the ransom paid. It is also the first ransom recovered by the Digital Extortion Task Force which was established by U.S. Department of Justice’s recently.
- This is a major victory in America’s ongoing battle against hacking for extortion. But the U.S. Department of Justice is vague about how exactly they do it. They simply said that the "keys" to the hacked Bitcoin wallet were "in the hands of the FBI." With this key, which is actually a password, agents can simply log in and send digital currency to another wallet they control.



# Similar events

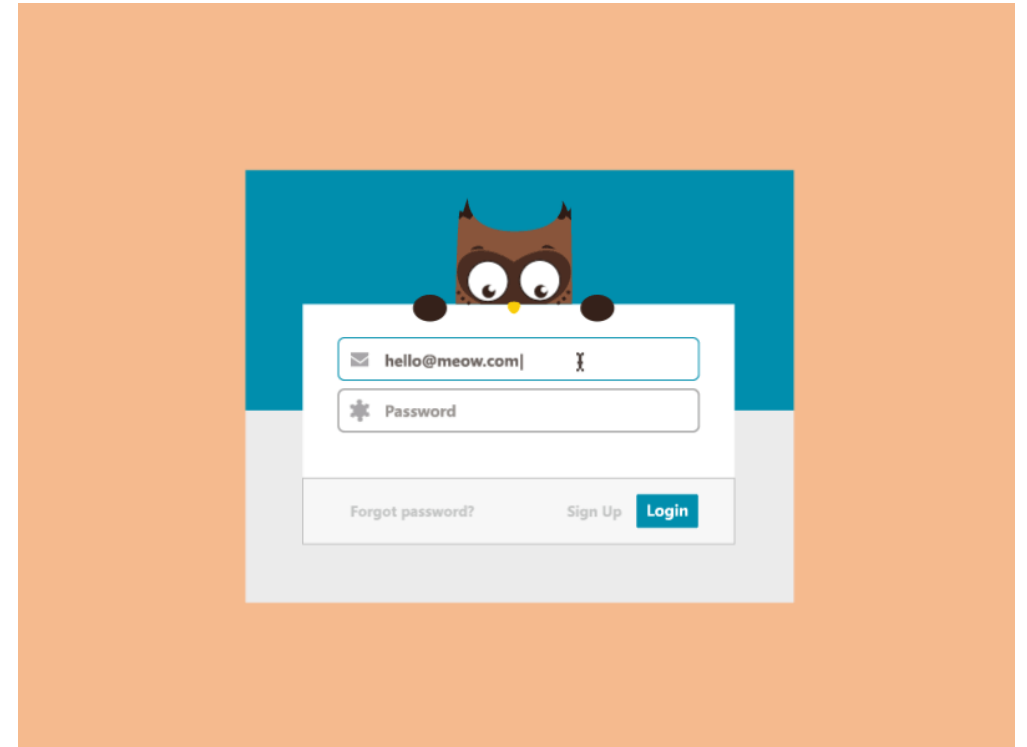
---

- 2021.2 A water treatment plant in Florida, USA, was attacked by hackers. The attacker remotely entered the computer system that monitors the content of chemical substances related to water treatment through a program that allows authorized users to access remotely.
- 2020.10 Sky Lakes Medical Center, a hospital in Oregon, USA, shut down its computer system after a ransomware attack, seriously affecting the hospital's normal operations and causing economic losses.
- 2020.5 Taiwan's two largest oil refineries (CPC and FPCC) suffered cyber attacks within two days, affecting the entire supply chain and even affecting customers who refueled at gas stations.
- 2020.2 A natural gas operator in the United States suffered a ransomware attack, which resulted in the plant's IT and OT network data being locked. The plant was forced to shut down for 2 days, and was notified by the Department of Homeland Security.
- ...

# 3. Various means of system attacks

## (1) SQL injection attack

- For example: the original SQL statement to verify the user name is
  - `select * from userinfo where id='username';`
- You enter your username:
  - `username'; delete from userinfo where '1'='1'`
- If the system is not protected, it becomes:
  - `select * from userinfo where id='username';`  
`delete from userinfo where '1'='1';`
- All the data in the database has been deleted!





Assume that the routing login page constructs dynamic sql statements by concatenating strings, and then verifies whether the user name and password exist in the database, assuming that its background sql statement is

```
sql='select * from users where user='&user&' and passwd='&passwd&'
```

If we use admin for the user name and '1 'or 'a'='a' for the password, then the query becomes

```
select * from users where user= 'admin' and passwd='1' or 'a'='a'
```

In this case, according to the rules of operation (do and first, then or), the final result is true, and then we can go into

# SQL injection attack hazards

- Collect database type, structure and other information to prepare for other types of attacks.
- Database information leakage: leakage of users' private information stored in the database.
- The database was maliciously operated: the database server was attacked, and the system administrator account of the database was tampered with.
- Web page tampering: tampering with specific web pages by manipulating the database.
- The website is hacked and malware is spread: modify the values of some fields in the database, embed hacker links, and carry out hacking attacks.
- The server was controlled remotely and a backdoor was installed. Operating system support provided by the database server allows hackers to modify or control the operating system.
- Destroy hard disk data and paralyze the entire system.

