The Malware Testing Toolkit AKA LHFC (Low Hanging Fruit Collector)

The idea behind LHFC: testing your defenses

You have invested time, effort, and money in defenses. But, how do you know they are working? Unless you are willing to intentionally get owned or you want to introduce a piece of malware into your environment, you need safe and effective ways to test your visibility. This is where LUCY's LHFC comes in place. There are multiple products that may help detect a malware activity. While it can be detected at the host level, you have another chance detecting it at the network level. These devices include, but are not limited to:

- **Firewalls** (unfortunately, the larger the network, the more difficult it can be to track down a host and determine the functionality of the host. Knowing the functionality can be instrumental in determining if the traffic is normal or suspicious)
- **Web Proxies**
- **IDS** (an intrusion detection system can potentially detect malware activity if a rule is triggered. This is useful as a layered defense, but the traffic will usually have to be something that is previously known and understood in order for a rule to hit. If the IDS has additional intelligence such as traffic thresholds or trending, then there is a low chance it could be detected from this capability)
- **Malware/anomalous traffic detection appliances** (Malware detection appliances go a step beyond traditional IDS by integrating multiple detection mechanisms into one device. Some for example, use an layered detection mechanism with Antivirus definitions, Network signatures, File Reputation, IP reputation & Static file analysis.
- **Security Information and Event Management (SIEM) solutions** (Security Information and Event Management solutions can also help detect the presence of a malware, but it is usually using logs from one or more of the devices mentioned above. The advantage here is greater

visibility by using multiple different types of logs—from hosts to network gear. Additionally, some advanced SIEMs can do trending to detect and understand what is normal and then set thresholds to alert on unusual traffic).

Background Info about APT (Advanced Persistent Threats)

An Advanced Persistent Threat is a Network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization. There are hundreds of millions of Malware variations which makes it extremely challenging to protect organizations from APT. Hackers who employ APTs are a different breed compared to traditional Malware attackers. A real and constant threat to the world's companies and networks, APT hackers tend to be well organized, working together as part of a professional team. Their goal, typically, is to steal valuable intellectual property, such as confidential project descriptions, contracts, and patent information. Generally, APT hackers employ familiar methods, using phishing emails or other tricks to fool users into downloading Malware.

Those who deal in APTs have the following in common:

- **Customized** – An attack on your network is a carefully planned heist. Attackers carry out extensive research and tailor the attack to evade your set defenses, explore your network, and steal determined types of high-value data.
- **Surgical** – Rather than being scattered to the wind, targeted attacks and APTs are carefully delivered to specific targets, often using highly convincing emails intended for a single individual within your organization as a penetration vector.
- **Highly Sophisticated** – Today’s targeted attacks and Advanced Persistent Threats use complex techniques to conceal themselves from your defenses. Once inside the network, they can alter their appearance, switch ports and protocols, and remain undetected for long periods of time as they move around the network to find and steal your data. Detecting these attacks requires a modern advanced solution that provides visibility into every corner of your network.

Since there are millions of Malware types, and even more combinations of attack patterns: How would a IT security officer know if the network can prevent APT attacks? This question can now be answered with LUCY’s Malware Testing Module (initially called Low Hanging Fruit Collector). It simulates APT behavior without harming your infrastructure. It enables you to test your defenses (AV, hardening, monitoring etc.).

So What is the Typical APT Behavior? APTs rapidly escalate from compromising a single computer to taking over the whole environment. They do this by reading an authentication database, stealing credentials, and reusing them. They learn which user (or service) accounts have elevated privileges and permissions, then go through those accounts to compromise assets within the environment. APTs often add stolen data to internal collection points before moving it outside over different channels.

What is LUCY's APT Simulation doing and which questions can the tool answer?

The malware simulation toolkit is an advanced malware simulation suite capable of emulating various

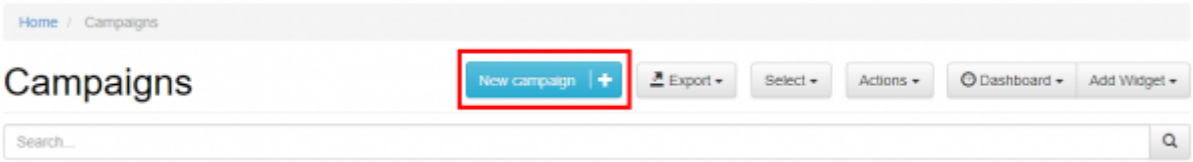
threat simulations. The toolkit is allowing an auditor to access an advanced set of features equivalent to many of the tools employed by criminal gangs. The tool therefore allows the user to perform security checks without involving employees outside your IT Department. Depending on your initial settings the tool can connect to the domain controller searching for passwords in configuration files, access shares in the network, search for sensitive data locally and remotely, search for privileged accounts and for clear text password hashes in the Memory. The Tool may also test if it possible to connect back to the attacker using common attack methods like reverse DNS or HTTP Tunneling Techniques. We simulate all those attack patterns and report the result back to the security officer allowing him/her to identify and close GAPS in the security infrastructure.

Main Questions answered by this tool:

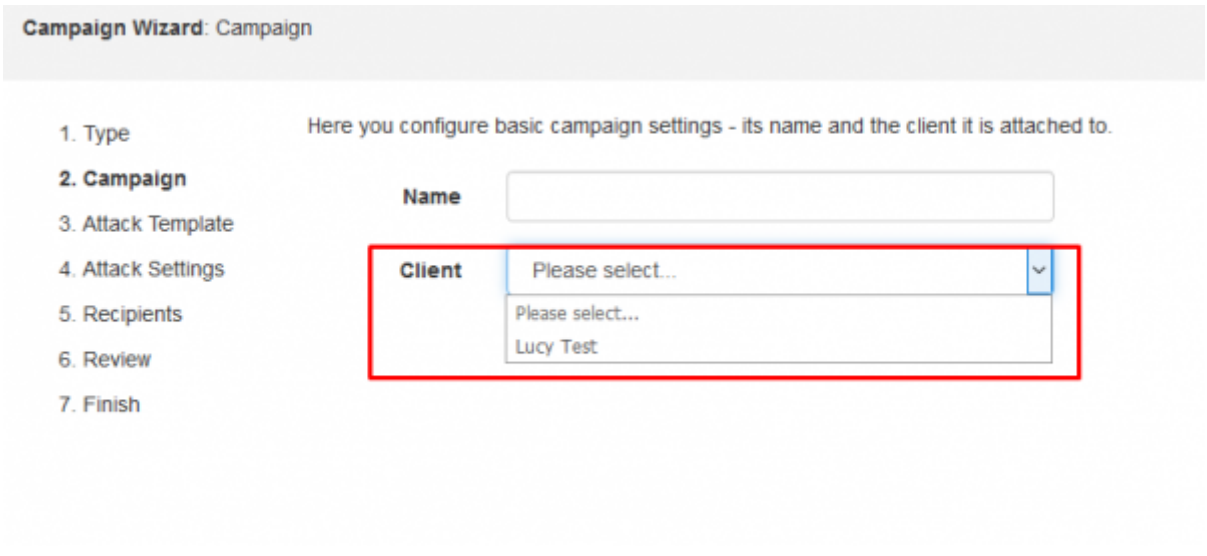
- Does your AV detect known Malware downloads?
- Is your SIEM able to trigger activities from this tool?
- Is Malware able to modify System Settings?
- Is Malware able to communicate to External servers?
- Can Malware access sensitive data on the local host or share drives?
- Etc.

