Technical Analysis on FOXACID

— A U.S. NSA-linked Cyber-Weapon

Jun. 29th, 2022

Executive summary

National Computer Virus Emergency Response Center (CVERC) has made technical analysis on an Exploit-Kit named FOXACID platform, which has been used as main infrastructure of Computer Network Exploitation (CNE) Operation by the Office of Tailored Access Operations (TAO, affiliated with U.S. NSA). Recently, artifacts of a malware family called "Validator" were discovered from several institutions of research located in China. A further analysis showed that the "Validator" is a backdoor known to have been used by TAO and as a default payload of FOXACID.

Introduction

FOXACID platform is an Exploit-Kit which support MITMA (Man-in-The-Middle-Attack), session hijacking, reconnaissance, automatic-exploitation and payload-delivery. With the help of FOXACID, TAO could compromise and get initial access of the victim's internal network, take lateral-movement, and finally deploy trojans and backdoors for persistence. FOXACID platform was designed and build in distributed architecture with multiple servers which categorized by their functions (SPAM, MITMA, Post-Exploitation, etc.) and targets (China, Russia, etc.).

Technical Details

Functionality

FOXACID platform is normally integrated with other NSA-linked weapons such as QUANTUM and SECONDATE, it will exploit the targets via XSS alongside the MITMA and the malicious scripts might come from single or multiple FOXACID servers. FOXACID has a collection of Zero-Day RCE vulnerabilities for widely-used internet browsers, such as Microsoft Internet Explorer, Mozilla FireFox, Apple Safari, Android Webkit, etc. At first, the CNE team of TAO take reconnaissance on targets with information-leak vulnerabilities. Then, based on result of reconnaissance, target will be exploited via known-vulnerabilities. For well-patched valuable targets, Zero-Day vulnerabilities will be used. Finally, spywares will be delivered for persistent remote control, monitoring and data exfiltration.

Architecture

FOXACID server AKA "FA Server" is the vital infrastructure of FOXACID platform for target selection, exploitation, and payload deployment, which is set up on IIS within standalone Microsoft Windows 2003 Server. As far as we known, FOXACID is targeting OS for desktop PC

including Windows, Linux, Solaris, Macintosh and OS for mobile devices such as Windows Phone, iOS and Android.

CDR is the method of data transfer used by FA Severs, which is a private data-encryption protocol used by NSA. FA servers are deployed in distribution structure, data on the low side is transferred in an encrypted format to high side. Then data will be decrypted and placed in its appropriated file location on the server. Data could be retrieved by Foxsearch, which is an intelligence search engine. FA server consisted mainly of three components, includes basic server-side software based on Perl scripts, plugins and payloads.

Attack Scenario

CNE team use FOXACID as a weapon for implant with no interaction during a MITMA. Following steps will be proceed:

Step 1: Reconnaissance

When victims' sessions were hijacked and redirected, plugin for information gathering is activated and collect the necessary data of target-hosts' running state.

Step 2: Exploitation selection

Decides adaptive exploitation for targets based on reconnaissance, then inject the shellcode to the stream responded to the victim's hosts.

Step 3: Payload implantation

Finds out whether the exploitation is success or fail. If succussed, certain types of persistent payloads will be implanted into the victim's hosts.

A user-interface is provided by FOXACID for configuration. In order to intercept and modify the victims' sessions, CNE team create customized filters, which include following types:

- **Modrewrite:** Replace matched resources in hijacked-sessions.
- **PreFilter:** Decide whether the host is a vulnerable target or not. If not matched, 404 or 200 message (redirect to certain resources) will be responded. If matched, exploitation will be proceed automatically.
- **PostFilter:** If exploitation is succeed, decide whether the target is valuable and implantable. If matched, certain malware as a payload will be delivered.

