Northwestern Polytechnical University was attacked by the US NSA network attack report (Part 1)

On June 22, 2022, Northwestern Polytechnical University issued a "Public Statement" stating that the school suffered an overseas cyber attack. The Beilin Branch of the Public Security Bureau of Xi'an City, Shaanxi Province immediately issued the "Police Information Bulletin", confirming that a number of Trojan samples originating from abroad were found in the information network of Northwestern Polytechnical University, and the Xi'an police have officially opened an investigation.

The National Computer Virus Emergency Response Center and 360 Company jointly formed a technical team (hereinafter referred to as the "technical team"), which participated in the technical analysis of the case throughout the process. The technical team has successively extracted a variety of Trojan samples from multiple information systems and Internet terminals of Northwestern Polytechnical University, comprehensively used the existing domestic data resources and analysis methods, and obtained the full support of partners in some countries in Europe and South Asia to fully restore The overall overview, technical characteristics, attack weapons, attack paths and attack sources of the relevant attack events are preliminarily determined, and it is preliminarily determined that the relevant attack activities originated from the “Office of Tailored Access Operation” (hereinafter referred to as the “Special Intrusion Operation”) of the National Security Agency (NSA). TAO).

1. Overview of the attack incident

This investigation found that in recent years, TAO, a subordinate of the US NSA, has carried out tens of thousands of malicious network attacks on network targets in China, and controlled tens of thousands of network devices (network servers, Internet terminals, network switches, telephone switches) , routers, firewalls, etc.), stealing over 140GB of high-value data. TAO continues to expand the scope and scope of cyber attacks by leveraging its cyber attack weapon platform, "zero-day vulnerabilities" (0days) and the network devices it controls, etc. After technical analysis and source tracing, the technical team has now clarified the network attack infrastructure, special weapons and equipment, and techniques and tactics used in the TAO attack activities, restored the attack process and stolen documents, and mastered the information of the US NSA and its subordinate TAO on China. Evidence related to cyber attacks and data theft on the Internet, involving 13 people who directly launched cyber attacks against China in the United States, as well as more than 60 contracts signed by the NSA with U.S. telecom operators to build a cyber attack environment through cover companies. More than 170 documents.

2. Analysis of attack events

In the cyberattack against Northwestern Polytechnical University, TAO used more than 40 different NSA-specific cyberattack weapons to continuously attack Northwestern Polytechnical University to steal its key network equipment configuration, network management data, operation and maintenance data and other core technologies data. Through forensic analysis, the technical team found that the attacker penetrated more than 1,100 attack links and operated more than 90 instruction sequences inside Northwestern

Polytechnical University, and located several stolen network devices from the intruded network equipment. Device configuration files, sniffed network traffic data and passwords, other types of logs and key files, and other key details related to the attack activity. The specific analysis is as follows:

(1) Related network attack infrastructure

In order to cover its attack operations, TAO will conduct a long period of preparation before starting operations, mainly to build anonymized attack infrastructure. TAO used two "zero-day vulnerability" exploiting tools for SunOS operating system it mastered, and selected servers with a lot of network application traffic such as educational institutions and commercial companies in China's neighboring countries as the attack target; after the attack was successful, the NOPEN Trojan was installed. Program (see related research report for details), which controls a large number of springboards.

TAO has successively used 54 springboards and proxy servers in the cyber attack against Northwestern Polytechnical University, mainly distributed in 17 countries including Japan, South Korea, Sweden, Poland, Ukraine, etc. 70% of which are located in China's neighboring countries, such as Japan, Korea etc.

The function of these springboard machines is limited to command relaying, that is, forwarding the springboard commands of the upper level to the target system, thereby masking the real IP of the NSA launching the network attack. At present, at least four IP addresses of TAO's control jumper from its access environment (US domestic telecom operator) have been mastered, which are 209.59.36.*, 69.165.54.*, 207.195.240.* and 209.118.143. *. At the same time, in order to further conceal the relationship between the springboard and the proxy server and the NSA, the NSA used the anonymity protection service of the US Register company to anonymize the traceable information such as related domain names, certificates and registrants, which cannot be accessed through public channels. make an inquiry.

Through the correlation analysis of threat intelligence data, the technical team found that the network resources used for the attack platform of Northwestern Polytechnical University involved a total of 5 proxy servers. IP addresses in places like the Netherlands and Colombia, and lease a batch of servers. The two companies are Jackson Smith Consultants and Mueller Diversified Systems. At the same time, the technical team also found that the TAO Infrastructure Technology Office (MIT) staff used the name "Amanda Ramirez" to anonymously purchase a domain name and a generic SSL certificate (ID: e42d3bea0a16111e67ef79f9cc2*** **). Subsequently, the above-mentioned domain names and certificates were deployed on the US-based man-in-the-middle attack platform "Foxacid" to attack a large number of network targets in China. In particular, TAO has launched multiple rounds of continuous attacks and stealing operations on Chinese information network targets such as Northwestern Polytechnical University.