LHFC SETUP

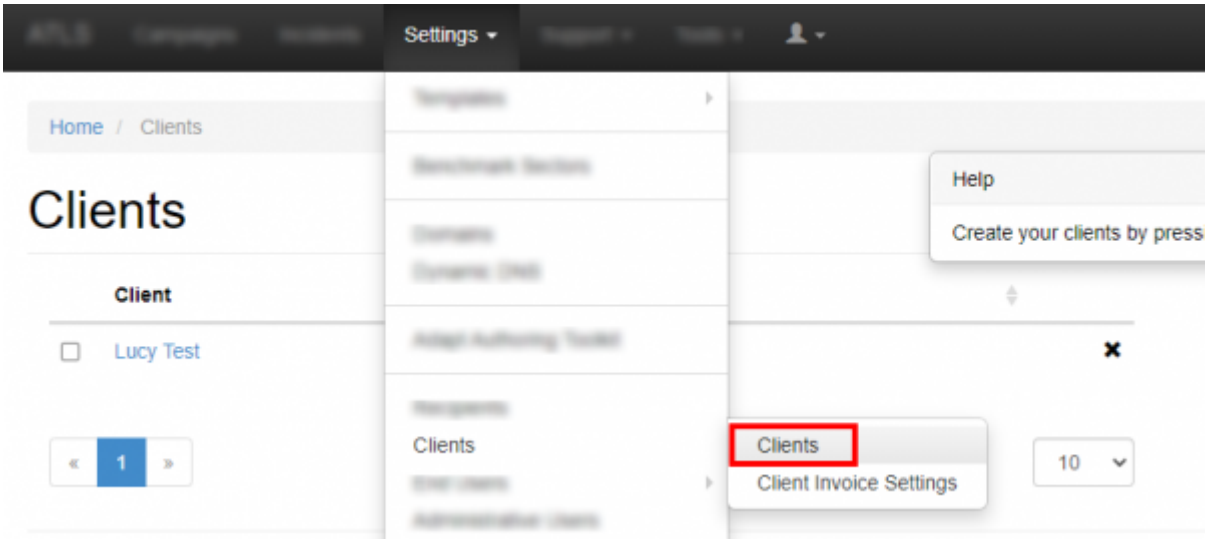
STEP 1 - Create a New Campaign After the login, you can create your first Phishing Campaign by pressing the button "**New**".Choose Your Configuration Mode: You may either continue with the Campaign or the Campaign Wizard. We recommend using the Setup Wizard when used for the first time.



STEP 2 - Select or Create a Client: Create a client or choose the built in client (a client can be your own organization or the company who asked you to perform a phishing test). This is important because you can also create view only accounts which are associated with those clients.

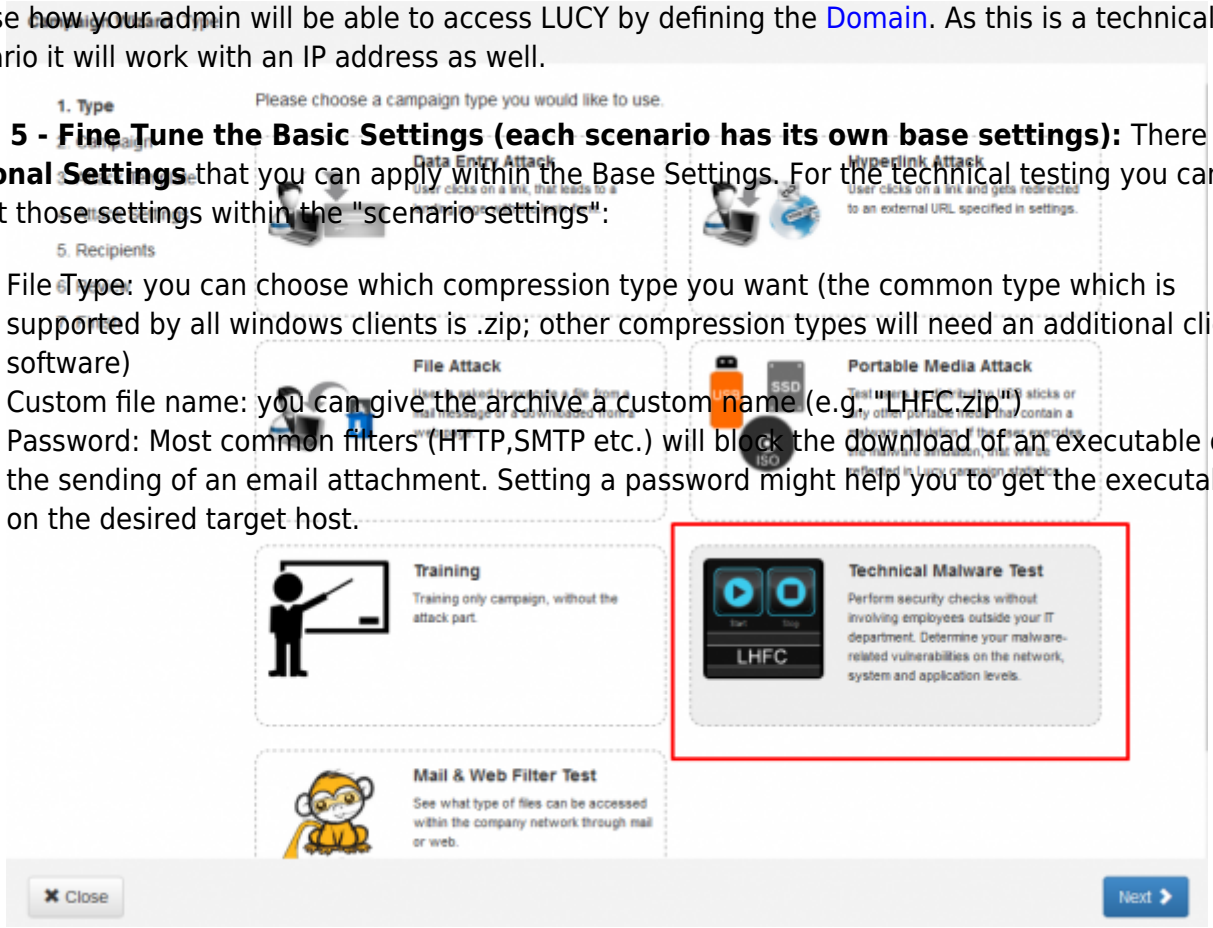


New clients can be created under "clients". In LUCY this is created under settings/clients.



