NSFOCUS

2020

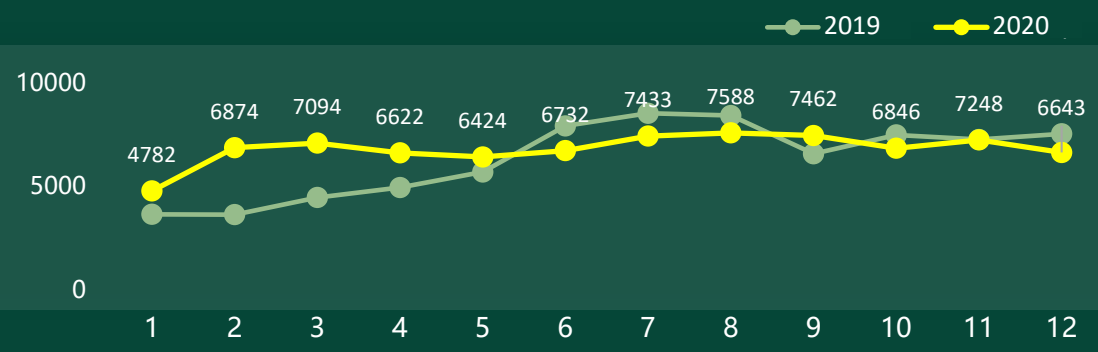
An Observation on Cyber Security Incidents

Abstract

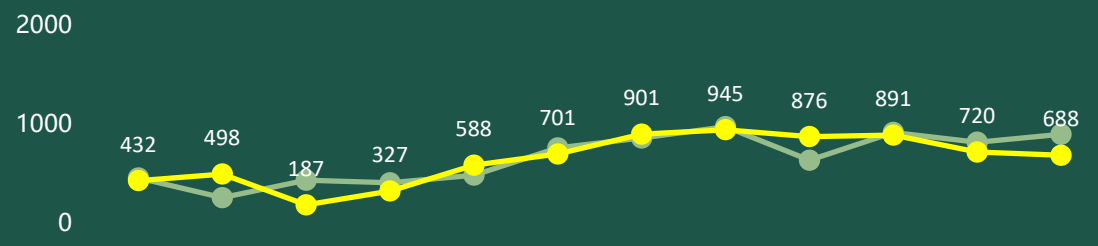
Annual Overview of Security Incidents

The following data is the monthly statistics of security incidents monitored throughout the year.

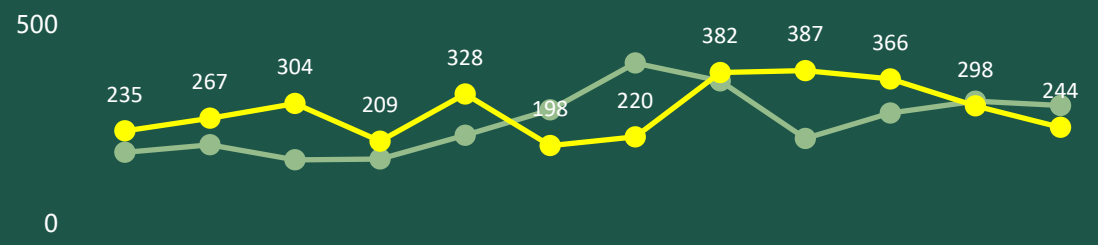
ALL CATEGORIES



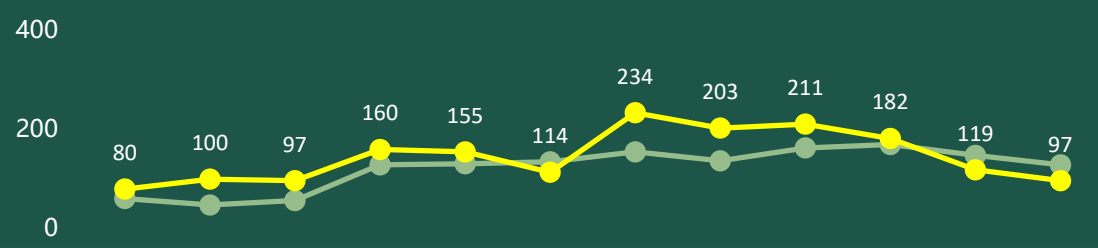
RANSOM WARE



INFORMATION LEAKAGE



INCIDENTS IN INDUSTRIAL CONTROL



80k+

A total of 81,748 security incidents were monitored and collected throughout the year. The information comes from international vulnerability databases, security vendors' websites, and social media.