这是一张相当有技术含量的号牌遮挡，其对交警系统SQL Injection的hack案例。当摄像头拍到你车牌号并把其转成文本后，插入数据库时的SQL注入。看到了吧，千万别惹程序员。



## (2) System security threat - Trojans

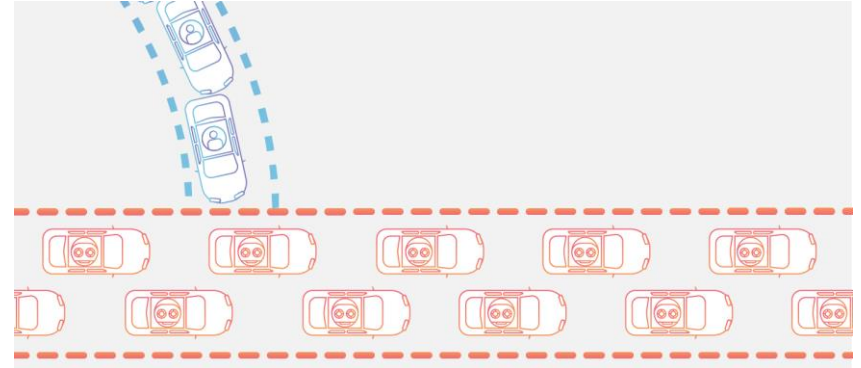
- Basic meaning: A piece of malicious code with special functions hidden in the normal program, which is a backdoor program with special functions such as destroying and deleting files, sending passwords, recording keyboards and attacking Dos.
- Category: Online Trojans; E-banking Trojans; Download Trojans; Agent Trojans; FTP Trojans; Communication software Trojans; Web page click Trojans.
- Characteristics: hidden, deceptive, stubborn, harmful.
- Transmission mode: Download; System vulnerability; Mail; Remote connection; Web pages; Worm virus.



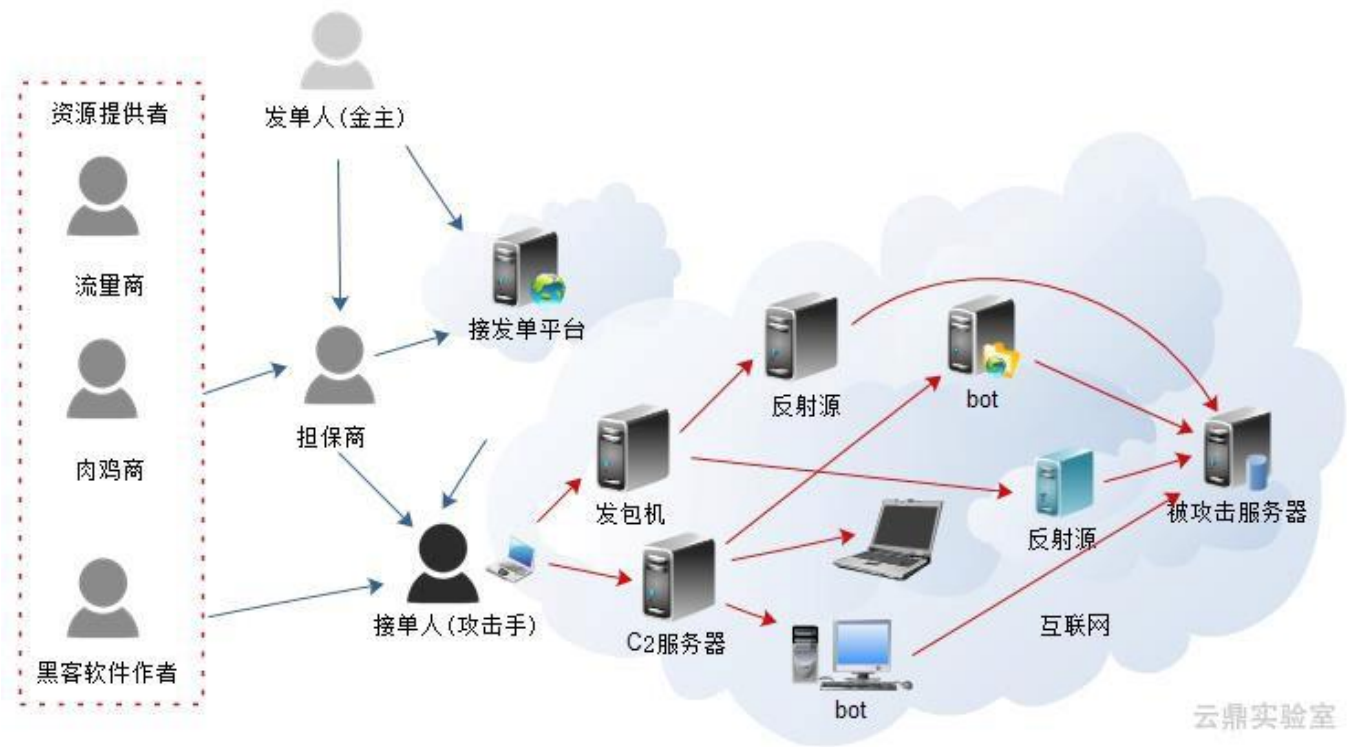


## (3) DDoS attack

- A Distributed Denial of Service attack refers to multiple attackers in different locations launching attacks against one or several targets at the same time, or an attacker controlling multiple machines located in different locations and using these machines to target victims. attack at the same time.
- Attackers use "broilers" (puppet machines, machines remotely controlled by hackers) to initiate a large number of requests to the target website in a short period of time, consuming the target website's host resources on a large scale and making it unable to serve normally.



- "Broiler" can be said to be the core weapon of DDoS attacks. One point mentioned here is that practice has proven that not only PCs will become "broilers" at present, it can be said that any IoT device may become a "broiler", such as: mobile phones, servers, smart speakers, etc.