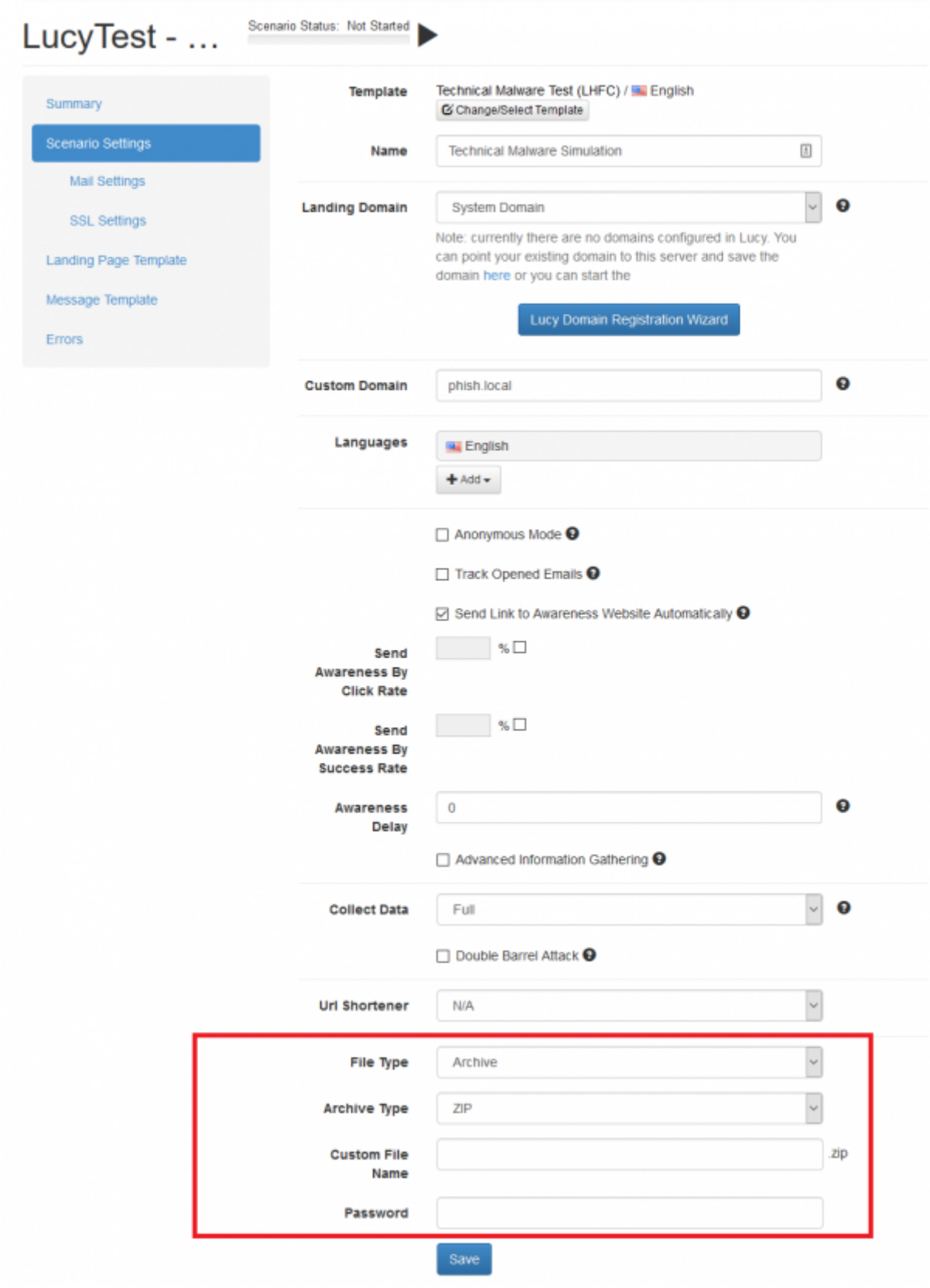
STEP 3 - Select your Phishing Scenario: Now you need to select one or multiple phishing scenarios. Since you are going to do a technical testing you need to pick the technical malware testing template:

STEP 4 - Configure the Base Settings of Your Campaign Once you have selected the scenario, you need to configure the **Base Settings** of the campaign. First give your campaign a name and then choose how your admin will be able to access LUCY by defining the Domain. As this is a technical scenario it will work with an IP address as well.

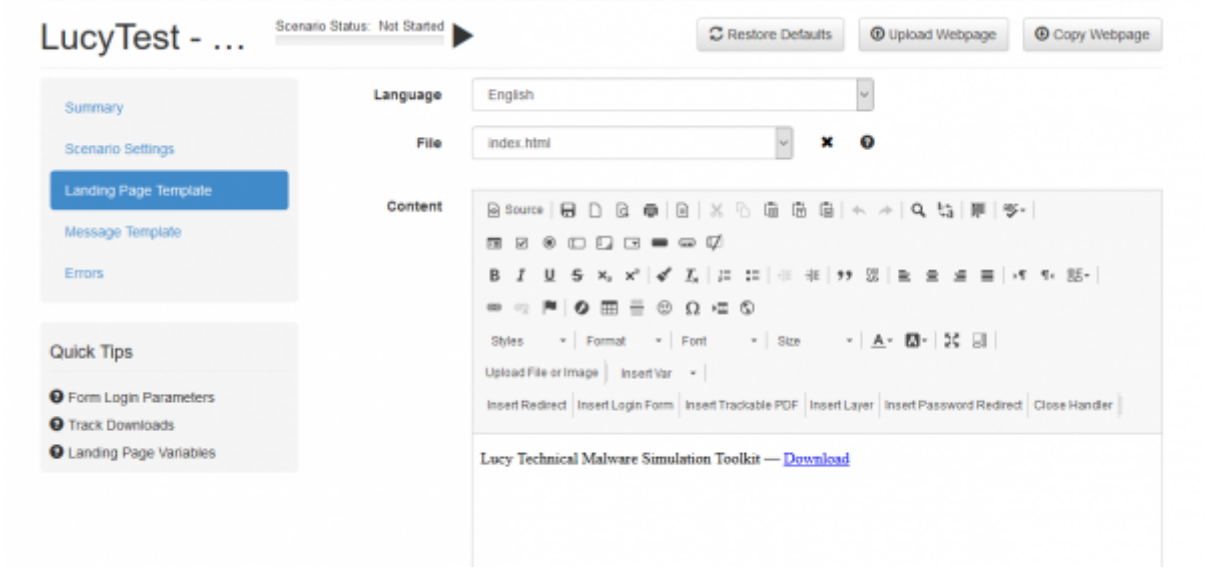


STEP 5 - Fine Tune the Basic Settings (each scenario has its own base settings): There a few **Optional Settings** that you can apply within the Base Settings. For the technical testing you can adjust those settings within the "scenario settings":

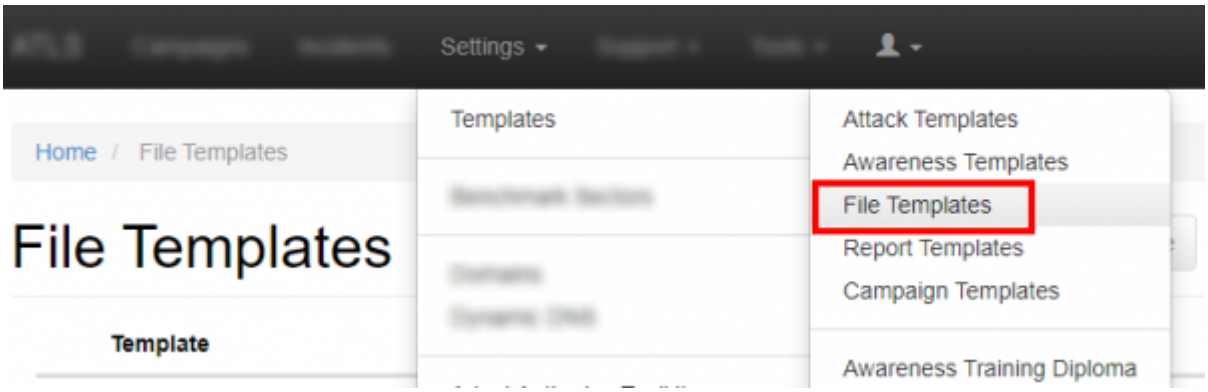
- File Type: you can choose which compression type you want (the common type which is supported by all windows clients is .zip; other compression types will need an additional client software)
- Custom file name: you can give the archive a custom name (e.g. "LHFC.zip")
- Password: Most common filters (HTTP,SMTP etc.) will block the download of an executable or the sending of an email attachment. Setting a password might help you to get the executable on the desired target host.



STEP 6 - Edit the LHFC download page: After saving the Base Settings, you can now Edit the Landing Page. On this page, you can configure the settings of the tool. When downloaded via email or the Web, the tool will be pre-configured with those settings.



