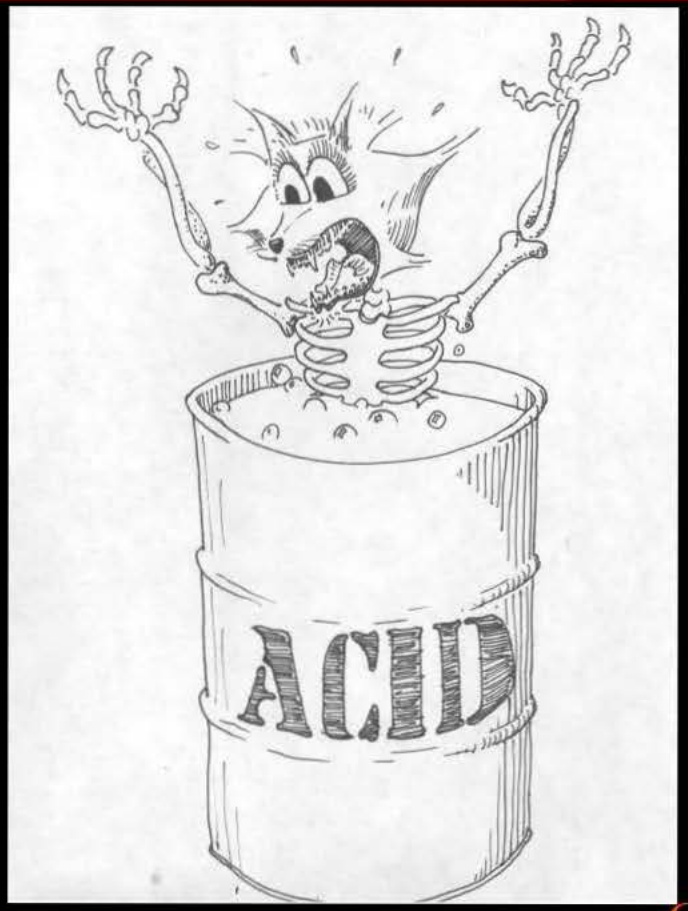
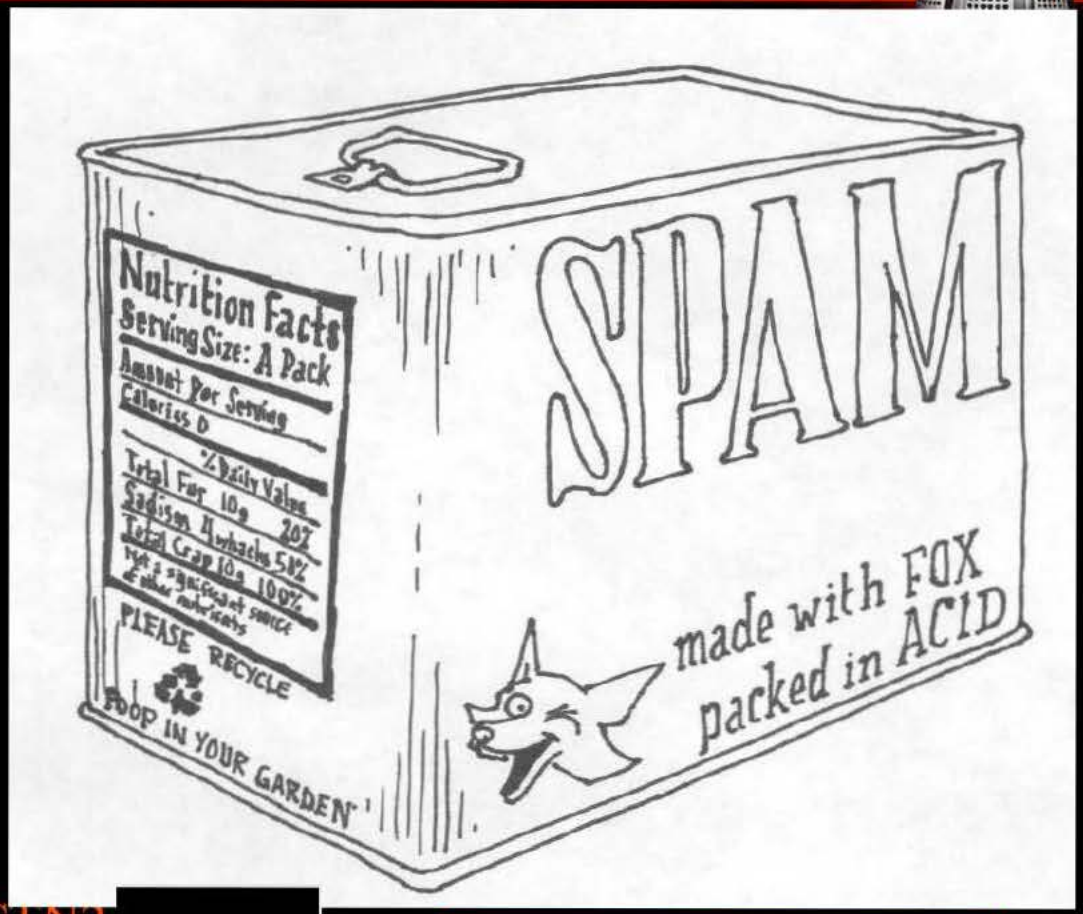
FOXACID