Components

Project Tracker

CNE teams manage FOXACID mission via Project Tracker, which is developed with PHP and Javascript. The Web interface of Project Tracker is fresh and simple, CNE operators could be easily aware of his own privileges based on background color. Red is read only, Green is modify, Black is admin. CNE operators are able to manage current projects, add a filter, add a project, add a server, add IPs of server, view projects that will start/end soon (3 days)

Tag Maker

CNE teams add “Tags” to FA servers. Each tag has different TTPs (Technique, Tactic and Procedures). Distinguish attributions like TLN, HMAC and MSGID might be assigned to tags. MSGID refers to certain hacktool, for example, the MSGID of SECONDDATE, which targeting the Routers and Firewalls, is “ace02468bdf13579”. In addition, tags also define the types of deployment. For example, SECONDDATE and MAGICBEAN should be using the “(WEB)” Deployment Types. YATCHSHOP tags should have “SPAM” and QUANTUMINSERT shoud have “QI”.

FABULOUSFABLE for SECONDDATE

As one of the most common weapons of CNE, SECONDDATE is mainly distributed via FOXACID. FABULOUSFABLE, AKA “FABFAB”, is used in automated SECONDDATE tasking. FABFAB interactive with SECONDDATE implants following a series of rules which had been configured by CNE operators, and collect the results, logs and data.

Modrewrites

Modrewrites filters are able to replace resources from hijacked-sessions. The rules of modrewrites in XML format are similar with other filters. As shown in Figure 1, when certain rule is matched, the whole tag or only a certain portion of tag incoming to the FA server will be rewrite.

```
<item name = “[path strings to be replaced]”/>
    <action rating=“999” name=“[replaced path strings]”/>
```

Figure 1. Rules of Modrewrites filters

CASTLECREEK Whitelist

CASTLECREEK Whitelist filters take up a majority of the Postfilter, and it is configured to deploy certain payload to the host with certain IP, as 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=“[IP address of the target host]”/>
        <action rating=“XXXX” maxThreshold=“10” name=“[filename of payload]”/>
    </filterMatch>
</filter>
```

Figure 2. Rules of CASTLECREEK Whitelist filters

Wrappers

Wrappers enable payload persistence. DireScallop, one of the Wrappers, is used to against targets that are using DeepFreeze products. DeepFreeze is used in many Internet cafes to prevent changes to a computer’s operating system and software applications. DireScallop is able to disable DeepFreeze without the need for a reboot. Implants can then immediately execute and re-enable DeepFreeze after gaining persistence.

Payloads

SECONDDATE

SECONDATE is a spyware which hide itself deeply in Routers and Firewalls with malicious activities of traffic interception, data exfiltration and modification.

Validator

Validator is a backdoor and as default payload of FOXACID.

MistyVeal

MistyVeal is a larger implant than Validator. In order to avoid detection, it has a configurable call back time that can be changed with a granularity of increments in Days, Hours, or Minutes. MistyVeal cannot call out on the network on its own, instead, it call out on the network via Internet Explorer and reuse the proxy of Internet Explorer.

Ferret Cannon

Ferret Cannon is a malware loader. With the help of Ferret Cannon, spywares made by NSA like United Rake, Peddle Cheap, PktWench and Beach Head could be easily deployed and support executable file in ".dll" and ".exe".

Operation of FOXACID

With public-disclosure from the NSA programs leaked by Snowden, we could take a glimpse of how FOXACID platform is operated.

FOXACID Team

One or more FOXACID coach and mentor are assigned to NSA TAO's CNE team. Each coach and mentor manage one or more FOXACID team and receive FOXACID briefing from FOXACID team leader. The members of FOXACID team have different roles, including CNE operations support, infrastructure maintain and develop plugins, exploits, hacktools, trojans, backdoors, etc.

Infrastructure

As shown in Figure 3, TAO has deployed lots of FA servers. Servers with ID which has a prefix of "XS" were assigned with role of cross-mission control. What notable is a server with ID of "XS11" was assigned to GCHQ, a UK intelligence agency, for supporting MITMA mission. "FOX00-6000" series support SPAM mission, and were distributed in Middle-East, Asia, Europe, Russia and other particular regions. "FOX00-6100" series support MITMA mission with the same distribution as "FOX00-6000" series. "FOX00-6400" series support CNE mission, "FOX00-6401" targets China, "FOX00-6402" targets Russia, "FOX00-6403" targets other objects. In addition, "FOX00-6300" might be used for supporting missions called "ENCHANTED".

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

Figure 3. Distribution and Roles of FA servers

Cases of Operation

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" />      //ProcessName of Kaspersky Anti-Virus software
      <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 -->     //ProcessName of Rising Anti-Virus software
            <item name="ravmon.exe"/> <!--foxtrack 1466 -->     // ProcessName of Rising Anti-Virus software
            <item name="ravmond.exe"/> <!--foxtrack 1466 -->     // ProcessName of Rising Anti-Virus software
            <item name="ravstub.exe"/> <!--foxtrack 1466 -->     // ProcessName of Rising Anti-Virus software
            <item name="ravtask.exe"/> <!--foxtrack 1466 -->     // ProcessName of Rising Anti-Virus software
            <item name="ravxp.exe"/> <!--foxtrack 1466 -->     // ProcessName of Rising Anti-Virus software
            <item name="ravservice.exe"/> <!--foxtrack 1466 -->     // ProcessName of Rising Anti-Virus software
            <item name="ravtray.exe"/> <!--foxtrack 1466 -->     // ProcessName of Rising Anti-Virus software
            <item name="RavAlert.exe"/> <!--foxtrack 1466 -->     // ProcessName of Rising Anti-Virus software
            <item name="RavUpdate.exe"/> <!--foxtrack 1466 -->     // ProcessName of Rising Anti-Virus software
            <item name="rfwproxy.exe"/> <!--foxtrack 1466 -->     // ProcessName of Rising Anti-Virus software
            <item name="rfwstub.exe"/> <!--foxtrack 1466 -->     // ProcessName of Rising Anti-Virus software
            <item name="rfwmain.exe"/> <!--foxtrack 1466 -->     // ProcessName of Rising Anti-Virus software
            <item name="rfwsrv.exe"/> <!--foxtrack 1466 -->     // ProcessName of Rising Anti-Virus software
            <item name="kvsrvxp.exe"/> <!--foxtrack 1466 -->     // ProcessName of Jiangmin Anti-Virus software
```