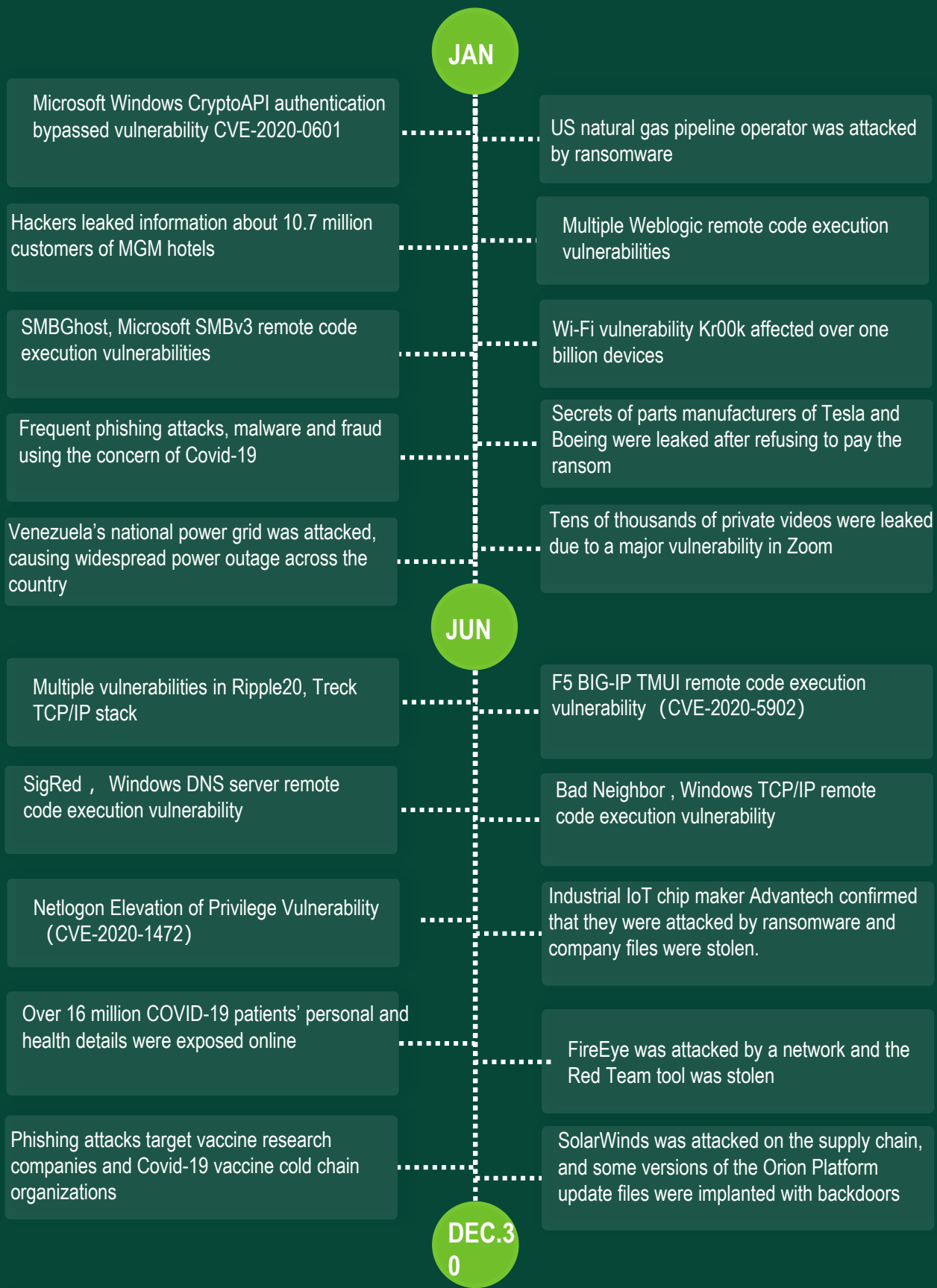
109

A total of 109 security advisories and 11 protection plans were issued this year.

CATE GORY

The security incidents observed throughout the year mainly fall into the following categories: vulnerabilities, ransomware, information leakage, industrial control, attack incidents, and malware.