CTN2
FOXACID/STAT

Mission

Mission Statement: Provide Points of Presence for follow on collection and exploitation through the deployment of content-based email, MitM/MotS Operations and Cross Site Scripting (XSS). In other words – provide "Initial Access".

Accomplished by:

- Development of XSS vulnerabilities against web mail services
- Injection of FA tags utilizing MitM/MotS techniques
- Maintenance of FA servers and exploit plug-ins
- Deployment of emails to targets; special request and spam

In layman's terms…

FOXACID was once a mission name referring to CT targets within Al-Qaeda.

It then became the name for the spam operation.

Now, it basically refers to the exploit servers that we leverage to provide initial access through browser exploitation. If we can get a target to visit our URL in his web browser by any means, we can potentially exploit him and deliver a back-door implant.

The Spam Mission

- FOXACID deploys “spam” email to targets. These emails are not like normal spam as they are malicious in nature, as opposed to just annoying.

- Inside of each email, we can include several methods of exploitation, depending on the mail service and target. These techniques are discussed later in the presentation.

- The overarching goal is to utilize social engineering via emails to gain access to a targets computer.

- The emails themselves can either be very generic or very targeted, depending on the target and nature of request. For obvious reason, it takes higher authority to deploy very targeted emails because of the level of guilty knowledge they must contain about the target.

XSS

• Cross Site Scripting can best be described as sneaking code, or more specifically JavaScript, into a webpage. Websites go to great lengths to prevent arbitrary code execution in user input (such as a search box, guest book, the content of an email, etc).

• In addition to website-based filters, we must also defeat browser-based filters. This means that in order to find an exploit, two HTML parsing filters must be defeated.

• The end goal is to somehow inject an <iframe> tag that links back to our servers. This is done by rigorous trial and error: a process that can often be tedious and unrewarding.

