US National Security Agency (NSA) "acid fox" vulnerability attack weapon platform technical analysis report

Recently, the National Computer Virus Emergency Response Center conducted a technical analysis of the US National Security Agency (NSA) "Acid Fox" vulnerability attack weapon platform (FoxAcid). The vulnerability attack weapon platform is an important infrastructure for cyber espionage operations conducted by the National Security Agency (NSA) Specific Intrusion Operations Office (TAO, also known as the "Access Technology Operations Office") against other countries, and has become a computer network intrusion operation. The main equipment of the team (CNE). The exploited weapon platform has been used in several notorious cyber-attacks. Recently, a number of scientific research institutions in China have successively discovered traces of the activity of a Trojan named "Validator", which is believed to be the standard backdoor malicious program used by the NSA "Sour Fox" vulnerability attack weapon platform by default. This situation highlights that the above-mentioned units have suffered a cyber attack on the US NSA's "acid fox" vulnerability attack weapon platform.

1. Basic situation

"Sour Fox" vulnerability attack weapon platform (FoxAcid) (hereinafter referred to as "Sour Fox Platform") is a man-in-the-middle hijacking vulnerability attack platform created by the Specific Intrusion Operations Office (TAO). , accurately identify the version information of the attacked target, automatically carry out remote vulnerability attack penetration, and implant Trojan horses and backdoors into the target host. The Special Intrusion Operations Office (TAO) mainly uses this weapon platform to carry out man-in-the-middle attacks on the office intranet of the victim unit, and break through and control the host of its office network. The weapon platform is mainly used by the specific intrusion operations office (TAO) to break through and control the host system located in the office intranet of the victim unit, and implant various Trojans and backdoors into it to achieve persistent control. The Sour Fox platform adopts a distributed architecture and consists of multiple servers, which are classified according to task types, including: spam phishing emails, man-in-the-middle attacks, post-penetration maintenance, etc. Among them, the specific intrusion operation office also set up dedicated acid fox platform servers for Chinese and Russian targets.

2. Specific functions

The sour fox platform is generally used in combination with man-in-the-middle attack weapons such as "QUANTUM (quantum)" and "SECONDDATE (second date)" to hijack network traffic to the attack target and insert malicious XSS scripts. According to the type of tasks and actual needs, the vulnerabilities of XSS scripts The exploit code may come from one or more acid fox platform servers. The vulnerability attack weapon platform integrates zero-day (0-day) vulnerabilities of various mainstream browsers, and can intelligently configure vulnerability payloads to carry out remote vulnerability overflow attacks on mainstream browsers on multiple platforms such as IE, Firefox, Apple Safari, and Android Webkit. During the attack process, the platform implements environmental detection on the target system in combination

with various information leakage vulnerabilities, and matches and filters the vulnerability payload according to the detection results, and selects appropriate vulnerabilities to attack. If the target value is high, and the target system version is relatively new and the patch is relatively complete, the platform will choose to use the high-value zero-day vulnerability to carry out the attack; on the contrary, if the target value is low and the system version is old, the platform will choose the lower value. The vulnerabilities have even been publicly exploited to carry out attacks. Once the vulnerability is triggered and meets the intrusion conditions, spyware will be implanted into the target to gain control of the target system, thereby realizing long-term monitoring, control and theft of the target.

3. Technical Analysis

(1) Technical framework

The acid fox platform server uses Microsoft's Windows 2003 Server and IIS as the basic operating system and Web application server. It is usually deployed on a dedicated server with an independent IP address to screen the target system and distribute the vulnerability load to complete the attack process on the target. The attack range includes various desktop systems such as Windows, Linux, Solaris, Macintosh and Windows phone, Apple , Android and other mobile terminals.

The CDR-encrypted data transmission rules of the National Security Agency (NSA) are adopted between the sour fox platform servers, and a distributed architecture is adopted. The bottom-level server encrypts the intercepted data and aggregates it to the top-level, and the top-level server decrypts and stores it according to a certain file structure. In order to use Foxsearch and other intelligence search tools to search. The complete acid fox platform server consists of three parts, namely: basic service software (developed based on Perl script), plug-ins and malicious program payload (Payload).

The sour fox platform mainly delivers vulnerability payloads through man-in-the-middle attacks. The weapon platform performs automatic sensorless implantation according to the target device information. The specific steps are as follows:

1. After the target network session is redirected and hijacked, the information collection module of the weapon platform first obtains the target device information by means of information leakage;

2. Match and filter the vulnerability payloads that meet the attack conditions according to the obtained information, and embed the payloads into the request response page to realize automatic delivery;

3. Determine whether the result of the vulnerability attack is successful, and upload the specified type of persistent payload to the target system according to the returned information.