All LHFC settings can be saved as general templates as well for future use:



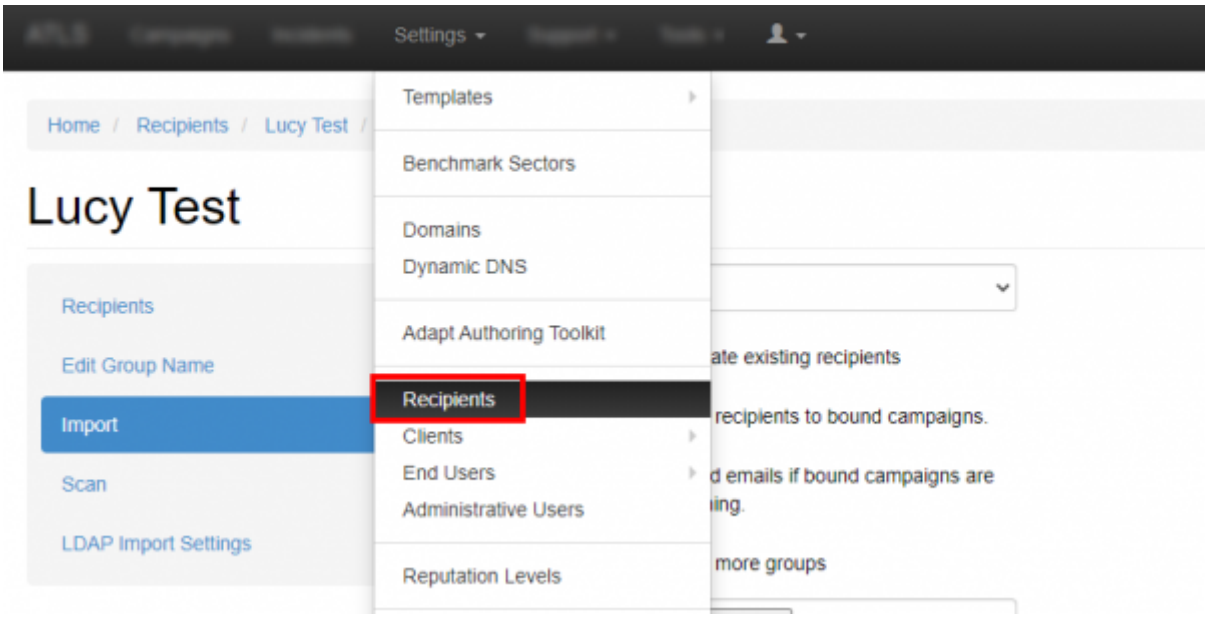
An important setting is “**showgui**”. If disabled the client won’t see the testing suite. Upon execution the vulnerability tests are performed automatically and all data is send back to LUCY. The toolkit process visible in the task manager runs in the background under its name (e.g. file.exe).

STEP 7 - Configure Message Settings (Email): It’s time to setup email communication. Choose your sender's name, email address and subject. The reason why you need a mail recipient is because within the mail you will find a custom download link to LHFC (keep in mind that LHFC is compiled on the fly within the campaign. That's why you cannot just download the tool from the file based templates).

When choosing the LHFC scenario, LUCY will offer you additionally to send the tool via mail. If you already have chosen a landing page where LHFC can be downloaded it is not necessary to attach it via mail as well. Therefore if you don't want LUCY to send the file via mail choose "NA" within the malware simulation template dropdown menu.

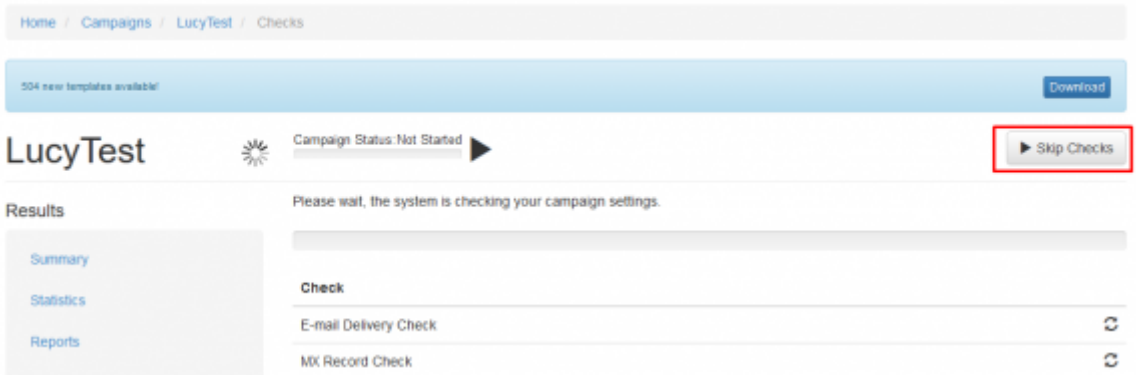
STEP 8 - Add Recipients to Your Campaign: You need to create the Recipients List in the Menu item "Recipients". In this case it would be the account of an admin, who will execute the file on the

target host.

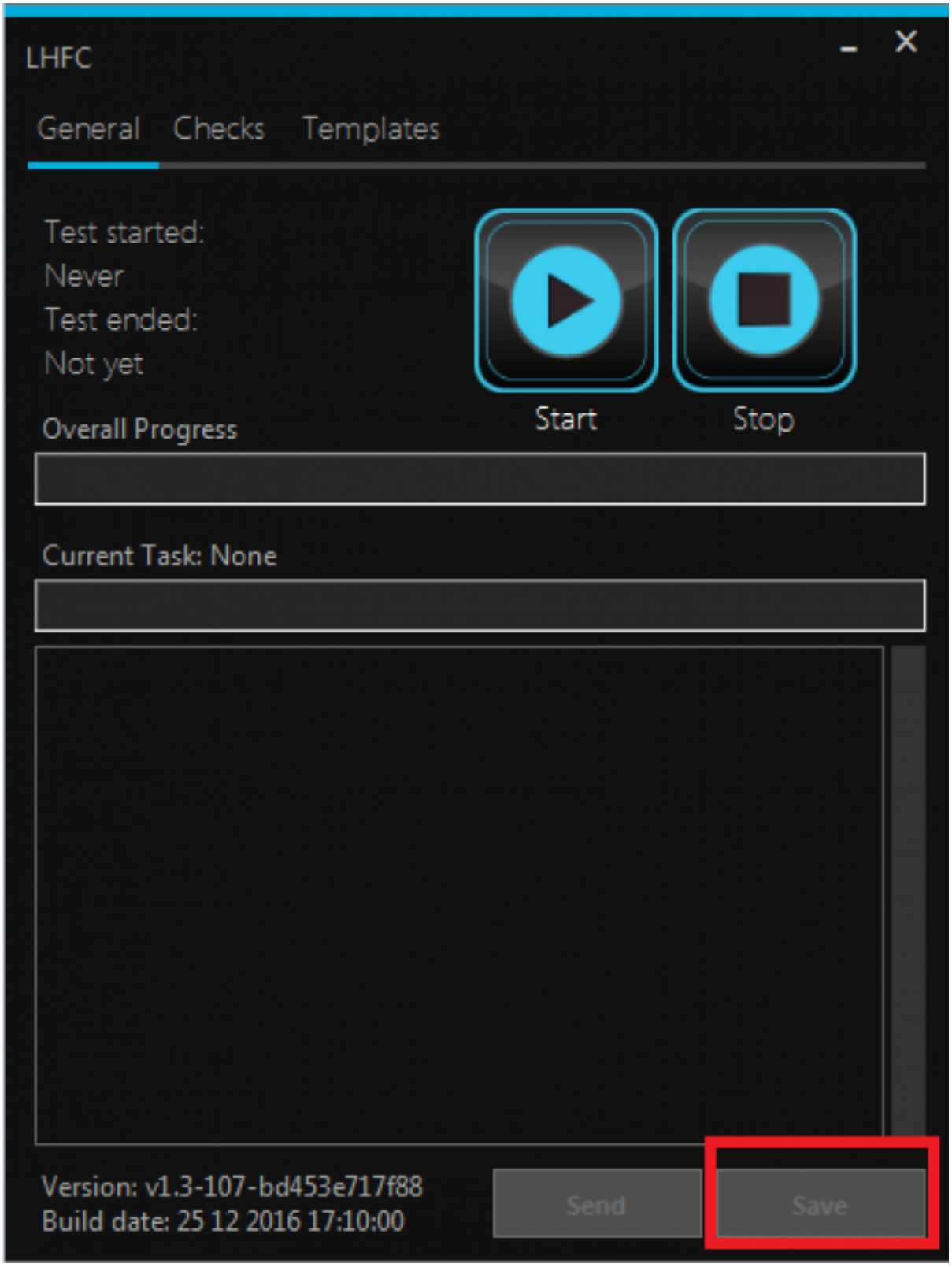


Please read the Recipients Settings Chapter for more configuration options.