XSS

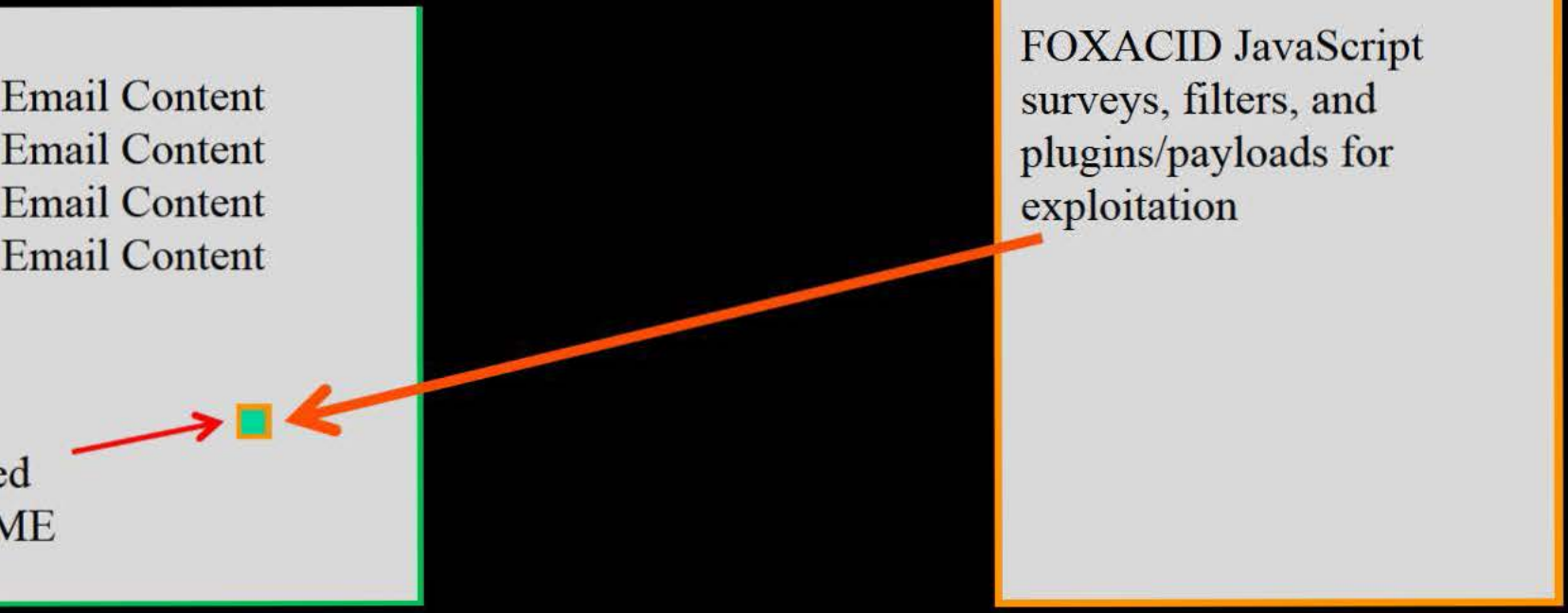
Target's Browser

Email Content
Email Content
Email Content
Email Content

Injected IFRAME

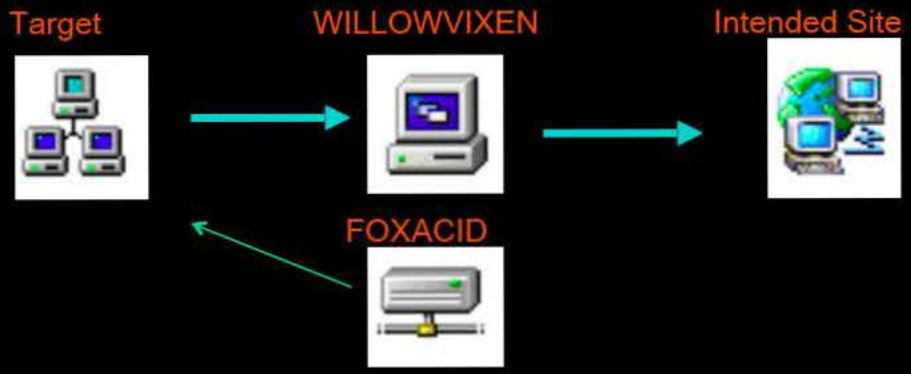
FOXACID Server

FOXACID JavaScript surveys, filters, and plugins/payloads for exploitation



WILLOWVIXEN

WILLOWVIXEN is a technique that permits exploitation by having the target browse to a website by clicking on a link in an email that we sent. The WILLOWVIXEN server receives the contact from the target and performs a redirection.



Draft Box Tagging

Draft Box Tagging: Provide tag injection by masquerading into an account and utilizing GENUINE DRAFT to append an iframe into the message.

This technique is design to be used against multiple targets that have a web mail account and leave messages in the draft box for communication purposes.