# DDoS attack types

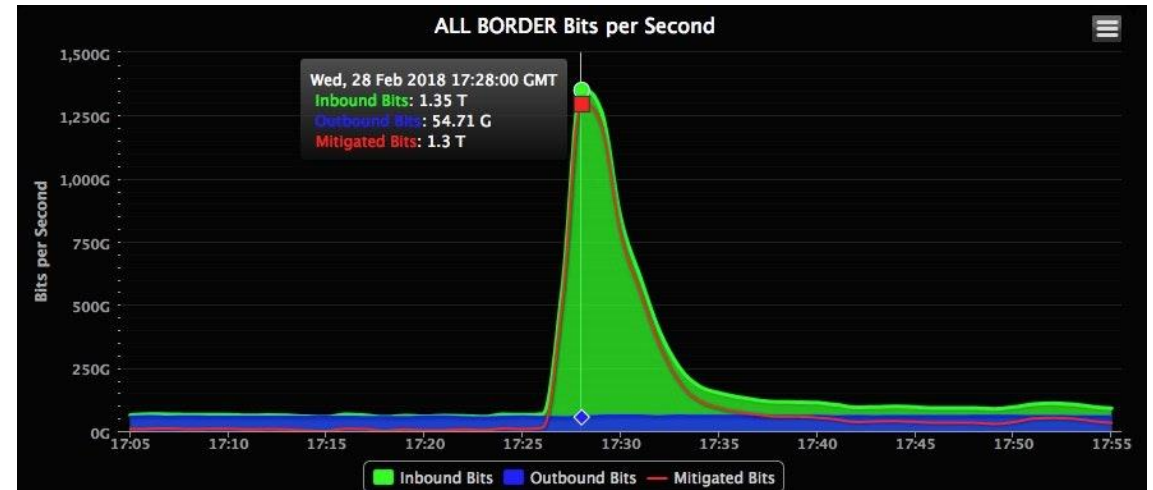
---

- Malformed messages: including Frag Flood, Smurf, Stream Flood, Land Flood, IP malformed messages, TCP malformed messages, UDP malformed messages, etc.
- Transport layer DDoS attacks: including Syn Flood, Ack Flood, UDP Flood, ICMP Flood, RstFlood, etc.
- DNS DDoS attacks: including DNS Request Flood, DNS Response Flood, fake source + real source DNS Query Flood, authoritative server attack and Local server attack, etc.
- Connection-type DDoS attacks: including TCP slow connection attacks, connection exhaustion attacks, Loic, Hoic, Slowloris, Pyloris, Xoic and other slow attacks.
- Web application layer DDoS attacks: including HTTP Get Flood, HTTP Post Flood, CC and other attacks.

# Case: GitHub suffered DDoS attack

- On February 28th, 2018, Eastern Time, GitHub was attacked with a bandwidth of up to 1.35Tbps in an instant. This DDoS attack can almost be called the largest and most powerful DDoS attack in the history of the Internet.
- Things didn't stop after the GitHub attack. Just a week later, DDoS attacks began again on sites like Google, Amazon, and even Pornhub. The bandwidth of subsequent DDoS attacks also reached a maximum of 1Tbps.

<https://www.wired.com/story/github-ddos-memcached>



# How to protect against DDoS attacks?

---

- An analogy example: I opened a Chongqing hotpot restaurant with 50 seats. Because the ingredients are of the highest quality, I am very honest. Normally, it is bustling with people and business is booming, but no one is paying attention to Ergou's hot pot restaurant opposite. In order to deal with me, Ergou thought of a way to invite fifty people to sit in my hot pot restaurant without ordering, so that other guests could not eat.
- High-defense server: High-defense server mainly refers to a server that can independently hard defend more than 50Gbps, which can help website denial-of-service attacks, regularly scan network master nodes, etc.; Chongqing hot pot restaurant has added two security guards, these two security guards can protect the store No harassment by hooligans, and regular patrols around the store to prevent harassment by hooligans.
- Blacklist: Faced with the gangsters in the hot pot restaurant, I took pictures of them and put them on file in anger, and banned them from entering the store. However, sometimes when I meet someone who looks like me, I will also ban them from entering the store. This is to set up a blacklist. This method adheres to the principle of "killing a thousand by mistake and not letting go of a hundred". It will block normal traffic and affect normal business.

- 
- DDoS cleaning: DDoS cleaning will monitor user request data in real time, detect abnormal traffic such as DOS attacks in a timely manner, and clean these abnormal traffic without affecting normal business development. DDoS cleaning means that after I find that a customer has entered the store for a few minutes but has not ordered food, I will kick him out of the store.
  - CDN acceleration: The full name of CDN is Content Delivery Network, which is content distribution network. CDN is an intelligent virtual network built on the existing network. It relies on edge servers deployed in various places and uses the load balancing, content distribution, scheduling and other functional modules of the central platform to enable users to obtain the content they need nearby and reduce network congestion. Improve user access response speed and hit rate. In reality, the CDN service distributes website access traffic to various nodes, so that on the one hand, the real IP of the website is hidden, and on the other hand, even if it encounters a DDoS attack, the traffic can be dispersed to various nodes to prevent the origin site from crashing. In order to reduce harassment by hooligans, I simply opened the hot pot restaurant online and provided takeout services. In this way, the hooligans could not find where the store was and couldn't act like hooligans.

## (4) More other types

- worm virus
- browser attack
- Malware attack
- Cross-site scripting XSS
- port scan
- insider attack



# Case: Fortresses are breached from within

- At around 19:00 on February 23, 2020, Weimob received a system monitoring alert and learned that the SaaS business service had failed and the production environment and data had been severely damaged.
- After investigation, the suspect is He, a core operation and maintenance staff member of the Operation and Maintenance Department of Weimob R&D Center. He logged into the company's intranet springboard through a personal VPN at 18:56 on February 23. Due to personal mental, life and other reasons, He He maliciously damaged Weimeng's online production environment and has been detained.
- This incident caused very heavy losses to Weimob Group. Within one day from February 24 to February 25, when the employees' malicious sabotage incident occurred, Weimob Group's market value evaporated by approximately HK\$963 million.