Step 9 - Start Your Campaign: Now you are ready to start. If you want to skip the checks, press "Skip Checks". Your first recipients should receive the emails within seconds. Please read the Start Campaign Settings Page for more configuration options. If you experience any problems with starting/running your campaign, please Consult the Troubleshoot Section first.



Step 12 - Track the output: Click "Statistics" within your campaign. Please read the Statistics Chapter for more configuration options. The output from LHFC can be found under "statistics/collected data" in case you have configured, not to show the GUI. An alternative is to create an report directly from the GUI. If you click on save report it will create a folder containing a html report within the same directory of LHFC. The save button is only available after all tests have been completed.



AV problems & security warnings

1. Antivirus flagged the tool as malicious: some antivirus solutions might flag the tool as a virus or suspicious file. Especially behavior based AV's may show such alerts. It means that your AV is able to detect certain methods used by the tool that are commonly used by malware. This is a good indication your AV is able to detect also malicious code without depending on signatures. Since the toolkit imitates malware activities this alert is not wrong by default. You can ignore it or if necessary disable your AV if this prevents you from completing the malware assessment

test.

2. Windows Security Warnings: there are multiple security warnings upon opening or execution of the file. If you open the file as a mail attachment or download, window will warn you that executable are dangerous and can harm your computer. This warning applies to all executable content and is not related to the toolkit. You can ignore this warning or adjust your windows security settings.

MALWARE TESTING TOOLKIT SINGLE CHECKS

Check Name	Background Info	Check Details
Command line access test	All tools tested within the custom malware test are custom made and use windows functionalities (not exploits) to access data within the protected network. This makes them harder to detect. Still they are not built in a way that they hide their malicious functionality (e.g. they post back data to a server using long base64 strings in a fix rhythm).	This tool will allow executing commands which are hardcoded into the code. We verify if an external program can initiate the shell and execute commands.
Recent documents access	If a malware is able to access the recent doc path it will learn a lot about what files were recently used and where they are stored. The tool is able to use the cached user credentials to access the last documents (locally or on a share drive).	This Tool will read out the absolute paths from the recent docs directory and try to access it.
Outlook access	An external tool is able to overwrite the security warning from outlook and access all your mails or even send mails via exchange on behalf of the user that got attacked.	This tool will use Outlook MAPI, overwrite the security message and try to access the last message in the inbox.
Screenshot test	A Malware that can make screenshots might even record on screen activity (like passwords entered within an onscreen keyboard).	This tool will try to make screenshots of the current desktop.
Webcam access test	A Malware that can make pictures with the webcam might be used to spy on users or to blackmail them.	This tool will try to take a picture with the webcam.
Microphone check	Malware is capable of not only embedding itself onto computer systems without being identified by traditional anti-virus applications, but able to execute total surveillance and monitoring that includes turning on your camera and microphone, copying your data, and recording emails and chat conversations.	We will test if it is possible for a third party application to access and record from an attached or built in microphone.

Check Name	Background Info	Check Details
Access to the Internet via IE	Inside-Out attacks try to initiate network connections from the trusted (corporate) to the untrusted (Internet) network. These attacks require that an “insider” execute code. This is either because the person that executes the code is unaware of security issues and doesn’t realize that an application can do anything to their system within the limits of the access that is granted to that user or purposely executing this code to bypass security restrictions (for unknown purposes). The technique derives its stealthy nature by virtue of the fact that it sends traffic through ports that most firewalls will permit through. In our scenario we used http as the protocol to send out the data. Even though an HTTP connection was designed to provide web services to users, HTTP is simply data passing between a client and a server with headers to identify it as web content. This means that an HTTP connection has become conduit for a full-fledged bi-directional connection between two networks. Inside out attack consists of three steps (Getting the backdoor in the network - delivery, Executing the backdoor by the user - execution, Sending the data out - output delivery)	We verify if a malware is able to connect back to the internet using the internet explorer via HTTP.
Access to the Internet via http	Malware could have its own custom web browser embedded.	We verify if a malware is able to connect back to the internet using an own HTTP class. This simulates a little portable tool with its own build in custom browser.
HTTP access with IE proxy	Malware could have its own custom web browser integrated and read out proxy details from registry.	We verify if a malware is able to connect back to the internet using an own HTTP class with the current proxy settings.
HTTP access with IE proxy with credentials	Malware could have its own custom web browser integrated and read out proxy details from registry and access the stored credentials	We will try to access the internet using the default credentials stored on the system. This simulates a malware which can bypass security controls like integrated windows authentication on a corporate proxy.
HTTP access with proxy from Firefox settings	In case the company disabled IE the malware could try to access the internet using Firefox.	We verify if a malware is able to connect back to the internet using an own HTTP class with the current proxy settings accessed in a different browser (Firefox).

Check Name	Background Info	Check Details
Access to the Internet via https	The malware might hide its activity by using an encrypted connection.	We verify if a malware is able to connect back to the internet via HTTPS using an own HTTP class simulating a malware that has a built in custom web browser to access the internet.
DNS tunneling test	By using DNS tunneling, a malware will be able to access a remote server via http even though the proxy is blocking the website. Normally when you consider a proxy server, all the HTTP traffic will be received by a proxy server, but no DNS traffic will fall on a proxy server. So exploiting this DNS traffic will allow us to use all blocked websites as well. So on a DNS tunnel, data are encapsulated within DNS queries and replies, and the DNS domain name lookup system is used to send data bi-directionally. Therefore, as long as you can do domain name lookups on a network, you can tunnel any kind of data you want to a remote system, including the Internet. We can use DNS records (NULL*TXT*SRV*MX*CNAME) to encapsulate (downstream) IP traffic.	We will test if we can resolve an external 3rd party domain on the client directly
ICMP test	ICMP tunneling works by injecting arbitrary data into an echo packet sent to a remote computer. The remote computer replies in the same manner, injecting an answer into another ICMP packet and sending it back. The client performs all communication using ICMP echo request packets, while the proxy uses echo reply packets.	We can send various ICMP packets with some random data and random sizes inside to an external host.
SMTP test	SMTP is a common protocol for malware to distribute among users	We verify if a malware is able to connect to the internet directly using a protocol like SMTP.
FTP test	A common protocol for malware to use to export collected data is FTP	We verify if a malware is able to connect to the internet directly using a protocol like FTP.
SSH test	Using SSH a malware could establish an outbound connection that cannot be logged	We verify if a malware is able to connect to the internet directly using a protocol like SSH.