In order to implement the above attack process, the sour fox platform provides a custom logic interface. Members of the computer network intrusion team of a specific intrusion operation office can configure a series of filter rules on the server to process network requests from victims, including: :

1. Modrewrite, which replaces the specified resource in the request;

2. PreFilter, which judges whether it is an attack object according to the characteristics of the victim's request, and if not, returns HTTP status code 404 or 200 (and points to a specific resource); if the victim

belongs to the scope of the attack object, it is passed to the vulnerability Exploit the module, and the exploit module automatically selects the corresponding vulnerability to attack;

3. Post-filter (PostFilter), after the vulnerability attack is successful, according to the detected target host information (including: software and hardware environment information, process information, etc.) The target of the condition can specify the malicious program payload (Payload) implanted into the target.

(2) Main functional components

1. Project Tracker

The computer network intrusion team uses the project tracker to manage all the action tasks using the acid fox platform. It is written in PHP+Javascript and provides a very simple Web management interface. The members of the action team know their permissions through the background color. The background color is red to represent only Read-only permissions, green for modification permissions, and black for administrator permissions. The functions that action team members can complete through the project tracker include: managing existing action tasks, adding filters, adding new tasks, adding new servers, adding server IP addresses, and viewing tasks that will be started or completed in the past three days, etc.

2. Tag Maker

The computer network intrusion team can use the tag editor to add tags (Tag) to the server under the specified task. Each tag corresponds to a set of attack techniques and tactics. The user can configure the unique identifiers such as TLN, HMAC, and MSGID of the tag. It is related to specific attack tools, for example, the MSGID corresponding to SECONDDATE for spyware implanted in routers and firewalls is "ace02468bdf13579". In addition, the label can also specify the implantation method. Different malicious payloads should choose different implantation methods according to their characteristics. For example, SECONDDATE or MAGICBEAN should use the "WEB" implantation method, YATCHSHOP should use the "SPAM" method, and QUANTUMINSERT should use the "SPAM" method. The "QI" method should be used.

3. SECONDDATE task automation script tool "FABULOUSFABLE"

SECONDDATE is one of the main malicious implants distributed by the CNE action team through the acid fox platform, so the acid fox platform provides an automated task script tool "FABULOUSFABLE" ("FABFAB" for short) specially designed for SECONDDATE. FABFAB can interact with SECONDDATE implants instead of action team personnel, and automatically distribute rules according to pre-set logic, and collect rule execution logs and related return data.

4. Tag Replacer (MODREWRITES)

The tag replacer is one of the core components of the sour fox platform. Through the tag replacer, the computer network intrusion team can arbitrarily replace the resources in the network traffic hijacked by it. The rules of the tag replacer are written in XML format, which is the same as the filter. . As shown in Figure 1, once resource paths in the traffic match the rule characteristics, they are replaced.

```
<item name = “[待替换资源路径]”/>
<action rating=“999” name=“[替换后资源路径]”/>
```

图 1 标签替换器规则

In fact, the label replacer rule also supports the replacement of part of the string in the path or resource, which has good adaptability and scalability.

5. CASTLECREEK Whitelist

The whitelist rule is based on the post-filter, which can implant the specified malicious payload on the host with the specified IP address. The rule sample is shown in Figure 2.

```
<filter lable=“IP Deploy Val-DH8” filterId=“FA-xxxxx-xxx-xxxx-xxxx-xxxx” enabled=“true”>
    <filterMatch datatype=“socketip” matchType=“ip”>
        <item name=“[目标 IP 地址]”/>
        <action rating=“XXXX” maxThreshold=“10” name=“[恶意负载文件名或代号]”/>
    </filterMatch>
</filter>
```

图 2 白名单规则

6. Wrappers

The wrapper is mainly used to assist subsequent implanted malicious payloads to achieve persistent residency. One of the wrappers is called DireScallop, which is specially designed for a system restore tool called DeepFreeze. This tool is mostly used in Internet cafes and can automatically restore the system after the computer restarts. DireScallop can stop DeepFreeze without restarting. Re-enable DeepFreeze after the malicious load, so that the malicious load is recorded in the restore image, so that the availability of the malicious load can still be maintained after the target host restarts.