## 关于微盟系统故障的通告

尊敬的微盟商户：

和您一样，我们一起度过了煎熬的36小时，我们预计此次故障还会持续一段时间，现就此次系统故障作如下通告：

2月23日19点，我们收到系统监控报警，服务出现故障，随后我们立刻召集相关技术人员进行定位，发现大面积服务集群无法响应，生产环境及数据遭受严重破坏。我们立刻启动应急响应机制，并与腾讯云技术团队一起研究制定生产环境和数据修复方案。

截止到2月25日7点，我们的生产环境和数据修复都在有序的进行，我们预计2月25日晚上24点前我们的生产环境将修复完成，微盟所有新用户将可恢复服务，老用户由于数据修复时间问题，我们将提供临时过渡方案，我们预计老用户数据修复将在2月28日晚上24点前完成。

我们事后对恶意破坏生产环境的犯罪嫌疑人进行追踪分析，成功定位到犯罪嫌疑人登录账号及IP地址，并于2月24日向宝山区公安局报案，目前犯罪嫌疑人已经被宝山区公安局进行刑事拘留，犯罪嫌疑人承认了犯罪的事实。犯罪嫌疑人乃微盟研发中心运维部核心运维人员贺某，贺某于2月23日晚18点56分通过个人VPN登入公司内网跳板机，因个人精神、生活等原因对微盟线上生产环境进行了恶意的破坏。

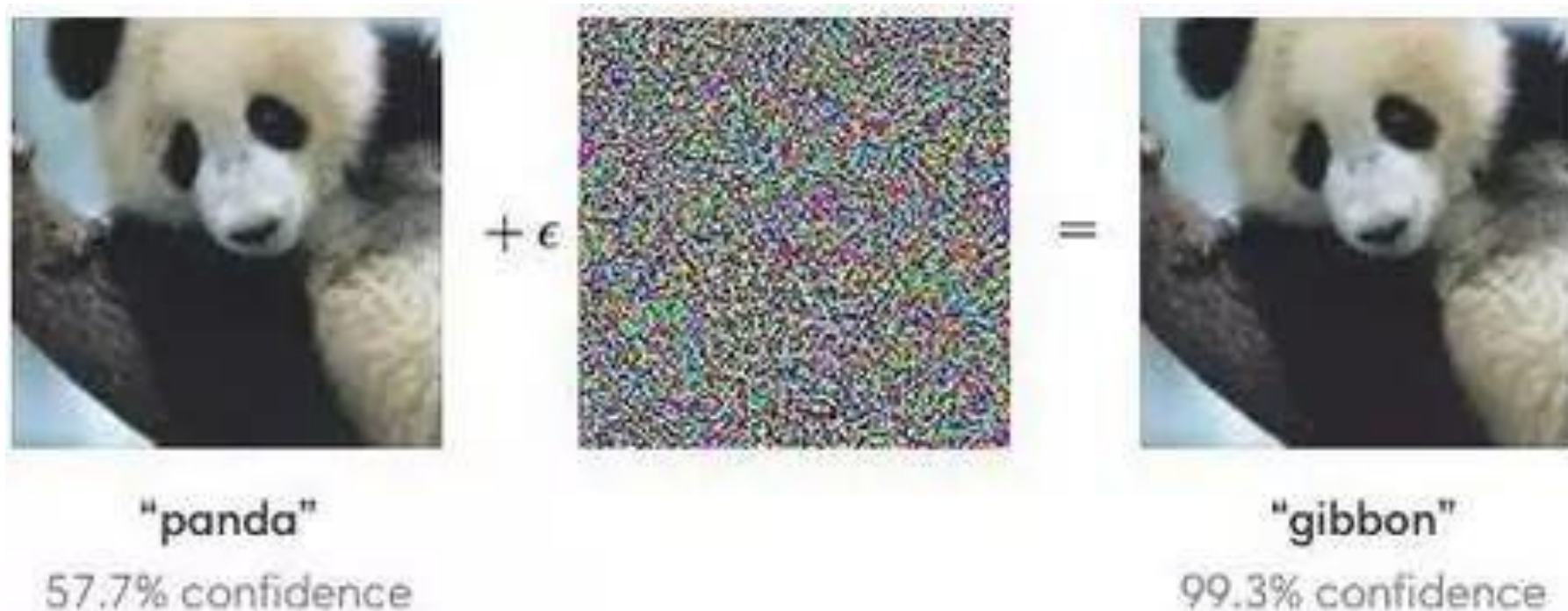
针对此次事故微盟深表歉意，我们正在拟定相关赔付方案来补偿因此次事故而遭受损失的商家，我们对此次因人为造成的事故灾难无比愧疚，我们今后将一定吸取这个惨痛的教训，加强对线上运维的治理，同时我们也对因远程办公而疏忽对员工的精神状态的关注而深表痛惜！

微盟集团



## (5) AI safety——GAN

- Systems based on deep neural network models are easily fooled. As shown in the figure, for a photo of a panda, after adding small artificially designed noise, the human eye cannot see the difference between the two pictures, but the computer will misjudge it as a gibbon with a probability of 99.3%.