Check Name	Background Info	Check Details
Check mounted shares	An attack can use one or many different methods to try and replicate between computer systems. When computers were provided a mechanism to connect to each other directly via a network, malware writers were presented with another transport mechanism that had the potential to exceed the abilities of removable media to spread malicious code. Poorly implemented security on network shares produces an environment where malware can replicate to a large number of computers connected to the network. This method has largely replaced the manual method of using removable media.	We will try to access known shares and test their access security and in a second step we will scan within the same network range as the host access to shares as an anonymous user.
Check non http on 80/443 port	Attack techniques have evolved to where traditional packet filtering firewalls, proxies, and even intrusion prevention systems are dramatically less effective at securing a corporate network. The common flaw in most perimeters is that they are designed to thwart inbound session establishment, while being relatively permissive in what they pass towards the Internet. If a malware can only contact remote hosts on certain ports (example: port 80), the solution would be to contact remote hosts via allowed port. This method is called HTTP tunneling, which is a method of evading network firewalls. When people hear the words HTTP tunnels they often think quite literally. To them it is some data being transported inside of HTTP data. This line of reasoning is in actuality not far off from the truth. Data is being transported via port 80 and that port is normally associated with HTTP, but that is where the literal interpretation mentioned above ends. Typically, data is not encapsulated within the HTTP protocol itself, but merely sent over port 80.	In this test we will try to establish a SSH connection to our host on port 80 & 443 and execute a few unix commands.

Check Name	Background Info	Check Details
Check domain shares	An attack can use one or many different methods to try and replicate between computer systems. When computers were provided a mechanism to connect to each other directly via a network, malware writers were presented with another transport mechanism that had the potential to exceed the abilities of removable media to spread malicious code. Poorly implemented security on network shares produces an environment where malware can replicate to a large number of computers connected to the network. This method has largely replaced the manual method of using removable media.	We will try to access known shares and test their access security and in a second step we will scan within the same network range as the host access to shares as an anonymous user.
Port scan	The malware, after infecting a host, will try to scan neighboring IP addresses to find the next targets. The malware writers do not depend on standard commands, as monitoring and restricting the commands might lead to containment of the malware Instead they try to evaluate the next host by scanning all the IP addresses in the address space of the host.	We will scan a small selection of hosts in the same network for some common ports.
Force firewall drops	A malware might try to connect on some random unknown ports back to the attacker	We will test if an outbound TCP connection on a very high port is possible. Usually such connections are suspicious and should be dropped. Your SIEM should be able to detect such abnormal network activity.
Direct DNS access	In this test we verify if a malware would be able to perform a DNS tunneling attack by simply resolving a third party domain from the client. If you see that the server resolves to an IP address it means that your client is able to make DNS queries to external domains using internal DNS forwarders. This is a basic requirement for a malware to communicate with an attacker in the internet via DNS. If you want to test if your SIEM is able to trigger real world DNS tunneling traffic please use the test "DNS tunneling test".	We will test if we can resolve an external 3rd party domain on the client directly.

Check Name	Background Info	Check Details
Suspicious communication	When you visit a malicious website, a number of actions may occur. A search result in Google may mark the result with the message "This website may harm your computer" and prevent you from visiting the address.The web browser, such as Internet Explorer, Firefox and Chrome, maintain their own list of known malware sites and will prevent or warn you from accessing the site. So usually you should be safe from known malware sites. But in this test you also want to check if your SIEM will detect suspicious GET requests to malware related sites.	First we try to parse a current list of a few malware releated websites like https://www.malwaredomainlist.com. The we try to make simple GET requests to a few selected sites to see if a connection to such malicious sites gets triggered.
File operations on share	Ransomware is malicious software that cyber criminals use to hold your computer or computer files for ransom, demanding payment from you to get them back. Sadly, ransomware is becoming an increasingly popular way for malware authors to extort money from companies and consumers alike	We will test on a mounted share (if detected) if multiple hundret write/read operations within a short time windows from the same source are possible.
IRC check	Internet Relay Chat (IRC) is an application layer protocol that facilitates communication in the form of text. The chat process works on a client/server networking model. These clients communicate with chat servers to transfer messages to other clients. IRC is an open protocol that uses TCP. Channels on a network can be displayed using the IRC command LIST. IRC is wideley used anmong the hacker community to share information.	We will test if we can connect to an external IRC server and channel, the send a couple of messages and after waiting a short period disconnect from thet server.
OS version	This check is only informational	In this step we try to identify which OS we are connected to.
Search for local administrators	Malicious Software infections on the client. If a user has local administrative rights they are able to disable the security enhancements that protect them (Firewall, Bitlocker, Antimalware etc.).	This check verifies if there are users which have local admin rights on the PC.
Firewall test	If someone brings in a laptop that is infected, it will try to infect everyone on the LAN, bypassing the corporate firewall. If you have local firewalls also running it will not successfully pass the virus on.	We verify is the firewall is running and then test, if it can be disabled.

Check Name	Background Info	Check Details
Antiviruses test	Even if you’re careful, you should use an antivirus. It’s possible you may be infected by a zero-day vulnerability in a browser plugin like Adobe Flash or your web browser itself. Even if you keep your browser updated, you may be infected by a new, unpatched vulnerability just by visiting a web page. Now, this isn’t extremely common — but it does happen. An antivirus is an important layer of protection, as it will help protect you even in the face of such vulnerabilities.	We verify if there is an Antivirus product running and if it can be disabled.
Downloading some viruses	Simda is a multi-component malware family that includes Trojan, backdoor, password-stealing, downloader and file-infector variants. It is very rare for a single malware family to possess all of these characteristics. Simda was first seen in mid-2009 with samples detected as Backdoor:Win32/Simda.A. This variant allows a remote user to connect to an infected machine and perform various malicious actions, such as stealing user credentials and taking screen grabs. At the same time, the backdoor component drops a malicious DLL that is injected into Windows processes to gather user information. The DLL is detected as PWS:Win32/Simda.A. The backdoor variant can exploit vulnerabilities to gain elevated privileges to perform more restrictive behaviors, such as Windows process injection. It may also gain admin privileges by trying to brute-force the administrator password with a dictionary attack. Once it gets access, it gathers user information such as user names and passwords, logs keystrokes, and takes screen grabs. The backdoor connects to its command and control server to report infection and download a configuration file. Once connected, a remote attacker can collect the stolen information and run other commands.	In this check we test if a known dangerous virus called SIMDA can be Downloaded. In case the download works we will test if the downloaded file can be placed under “documents” folder.

Check Name	Background Info	Check Details
Access to hosts file	Imagine clicking on www.thewindowsclub.com and seeing a completely different web site load in your browser. Malware can redirect Web addresses on your computer by altering your hosts file. This is referred to as the Host File Hijack.	We verify if write access to the host file is granted
Add new user	Windows 8 also introduces the ability to create and login as a Local account or a Microsoft account. A Local account is an account that is local to your computer and is not integrated into any of Microsoft's online services. This account is the same as what was used in previous Windows versions. A Microsoft account, which was previously known as a Windows Live ID, is an online account that you register with Microsoft and that allows you to integrate all of Microsoft's online services into Windows 8. These services include the Windows Store, SkyDrive, Calendar, Hotmail, and the ability to synch your account settings and preferences to other Windows 8 machines you may use. Ultimately, there is no wrong choice when selecting the type of account to use as you have the ability to switch between a Microsoft account and a local account at any time. If a malware is able to create users it might “backdoor” the system and allow access that bypass other security mechanism in place.	We try to add local users.
Analyze patch level	If there is a patch missing and an exploits exists the system can be easily compromised.	The most obvious thing we need to look at is the patch level. We will compare the patches with current exploits. As always with Windows, the output isn't exactly ready for use. Here we look for privilege escalation exploits and look up their respective KB patch numbers. Such exploits include, but are not limited to, KiTrap0D (KB979682), MS11-011 (KB2393802), MS10-059 (KB982799), MS10-021 (KB979683), MS11-080 (KB2592799).