Figure 4. Case 1

As a fragment of filter from FA server shown in Figure 4, we could easily find out that the FA server is supporting the CNE mission targeting hosts located in China. Apparently, the filter contains a lot of rules which intend to match popular Anti-Virus solutions in China, such as Rising and Jiangmin from local vendors, and Kaspersky from Russia. And Kaspersky is also a top vendor in Russia.

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" />    //Owned by Pakistan Telecommunication Company Limited (AS17557)
        <action rating="1070" maxThreshold="10" name="FerrentCannon-Win32-1.0.0.1-VALDMW" />
    </filterMatch>
</filter>
```

Figure5. Case 2

From a fragment of filter on a FA server, as shown in Figure 5, we believe that this FA server is attempting to attack the host with IP address of "203.99.164[.]199" and try to implant FerrentCannon into the target for more spywares deployment. And "203.99.164[.]199" is owned by Pakistan Telecommunication Company Limited (AS17557).

Conclusions

Learned from above, we believe the project of FOXACID platform is still running by US government, and everyone should know the following facts:

- FOXACID is a common cyber-weapon used by CNE team affiliated with TAO of NSA, and plays a vital role in globe cyber-espionage operated by NSA, especially against China and Russia.
- FOXACID adopts modular structure with features including high-scalability and cross-mission support when integrated with TAO's project management instruments.
- FOXACID supports cross-platform attack, combined with other cyber-weapons of TAO, it is able to compromise any network devices. FOXACID is a veritable "Black Hole" of the internet.

CVERC encourage all users from all over the world to be aware of the risk and the fact that Chinese research institutions were not the only victims. Organizations of governments, academies, business around the world might have been compromised by NSA with FOXACID. When running a new "Color Revolution" operation, FOXACID facilitates US intelligence agencies with the abilities to steal sensitive data at any time, and cause outage of critical infrastructures at war time.