(2) Related cyber attack weapons

TAO has successively used 41 kinds of NSA's special network attack weapons and equipment in the network attack on Northwestern Polytechnical University. And during the attack process, TAO will flexibly configure the same cyber weapon according to the target environment. For example, among the cyber weapons used in the cyber attack on Northwestern Polytechnical University, only the backdoor tool

"Cunning Heresy" (named by NSA) has 14 different versions. The technical team divided the categories of tools used by TAO in this attack into four categories, including:

1. Vulnerability attack breakthrough weapons

TAO relies on such weapons to carry out attack breakthroughs on Northwestern Polytechnical University's border network equipment, gateway servers, and office intranet hosts. It is also used to attack and control overseas springboards to build an anonymous network as a cover for action. There are 3 types of weapons:

① "Razor"

This weapon can carry out remote vulnerability attacks on Solarise systems with X86 and SPARC architectures that have opened specified RPC services. When attacking, it can automatically detect the open status of the target system services and intelligently select the appropriate version of the exploit code to directly obtain the complete information on the target host. Control. This weapon was used to attack the springboards in Japan, South Korea and other countries, and the controlled springboards were used in the network attack on Northwestern Polytechnical University.

② "Island"

This weapon can also implement remote overflow attacks on Solaris systems that have opened specified RPC services, and directly gain complete control over the target host. The difference from "Razor" is that this tool does not have the ability to autonomously detect the opening of the target service, and the user needs to manually configure the target and related parameters. The NSA used this weapon to attack a border server at Northwestern Polytechnical University.

③ "Sour Fox" weapon platform

This weapon platform is deployed in Colombia and can be used in combination with the "second date" man-in-the-middle attack weapon. It can intelligently configure vulnerability payloads to carry out remote overflow attacks against mainstream browsers on multiple platforms such as IE, FireFox, Safari, and Android Webkit, and obtain the target system. (see: National Computer Virus Emergency Response Center "National Security Agency (NSA) "Acid Fox" Vulnerability Attack Weapon Platform Technical Analysis Report"). TAO mainly used this weapon platform to intrude the host of the office intranet of Northwestern Polytechnical University.

2. Persistent control weapons

TAO relies on such weapons to covertly and persistently control the Northwestern Polytechnical University network. The TAO action team can send control commands through encrypted channels to operate such weapons to infiltrate, control, and steal the Northwestern Polytechnical University network. There are 6 types of weapons in this category:

①"Second date"

This weapon resides on network edge devices and servers such as gateway servers and border routers for a long time, and can perform precise filtering and automatic hijacking of massive data traffic to

achieve man-in-the-middle attack functions. TAO installed the weapon on the border equipment of Northwestern Polytechnical University, hijacked the traffic flowing through the equipment and directed it to the "Sour Fox" platform to carry out the vulnerability attack.

②“NOPEN”

This weapon is a remote control Trojan that supports multiple operating systems and different architectures. It can receive commands through encrypted tunnels to perform various operations such as file management, process management, and system command execution. For details, please refer to: "NOPEN" Remote Control Trojan Analysis Report of the National Computer Virus Emergency Response Center). TAO mainly uses this weapon to implement persistent control over the core business servers and key network equipment inside the Northwestern Polytechnical University network.

③ "Rage Jet"

This weapon is a Windows-based remote control Trojan that supports multiple operating systems and different architectures. It can be customized to generate different types of Trojan servers according to the target system environment. The server itself has strong anti-analysis and anti-debugging capabilities. ability. TAO mainly uses this weapon to cooperate with the "Sour Fox" platform to implement persistent control over the personal hosts within the office network of Northwestern Polytechnical University.

④ "Cunning Heresy"

This weapon is a lightweight backdoor implantation tool that deletes itself after running. It has the ability to escalate privileges. It persists on the target device and can be started with the system. TAO mainly uses this weapon to achieve permanent residency, so as to establish an encrypted channel to upload the NOPEN Trojan at the right time, and ensure long-term control of the information network of Northwestern Polytechnical University.

⑤ "Stoic surgeon"

This weapon is a backdoor for 4 types of operating systems, including Linux, Solaris, JunOS, and FreeBSD. The weapon can run persistently on the target device and hide the specified files, directories, processes, etc. on the target device according to the instructions. TAO mainly uses this weapon to hide the files and processes of the NOPEN Trojan and prevent it from being discovered by monitoring. A technical analysis found that TAO used a total of 12 different versions of the weapon in its cyberattack on Northwestern Polytechnical University.

3. Sniffing secret weapons

TAO relies on such weapons to sniff the account passwords and command line operation records used by Northwestern Polytechnical University staff to operate and maintain the network, and steal sensitive information and operation and maintenance data within the Northwestern Polytechnical University network. There are two types of weapons:

①"Drinking tea"

This weapon can reside in a 32-bit or 64-bit Solaris system for a long time, and obtain account passwords exposed by various remote login methods such as ssh, telnet, and rlogin by sniffing inter-process communication. TAO mainly uses this weapon to sniff account passwords, command line operation records, log files, etc. generated by business personnel of Northwestern Polytechnical University when they perform operation and maintenance work, and compress and encrypt them for download by NOPEN Trojan.