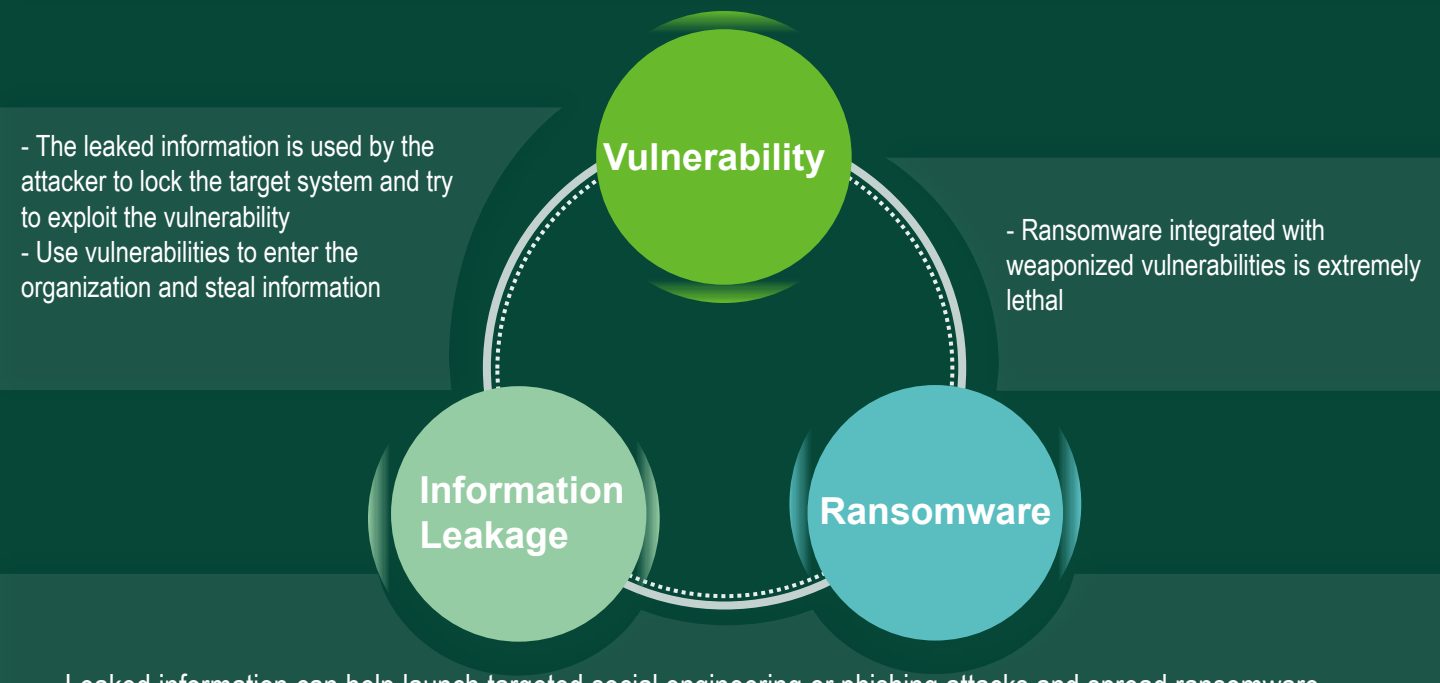
Top 20 Security Incidents of 2020



Individuals and companies pay more attention to high-risk vulnerabilities year by year, and the direct impact of these vulnerabilities has been greatly reduced in earlier years. However, even if the vulnerabilities are fixed, several types of attacks still have been active for many years, and their impact can penetrate all aspects of production and life. Ransomware and information leakage are the most persistent attacks among these secret operations.

Insights on 2020 Security Incidents

Attack methods are used tactically. A group of attack methods "support" each other to maximize their attack effects. Vulnerabilities, information leaks, and ransomware are a perfect group used by attackers. A single high-risk vulnerability is threatening enough to attract the attention of security experts, but this is only the beginning. After some vulnerabilities get weaponized by attackers, they can be used to infiltrate the target system to execute blackmailing. Information is again used as a bargaining chip to be traded on the black market, which continues to generate profit. Observing the network attacks in recent years, it is found that this model has been widely used by attackers.



The "Three Dark Brothers" who are ravaging virtual cyberspace are also "strengthening" in the field of industrial control.

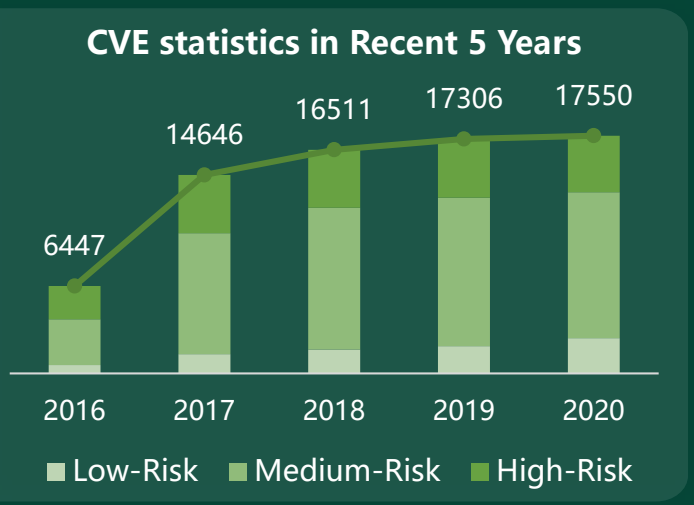
Industrial control system is the infrastructure of many national core industries such as water conservancy, electricity, petrochemical, manufacturing, aerospace, etc. Therefore, attackers driven by factors such as interests and politics are also eyeing it. Many vulnerabilities remain unfixed due to the difficulty of updating and replacing industrial control system software and hardware; the cost of lagging the industrial production brought by ransomware forces many companies to pay attackers.