Server	*Mission*
XS10	YachrShop
XS11	GCHQ MITM
FOX00-6000	***Test Server(Spam)***
FOX00-6001	CT Spam
FOX00-6002	ME Spam
FOX00-6003	AA Spam
FOX00-6004	RU Spam
FOX00-6005	EU Spam
FOX00-6100	***Test Server(MITM)***
FOX00-6101	CT MITM
FOX00-6102	ME MITM
FOX00-6103	AA MITM
FOX00-6104	RU MITM
FOX00-6105	EU MITM
FOX00-6106	CT-MAC
FOX00-6300	***Test Server(Enchanted)***
FOX00-6401	CCNE China
FOX00-6402	CCNE Russia
FOX00-6403	CCNE Other

图 3 FA 服务器分布及任务用途分类

(3) The main malicious payload implanted

1. SECONDDATE (second date)

The spyware programs targeting routers and firewalls can lurk in network devices and perform malicious operations such as stealing, hijacking, and replacing network traffic data according to the rules distributed by the acid fox platform components.

2. Validator

Validator is a backdoor malicious program used by default on the acid fox platform, which can achieve long-term control of the target.

3. MistyVeal

MistyVeal is an enhanced version of the Validator backdoor and can be configured to backlink at fine-grained incremental time intervals to evade feature detection. And it will use the IE browser as a backlink channel, and can reuse the proxy server settings of the IE browser, and it is only valid for the IE browser.

4. Ferret Cannon

Ferret Cannon is an executable program dropper. With Ferret Cannon, the acid fox platform can target a variety of spyware tools, such as: United Rake, Peddle Cheap, PktWench and Beach Head, etc. The

executable program can be .dll or . exe.

4. Mode of operation

Based on the information disclosed by Snowden, a former employee of the US National Security Agency (NSA), we can partially analyze how the acid fox platform operates as follows:

(1) Staffing

One or more acid fox project instructors will be set up in the computer network intrusion operation team of a specific intrusion operation office. These instructors can lead one or more acid fox operation groups. The operation group includes multiple computer network intrusion operation team members, respectively. Responsible for directly supporting specific network intrusion operations, maintaining infrastructure such as acid fox servers and software, and developing and testing new plug-ins, exploit codes, auxiliary intrusion tools, and Trojan backdoors and other malicious payloads according to mission needs.

(2) Construction of positional infrastructure

As shown in Figure 3, the specific intrusion operations office deploys acid fox platform servers around the world, where the server numbered with the prefix XS is the main server for coordinating multiple tasks, it is worth noting that the server numbered XS11 is explicitly assigned to the United Kingdom The intelligence agency "Government Communications Headquarters" (GCHQ) carried out man-in-the-middle attacks; the acid fox platform servers numbered FOX00-60XX series were used to support spam and phishing email operations, and the servers were distributed according to the target area, including the Middle East, Asia, Europe, Russia and other specific regions; the servers numbered FOX00-61XX series are used to support man-in-the-middle attacks, and the server distribution is the same as the FOX00-60XX series; it is worth noting that the servers numbered FOX00-64XX series It is used to support the computer network intrusion team's vulnerability attack operations. The server numbered FOX00-6401 is specifically aimed at China, the server FOX00-6402 is aimed at Russia, and the server No. FOX00-6403 is aimed at other targets. In addition, the server FOX00-6300 may be used in the attack code-named "ENCHANTED".