② "Operation behind enemy lines" series of weapons

This series of weapons is specially designed for the specific business systems of telecom operators. According to the different types of business equipment being charged, "operation behind enemy lines" will be used in conjunction with different analytical tools. TAO used three types of hacking tools against telecom operators, including "Magic School", "Clown Food" and "Cursed Fire" in the cyber attack on Northwestern Polytechnical University.

4. Concealed weapons

TAO relies on such weapons to eliminate traces of its behavior within the Northwestern Polytechnical University network, hide and cover up its malicious operations and stealing behaviors, and at the same time provide protection for the above three types of weapons. 1 such weapon has been found:

"Toast Bread", this weapon can be used to view and modify log files such as utmp, wtmp, lastlog, etc. to remove traces of operations. TAO mainly used this weapon to remove and replace various log files on the alleged Northwestern Polytechnical University's Internet access device, to hide its malicious behavior. TAO's cyber attack on Northwestern Polytechnical University used 3 different versions of "toast".

3. Attack source tracing

Based on the above-mentioned technical analysis results and traceability investigation, the technical team preliminarily determined that the cyber attack on Northwestern Polytechnical University was carried out by TAO (code S32) under the Data Reconnaissance Office (code S3) of the Information Intelligence Department (code S) of the National Security Agency (NSA).)department. The department was established in 1998, and its force deployment mainly relies on the encryption centers of the US National Security Agency (NSA) in the United States and Europe. The six crypto centers that have been announced so far are:

1. NSA headquarters in Fort Meade, Maryland, USA;

2. NSA Hawaii Crypto Center (NSAH), Oahu, Hawaii, USA;

3. NSA Crypto Center Georgia (NSAG), Fort Gordon, Georgia, USA;

4. NSA Crypto Center of Texas (NSAT) in San Antonio, Texas, USA;

5. NSA Colorароo Crypto Center (NSAC) at Macley Air Force Base, Denver, Colorado, USA;

6. The NSA European Crypto Center (NSAE) at the US military base in Darmstadt, Germany.

TAO is a tactical implementation unit of the U.S. government that specializes in conducting large-scale cyber attacks on other countries and stealing secrets. It consists of more than 2,000 military and civilian personnel. Its internal institutions include:

The first: Remote Operations Center (ROC, code S321), mainly responsible for operating weapon platforms and tools to enter and control the target system or network.

Second Division: Advanced/Access Network Technology Division (ANT, code S322), responsible for researching related hardware technologies and providing hardware-related technologies and weapons and equipment support for TAO network attack operations.

Third Division: Data Network Technology Division (DNT, code S323), responsible for developing complex computer software tools to support TAO operators in carrying out cyber attack missions.

Fourth Division: Telecommunications Network Technology Division (TNT, code S324), responsible for researching telecommunications-related technologies and providing support for TAO operators to covertly penetrate telecommunications networks.

Fifth Division: Mission Infrastructure Technology Division (MIT, code-named S325), responsible for developing and establishing network infrastructure and security monitoring platforms for building attack action network environments and anonymous networks.

The sixth place: The Access Operations Office (ATO, code S326) is responsible for the backdoor installation of the products to be delivered to the target through the supply chain.

The seventh place: Requirement and Positioning Division (R&T, code S327), receives the tasks of various relevant units, determines the reconnaissance target, and analyzes and evaluates the intelligence value.

S32P: Project Planning Integration Office (PPI, code S32P), responsible for overall planning and project management.

NWT: Network Warfare Team (NWT), responsible for liaison with the Network Warfare Team.

The US National Security Agency (NSA) attack on Northwestern Polytechnical University is code-named "Stop XXXX" (shotXXXX). The operation is directly commanded by the person in charge of TAO, and MIT (S325) is responsible for constructing a reconnaissance environment and renting attack resources; R&T (S327) is responsible for determining the attack strategy and intelligence assessment; ANT (S322), DNT (S323), TNT (S324) is responsible for providing technical support; ROC (S321) is responsible for organizing attack and reconnaissance operations. It can be seen that those directly involved in command and operations mainly include the head of TAO, S321 and S325 units.

The TAO director during the NSA attack on Northwestern Polytechnical University was Robert Edward Joyce. Born on September 13, 1967, this person attended Hannibal High School, graduated from Clarkson University with a bachelor's degree in 1989, and graduated from Johns Hopkins University with a master's degree in 1993. He joined the National Security Agency in 1989. He once served as the deputy director of TAO, and served as the director of TAO from 2013 to 2017. Beginning in October 2017 as Acting U.S. Homeland Security Advisor. From April to May 2018, he served as the White House State

Security Adviser, and then returned to the NSA as a senior adviser on cybersecurity strategy to the director of the National Security Agency. He is currently the director of NSA cybersecurity.

4. Summary

Based on the analysis results of the National Computer Virus Emergency Response Center and the joint technical team of 360 Company, this report reveals the truth that the US NSA has long been conducting cyber espionage activities against Chinese information network users and important units, including Northwestern Polytechnical University. The follow-up technical team will also release more technical details of the relevant incident investigation in succession.