Background Info

It is increasingly important for enterprises to thoroughly educate employees on the dangers of using Web browsers. Employees should be aware of acceptable use policies and Internet access security processes. With LUCY you are already able to perform phishing attack simulations and tell if users click on a potential phishing link. But how can an organization determine whether the user's browser is configured using safe settings? If the user accesses the link from a corporate PC, you might be able to answer this question. But what if the user accesses the corporate email from his private workstation or mobile device? One answer is the Advanced Information Gathering, a security testing framework that helps companies deliver effective user awareness training surrounding these issues.

By using techniques similar to common drive-by Malware, testers can assess the security of a target’s internal environment, bypassing the hardened perimeter. Unlike other security frameworks, Advanced Information Gathering looks past the hardened network perimeter and client system and examines exploitability within the context of the one open door: the web browser. Advanced Information Gathering can be used to "safely" expose Web and browser-based vulnerabilities like cross-site scripting (XSS) using client-side attack vectors. If a user clicks on a link that Advanced Information Gathering put there, it will hook the user's browser into the Advanced Information Gathering server which is now also part of LUCY. The tool can also issue commands to the browser, such as redirection, changing URLs, generating dialogue boxes and more. It has the ability to run Malware on the hooked browser IP address and use it as a launching point to infiltrate other computers on the same network, effectively spreading the Malware. With the integration of Advanced Information Gathering into LUCY, companies can now answer two main questions: Would an employee fall for a phishing attack? And if they do, would their browser security settings have prevented more damage from browser exploitation type Malware?

Advanced Information Gathering setup in LUCY

As Advanced Information Gathering is running in the background of a phishing landing page it only will work in scenario's, where a landing page which the user can access, is activated.

To enable Advanced Information Gathering go into the Base Settings of the campaign, select the scenario in which you want to activate it and then go to scenario settings. At the bottom, you will find a checkbox "Advanced Information Gathering" which you need to activate.