Analysis and Response to ATW's Data Breach Incident in China

Antiy Product Promotion Center

Completion time of first draft: 20 Feb, 2023
Time of first release 19 Feb, 2023

The original report is in Chinese, and this version is an AI-translated edition.

1 Overview

Since October 2021, a hacker group called "AgainstTheWest" (ATW) has attacked platforms such as SonarQube, Gitblit and Gogs, stealing codes and data of many enterprises and public institutions in China and illegally selling them in overseas hacker forums. More than 150 institutions have been affected, including finance, medical care, government, armed forces, universities and other industries. The hacker organization stole a large number of information system source code data from the victim unit and carried on the illegal sale in the overseas hacker forum RaidForums. Based on the analysis of the gang's common attack methods, data leakage and other relevant information, Key codes and data are often stolen by the attacked unit or supply chain unit due to security vulnerabilities in the relevant code quality management / storage platform and the automation code building / testing platform. In that early stage of ATW, the main attack target was the SonarQube code quality management platform in 2021, and in the early stage of 2022, ATW's attack target was expand to include Gitblit, Gogs and other code storage management platforms.

The ATW organization is a highly pro-Western foreign hacker organization with strong political inclination, which launched cyber attacks against Russia, Belarus and other countries in the name of "# FreeUkraine" during the Russia-Ukraine conflict.

ATW selects units with certain influence and sensitivity, and regards the theft of upstream supplier codes as the theft of key information of sensitive users. And the release of data leakage related information with obvious packaging color, trying to exaggerate the seriousness of the event. This kind of data leakage events to some extent form the amplification chain effect that extends from the net space domain to the cognition domain. China is a big network country and one of the countries facing the most serious threat of network security. In recent years, the security risks introduced by third-party suppliers have never stopped, and cyber attackers have become a regular attack mode by breaking into software and hardware suppliers to realize chain breakthroughs in downstream government and enterprise application scenarios. There is also a growing trend of information theft and sabotage caused by cyber attacks. In the current complex international situation, if ATW widely share all the source codes that have been stolen to other attack organizations around the world, it will bring a lot of chain risks. Therefore, it is necessary to respond calmly and avoid excessive panic. at the same time, it is necessary to systematically sort out related risks, make unified arrangements and strengthen prevention.

In terms of the typical problems exposed in the security incidents of software supply chains, first, government and enterprise users lack unified working mechanisms and procedures from the perspective of upstream supply chain network security. There are no overall requirements on network security for the qualification entry of suppliers, and no management requirements, operating standards and corresponding inspection mechanism for secure network access of software and hardware equipment. And the insecure configuration and over-open access policy in the system; second, the software code security engineering capability is poor in the development security aspect, It generally lacks the full-life-cycle code security engineering capability, lacks the original integrated factory security mechanism, and is prone to serious security vulnerabilities and even low-level problems. after accessing the government-enterprise network, It is difficult to support the requirements of manageability and defensibility. Third, the comprehensive protection capability of software R & D environment is weak, and there are no targeted protection measures for the scenarios such as design, development, compilation, testing, signature and distribution, which results in relevant environment and process being invaded by attackers. The software is embedded with fragile code and bundled with malicious code, which brings a series of serious risks.

2 Disposal suggestions

For government, enterprise, public institutions and software suppliers, Antiy Product Promotion Center suggests:

1. Comprehensive self-inspection and self-inspection of potential risks

Comprehensively analyze the distribution, source and controllability of internal and external assets, strengthen account security management and self-inspection, avoid weak passwords, theft or divulgement of access rights, and prevent account security risks such as library collision attacks.

2. Actively introduce advanced software security methods

Adopt advanced software security development methods such as SecDevOps, establish and improve the matching code security policy, and continue to operate, and enhance code security in every link in the whole life cycle of code from the perspective of security operation.

3. Improve the safety standard system of supply chain

Improve software security performance evaluation and security event handling procedures. Implement security review and tracking of external service providers, establish a security assessment and access mechanism for suppliers, and ensure the transparency of open source codes, third-party libraries and other components used in software products (parts and products). Timely handle security vulnerabilities of external code components, ensure timely tracking and inspection of assets when security vulnerabilities are found, and ensure supply chain security.