Cyber Security Under the Covid-19

Due to Covid-19, many attackers took advantage of the public's attention to the pandemic, which raised the risk of information leakage and the spread of malware.

The occurrence of large-scale public security incidents like the pandemic will also affect cyberspace. Whether it is malicious apps or false rumors, it has brought great challenges to the management of cyberspace security. Cybersecurity cannot be completely separated from physical security, a comprehensive evaluation should be conducted in all aspects to avoid the spread of large-scale malicious attacks.

Observation on Vulnerabilities



The total CVE number reached a new peak for four consecutive years

Since 2017, the number of CVEs has soared to more than 14,000, and the number of CVEs released every year has reached a new peak. In terms of this year's growth, the impact of the pandemic should be considered one of the reasons.

During the pandemic, organizations may be more inclined to quickly bringing applications to market than maintaining code security. This year, the number of people working remotely in various countries has increased rapidly. Personal devices have been connected to the company's network. Collaboration software such as video conferencing, document collaboration, and virtual private networks have naturally become new targets of white-hat hackers and attackers.

Discovered vulnerabilities remain unpatched while new ones emerge constantly

According to statistics, vulnerabilities have an average life cycle of seven years, and vulnerabilities frequently exploited in 2020 will almost certainly continue to be exploited in 2021. Vulnerabilities that can be repeatedly exploited have basically been weaponized, or at least have publicly/semi-publicly available programs, and their targets are mostly widely used operating systems, personal/corporate software, components, etc. The vulnerability involved in FireEye's stolen Red Team Toolkit can prove this. The following is a list of some common software vulnerabilities that have received widespread attention this year:

Windows	**Bad Neighbor**	Windows TCP/IP remote code execution vulnerability CVE-2020-16898
	SigRed	Windows DNS server has vulnerability CVE-2020-1350 with Worm Features
	SMBGhost	RCE vulnerability CVE-2020-0796 with Worm Features in SMBv3
	Exchange	Exchange remote code execution vulnerability CVE-2020-0688 was exploited by several APT organizations
Oracle	**Weblogic**	CVE-2020-2551/14882/14883
Apache	**Tomcat**	Apache Tomcat file contains vulnerability CVE-2020-1938
Browser	**IE 0-day**	Exploited by APT organization Darkhotel along with Firefox 0day (CVE-2019-17026)
	Chrome 0-day	CVE-2020-15999 combined with social engineering, spotted attacks in the wild
	Firefox 0-day	CVE-2020-6819/6820 Mozilla spotted targeted attacks in the wild
	IE 0-day	CVE-2020-1380 spotted in Operation PowerFall attack
Remote Work	**Zoom**	Attackers execute remote code through Zoom chat function to gain control over user's device

When dealing with tens of thousands of vulnerabilities in the whole year, we should first fix those vulnerabilities that have been or easily weaponized, and make choices through reasonable grading!

Three Steps to Deal With Vulnerabilities

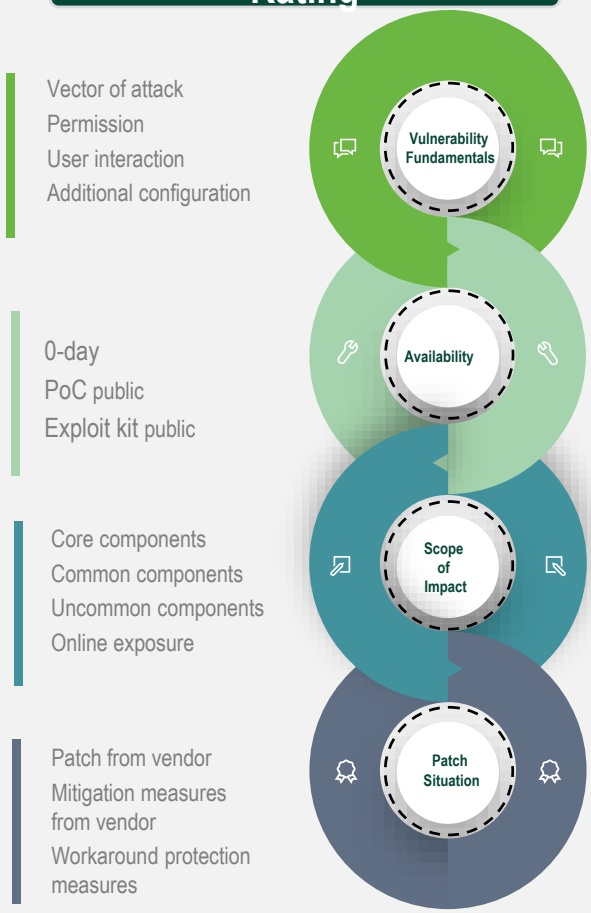
1. Precaution

- Assets management
- System, software and component management
- Follow-up of updates
- Active risk identification

Check the commonly used systems and modules of all business lines. Pay close attention to official and third-party security announcements to ensure that you are aware of new vulnerabilities as soon are as possible.