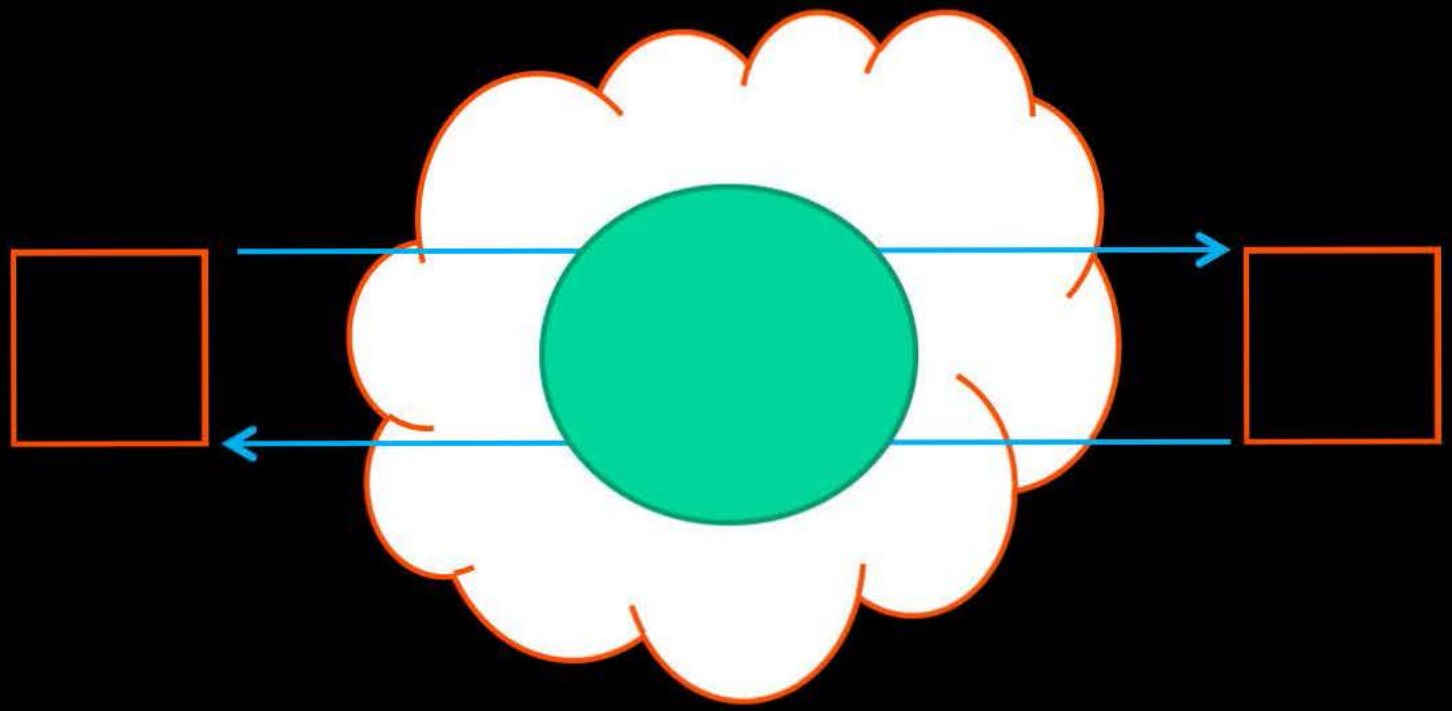
MitM vs. MotS

- Man in the Middle
  - Refers to an entity located between nodes that are communicating
  - every message between the nodes must pass through the MitM
  - in a position to **observe and modify** messages between the nodes
- Man on the Side
  - only passively observe messages between nodes
  - **sees every message** between the nodes, but it **cannot modify** the messages
  - inject new messages into the network