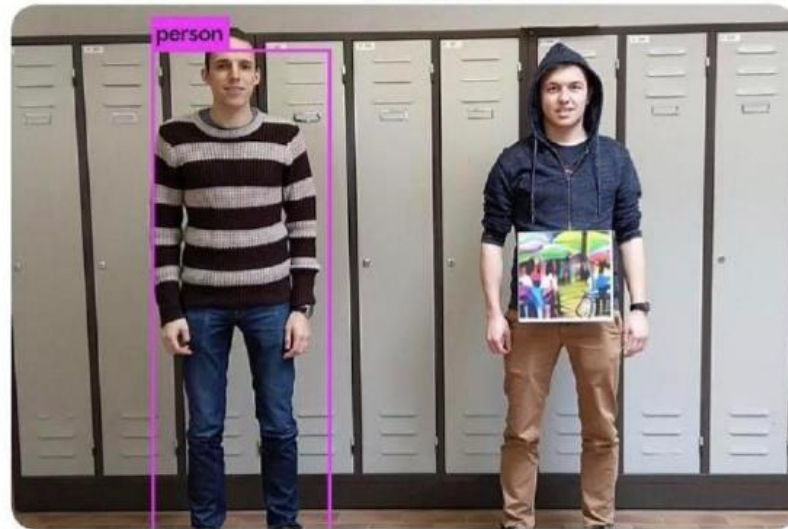


- For some artificially generated noise or textures that are meaningless to the human eye, the computer will also classify them into certain categories with a very high probability. The above-mentioned samples deliberately designed and generated by malicious attackers to deceive artificial intelligence systems are called adversarial samples.
- For example, for an unmanned driving system that can automatically recognize traffic signs, if an attacker generates an adversarial sample of a no-passage sign, the automatic recognition system will misjudge it as a passable sign. This can have catastrophic consequences when a self-driving system and a human driver are behind the wheel at the same time. (There is basically no difference between the two to the naked eye.)



# AI隐身 AI stealth

比利时天主教鲁汶大学的学生展示了AI时代的「隐身术」，只要将一张利用对抗网络生成的图像放在身上，AI系统就无法检测出这是一个人。论文 [arxiv.org/pdf/1904.08653...](https://arxiv.org/pdf/1904.08653...)



Students at the Catholic University of Leuven in Belgium demonstrated the "invisibility" of the AI era, in which the AI system could not detect a person as long as an image generated using the adversarial network was placed on the body

# 3. 钻系统的漏洞

## Exploit system vulnerabilities

# 1. Get the best deal

---

- **quotation**
- In July 2018, in the system upgrade of the Kuaishou, there was a small bug in the cash withdrawal system. After the order failed, Huang Diamond was withdrawn and returned to the Kuaishou user account, but the payment gateway did not stop the transfer request and kept trying. During this period, if the corresponding Wechat account opens real-name authentication, the funds will be transferred from the Kuaishou enterprise account to the personal Wechat account, and the user will receive cash withdrawal without deducting the yellow diamond. Using this vulnerability, 27 people stole 6.72 million yuan from 4,629 orders of 827 users of Kuaishou in 24 days.
- The defendant Xie and others used the live streaming function of the accounts they controlled to first save the corresponding yellow diamonds to 2,000 yuan through mutual rewards between accounts, and then associated accounts that had not opened or had canceled WeChat real-name authentication to repeatedly submit withdrawal applications, and in a short period of time Open WeChat real-name authentication within the account, and after the funds arrive in the WeChat account, they can be quickly transferred out and distributed for the second time through the bound bank card.
- In this way, a black chain of renting accounts, tips, cash withdrawals, transfers, and money withdrawals quickly formed and spread until Kuaishou Company summarized financial data and found that the user's cash withdrawal amount did not match the personal tax data, and the cash withdrawal amount was obviously abnormal. This vulnerability has been corrected.
- The court found that in the 12 days starting from 1:00 on July 21st, 2018, to 22:00 on August 2nd, 2018, only Xie acquired 10 groups of other people's accounts through the above method, and evacuated a total of more than 1.25 million yuan in funds . Xie was eventually fined 110,000 yuan and ordered to compensate for economic losses of more than 1.25 million yuan. At the same time, Xie and 26 others were sentenced to fixed-term imprisonment ranging from 11 and a half years to one year and one month for the crime of theft.

- 
- The black industrial chain formed by network vulnerabilities is the focus of judicial crackdowns
  - Getting the best deal is an Internet phenomenon associated with e-commerce. The behavior of getting the best deal can be divided into three categories according to the severity:
    - (1) Ordinary users who follow the platform's discount rules and occasionally exploit platform loopholes to obtain discounts for their own use;
    - (2) The "coupon clipping" who takes advantage of omissions in the platform's preferential rules and uses information and technological advantages to seize discounts and then resell and realize them;
    - (3) A black and gray production chain that exploits system vulnerabilities to maliciously make profits. The Kuaishou theft case mentioned above falls into the third category.
  - For the first type of behavior, users have normal consumption behavior and do not need to worry within the scope of laws, business rules and market laws. In fact, consumers at this level should focus on protecting their own rights, especially when the loss is caused by the platform's own fault and the consumer does not have any intention of fraud. In this regard, different platforms have different reactions. For example, Qunar.com and China Eastern Airlines have issued ultra-low-price air ticket orders due to system errors, and finally announced that they will issue tickets normally; however, Marriott Hotels experienced a hotel order error, and the hotel finally canceled the reservations of users who had booked rooms. The platform Compensation of 5,000 points.

- 
- The black industrial chain formed by network vulnerabilities is the focus of judicial crackdowns
  - For the coupon clippings, those who obviously maliciously violate platform rules and exploit system loopholes are considered unjust enrichment in civil legal relations, and the damaged platform can request return. However, the criminal legal evaluation is relatively ambiguous and cannot be generalized. However, if there is subjective malignancy and the amount of illegal income is relatively large or the impact is relatively large, it will also constitute a criminal offence.
  - The black and gray industry chains that exploit system vulnerabilities to maliciously make profits is currently the focus of the crackdown. This case presents a new trend of black industry: illegal payment channels are transferred to ordinary personal accounts.
  - Generally speaking, the supply chain of online black products can be divided into three major elements: materials, traffic and payment. Maliciously registered accounts are the main sources of supply of materials, and virtual commodity transactions are the main channel for monetization; in wool gray products, it is refined into: Card merchants are responsible for registering platform accounts - network hackers are responsible for buying and selling "flash sale software" - "coupon clipping" are responsible for using it on the platform - and the recipient is responsible for monetizing it in the secondary market.
  - However, as various Internet platforms, especially several Internet giants, jointly crack down on malicious registrations, technical barriers are getting higher and higher, and the cost of "maintaining an account" is increasing day by day. Therefore, black industry targets ordinary personal accounts, such as those provided by Xiao Xu, Hu and others. Such accounts are normal accounts and cannot be technically identified. Although this provides convenience in fighting crime, it also makes it difficult to trace the source. Predicate crimes pose challenges.