(3) Examples of attacks

1. Case 1

```
<filter lable=”Implant deployed – already, self or otherwise deleted” filterId=“FA-b91fb762-3fea-4b6d-aa39-262312512625” enabled=“true”>
<filterMatch dataType=”implant” matchType=”ci_string”/>
    <item name=”Mistyveal”/>
<action rating=”1004” maxTime=”43200” includeTid=”true” name=”404”/>
</filterMatch>
</filter>
<filter lable=”IEKAV_MV” filterId="FA-a950dbf0-e918-4eb8-ab79-34bff13f50a1" enabled="true">
    <filterMatch dataType="process" matchType="ci_contains">
        <item name="avp.exe" />     //卡巴斯基杀毒软件进程
    <filterMatch dataType="process" matchType="ci_contains">
        <item name="iexplore.exe" />    //IE 浏览器进程
    <action rating="1003" name=""Mistyveal-Win32-11.0.1.1" /> //植入 Mistyveal 后门
    </filterMatch>
    </filterMatch>
</filter>
<filter lable="tid match deploy MV - bad process 404" filterId="FA-1a3f9db0-5abd-4254-99a6-01dc9f6e3eec" enabled="true">
    <filterMatch dataType="tid" matchType="ci_string">
        <item name="177312"/> <!--foxtrack 1710-->
        <item name="183556"/> <!--foxtrack 1897-->
        <item name="183560"/> <!--foxtrack 1897-->
        <item name="183587"/> <!--foxtrack 1897-->
        <item name="186675"/> <!--foxtrack 1897-->
        <item name="186677"/> <!--foxtrack 1897-->
    <filterMatch dataType="process" matchType="ci_contains">
        <item name="ccenter.exe"/> <!--foxtrack 1466 -->     //瑞星杀毒软件进程
        <item name="ravmon.exe"/> <!--foxtrack 1466 -->     //瑞星杀毒软件进程
        <item name="ravmond.exe"/> <!--foxtrack 1466 -->     //瑞星杀毒软件进程
        <item name="ravstub.exe"/> <!--foxtrack 1466 -->     //瑞星杀毒软件进程
        <item name="ravtask.exe"/> <!--foxtrack 1466 -->     //瑞星杀毒软件进程
        <item name="ravxp.exe"/> <!--foxtrack 1466 -->     //瑞星杀毒软件进程
        <item name="ravservice.exe"/> <!--foxtrack 1466 -->     //瑞星杀毒软件进程
        <item name="ravtray.exe"/> <!--foxtrack 1466 -->     //瑞星杀毒软件进程
        <item name="RavAlert.exe"/> <!--foxtrack 1466 -->     //瑞星杀毒软件进程
        <item name="RavUpdate.exe"/> <!--foxtrack 1466 -->     //瑞星杀毒软件进程
        <item name="rfwproxy.exe"/> <!--foxtrack 1466 -->     //瑞星杀毒软件进程
        <item name="rfwstub.exe"/> <!--foxtrack 1466 -->     //瑞星杀毒软件进程
        <item name="rfwmain.exe"/> <!--foxtrack 1466 -->     //瑞星杀毒软件进程
        <item name="rfwsrv.exe"/> <!--foxtrack 1466 -->     //瑞星杀毒软件进程
        <item name="kvsrvxp.exe"/> <!--foxtrack 1466 -->     //江民杀毒软件进程
```

图 4 攻击案例 1

As shown in Figure 4, the filter rule fragment on the sour fox platform server, it can be judged that the server mainly targets Chinese host targets, and the filter focuses on Kaspersky Antivirus, Rising Antivirus, Jiang The processes of popular antivirus software in China, such as civilian antivirus software, were matched and the implantable conditions were judged.

2. Case 2

```
<filter lable="IP Deploy Val-DH8" filterId="FA-c52126fb-f005-4ebd-9f70-fe3b3d1b2248"
enabled="true">
    <filterMatch dataType="socketip" matchType="ip">
        <item name="203.99.164.199" />  //IP 地址归属于巴基斯坦电信公司（AS17557）
        <action rating="1070" maxThreshold="10"
name="FerrentCannon-Win32-1.0.0.1-VALDMW" />
    </filterMatch>
</filter>
```

图 5 攻击案例 2

As shown in the filter rule fragment on the server shown in Figure 5, it can be judged that the FA server is used to attack the target of IP address "203.99.164[.]199", and the FerrentCannon malware mentioned above will be implanted into the target. payload to further deliver other spyware to the target. After investigation, the IP address "203.99.164[.]199" belongs to Pakistan Telecom.

V. Summary

The above technical analysis shows that the US NSA "acid fox" vulnerability attack weapon platform is still one of the main battle network weapons of the US government. There are three conclusions worthy of the international community's close attention: **First** , the vulnerability exploitation platform is a specific platform of the US National Security Agency NSA. The main battle equipment of the computer network intrusion team under the Intrusion Operations Office (TAO) has been widely used in the network intrusion operations carried out by the computer network intrusion team alone or in cooperation. The attack range covers the world, of which China and Russia are the key targets. **Second,** the weapon platform adopts a highly modular structure and has high scalability. At the same time, it can be highly integrated with the project management tool of a specific intrusion operation office to achieve efficient cross-operation support. **The third is to** support cross-platform attacks. After integrating with other network weapons of the specific intrusion operations office (TAO), it can attack almost all devices with network connection capabilities, which is a veritable network "black hole".

China's National Computer Virus Emergency Response Center issued an early warning to Internet users around the world. China's scientific research institutions are by no means the only targets of NSA cyberattacks. Government institutions, scientific research institutions and commercial enterprises around the world may be being remotely controlled by the acid fox platform. , usually remote access to important data, paralyzed important information infrastructure in wartime, paving the way for the American-style "color revolution".

- Technical Analysis on FOXACID