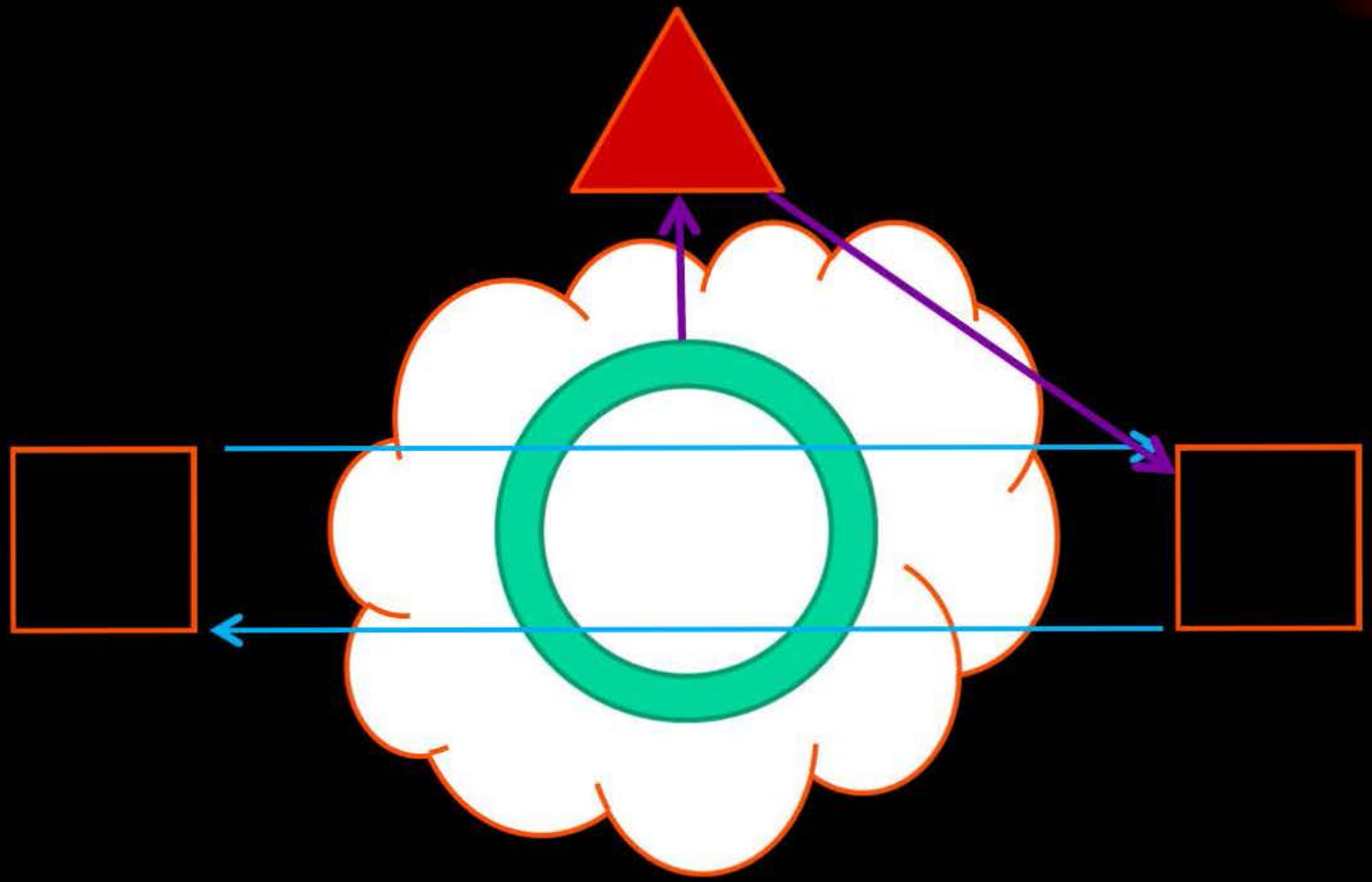
MitM vs. MotS

- Man in the Middle
  - Refers to an entity located between nodes that are communicating
  - every message between the nodes must pass through the MitM
  - in a position to **observe and modify** messages between the nodes
- Man on the Side
  - only passively observe messages between nodes
  - **sees every message** between the nodes, but it **cannot modify** the messages
  - inject new messages into the network