4. Strengthen the online safety testing of software systems

Before the system is put into use, the vulnerability scanning device, the malicious code detection system, the software composition analysis system and the application security detection system are used to detect the malicious code and vulnerability in the WEB application. The static analysis security testing system and the dynamic security analysis testing system are used to check the API interface for vulnerabilities, unauthorized access, overflow and improper access control, and the multiple security access mechanism of the internal platform is added. Prevent the uncontrolled transmission of sensitive information. And regularly review the applications that have been put online to ensure the continuous effectiveness of relevant safety technical measures.

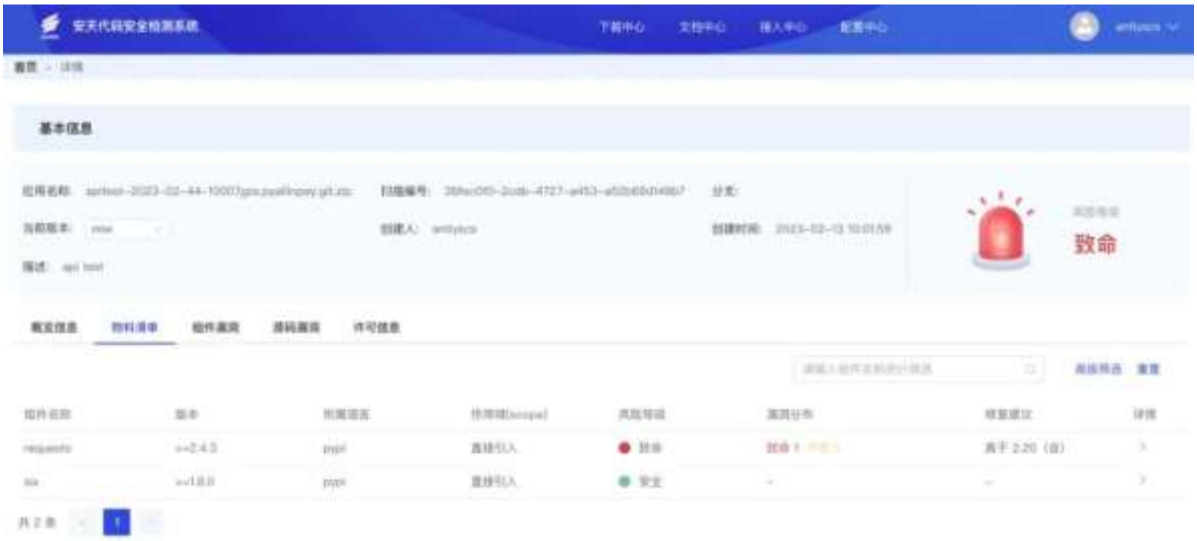
5. Strengthen the protection of software R & D environment

Comprehensively identify the code, data and other executors of the software R & D environment, conduct fine-grained control, and establish the metadata attribute and system behavior set of executors included in the operating system and application software. A supporting continuous monitoring mechanism shall be established to generate comprehensive analysis conclusions and statistics of unusual features through the identification and analysis of the whole life cycle, so as to timely detect potential hazards, ongoing abnormalities and threatening events and effectively handle them.

In response to such incidents, Antiy provides code security detection and software R & D environmental security governance solutions to government and enterprise customers and software suppliers. This solution