360导航\_新一代安全上网导航 X 微信刷票\_360搜索 X 微信投票刷票器|微信投票

http://mxtx777.net/user.php

收藏 手机收藏夹 我的收藏 淘宝网 龙部落-2014最新 电影天堂\_免费电影 天天美剧 | 美剧排 优酷网

## MP会自动过滤做过的投手, 3方只有发布时填写“公众号”栏的任务

**注意: 自助查图时, 请根据实际缺量情况和具体任务情况判定  
添加了客户查图专用链接, 请进入查图页面获取。**

### 发布任务

任务步骤:

任务网址:

若是扫码, 请填写二维码网址 (推荐百度网盘)。关注的最好不要与网址, 而是填写公众号。直投的, 请填写网址

接手模式:

单价:

限速:  1分钟最多多少票 0为不限制

是否每天可投:  每个微信号只能投一次  
 每个微信号每天可投

需求数量:

公众号名称:  公众号名分为 公众号名称  
和 公众号 (为保持一致  
性, 请填写公众号名称, 一般为中文)

[不知道如何发布? 请点击这里](#)

注意事项:  
1: 本平台为人工平台, 如发现投手作弊, 请通过“投诉”功能举报。  
2: 初次使用请少量试单。

## 2. coupon loophole

---

- Pinduoduo's "coupon loophole"
- At the beginning of 2019, Pinduoduo launched its "New Year's Day" promotion, during which a large number of coupons normally issued by the platform were consumed. As of 9 a.m. on the 20th, the sum of stolen coupons and normal coupons exceeded the platform's preset threshold. After the system monitored the abnormality and automatically alerted the police, Pinduoduo repaired the relevant loopholes as soon as possible.
- Pinduoduo said that the relevant coupons stolen by the "coupon loophole" exploited by the black and gray product gangs were specially generated due to the program recording needs when Pinduoduo previously cooperated with a TV program (Jiangsu Satellite TV's "If You Are the One"). Coupon type, only for on-site guests.
- In addition, this type of coupon has never appeared in the normal online promotion activities of the platform at any time or in any way, and has never even had any online entrance. Incidents such as "operating to issue low-price air tickets" are fundamentally different in nature.
- The relevant coupons in this incident were all obtained by scanning QR codes generated by black and gray production gangs through abnormal channels. This QR code was mostly circulated among related black and gray production groups on social platforms. Pinduoduo has never generated any QR codes for this type of coupons, and has never displayed such coupon-related information and QR codes in its APP and mini programs.

- 
- Pinduoduo's "coupon loophole"
  - Pinduoduo revealed that with the QR code generated by Heihui Products through this abnormal method, each user with authentication information can only receive one unlimited 100 yuan coupon, instead of the "unlimited" coupon for a single ID circulated on the Internet. receive"
  - Therefore, some black and gray industry gangs use illegal means such as "cat pools" (using mobile phone cards to maintain a large number of virtual accounts) to realize the simultaneous operation of N black mobile phone cards, steal such coupons in batches, and use mobile phone bills, Q coins and other virtual recharge methods, trying to quickly transfer such ill-gotten gains in a short period of time.
  - The person in charge of Pinduoduo's risk control team said that after stealing huge amounts of coupons and transferring their ill-gotten gains, the black and gray product gangs quickly shared the QR codes through the Internet and social groups, hoping to achieve the effect of "the law does not punish the public". Go out and induce some ordinary consumers to follow suit and scan codes, and fabricate rumors such as "Pinduoduo platform lost 20 billion yuan in coupon issuance" on social platforms and groups, hoping to avoid criminal liability and confuse the public.

# 3. Get good reviews

---

- Steam removes all games from "Shiqu Interactive Technology"
- In 2017, Valve removed two games called "The Dawn: First War" and "Last Stand" from Steam because it was discovered that the developers used loopholes to gain praise.
- It is reported that some developers will try to increase the ratings of the game by brushing up positive reviews, and use such unfair means to attract players to download. The main reason is that when many consumers buy a game, in addition to the developer's introduction, promotional videos and screenshots, everyone is accustomed to checking the community's evaluation. If it is good, they will choose to buy it.
- As one of the world's largest game distribution platforms, Steam has become the first choice for many VR game manufacturers. However, "fake praise" has caused some players to be misled by these irresponsible reviews. Players have lost trust in VR games, which has affected the development of the entire VR game industry.

# 4. 将系统用于服务犯罪

## Use the system to serve crimes

# 1. Gray industrial chain

---

- Gray industry: an unreasonable but objectively existing industry between legitimate industries (white) and illegal industries (black).
- Simply put, gray industries are projects or industries that skirt the law and make huge profits.
- Internet gray industry:
  - (1) Gray industry formed by gray software
    - Gray software, also known as malware and rogue software, all have some common characteristics: users install it without authorization or knowledge. It has certain practical value, but it also brings potential threats to users' software, hardware and personal information. , difficult to uninstall, etc. Gray software has roughly gone through four stages: malicious web page code, plug-in promotion, software bundling and rogue software virusization. Currently, there are several main categories of gray software: adware, spyware, behavior recording software, and malicious sharing software.
  - (2) The gray industry formed by Internet trolls
    - After continuous development, the Internet trolls have further developed and formed a large number of more advanced forms of Internet public relations companies. These public relations companies can organize thousands of "water armies" to hype topics and guide public opinion, and have become an industry with very mature operating procedures. For example, many of the messages and news seen on the Internet, especially the many popular posts, hot topics, and "Internet celebrities" in forums that can mobilize popularity, may be untrue and are planned and manipulated by public relations companies.