At the same time, do self-checks on hidden dangers of certain key modules, once find any, solve them as soon as possible.

2. Risk Evaluation and Rating



Not All Vulnerabilities Are "Urgent"

Vulnerabilities can be roughly assessed from four aspects:

1. Vulnerability fundamentals

Check whether it can be triggered remotely, whether specific permissions are required, whether user interaction is required, whether additional configuration is required.

2. Availability

Is it a 0-day vulnerability? Is there a public PoC? Is there a public Exploit kit?

3. Scope of impact

Check whether the core components are affected, whether the common components are affected, whether the online exposure of the affected components is large.

4. Mitigation

Check whether the vendor has provided a patch, whether there is any official mitigation measures given, if not, check whether there are workaround protection measures.

3. Emergency

- Technical analysis
- Impact analysis
- Upgrade of detection & protection product
- Complete solution

After confirming the threat level of the vulnerability, take corresponding emergency measures.

By analyzing the causes of vulnerabilities and attack chains, prepare detection and protection measures. Analyze the specific impacts and form a complete protection plan.

Observation on Ransomware Incidents

Ransomware incidents keep rising in various types
with increased ransom demand

Top 5 Victims

Municipal & public sector
Manufacturing
Education institution
Hospital
Industrial Control

Top 10 Active Ransomware

Sodinokibi/REvil
Maze
SNAKE/EKANS
Ryuk
Nemty
Nephilim
NetWalker
DoppelPaymer
CLOP
Tycoon

Top 5 Targets

USA
Australia
Canada
UK
Germany

Ransomware trend and features

Accounts for **1/4** of annual cyber attacks

Highest ransom exceeds **$40 million**

RaaS becomes more popular

Enterprises pay **20-40** times more ransom than individuals

Mostly use **phishing emails** to spread

Sensitive info will be **stolen** before encryption

Sensitive data will be **publicly auctioned**

Mostly lasts for **7 days**

Common situations after blackmailing:

- Ransomware's impact is beyond the expectation
- Business breakdown costs much more than the ransom
- Decryption will become more difficult with ransomware spreading and evolving.

Recovery or pay the ransom?

Recovery + Pay the Ransom

After reviewing some previous public blackmail incidents, it is found that in some cases, after consulting experts in detail and carefully assessing the risks, the payment of ransom may also be considered as one of the decision-making considerations. In these cases, the core business cannot be fully recovered through technical means, or the cost of business interruption is much higher than paying the ransom.

Information Collection & Assessment

After being attacked, the infected system should be isolated immediately. Confirm affected scope, assess the degree of damage, and verify backup availability.