Check Name	Background Info	Check Details
Passwords in configuration files	If passwords can be accessed an hacker or a malware might be trying to use them to elevate their privileges.	We have a look at mass rollouts. If there is an environment where many machines need to be installed, typically, a technician will not go around from machine to machine. There are a couple of solutions to install machines automatically. What these methods are and how they work is less important for our purposes but the main thing is that they leave behind configuration files which are used for the installation process. These configuration files contain a lot of sensitive information such as the operating system product key and Administrator password. What we are most interested in is the Admin password as we can use that to elevate our privileges. Typically these are the directories that contain the configuration files (however it is a good idea to check the entire OS).
Passwords in policies	GPO preference files can be used to create local users on domain machines. When the box you compromise is connected to a domain it is well worth looking for the Groups.xml file which is stored in SYSVOL. Any authenticated user will have read access to this file. The password in the xml file is "obscured" from the casual user by encrypting it with AES. It is only obscured because the static key is published on the msdn website allowing for easy decryption of the stored value.	On the recommendation of Ben Campbell we are adding Group Policy Preference saved passwords to the list of quick fails.

Check Name	Background Info	Check Details
Check alwaysInstallElevated	Malware could install itself permanently even though it does not run under admin rights	We look for is a registry setting "AlwaysInstallElevated". If this setting is enabled it allows users of any privilege level to install *.msi files as NT AUTHORITY\SYSTEM. It's a Group Policy setting for Windows Installer that, if enabled, runs any Windows Installer Package (.msi file) that the user launches under the all-powerful Local System account. The idea behind this setting is to allow users to install applications that they need, without directly granting the user administrative rights. However, it makes no distinction between a management-approved, digitally-signed installer of a business-critical application from a trusted publisher, and an unsigned MSI wrapper around a malicious script. That's a real problem. Anybody can create an MSI – it doesn't take deep knowledge, expensive developer tools or admin rights. In an environment with this setting, any user who wants admin rights can get them, and any malware that runs can silently take over the whole system.
Test write access	Permissions are what you configure for resource access. A resource is a file, folder, Registry key, printer, or Active Directory object (if on a Domain Controller). Permissions are what you configure on the Access Control List (ACL). Permissions define "who" can do "what" to a resource.	We verify if a malware has write access to important system files.
Access to autostart	The Windows Startup folder can include shortcuts, documents, executable, or other types of files and programs to be launched when Windows is started. The current logged on user can view startup folder inclusions through the Start menu. Except in the case of rootkit-enabled malware, it's often possible to remove an infection (at least the active components) by removing their startup points. Following is a list of some of the more frequently used autostart entry points in Windows, including startup folders, registry keys, and ini files.	We verify if we are able to place an exe in the autostart folder.

Check Name	Background Info	Check Details
Mimikatz	Mimikatz is a slick tool that pulls plain-text passwords out of WDigest interfaced through LSASS. The key feature of this tool that sets it apart from other tools is its ability to pull plain-text passwords from the system instead of just password hashes. If your intention is to stay within the Windows environment and pass the hash this may not be that big of a deal. However, if you are exploring the curious case of password reuse across different environments—the plain-text password can be quite useful. For example, you have compromised a “Good for Enterprise” server that has a web interface which is not tied into AD single sign on. It might be useful to have the Good admin’s plain-text password to try against the Good for Enterprise web interface. Additionally, unless you have significant computational power, you may not crack an NTLM password hash—thus pulling the plain-text proves useful once again. After a user logs on, a variety of credentials are generated and stored in the Local Security Authority Subsystem Service, LSASS, and process in memory. This is meant to facilitate single sign-on (SSO) ensuring a user isn’t prompted each time resource access is requested. The credential data may include NTLM password hashes, LM password hashes (if the password is <15 characters), and even clear-text passwords (to support WDigest and SSP authentication among others. While you can prevent a Windows computer from creating the LM hash in the local computer SAM database (and the AD database), though this doesn’t prevent the system from generating the LM hash in memory. WDigest is a DLL first added in Windows XP that is used to authenticate users against HTTP Digest authentication and Simple Authentication Security Layer (SASL) exchanges. Both of these require the user’s plain-text password in order to derive the key to authenticate—thus why it is stored in plain-text.	We try to access clear text credentials in memory within this check

Check Name	Background Info	Check Details
Autorun	According to a biannual Security Intelligence Report from Microsoft, AutoRun—the feature in Windows that automatically executes files when you plug in a USB or connect to a network—accounts for almost half of all malware infections.	We test if Autoplay is enabled
Cscript decoder test	Malware writers know that once their code is understood it most likely to be detected by anti-malware applications. To delay detection by such applications, they resort to a wide range of techniques. Javascript for example can also be used by malware writers to infect innocent users. In recent years, the malware, virus written in scripting language are spreading rapidly worldwide. Windows applications and processes may be automated using a script in Windows Script Host. Unfortunately, Viruses and malware could be written to exploit this ability as well: an attacker can generate some code (example JavaScript code) and compile an executable using windows cscript.	In this test we verify if we are able to create an executable using window’s cscript.
Execution in temp folder test	Lots of programs, legitimate or otherwise, will want to execute from the temporary folder in windows (%temp%). Installers typically unpack themselves to a subfolder of this when you run setup.exe on a compressed installer archive. So the reason why malware likes to execute from these locations is because legitimate software likes to execute from these locations. They're areas that the user's account should expect to have some level of access to.	We will place and execute an executable within the temp directory.
Process spoofing test	Malware tends to use process names that look strikingly similar to common process names. It's more like spoofing them into a name that you might think is the real thing but it’s not. Sometimes the names are actually valid but the path is different.	We will create a new process using a known windows process name.

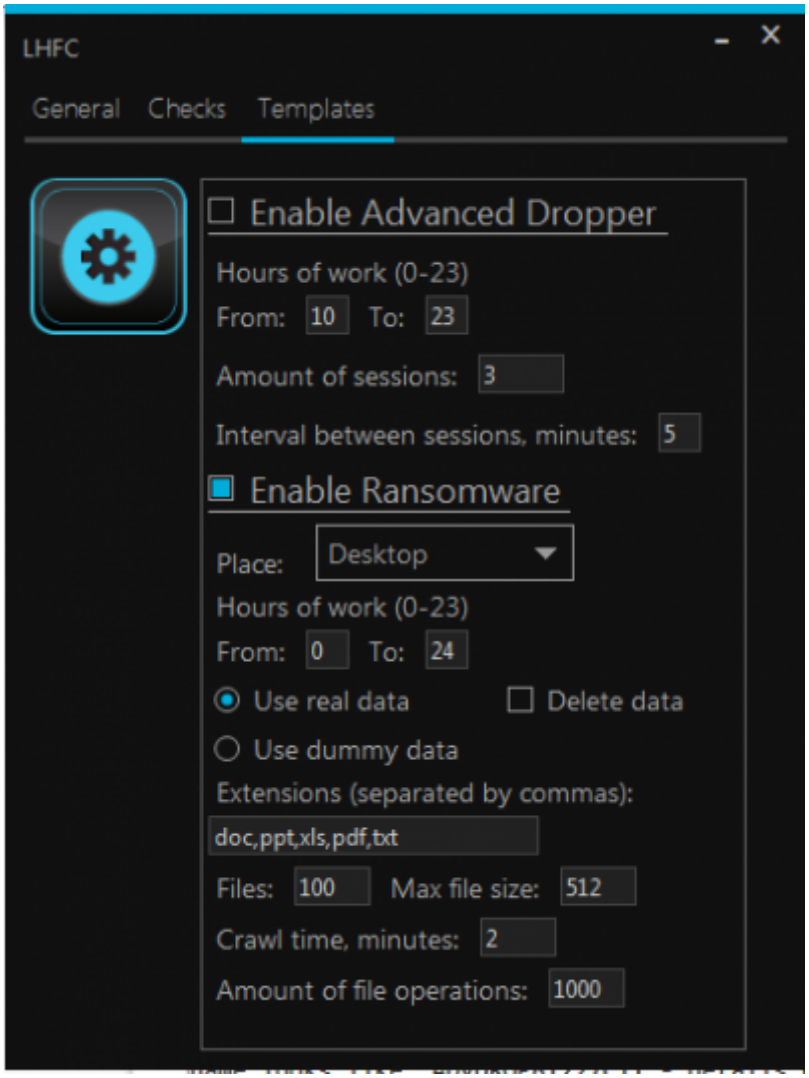
Check Name	Background Info	Check Details
Check service install	A common misconception when working on removing malware from a computer is that the only place an infection will start from is in one of the entries enumerated by some AV solution. Malware also attempt installing a part of themselves as a service (please note it will need some advanced rights to do so). When cleaning a computer the standard approach is to clean up the Run entries and the other more common startup entries first. For the most part, that will be enough to remove the infection. The problem arises when the log looks clean and yet there are still problems. One place to continue looking for the infection is in the operating system's services to see if there is a service that does not belong there and could possibly be loading the infection. A service is a program that is automatically started by Windows on startup or through some other means and is generally used for programs that run in the background.	We try to register a new windows service.
Check task manager killer	The Task Manager is one of Windows tools that help to monitor and manage operating system. You can use it to forcefully quit an application that hangs or stop a single process ran in the OS environment. So, you can stop malicious processes with your Task Manager as well if this windows utility is not blocked by the malicious program that infected your PC. Malicious programs often block Task Manager and other system tools.	We will test if your task manager can be blocked and if this activity will trigger any event in your monitoring system.

