# OUTBOUND COMMUNICATION REQUIRED BY LUCY SAAS: SORTED BY TYPE OF ACTION

LUCY SaaS might initiate certain communication channels to servers on the internet:

- **License Server**: Local License Server will download updates, templates and upload generalized workstation billing stats to our central license server over HTTPS protocol. Local License Server will also serve as an OS package mirror, so it will fetch updated OS packages from our central license server as well. No information about your particular workstations, clients, accounts or anything else is transmitted to our server.
- **Vulnerability Checks**: If you need the client vulnerability detection feature enabled, you should also allow port 80 connection to static.nvd.nist.gov (129.6.13.177). That host is used to download NIST CVE database with vulnerabilities. This feature is not critical and may be disabled.

# OUTBOUND COMMUNICATION: SORTED BY PORT & IP

Local License Server

| IP | Function | Port | Protocol |
|---|---|---|---|
| 162.55.130.83 (update.phishing-server.com) | Lucy Update/License Server/HTTP proxy | 80/443 (HTTP/HTTPS) | TCP |
| 162.55.130.83 (update.phishing-server.com) | Linux repository | 80 (HTTP) | TCP |
| 8.8.8.8 (or any other DNS Server) | Your DNS Server | 53 (DNS) | UDP |
| nvd.nist.gov | NIST CVE database (Optional) | 443 (HTTPS) | TCP |
| 116.203.185.12 (changelog.lucysecurity.com) | Fetch LUCY Update News (Optional) | 80 (HTTP) | TCP |
| is.gd | URL Shortening service (Optional) | 443 (HTTPS) | TCP |
| api-ssl.bitly.com | URL Shortening service (Optional) | 443 (HTTPS) | TCP |
| api.authy.com | Two-factor authentication service (Optional) | 443 (HTTPS) | TCP |

# INBOUND COMMUNICATION

In order to reach LUCY SaaS Workstations from the internet, ports 80 and 443 have to be open on incoming proxy servers. No other ports are required. If LUCY should forward mails from users that respond to a phishing simulation, port 25 (SMTP) needs to be opened as well.

| Source IP | Destination | Port | Prot | Comment |
|---|---|---|---|---|
| ANY | Your LUCY SaaS Proxy IP(s) | 80/443 (HTTP/HTTPS) | TCP | Needed for accessing the landing pages & for certificate verification (http) |

| Source IP | Destination | Port | Prot | Comment |
|---|---|---|---|---|
| ANY | Your LUCY SaaS Proxy IP(s) | 25 (SMTP) | TCP | Only needed, if you want to catch email replies |

# MALWARE SIMULATION COMMUNICATION

Upon execution, the malware simulation tool will open the built in Internet Explorer or other default browser (in hidden mode) and send out the collected data to LUCY via HTTP or HTTPS (it will automatically choose HTTPS if you run your campaign via SSL). This tool will also work in environments where the Internet is accessed with Proxy servers - only allowing access for authorized Windows users.

From:
https://wiki.lucysecurity.com/ - **LUCY**

Permanent link:
**https://wiki.lucysecurity.com/doku.php?id=network_communication_-_lucy-saas**

Last update: **2021/09/29 10:30**