Man in the Middle…



Man on the Side…



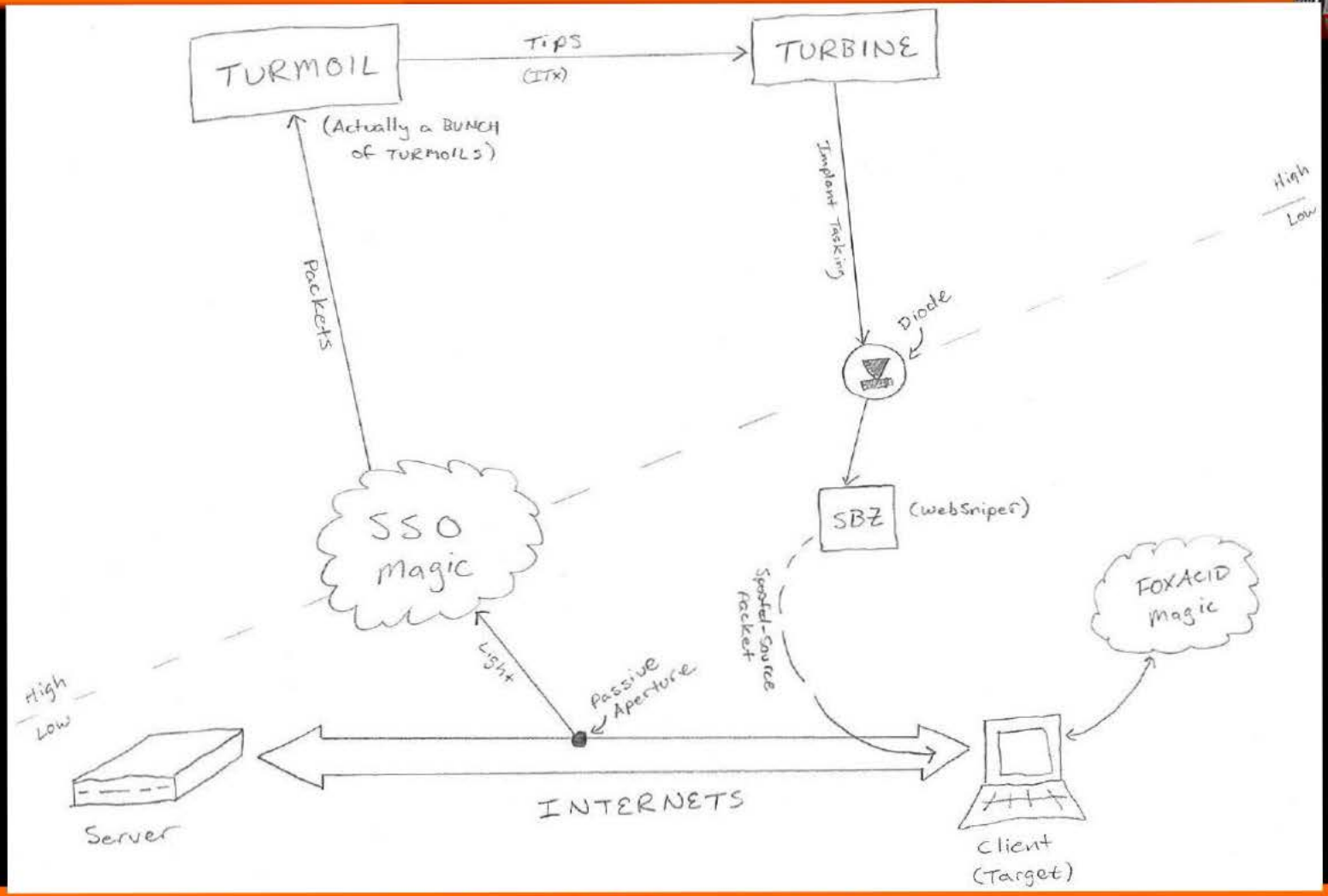
SECONDDATE

- SECONDDATE is an exploitation technique that takes advantage of web-based protocols and man-in-the-middle (MitM) positioning.
- SECONDDATE influences real-time communications between client and server and can quietly redirect web-browsers to FA servers for individual client exploitation.
- This allows mass exploitation potential for clients passing through network choke points, but is configurable to provide surgical target selection as well.

QUANTUMTHEORY

- QUANTUMTHEORY is the overarching mission name to a set of MotS techniques utilizing our passive collect system as well as active components to react to real-time traffic captures.
- Basically: we see traffic with our massive passive collect system, we react to it by putting a packet on the wire spoofing some end of the communication in an attempt to redirect the target to FOXACID in some manner or fashion.
- Quantum is generally a low-latency operation, meaning we have to get a tip, process it, craft a response, and send a packet to the target all before the actual expected response reaches them.
- This is known as “The Race Condition”.