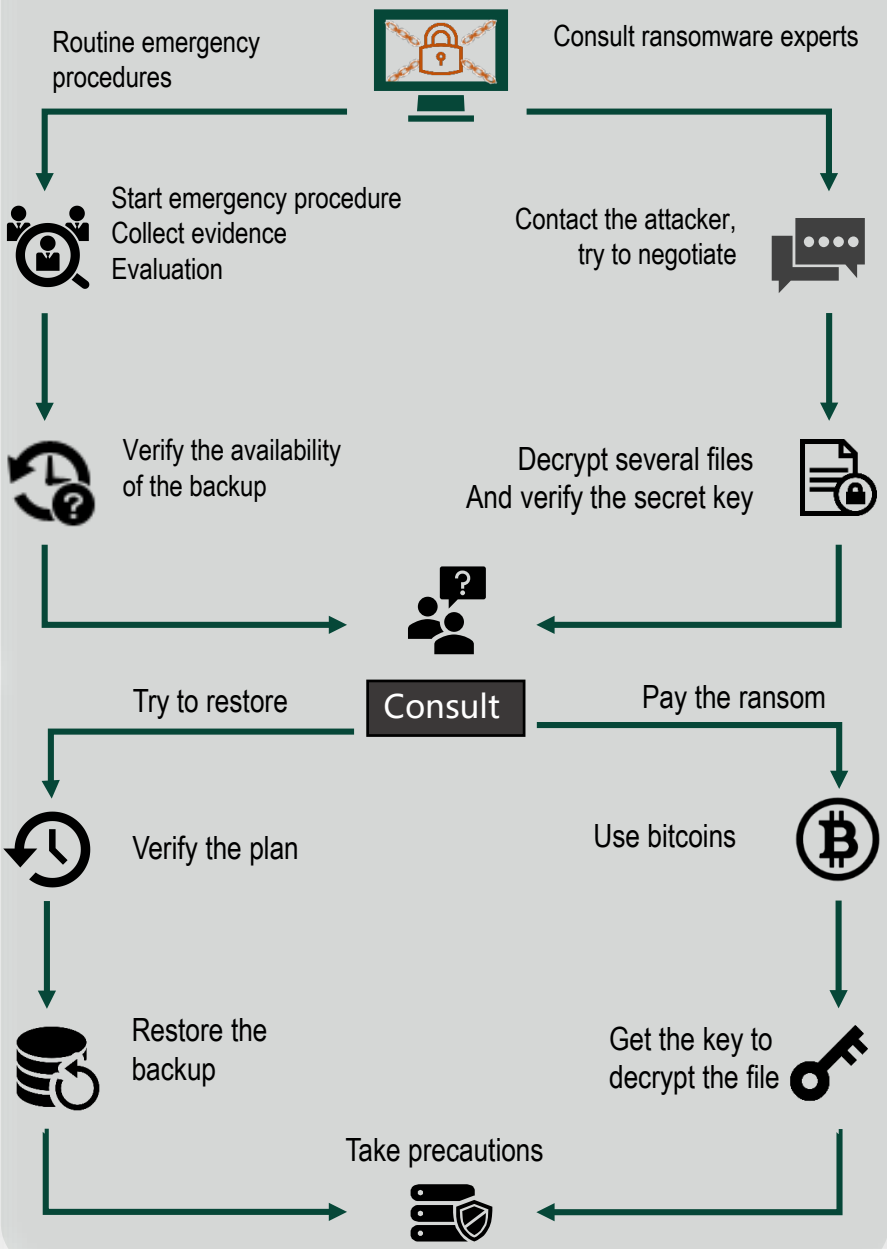
At the same time, consult ransomware experts and try to negotiate with the attacker to verify its decryption ability.

Take Actions & Conclusion

Confirm the feasibility of the technical solution, if there is a backup available, use the relevant backup to restore the business.

Otherwise, after consulting the experts and assessing the risk, determine the payment plan and restore the data by paying the ransom

Two-way Response Process



Precaution is always better than cure

Improve employee security awareness and avoid being attacked by phishing and social engineering attackers
Improve the quality of backup system and emergency plan for key business
Enhance internal malware detection capabilities through technical means

Observations on Information Leakage

Medicine
The highest cost industry

~70% Leaked info
Contains E-mail addresses

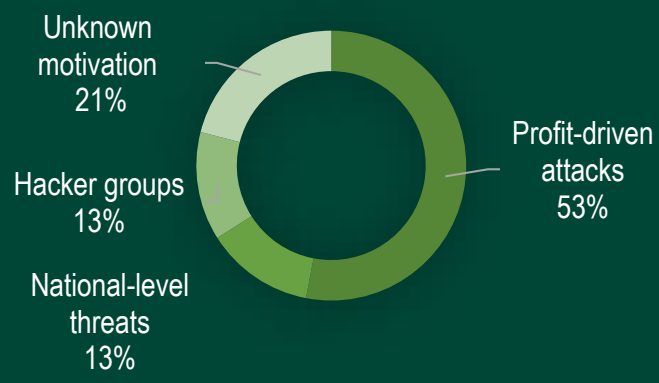
~200 days
Average time required for discovery and control

~80% Leaked info
Contains customer personal information

Remote working
Remote working under Covid-19 increases the risk of leakage

~50%
Malicious attacks account for the highest proportion of leakage

Malicious Attack Threats



Analysis on affected industries

Accommodation, Transportation, Medical & Health Industry
Hotels, airlines, hospitals, etc. all require personal information that attracts attackers for its generous profit.

Internet industry
Such as social networking sites, recruitment sites, e-commerce sites, etc., where the data not only contains the user's personal information, but also reflects the user's relationship graph.

Government and public service sectors
In addition to holding a large amount of citizen information, it also involves some confidential information that draws attackers' attention.

Case Example

Hotel	Marriott hotel data leakage, affecting 5.2 million guests
Government	Information on 4.9 million Georgian voters is disclosed
Medicine	Minnesota hospital was hacked, leaking information about 50,000 patients
IT	FireEye was invaded by a hacker organization, and red team attack tools were stolen
Social Media	267 million Facebook records sold for $600 on hacker forums

Driven by profit, private information has become a major goal of profit. The leaked information may be used for reselling, fraud, extortion, social work, etc.

