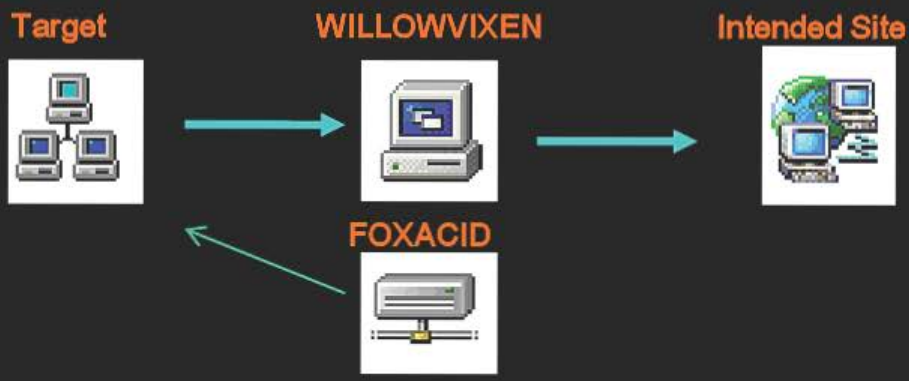
FOXACID these days…

- 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".

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.



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.