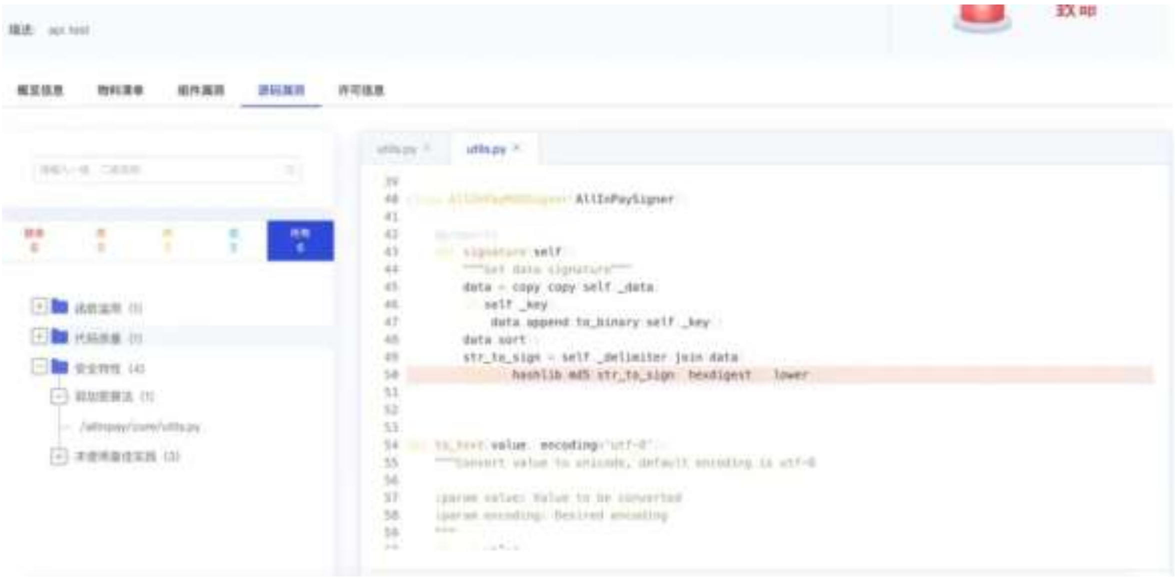
integrates the executive governance services of Antiy software composition analysis system, Antiy static application security test system, Antiy code security detection system and software development environment.

The safety software composition analysis system can effectively identify the non-safety components in the project, output the software composition list (SBOM), and create a "static snapsh ot" for the project. Antiy static security testing system can identify the potential vulnerabilities and backdoors in the source code, and help the R & D personnel to find and repair the problems in time. Safe code security inspection Enabling enterprise security development according to the process, solve the code security problem in the early development process, and the system supports access to the continuous integration and continuous delivery (CI / CD) process. For the code security of enterprises to establish a continuous monitoring, effectively improve the code risk of enterprises to respond to the capacity.



组件名称	版本	所属语言	作用域(scope)	风险等级	漏洞分布	修复建议	详情
requests	>=2.4.3	pypi	直接引入	● 致命	致命 1 [illegible]	高于 2.20（含）	>
six	>=1.8.0	pypi	直接引入	● 安全	-	-	>

Figure 1: Interface of bill of materials output by safety code detection system 1



```
class AllInPayMD5Signer(AllInPaySigner):

    @property
    def signature(self):
        """Get data signature"""
        data = copy.copy(self._data)
        if self._key:
            data.append(to_binary(self._key))
        data.sort()
        str_to_sign = self._delimiter.join(data)
        return hashlib.md5(str_to_sign).hexdigest().lower()


def to_text(value, encoding='utf-8'):
    """Convert value to unicode, default encoding is utf-8

    :param value: Value to be converted
    :param encoding: Desired encoding
    """
```

Figure 2: The interface of source code vulnerability detected by the safe code security detection system 2

In addition to the measures taken to address the security risks of software supply chains such as software being embedded with fragile codes and binding of malicious codes, It is also necessary to comprehensively identify and control the codes and executors of the software R & D environment (including new executors generated by iteration in the process of R & D and testing), and strengthen the security protection capability of the software R & D environment. Taking the governance of the execution entity as the main work, the metadata attributes and system behavior sets of the execution entities included in the operating system and application software are established. Through the identification and analysis of the whole life cycle, comprehensive analysis conclusions and statistics of unusual features are generated to timely find and effectively deal with potential hazards and ongoing unsafe events. The executive governance value-added services of Antrand can empower the terminal executive governance capability for Antrand terminal security detection products and other terminal security products. The Bank will realize the collection of all-element information, refined identification, security baseline construction and fine-grained control of the execution entity under differentiated terminal scenarios. The executive governance module links the Antiy threat intelligence subsystem with the Antiy executive reputation identification subsystem. In combination with safety service personnel and emergency response personnel, provide exclusive, automated, comprehensive and sustainable executive governance solutions for the network environment of government and enterprise customers and software suppliers.