Check Name	Background Info	Check Details
Check system restore point	Invalid registry entries can be added by viruses looking to infect and create havoc on your system. Viruses can also disable your Windows System Restore feature. The system restore feature exists in Windows operating systems. This feature ensures that program installations and updates can be rolled back in the case that something goes wrong. If you're a little tech-savvy, you know that you can go into your computer's System Properties to run a System Restore if you ever want to revert your computer or files back to a state before the current day, undoing all changes made (by you or malware) in the days after your selected Restore Point. But some viruses can actually disable your System Restore feature, making it impossible to restore system properties to a state prior to the moment things were changed by you or the Virus. In this test we try to disable the system restore feature. This usually is only possible with advanced user rights.	We will attempts to disable the windows system protection.
Check hidden process	Malware, especially rootkits are one of the advanced species in today's every changing technical world. They are known for their sophisticated techniques to hide their presence often evading their detection from top notch Antiviruses and detection tools. Antivirus solutions often hit the wall when it comes to Rootkit detection and there is a greater need for dedicated Anti-Rootkit tools. Malware can use different techniques to hide their process and to prevent its termination. One such method is to hook the NtOpenProcess function (OpenProcess API internally calls NtOpenProcess) and return negative result whenever Anti-Rootkit application try to open such process. As a result Rootkit process will remain hidden from any process viewer tools. This is just one of the method and often you will find more such internal functions such as NtQuerySystemInformation being hooked to filter out their process from the list.	We will hide a process for a few seconds.

Check Name	Background Info	Check Details
Harvest IE passwords	Having your Web browser remember your passwords and/or credit card details can be convenient, but it poses some security risks. Internet Explorer stores two type of passwords, Autocomplete and HTTP basic authentication based passwords. Autocomplete passwords are normal website login passwords such as email, forum websites. HTTP basic authentication password is the one which is required to login to website itself.	We try to access IE passwords using different methods.
Keylogger check	In its simplest form, a keylogger trojan is malicious, surreptitious software that monitors your keystrokes, logging them to a file and sending them off to remote attackers. Keyloggers and other forms of remote-access trojans tend to be the most determined malware, taking extra steps to stealth its presence, including through the use of rootkits.	We will run a custom keylogger for a few seconds.

Malware Testing Templates

Beside single checks LHFC is also able to perform tests based on a template (please note that it is not possible to run single checks and a template at the same time). Currently there are two templates implemented which are described in detail.



Advanced Dropper Template

This template simulates some aspects of malware behavior like the famous finfisher but without any modifications to the system (hooks, MBR changes etc.). All activities will run with standard user rights. The tool will first create a subfolder in the TEMP folder (its name looks like TMP6BCF227D - details will be written in the report), put in the subfolder a file called malware.jpeg. Then the image will be decrypted and launched from the current location. The file it contains is the standard LUCY dropper (reverse HTTP/HTTPS connection using the browser to make base64 POST requests). The new process name is then called 'malware.jpeg'. The dropper also will create a log file "log.txt" that is located in the TMP* folder. Next the process creates a hidden folder in the TEMP (its name looks like "ADVDROP81227C11"- details will be written in the log.txt) and then begins to harvest information. For each session of the information gathered the dropper creates a subfolder in the hidden folder (its name look like "82C89047" so you should see something like" ADVDROP81227C11\82C89047" in the temp folder). In this subfolder the dropper places harvested files and later encrypts them. After the encryption the LUCY URL is called and the dropper will send files back to LUCY via POST (HTTP or HTTPS - depending on your campaign settings).

There are LUCY variables for this template that can be defined. For example we can set the working hours (currently set from 10:00 to 00:00, so if you launch the template in 9:00 then the dropper will wait until 10:00), amount of sessions (currently set to 3, so the dropper will make 3 subfolders in the ADVDROP81227C11 with its data sets), intervals between sessions within a minute (currently 5 minutes, so the dropper will work about ~10 minutes) and the maximum size of the file for the tool to send/encode within the POST requests.

Ransomware Template

Ransomware is a type of malware that prevents or limits users from accessing their system or files. This type of malware forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems, or to get their data back. Some ransomware encrypts files (called Cryptolocker). Other ransomware use TOR to hide C&C communications (called CTB Locker).

Our template simulates a type of ransomware that locks files like documents, spreadsheets and other important data and then make a encrypted copy either on a share drive that has write access or locally. The idea behind this template is to find out if the information gathering activities or the big amount of read/write operations on a drive from a single PC trigger any sort of alarm in your monitoring system.

Within the tool you can specify a few settings:

- Specify a file List to search (default: doc,ppt,xls,pdf,txt)
- Specify to work with dummy data or real data the tool discovers in the network
- Set the maximum file size to process (default max 512 KB)
- Set the number of Files (Default max 100) to copy
- Set timing options (like when to run, which time period & maximum time to crawl a drive)
- Set an option to leave a copy of data on PC/Share or delete it after running. When the ransomware works with dummy data, it deletes the files right after the creation even if "Delete data" is unchecked. (it should not delete any data when it works with real data). This setting is necessary because the ransomware creates many files with relatively big sizes. By default it creates 1000 files with 512 kb size each, so it will be 0.5 Gb overall.

When started the tool will create a separate executable (example: C:\Users\Test\Desktop\2afbaff8-f048-445c-bcf3-05b7d8d33133\rnsmw.exe) which will try to discover local and remote share drives (as an anonymous and an authenticated user). LHFC will then make read/write tests on the discovered dives. If the setting "work with real data" is selected LHFC will search recent docs to get a file list as well. If a write right on a share drives exist, LHFC will place a folder "LUCY RANSOMWARE SIMULATION" there. If no write right exists, LHFC will create a folder locally based on the path specified in the settings. In real data mode LHFC will make a COPY of files which were previously enumerated (the original files will not be touched by tge tool) and then encrypt the COPY and place in that new folder. If you selected "leave data" you can look at the harvested information using the SimpleXorEncrypter.exe. All harvested files can be decypted with the tool. So in order to unencrypt a file you should use this unencrypter. It is a command line tool. For example, command "SimpleXorEncrypter.exe -u avdata.txt avdata_unencrypted.txt" will unencrypt the file avdata.txt.

When the ransomware ends his work it writes in the log "The programm will exit." (except if the process was killed or it was impossible to write into the log file). Until that it should be considered that the ransomware is still executing. On every run the ransomware should create a new folder for the log. The logfile looks like in this example: