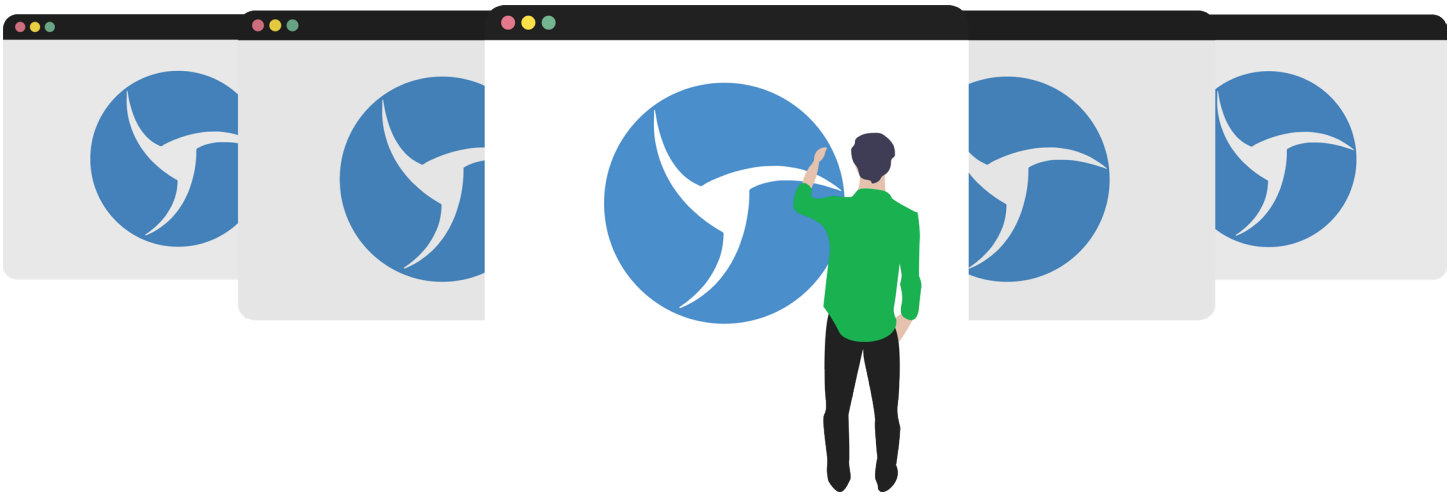
Recorded Future

MALWARE/TOOL PROFILE

Profiling the Linken Sphere Anti-Detection Browser

By Insikt Group®



CTA-2020-0107

This report includes a detailed analysis of the Linken Sphere anti-detection browser and is based on the Recorded Future® Platform, underground forums, Linken Sphere's official website and forum, as well as OSINT. This profile will be of most interest to financial, e-commerce, and social media companies who are targeted by cybercriminals, organizations seeking to track illegal activities within the underground community, as well as to anyone looking to understand popular tools used by cybercriminals to bypass fraud detection systems. This report is the first part of the Insikt Group research devoted to the Tenebris team tools. An in-depth technical analysis will be provided in follow-up research.

Executive Summary

Multiple e-commerce and financial organizations around the world are targeted by cybercriminals attempting to bypass or disable their security mechanisms, in some cases by using tools that imitate the activities of legitimate users. Linken Sphere, an anti-detection browser, is one of the most popular tools of this kind at the moment.

Every web browser has a unique "fingerprint" used by other websites to verify its legitimacy. E-commerce companies and banks often use this type of fingerprinting to block transactions from browsers that have previously been recognized as insecure or involved in fraudulent activity. The practice by cybercriminals of using various virtual machines, proxies, and VPN servers is not so effective since the anti-fraud systems have capabilities to identify suspicious IP addresses and virtual machines. As a result, cybercriminals have developed anti-detection software, such as Linken Sphere, that allows them to change all web browser configurations dynamically and generate an unlimited number of new ones, imitating the activities of legitimate users.

Linken Sphere was first introduced on several Russian-speaking underground forums on July 4, 2017, by the threat actor "nevertheless." Linken Sphere allows users to create multiple virtual accounts that imitate the activities of real users and provide unique device fingerprints. As a result, Linken Sphere has become popular among cybercriminals who seek to circumvent anti-fraud systems.

Key Judgments

- Linken Sphere is a Chromium-based web browser that allows cybercriminals to bypass anti-fraud systems of various organizations by imitating a real user's behavior.
- This user imitation includes intelligent timing to emulate human behavior and fool AI-based fraud detection, as well as an API that can be used to plug in both simple PHP-scripting based chatbots and more sophisticated, AI-powered chatbot programs. If such user imitation worked perfectly, it would actually pass the famous Turing Test, defined by computer pioneer Alan Turing in the 1950s to decide whether a machine acted intelligently enough to be indistinguishable from a human. To date, no system has passed this test, even though there have been numerous claims in recent years.
- Linken Sphere allows cybercriminals to create an unlimited number of accounts compatible with various operating systems.
- Linken Sphere was launched in July 2017 and quickly obtained recognition on the dark web due to substantial functionality, affordability, high-quality technical support, and advertising across major underground forums.
- Tenebris Team forum, the official forum of Linken Sphere, was created in May 2018, and ls.tenebris[.]cc is the official website to purchase it.
- On June 1, 2019, Linken Sphere was updated to version 7.99, likely due to increased client complaints of flaws in functionality in the previous versions.

Linken Sphere official logo.

Background

Linken Sphere (named “Сфера” in Russian) is a multi-functional and multi-purpose anti-detection browser and software that is widely used by cybercriminals to bypass the anti-fraud systems of financial organizations. It was first introduced on the dark web on July 4, 2017, by the Russian-speaking threat actor “nevertheless.” The threat actor is also one of the administrators of Tenebris Team forum, the official forum of Linken Sphere.

Other staff members of the Linken Sphere team are “dev.tenebris,” another administrator of Tenebris Team forum responsible for the technical development and support for the product, as well as the threat actors “S1neka,” “KirillGochan,” and “Zimbabve,” who are all moderators.

Though Linken Sphere is popular among cybercriminals, the creators claim that it was officially created for legitimate uses by groups such as the following:

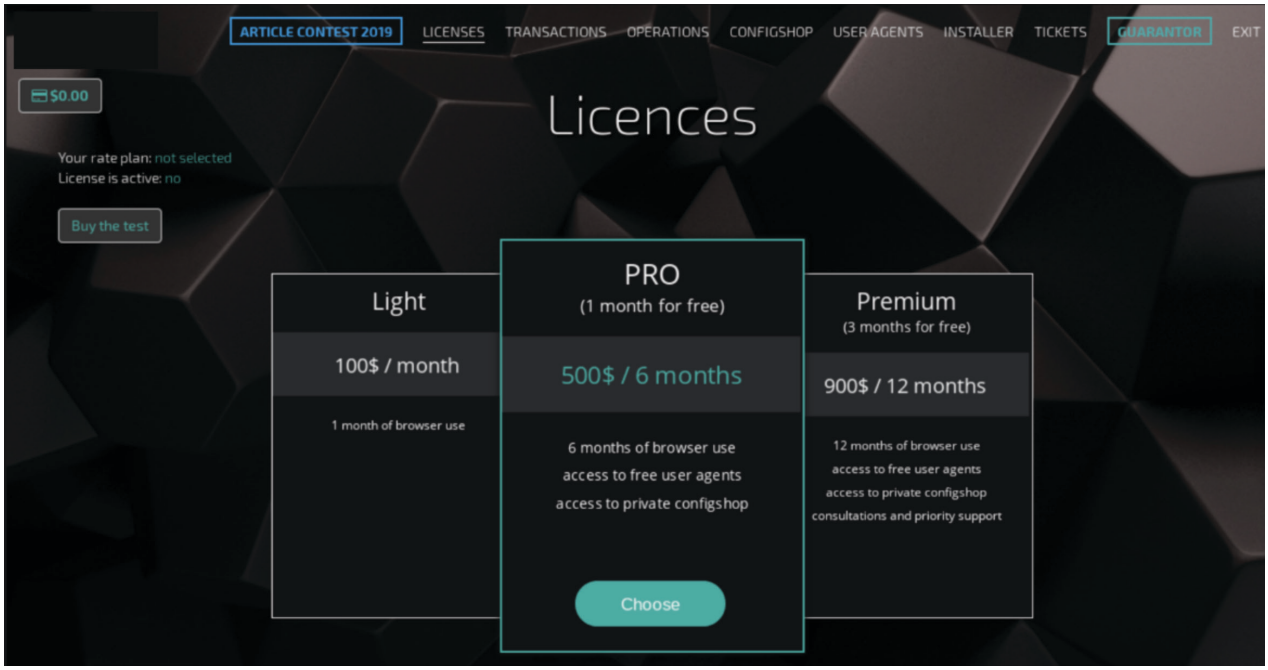
- Penetration testers
- Social media professionals
- Professionals working with advertisements based on keyword searches
- Bonus hunters who create multiple accounts for online gambling and gaming to earn monetary bonuses from specific deals offered by organizers
- Privacy advocates
- Those who operate multiple accounts simultaneously for work

The authors of the project openly hold conferences in Russia and Ukraine, and create YouTube promotional videos for both Russian- and English-speaking audiences.

According to Tenebris Team forum, there are three types of licenses for the latest Linken Sphere version, 7.996, introduced on September 13, 2019:

- "Light," for $100 per month
- "PRO," for $500 for six months, which provides access to the store with configs, including a one-month free trial of the product
- "Premium," for $900 for 12 months, which provides access to the store with configs and priority service, including a free three-month trial

According to the rules, it is possible to transfer the licenses to a third party, but the buyer and the seller must contact the support service to confirm this transaction.



Linken Sphere offers three types of licenses: Light, PRO, and Premium.

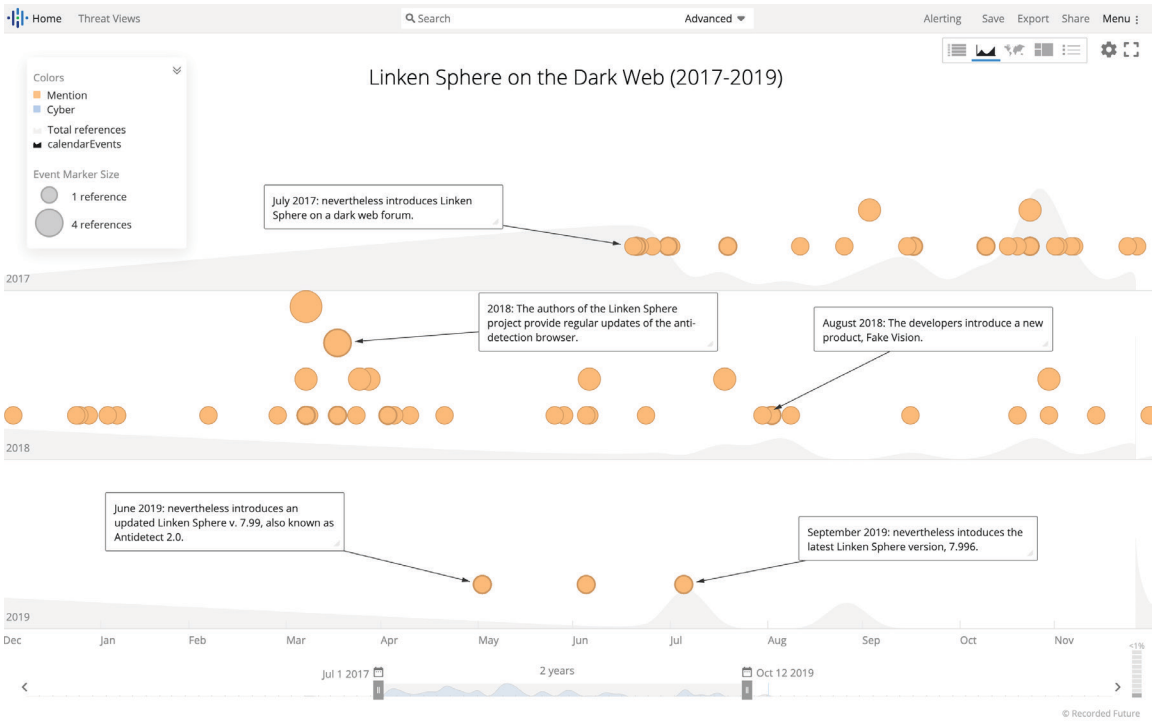
Technical documentation for Linken Sphere is available in English, Russian, Spanish, German, and Chinese. The developers recommend that new users connect through Tor to create and configure new Linken Sphere accounts.

After authorizing a personal account, users obtain access to the functionality of the user panel. The primary options of the user panel are:

- "Success Account" — Displays the enabled (current) account
- "Current Balance" (Russian, "Тарифный план") — Displays the current balance of the account with an option of its replenishment
- "Buy a Test" ("Купить тест") — A one-time test purchase of the Light license is available per account
- "Licenses" ("Лицензии") — Displays information about the type of active license and the remaining validity period, with an option to renew
- "Transactions" ("Транзакции") — Displays the user account activity, including cryptocurrency wallets with transaction activities
- "Operations" ("Операции") — Displays all purchased licenses and configurations

- “Configshop” (“Конфигшоп”) — Provides access to the configuration store
- “UserAgents” (“Юзерагенты”) — Displays available configurations for the PRO and Premium licenses
- “Installer” (“Установщик”) — Provides software installation guidance
- “Support Tickets” (“Тикеты”) — Ticket system provides technical and general support for Linken Sphere users
- “Automatic Guarantee Service” (“Гарант”) — An escrow service system to reduce the potential risk from deals and transactions

According to the developers, the software is compatible with various operating systems, including Windows (x64) versions 7, 8, and 10; macOS starting from Yosemite; and Linux OS: Ubuntu, Linux, Mint, Kali Linux, Gentoo (Calculate Linux), Fedora, Debian, OpenSUSE, Slackware, Mageia, PCLinux, and Kubuntu. Linken Sphere versions 7.99 and newer cannot be installed on Linux OS at the time of this writing. Linken Sphere can be installed on a local or remote computer, as well as on virtual machines such as VMWare or VirtualBox. PC system minimum requirements are as follows: 2xCore 1.7GHz, 2Gb RAM. Linken Sphere can be downloaded and installed on multiple devices; however, only one account is allowed at a time. User data is stored in the cloud storage of sessions and is also saved after uninstalling or reinstalling Linken Sphere.



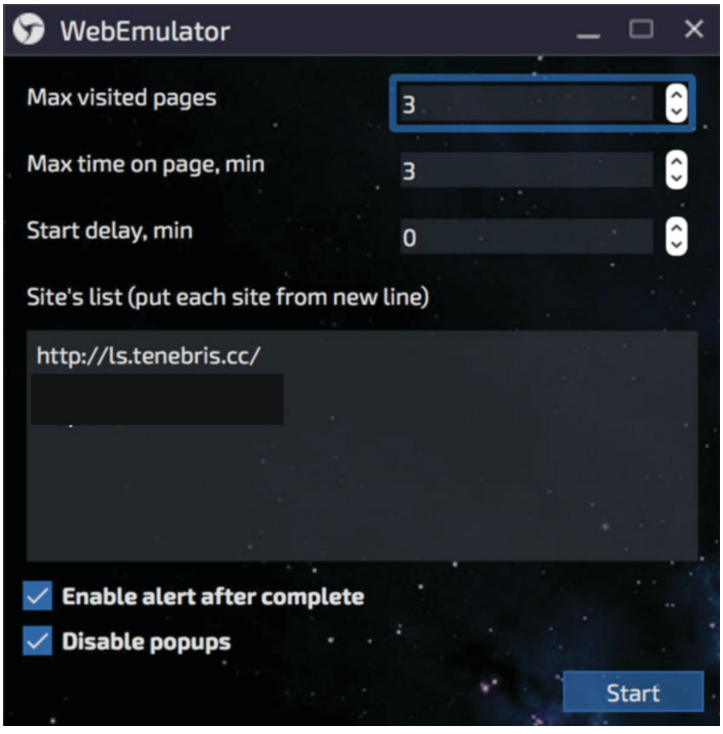
Linken Sphere offers three types of licenses: Light, PRO, and Premium.

Threat Analysis

The general technical specifications of Linken Sphere, as outlined on Tenebris Team forum by the threat actor “nevertheless” and on the official website ls.tenebris[.]cc, are provided below:

- Linken Sphere is based on the Chromium web browser; its developers used its source code and removed all tracking functions enabled by Google
- Operates in the “Off-the-Record Messaging” mode
- Does not use any hidden Google services
- Encrypts all saved data using the AES 256 algorithm
- Connects to the internet via various protocols, including HTTP, SOCKS, SSH, TOR, TOR + SSH, and DYNAMIC SOCKS
- Each session creates a new configuration and users do not need multiple virtual machines
- Allows working with different types of connections in multi-thread mode at the same time

- Includes built-in professional anti-detection with regular updates of configurations of the user's agents, extensions, languages, geolocation, and many other parameters, which are able to change in real time
- Saves fingerprints and cookie files after every session, allowing the use of a saved session by multiple users without needing to switch between virtual machines
- Does not require specific settings to start working proactively, anonymously, and securely
- Contains a built-in license with location database GeoIP2 MaxMind, allowing users to configure time and geolocation immediately
- WebEmulator, called "Прогреватор" in Russian, is an option created to "warm up" websites in an automated mode. This function allows collecting needed cookie files automatically between websites before working with a new account. WebEmulator operates in the background with multi-thread mode, allowing the set up of parameters for visiting websites such as the number of visited pages, time spent on each page, pauses, and delays between visits. WebEmulator enables alerts after task completion.



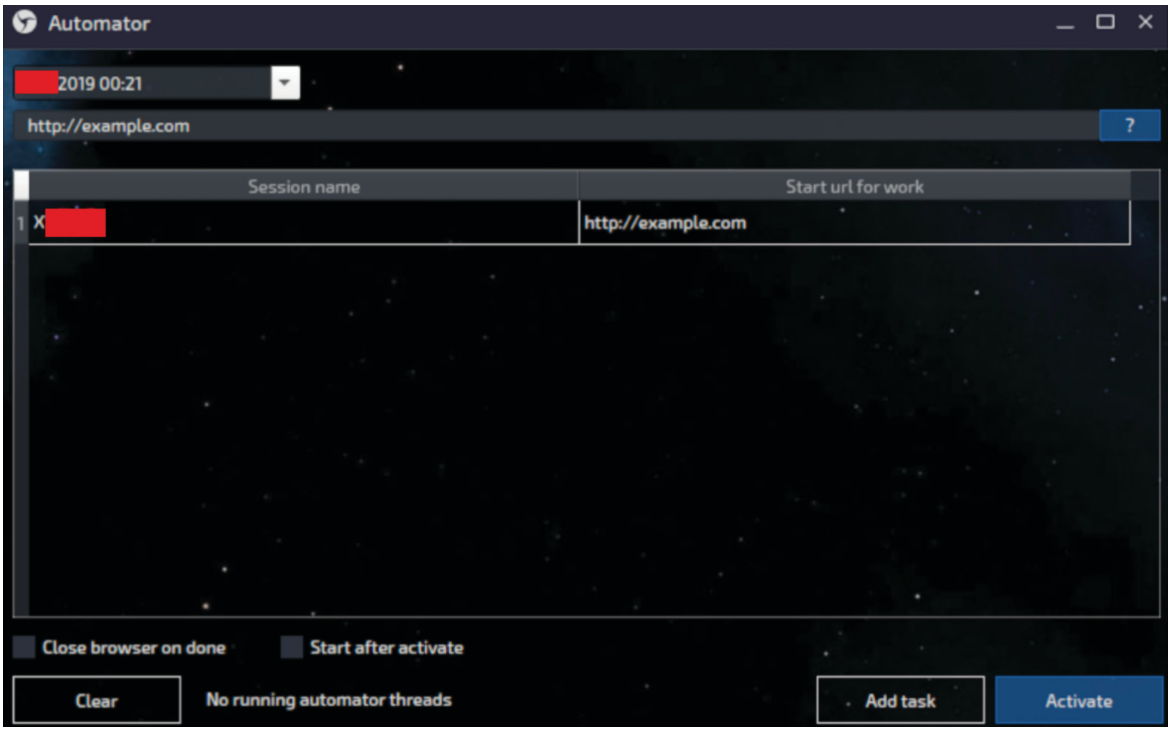
Web Emulator module for automated harvesting cookie files.

Linken Sphere allows users to deliberately leak a fake IP through WebRTC. The function is enabled during the whole session and misleads targeted organizations by leaking fake IP addresses and masquerading as legitimate users. It also allows connection through Proxifier, Bitvise, and Plink.

WebEmulator provides touch screen, mobile device, manual, and automated input emulation when copying text while visiting websites in the background mode, imitating the behavior of real users, and increasing the level of trust for such accounts.

On June 1, 2019, Tenebris Team forum developers announced Linken Sphere v. 7.99. The new version is likely meant to address the increased complaints by users that the previous versions did not provide sufficient anonymity, among other issues. The developers stated that the previous release was modified with new features, including:

- Automator (Russian, "Автоматор") — an updated module which allows Linken Sphere to bypass CAPTCHA with the emulation of human behavior, making it useful for automated registration of new accounts according to the developers
- The ability to save and encrypt passwords for easy access
- The ability to store and edit cookie files
- A new local backup algorithm that saves cookie files on an active machine, preventing their loss due to a slow or unstable internet connection
- A new mechanism of human text input emulation, using intelligent timing algorithms to defeat the majority of machine learning anti-fraud detection systems, which are able to identify automated input
- "Simple" — a new user interface that increases the speed of Linken Sphere operation while using remote devices
- Session synchronization — a new feature that creates a virtual office with access to any data using any connected device, allowing partners to not only transfer needed sessions between each other, but also to initialize work with a large amount of information at the same time, displaying statuses of these sessions and the most important information



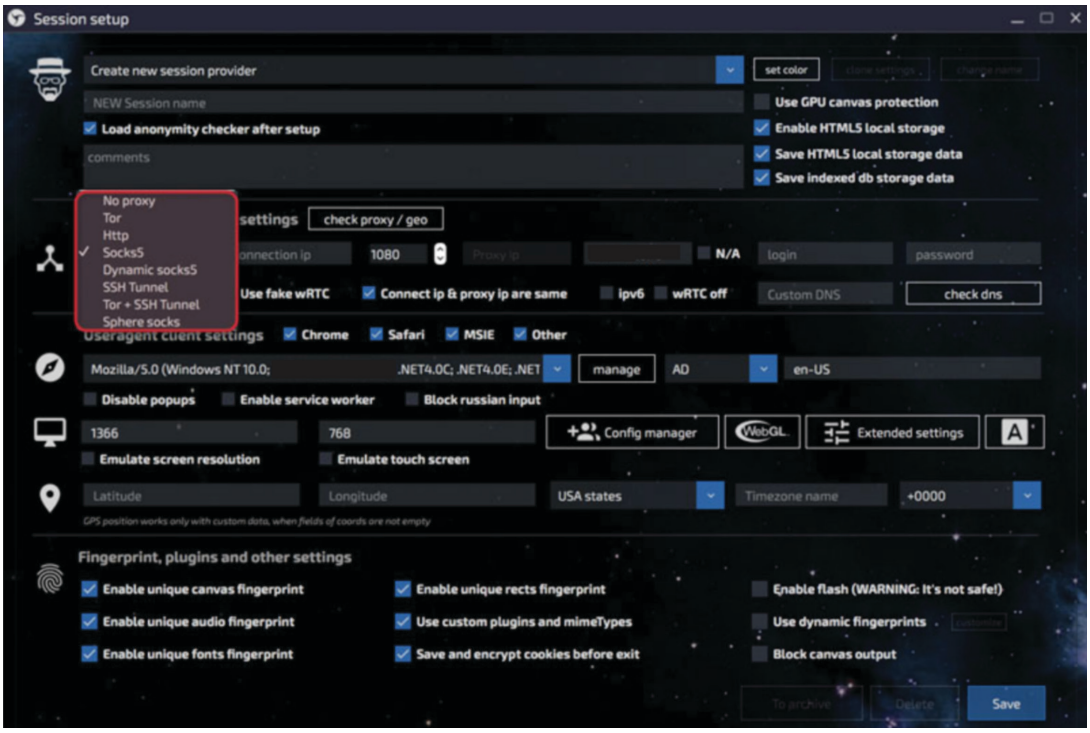
Automator module for bypassing website CAPTCHA.

Network Connection

Linken Sphere can connect multiple users simultaneously to the internet in what are referred to as "sessions." Each session can be named individually. Linken Sphere allows working on multiple devices and is not tied to particular hardware. Users can have the browser on different devices with various operating systems, but can only work with one username and password at a time. The developers stated that cloud access allows users to launch Linken Sphere from any device.

Each session connection can be configured individually in the following ways:

- No Proxy: Direct connection to the internet
- Tor: Connects through the Tor browser
- Secure Socket Shell (SSH) Tunnel: Linken Sphere remote section tunneling through SSH
- Tor + SSH Tunnel: SSH (encrypted) tunneling run via Tor proxies
- Dynamic SOCKS: SSH dynamic port forwarding via SOCKS allows communication not via a single port, but across a range of ports. This option will make SSH act as a SOCKS proxy server
- SOCKS5: An internet protocol providing authentication so only authorized users may access a server that also supports both TCP and UDP protocols
- Hypertext Transfer Protocol (HTTP) Connection
- Sphere SOCKS: SOCKS provided by the Linken Sphere developers



Session setup interface allows users to select an appropriate connection through various protocols.

Fingerprints

According to the developers, Linken Sphere includes approximately 50,000 device fingerprints and a config generator to create additional custom fingerprints. The users of the PRO and Premium licenses have access to approximately 150,000 fingerprints and 13,000 user agents on Tenebris Team forum, which are regularly updated.

Linken Sphere can modify the following fingerprints:

- Canvas: A part of HTML5 Canvas element displaying graphics on the webpage, which is widely used to identify users by the features of their video system
- Fonts: Another element that can be used to identify users
- Plugins: Installed and enabled plugins help to identify users
- Audio (Acoustic) Fingerprint: The role of an audio fingerprint is to capture the signature of a piece of sound, which allows it to be differentiated from other sounds
- WebGL: Javascript API for work in 3D graphics in the web browser without the use of plugins
- Geolocation: Anti-fraud system can compare users' IP addresses and their physical geolocation
- ClientRects: A method of identifying users using hashes obtained as a result of image scaling
- Ubercookie(s): A hash of ClientRects and Audio fingerprints allowing the device to be identified
- Web Real-Time Communication (WebRTC) (Including Device Hashes): A technology that is used for device-direct connection to media services such as microphones or cameras, and allows WebRTC to obtain a real IP address by bypassing VPN and proxy services; cameras and microphones have their own location indicators which also need to be changed
- Cascading Style Sheets (CSS): A method used to identify a real extension of the window using CSS technology

- Touch Emulation: A method allowing touch screen emulation without showing a mouse cursor; after setting up a user agent as a portable device, the anti-fraud system can still detect mouse cursor since it is still on a display
- JS Navigator (JavaScript Windows Navigator): Contains time, language, and extensions; the parameters of the web browser that are transmitted with the information about the program
- HTTP Headers: One of the primary browser fingerprints that allows anti-fraud defenses to identify users
- Domain Name System (DNS): Ability to use own DNS for each session
- Local IP Address: An indicator that helps to reveal the user's possible real location

According to the developers, the fingerprints listed above depend on the hardware. If the user transfers the same fingerprints from one machine to another, then the final fingerprints will be different. Some of the fingerprints, such as WebGL, Fonts, and Plugins, are included in the configs, while others like Canvas, Audio, and ClientRects are not, but are generated when the session is created.

Linken Sphere 'Configshop' Browser Configurations

According to the offer, the developers provide individual high-quality configs with the combination of the fingerprints emulating real devices. The average price per config is $3.

Configshop interface with the option to buy and import new configs.

Users of PRO and Premium licenses who prefer to manually configure sessions can receive free, fresh user agents for various devices in this section. The list of available user agents is constantly updated.

Free user agents available for PRO and Premium licenses.

Users with the PRO and Premium licenses can import configs in bulk, but not more than 100 configs per one time.

Risk Mitigation

Recorded Future will continue to monitor the development of the Linken Sphere anti-detection browser and will inform its clients of software updates and new functionalities to help clients incorporate them into anti-fraud systems in order to identify potentially fraudulent activities.

Insikt Group recommends the following general measures to protect against the targeting of organization websites and networks:

- Keep all software and applications up to date; in particular, operating systems, antivirus software, and core system utilities.
- Filter email correspondence and screen attachments for malware.
- Make regular backups of your system and store the backups offline, preferably offsite so that data cannot readily be accessed via the network.

- Have a planned incident response and communications plan.
- Adhere to strict compartmentalization of company-sensitive data. In particular, review the data that anyone with access to an employee account or device would have access to (for example, explore what would happen if the device were compromised through device or account takeover via phishing).
- Seriously consider instituting role-based access, limiting company-wide data access, and restricting access to sensitive data.
- Employ host-based controls; one of the best defenses is to conduct client-based host logging and intrusion detection capabilities.
- Implement basic incident response and detection deployments and controls like network intrusion detection systems, IDS, NetFlow collection, host logging, and web proxy, alongside human monitoring of detection sources.
- Be aware of partner or supply chain security standards. Being able to monitor and enforce security standards for ecosystem partners is an important part of any organization's security posture.

Outlook

Linken Sphere has been one of the primary anti-detection browsers on the dark web since its release in 2017 due to extensive functionality, high-quality technical support, and a successful business model. In 2019, Linken Sphere was updated with the new version 7.99 and described as a new product with all new functionality. It is likely that the developers decided to significantly overhaul the product in order to not lose a competitive advantage on the dark web against anti-detection browsers like AntiDetect and FraudFox. The low price of $100 per license is affordable for most cybercriminals and contributes to the influx of new users.

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.