Figure 3: Overview of governance of a certain software R & D enterprise-full-scale executor 3

Only when the fine-grained control of the executor is well conducted can the key security defense actions such as "identification, shaping, protection, detection and response" of the software R & D environment be practiced.

- **Identification: Be able to effectively clarify the system environment and business environment: Master the supporting relationship between the behavior and business of the executor; understand the executor and its required authority; Identify the capability of the executor and its corresponding relationship with vulnerability and exposed surface.**

- **Shape: Control connection, control connection according to purpose; converge exposed areas, open services and access to execution and update capacity of control executors; reduce information overflow and identify access to private data. Control the transmission of user privacy actions.**

- **Protection: Identify the object of resource access, connection, creation, writing and execution of the executor, judge its behavior purpose, and timely reject, block or stop violations.**

- **Detection: Based on the distribution of executors and behavior monitoring, screening out the executors that are worthy of attention and unknown; providing the basis for abnormal behavior; based on the behavior of executors and user operations, inferring the user behavior and its purpose.**

- **Response: Based on the potential and activation capability of the executor, create channels and other means to support the tracing of the attack source; based on the behavior and potential behavior of the attacking executor, support environment and data recovery, policy adjustment.**

Appendix: About Antiy

Antiy is committed to enhancing the network security defense capabilities of its customers and effectively responding to security threats. Through more than 20 years of independent research and development, Antiy has developed technological leadership in areas such as threat detection engines, advanced threat countermeasures, and large-scale threat automation analysis.

Antiy has developed IEP (Intelligent Endpoint Protection System) security product family for PC, server and other system environments, as well as UWP (Unified Workload Protect) security products for cloud hosts, container and other system environments, providing system security capabilities including endpoint antivirus, endpoint protection (EPP), endpoint detection and response (EDR), and Cloud Workload Protection Platform (CWPP) , etc. Antiy has established a closed-loop product system of threat countermeasures based on its threat intelligence and threat detection capabilities, achieving perception, retardation, blocking and presentation of the advanced threats through products such as the Persistent Threat Detection System (PTD), Persistent Threat Analysis System (PTA), Attack Capture System (ACS), and TDS. For web and business security scenarios, Antiy has launched the PTF Next-generation Web Application and API Protection System (WAAP) and SCS Code Security Detection System to help customers shift their security capabilities to the left in the DevOps process. At the same time, it has developed four major kinds of security service: network attack and defense logic deduction, in-depth threat hunting, security threat inspection, and regular security operations. Through the Threat Confrontation Operation Platform (XDR), multiple security products and services are integrated to effectively support the upgrade of comprehensive threat confrontation capabilities.

Antiy provides comprehensive security solutions for clients with high security requirements, including network and information authorities, military forces, ministries, confidential industries, and critical information infrastructure. Antiy has participated in the security work of major national political and social events since 2005 and has won honors such as the Outstanding Contribution Award and Advanced Security Group. Since 2015, Antiy's products and services have provided security support for major spaceflight missions including manned spaceflight, lunar exploration, and space station docking, as well as significant missions such as the maiden flight of large aircraft, escort of main force ships, and Antarctic scientific research. We have received several thank-you letters from relevant departments.

Antiy is a core enabler of the global fundamental security supply chain. Nearly a hundred of the world's leading security and IT enterprises have chosen Antiy as their partner of detection capability. At present, Antiy's threat detection engine provides security detection capabilities for over 1.3 million network devices and over 3 billion smart terminal devices worldwide, which has become a "national-level" engine. As of now, Antiy has filed 1,877 patents in the field of cybersecurity and obtained 936 patents. It has been awarded the title of National Intellectual Property Advantage Enterprise and the 17th (2015) China Patent Excellence Award.

Antiy is an important enterprise node in China emergency response system and has provided early warning and comprehensive emergency response in major security threats and virus outbreaks such as “Code Red”, “Dvldr”, “Heartbleed”, “Bash Shellcode” and “WannaCry”. Antiy conducts continuous monitoring and in-depth analysis against dozens of advanced cyberspce threat actors (APT groups) such as “Equation”, “White Elephant”, “Lotus” and “Greenspot” and their attack actions, assisting customers to form effective protection when the enemy situation is accurately predicted.