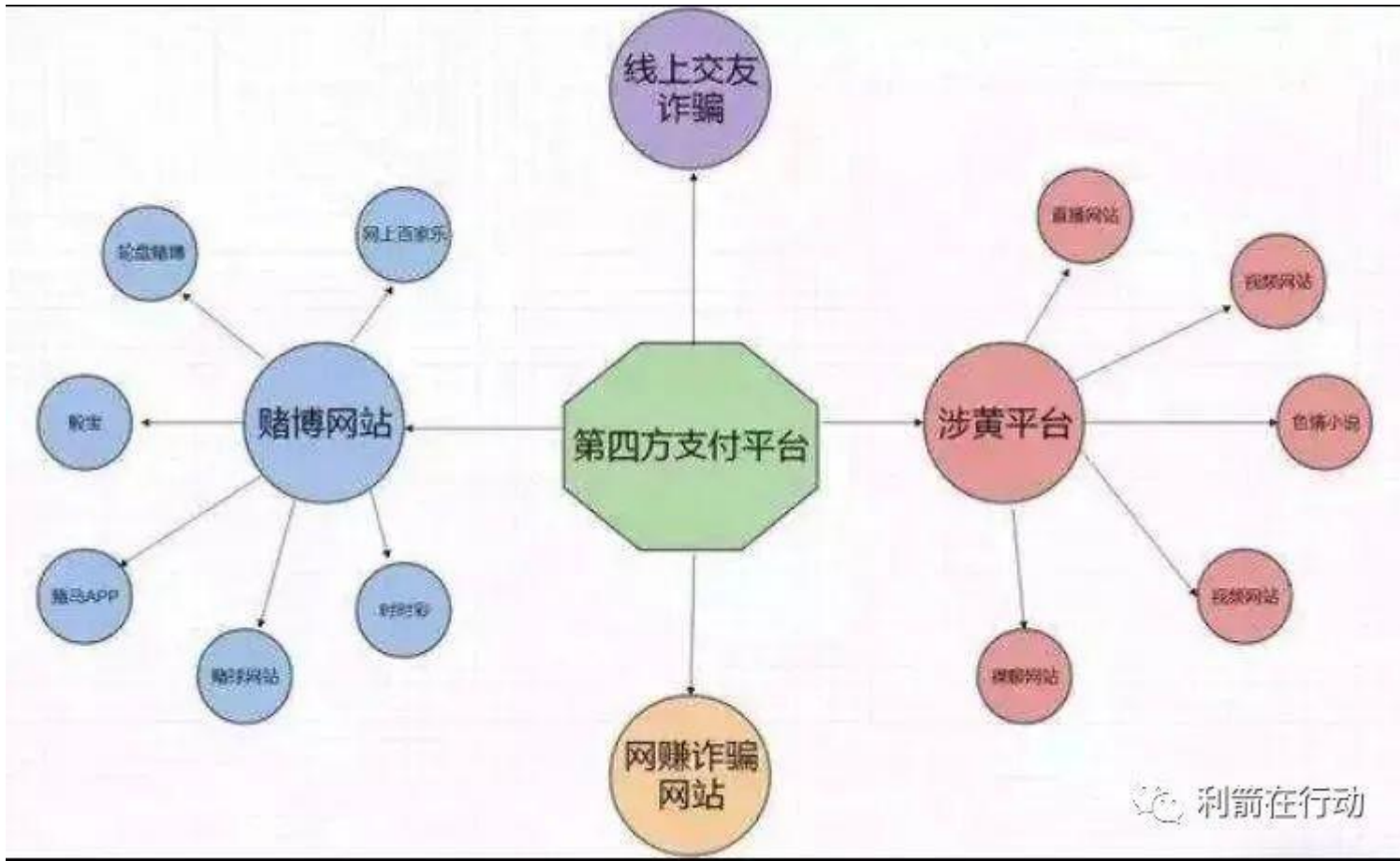
- 
- (3) The phenomenon of some legal companies participating in gray industries
  - Many legal companies often participate in the Internet gray industry in various forms, and it is the participation of these legal companies that make the gray industry develop and grow with great momentum.
  - For example, a well-known search engine service provider used the advantages of its search engine to make money through bidding rankings, which was questioned by all walks of life. On the other hand, it can filter search results as needed, thus benefiting customers from blocking certain unfavorable information. Internet companies use their powerful resource gathering capabilities to publish soft articles on the Internet for their clients to guide public opinion, confuse the public, and even control adverse information. On trading websites such as Taobao, the reputation system is to a large extent an important reference for buyers to make purchases. It is precisely because of this that the reputation evaluation system is systematically manipulated through the Internet. It is very serious and has formed a complete gray industry chain.



## 2. Fourth party payment

---

- Fourth party payment
- In recent years, "third-party payments" such as Alipay and WeChat have become popular across the country because of their efficiency and convenience. However, third-party platforms such as Alipay and WeChat Tenpay are strictly supervised and illegal websites cannot be accessed. Some illegal "fourth-party payment platforms" have emerged. They are online platforms engaged in illegal crimes such as gambling and private lottery or drug trafficking. Provide fund payment and settlement channels for crimes such as fraud and fraud, and obtain high returns from it.
- Fourth-party payment, also known as "integrated payment" or "one-code payment", is a comprehensive payment service that integrates multiple payment service methods such as banks and third-party payment through technical means. Common Polymer payment products include Polymer code scanning, smart POS, code scanning gun, code scanning box, etc. Fourth-party payment initially appeared as a third-party payment outsourcing service provider and has developed rapidly with the explosive growth of mobile payment scale.
- Case
- From the end of 2018 to August 2019, in order to obtain huge illegal profits, Liu Moumou and others used registered shell companies to illegally provide others with corporate bank settlement account cash-outs or corporate bank settlement account transfers in the form of public to private transactions and cash withdrawals. Personal account services, providing cover for "Grand Slam" gambling platforms, etc.
- Yi and others applied for tens of thousands of IoT cards from all over the country, and then used their IoT mobile phone numbers to apply for mobile phone recharge card passwords from a communications company. After gamblers recharge and complete payment on "Grand Slam", etc., they will go through The "Huarong Jufu" payment and settlement system established by Liu Moumou's gang was circulated, and Yi Moumou and others collected card secrets for "money laundering". The "laundered" funds were paid by Liu Moumou's gang and cashed out to gambling personnel. The platform established by Liu Moumou and others has the function of agency payment and settlement. The upstream is responsible for docking the inflow of merchants' funds, and the downstream is responsible for docking the outflow of merchants' funds.