With the development of self-media, the exposure of sensitive personal information on the Internet has become more common. The collection of certain biological information is even carried out without knowing or involuntarily.

The security of private information requires the joint protection of personal awareness, corporate responsibility, and laws and regulations.

When Info Leakage Happens

Reason

- Malicious attacks

Beijing deliberate, targeted, profitable makes it one of the main attack reasons.

- Insider threat

The internal personnel who have access to sensitive data obtain the data and sell it to the outside.

- System & man-made failure

- Irregular websites, platforms, and APPs over-collection and induce collection of information. Mass data has not been properly processed in transmission and storage, and it has become the transaction object in the " black industry chain".

Info Type TOP3

- Citizen info

Various personal information of citizens, including identifier, credit cards, bank accounts, etc.

- ID, web accounts

There are numerous fictitious information in the website and APP account, but the account password is often used to hit the database, and influence will dive deeper into expanded scope.

- Sensitive business info

Including employees' information, as well as various confidential information related to bills, contracts, transactions, and customers. The scope of involvement is large with bad impact on society.

After Info Leakage Happened

Influence

- Economic loss:

The attacker used the leaked data to ask the network operator for money and defraud the affected individuals.

- Damaged reputation:

Either the information was disclosed for not meeting the attacker's extortion request, or the information was sold after being leaked. The reputation of the information source and entity will be severely damaged.

- Lasting impact:

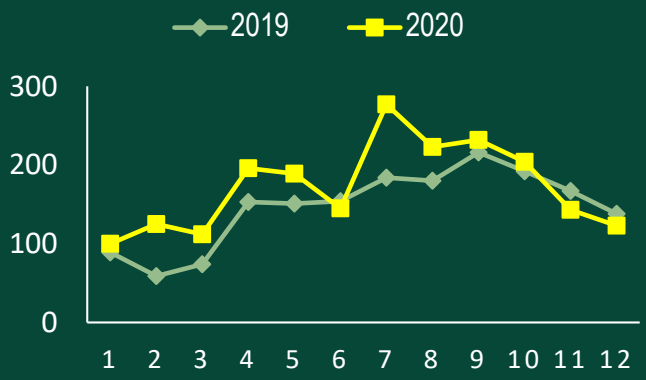
The impact of information leakage is long-lasting and may last for many years. It cannot be completely eradicated with the opening and resolution of a single incident. It is more like a sequelae, which may be used by malicious attackers in an uncertain period.

Advice

- Any individual or organization shall report actions that endanger network security to the supervision departments.
- If an individual discovers that a network operator has collected or used his/her personal information in violation of laws, administrative regulations, or agreement by both parties, he/she has the right to request the network operator to delete his/her personal information.
- No individual or organization shall steal or obtain personal information in other illegal ways, or illegally sell or provide personal information to others.
- Raise the awareness of information protection and seek help from the law.

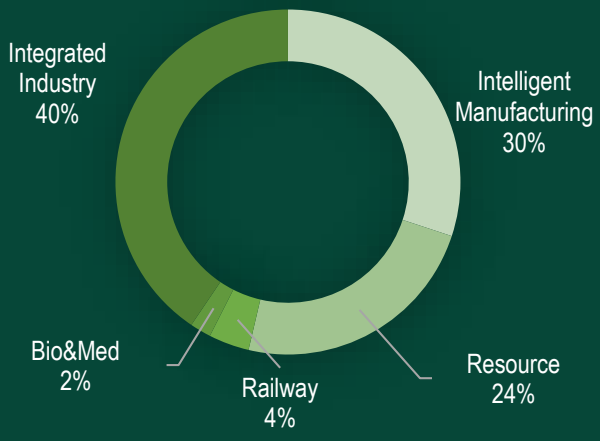
Observations on Security Incidents in Industrial Control

Annual Overview



The figure above shows the statistics of the annual number of industrial control vulnerabilities and incidents (events, research, etc.).
At the beginning of the year, due to the pandemic, the overall attention on industrial control vulnerabilities was slightly lower than that of the whole year, but it started to increase steadily in the middle of the year and fell back at the end of the year.

Related Industries



The above picture shows the distribution of the relevant industries for the annual industrial control events. Intelligent manufacturing is the industry most favored by attackers. In addition, since industrial control equipment can usually be used in multiple industries, most of the attacks involve integrated industries.