QUANTUMTHEORY



QUANTUMINSERT

- QUANTUMINSERT (QI) is a the most basic of Quantum missions.
- Targets with this method are selected based on their home network and destination of their web activity; Targeting is IP based.
- We shoot into random web traffic with a throttle in place to prevent overshooting. The hope is to land and HTML redirect to FOXACID inside of an HTML page.
- The problem is, only about 15% of the web is HTML based, these days. The rest of it is JavaScript/Flash/Images/CSS etc etc.
- Because of this, QI generally has a low success rate when juxtaposed with a shots-taken count. It's main advantage is all we need is an IP and web traffic at a good passive collect site for a chance of success.

QUANTUMBISCUIT

- QUANTUMBISCUIT (QB) is another, more pinpoint Man on the Side (Man on the Side) Quantum mission.
- This method utilizes strong selectors within web traffic. The most common of which is a Yahoo email address converted to an L-cookie.
- Because tasking is “strong selector” based, we don’t need an IP address or any other information. All we need is a SIGAD where the user is active and their respective selector.
- Actual methodology itself is very similar to QI. We’re attempting to beat the servers response HTML with our own, malicious HTML back to the target when a tip is received.

QUANTUMDIRK

- A new type of QUANTUM-enabled ops, called QUANTUMDIRK, has recently been developed and is showing great potential.
- This method injects on long polls that are usually based in the chat features on many webmail sites such as Facebook and Yahoo.
- The client (the users browser) sends out a poll request to update information displayed in the browser, such as a chat message box.
- This poll can be open for anywhere from 1 second to 2 minutes. This is an eternity for Quantum, as usually we're working in the realm of 50 ms, so success rate is upwards of 80% (for Facebook).
- Payloads are unique to each service, so more research/maintenance goes into these methods.

Plugins

- The FOXACID server is loaded with plugins. A plugin is just another name for a browser exploit. These are the real heroes of FOXACID.
- A browser exploit can be anything from a native exploit (IE has plenty) to plugin exploits such as Flash.
- These exploits essentially allow native code to be run within the context of the browser. This allows FOXACID to do its magic.
- The process is: The target hits our webpage through some form of redirection. A plugin (exploit) is determined and loaded based on returned JavaScript survey data, and FOXACID is now living under the context of the victims browser (for example, firefox.exe). At this point we're able to drop the files we need to gain persistence.

VALIDATOR

- VALIDATOR is a program that is designed for installation on target computers in a variety of ways.
- Its main function is to serve as a download agent for the Olympus installer, but it has other features that make it useable as an implant with exfiltration capabilities.
- These features include uploading/downloading files to/from a target, obtaining limited system information, finding a path out of the target (either dialup or direct connect).
- VALIDATOR can also delete itself via command or by built-in timer.

MISTYVEAL

- MISTYVEAL is essentially another version of VALIDATOR, and is even referred to in some cases as VALIDATOR version 11.
- It uses the same VALIDATOR LP, and may be deployed via FOXACID, and has been made to look as much as possible like a normal VALIDATOR. However it works differently enough, and has some caveats, hence the reason it was given its own cover-term.
- MISTYVEAL is an internet explorer Browser Helper Object. It is essentially a plugin written in native code that is loaded with Internet Explorer. Because of this, IE must be loaded for MISTYVEAL to run.
- The benefit to this is it is able to utilize any proxies the system is using. If IE can go to google.com, MV can contact the ROC.

FOXACID these days…

- XSS is becoming less and less viable with each passing day. It's just too hard to develop and too easy to circumvent. Because of this (and other technical/OPSEC issues), the bulk spam mission is becoming less and less viable as well.
- The new exploit hotness is Quantum. Certain Quantum missions have a success rate as high as 80%, where spam is less than 1%.
- So, as spam and in-line XSS slowly fade away, the new exploit development push is for those utilizing MitM or MotS capabilities, as well as many other very unique techniques.
- Bottom line – if we can get the target to visit us in some sort of web browser, we can probably own them. The only limitation is the "how".

Fin.

Questions?