- The illegal payment and settlement engaged in by Liu Moumou and others is a new type of crime. It is an illegal business operation carried out by criminals relying on the Internet without permission. It plays an intermediary role in the entire fund transfer process. The payment platform built to provide illegal payment and settlement services for illegal crimes is called a "fourth-party payment platform." This channel has not obtained the national payment and settlement license, violates the national payment and settlement system, relies on formal third-party payment platforms such as Alipay and Tenpay, and is illegally established through a large number of registered merchants or personal accounts.
- Since the "fourth-party payment" platform does not have a payment license and is established by individuals, the security of funds is not guaranteed.

## 2. Two cards crime

---

- **"Two cards" crime**
- It refers to the illegal and criminal activities of illegally renting, selling, and purchasing "two cards". The so-called "two cards" refer to mobile phone cards and bank cards. Bank cards include personal bank cards, corporate accounts, and settlement cards, as well as non-bank payment institution accounts, that is, third-party payments such as WeChat and Alipay that are commonly used by the public. .
- In August 2020, after taking a break from school, Liu, a student at a certain college, took the initiative to join a card selling gang and became a "card collector" in order to make money as soon as possible. During this period, he purchased and sold 871 mobile phone cards, making a profit of more than 15,000 yuan; Nine people, including Wu Mouhao, a student at a certain university or technical secondary school, sold 9 sets of bank card information to the fraud gang. Knowing that the funds transferred into his bank account were the criminal proceeds of others, he still transferred fraudulent funds ranging from 24,500 yuan to 291,600 yuan.
- The Supreme People's Procuratorate and the Ministry of Education recently jointly issued a batch of typical cases of "two card" crimes committed by school students, further revealing the harm of telecommunications and network fraud crimes, strengthening warning education, and striving to create a better environment for school students to grow and become successful.

# 3. call center scam

---

- **call center scam**
- VoIP users get the caller ID field, which can be set to whatever they want. This is a key advantage for scammers because they don't need a lot of technology to do the job. Scam perpetrators have developed software to reset PINs and gain access to accounts and IVR systems. .
- Call centers are a lucrative channel for fraudulent activity. More than 100 billion call center calls are made every month. Scammers realize this and infiltrate customer accounts through attacks on phone systems. There are three main types of call center scams:
- (1) Account Takeover – Scammers pose as legitimate customers and change the account's contact information or PIN number through a call center agent.
- (2) Credit card fraud – Criminals use stolen credit card information to issue orders over the phone. Often, orders are processed and shipped before the fraud is discovered.
- (3) Data leakage-criminals use phone channels for reconnaissance. Attackers have found that phone channels are a weak link for businesses and consumers.

# 4. CaaS

---

- **Crimeware-as-a-Service, CaaS**
- Refers to the behavior of technicians providing products and services to other cybercriminals in the cybercriminal ecosystem. This model facilitates the activities of cybercriminal groups, allowing even technically inexperienced criminals and advanced threat actors to quickly carry out sophisticated attacks without the need for advanced technology.
- CaaS lowers the threshold for threat attackers to launch network attacks and is an excellent choice for advanced threat attackers. The crimeware-as-a-service model makes it difficult to attribute crimes to a specific individual because the execution and attack tools are shared among multiple cyber attackers.
- Under the CaaS framework, the most popular products include malware, ransomware, phishing tools, and infrastructure control. Most of these services are characterized by ease of use and a strong customer orientation. They usually have a console or dashboard that is easy for users to manage.
- The cost of criminal activity is shared among all "customers," thanks to a subscription-based or flat-rate model that makes cybercrime services more convenient and attractive. In this case, cyber attack service providers can increase their revenue, while customers can benefit from a reasonable reduction in the expenses spent on managing illegal operations.

- 
- **Crimeware as a Service (Crimeware-as-a-Service, Caas)**
  - The degree of specialization in the cybercrime threat field is increasing, which makes the CaaS model very dangerous. Some criminal organizations are particularly focused on providing criminal services and products to other criminal groups, rather than directly targeting users and organizations with their means.
  - In the context of the widespread use of CaaS solutions, there has been an increase in less tech-savvy cyber criminals.
  - CaaS services are fairly easy to find in cybercrime forums and dark web marketplaces, and are highly influential. Criminals can rent a botnet simply by placing an order and making a payment with bitcoin. Thousands of infected machines around the world can then be hired for a variety of illegal activities, such as distributing malware, launching DDoS attacks, or sending spam.
  - In recent months, the popularity of ransomware as a service (RaaS) has led to a rapid rise in the number of ransomware attacks.
  - RaaS is available on a cloud subscription model to anyone who can pay a subscription fee. On the other hand, some ransomware operators do not charge a subscription fee, but instead use the "affiliate" model, whereby they receive all the ransom money that the affiliate extorts from the victim, keep a certain percentage for themselves as a commission, and then pass the rest on to the affiliate.

# 谢谢！

Thank you for your attention.

[liuyuewen@xjtu.edu.cn](mailto:liuyuewen@xjtu.edu.cn)