Typical Cases

Ripple20 (Supply chain risk)	- Treck TCP/IP Protocol stack vulnerability - Affected the security of global IoT and industrial Internet supply chains
Large-scale blackouts across Venezuela (hacker attack)	-After 10 months, the main line of the State grid was hit hard again -The country's critical infrastructure is a major goal of the political game
EDP encountered blackmail (Ransomware)	-Use 10TB of sensitive data to demand tens of millions of dollars -Giant manufacturers are more likely to become cash cows for attackers

Current Situation

70% More than 70% of industrial control vulnerabilities are critical.

Nday Most of the exploited are Nday. This is closely related to the difficulty of fixing industrial control vulnerabilities.

DDoS Vulnerabilities lead to DDoS attacks. Compared with other industries, DDoS attacks have more deadly impact on the industrial control industry.

Observations on Current Threats to Industrial Control

Main Threat Source

Ransomware with the ability to disrupt industrial processes is the biggest threat to industrial production. The forced shutdown of production lines, high ransoms, and the theft of sensitive information such as core manufacturing processes are all harms that ransomware can cause wherever it goes.

Some phishing emails carry the malicious software, inducing employees to click on links or download attachments to release malicious software. Some phishing emails use social engineering methods to directly request sensitive internal information for the next attack.

The cyber invasion of Israel's water infrastructure in 2020 was due to PLCs exposed on the Internet. Every exposed device opened a door to the core of the enterprise for attackers.

A single point of failure in the upstream will affect a broad range in the downstream. A vulnerability in any link of the supply chain may bring huge damage to other links, and make recovery of affected products complicated. For example, Ripple20, AMNESIA33

Attack Trend

More and more national-level advanced attack groups are targeting industrial control systems. These groups have deeper research on target systems, so the malicious tools they develop and use against industrial control equipment and production lines are more targeted and lethal.

For example, the ELECTRUM used Industroyer, a malicious software specifically targeted at industrial control systems, to cause widespread power outages in Ukraine. There is also IRONGATE, a malware that specifically targets Siemens SCADA devices.

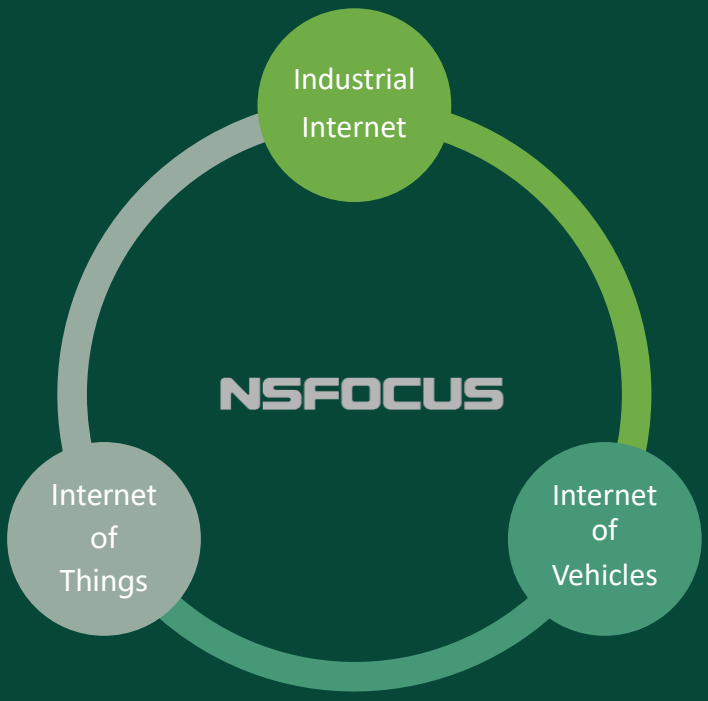
The Venezuelan blackout and cyber attacks targeting Israeli water conservancy facilities also can prove that.

IT Security Vs. ICS Security

- When protecting traditional IT systems, more attention is paid to the protection of information (confidentiality), while for ICS systems, more attention is paid to protecting the process (availability).
- Because the ICS system must ensure the continuity of system operation, there are many known vulnerabilities that have not been fixed. Therefore, the solution of patching and updating the system in time is not applicable to the ICS system in reality.
- In an ICS system, system components and equipment may be distributed hundreds of kilometers away (such as pipelines, power grids, etc.), which makes physical security also particularly concerned, because remote sites are also very likely to be the entrance for attackers to enter the ICS.

Advice

- Responding to asset exposure: Regularly sort out assets, and strictly control the exposed assets. If the business needs to be opened on the Internet, authentication and security assessment are essentials.
- Responding to phishing emails: Improve personnel security awareness, identification and risk-handling capabilities through training and drill practice.
- Introduce various detection and protection products, such as using industrial control intrusion detection systems to detect industrial control attacks, and using industrial firewalls or other protective equipment to realize logical isolation of industrial control network security areas.
- Perform and verify backups regularly.



SECURITY MADE SMART AND SIMPLE