Open Threat Intelligence using Neuro-Ledger

Executive Summary

Peter Waher

Trust Anchor Group AB
peter.waher@trustanchorgroup.com

Abstract. This paper describes how the Neuro-Ledger® can be used to create an open and distributed infrastructure for cyber-security related threat-intelligence that can be shared between services on the Internet.

Keywords: Neuro-Ledger, DLT, Open Intelligence, Cyber-Security.

1 Introduction

Anyone who has published a service online knows the vast amount of intrusion attempts that happen on the Internet daily. Creating an open service inviting anyone (of good will) is a challenge. Seldom, if ever, do developers have the full picture of the amount and types of threats available. They don't even fully understand the different threat vectors through which threats can appear. Most developers work in closed environments, where they must solve all issues themselves. Very little cooperation exists across sectors in the industry. Many choose, therefore, to use third-party solutions in hopes that they will make their execution environments more secure. How they do this remains a mystery and a closely guarded trade secret of the corresponding third-party. This paper proposes an alternative solution to such third-party solutions to cyber-security: A real-time, distributed open-intelligence infrastructure, where participants can share threat intelligence between themselves, and thus cooperate to create a safer Internet.

2 The Neuro-Ledger®

The Neuro-Ledger® is a next-generation distributed ledger (DLT) that solves many of the inherent problems presented by traditional blockchain-based distributed ledgers. Instead of blocks chained together, blocks are standalone, and the distributed ledger is federated, as well as distributed. This means that any domain is free (using principles of local governance) to generate any blocks it chooses to, and then to distribute them according to principles set forth by cooperating domains. Any domain can interoperate and cooperate in any exchange of information agreed upon. Not chaining the blocks together into one single chain provide multiple benefits for the distributed ledger:

- The ledger has global scalability of content, global scalability of access and a resilient infrastructure. This is the result of participating nodes not having to contain all information about everything but can restrict themselves to information of interest.
- There is no need for energy-wasting Proof-of-Work or Proof-of-Stake to generate blocks. Blocks are protected by a public-key infrastructure, where each domain signs its own blocks. A domain does not need the permission or acceptance from other domains, to produce blocks under its domain. A domain does not need to accept blocks from other domains, to be able to process blocks of its own choosing or making.
- There are no explicit costs (such as gas) to mint blocks.
- Blocks can be given life-cycle restrictions, purging the ledger of old and obsolete information over time.
- It is also possible to transparently modify or delete erroneous or personal information from the ledger, making it possible to comply with privacy legislation worldwide.
- The ledger can process private, sensitive or confidential information directly.
- Heterogeneous networks can cooperate on the network, as there is no competition between nodes.
- The design follows the basic design of the Internet, making it relatively easy to implement in Internet-based infrastructure and operations.

For more information about the Neuro-Ledger®, and how it solves the above-mentioned problems, see the *Neuro-Ledger, Executive Summary*[1]

3 Open Threat Intelligence using the Neuro-Ledger

The Neuro-Ledger® has an internal real-time threat-analysis feature that analyzes incoming communication on different protocols, and flags endpoints for suspicious activity. This includes tasks such as trying to access resources that do not exist, or exists in other systems, attempting to login using erroneous credentials or using vulnerable ciphers or invalid certificates, etc. Honey pots also exist making it more difficult and time-consuming to scan a Neuro-Ledger® for hosted services. If the suspicious activity persists over time, the endpoints get flagged and temporarily blocked using a short time interval. If the endpoint persists with its suspicious behavior over longer periods of time, the endpoint gets blocked for successively longer times. Finally, the endpoint gets blocked permanently (or until manually unblocked by an operator). The threat analysis is stored on the Neuro-Ledger® and distributed with cooperating domains. Such domains, therefore, gain access to this information and can make security decisions in real-time based on analysis made on other domains.

4 Open Threat Intelligence API

The Neuro-Ledger® and the Neuron® come with an Agent API, providing agents with a HTTP-based RESTful API[2] that is easy to access. Since the Neuro-Ledger® is distributed, there is no central endpoint to access this API. Instead, you instantiate a Neuro-Ledger® in your environment[3], subscribe to the block collections related to Open Threat Intelligence[4], and call the API endpoint in your local environment. As access and processing are distributed, the load placed on the API by different services on different domains does not affect performance for others.

For experimentation and learning, two public endpoints exist at the time of writing: One originally funded by the Swedish Internet Society[5], and one funded by TAG[6]. As these exist for experimentation and learning purposes, there is no service agreements involved, nor a guarantee of service uptime or performance, as the nodes are used for different projects with different purposes and may be updated or purged at any time.

From the Open Threat Intelligence API, any service gains access to both information made available by Neuro-Ledger®, as well as connected services. Neuro-Ledger® provides information about its threat analysis, including information of endpoints in different protocols being temporarily or permanently blocked, and if temporarily blocked, when the endpoint is allowed to login at the earliest[7]. Connected services and agents can also by themselves provide open intelligence information about endpoints, that are then shared by other connected services and endpoints throughout the federated Neuro-Ledger® network[8]. Such information can include any collection of information tags, that services can use to perform security decisions. Internet Standard bodies can also standardize the names of such tags, to foster global interoperability regarding threat analysis and open intelligence in the field.

5 Agent API

Each Neuron® publishes an Agent API, a HTTP-based RESTful API that allows agents to interact with the Neuron® network, which includes the Neuro-Ledger®. Connectivity is properly authenticated, and each agent can optionally associate the account on the federated network, with a *digital legal identity*[9]. Such digital legal identity information can be included in the open intelligence information, if chosen to by the publisher. This information is also very difficult to spoof. If provided, it helps recipients determine if they can trust the information and base security decisions on the information. The digital identity can also be used for password-less authentication and multi-factor authentication in distributed federated environments using Neuro-Access™ smart phone app or Agent API clients[10].

6 The Neuro-Foundation

The Neuro-Ledger® was originally developed by Peter Waher, and the Trust Anchor Group, a Swedish company (of which Peter is a founder) developing the TAG

Neuron®. The Neuron® is an infrastructure component that facilitates the creation of open, interoperable, and yet secure networks over the Internet. This includes concepts such as self-sovereign digital identities, legally binding smart contracts, tokenization of physical assets, and programmable payments. The TAG Neuron® is based on the Neuro-Ledger®, and associated services. As part of a process where the TAG technology is accepted by larger operators world-wide, much of the Neuron-based technologies are at the time of writing being moved to the Neuro-Foundation[11], a Not-for profit organization supported by its member organizations and commercial licenses of its software. As a part of this move, source code is also made freely accessible open source. This includes the Neuro-Ledger®. The Neuro-Ledger® is, therefore, free to use for non-commercial purposes. Commercial use requires a commercial license with the Neuro-Foundation, to help finance the maintenance and development of the Neuro-based technologies.

[1] Neuro-Ledger, Executive Summary, 2019-10-11, https://neuro-foundation.io/Papers/Neuro-Ledger,%20Executive%20Summary.pdf

[2] Agent API: https://neuro-foundation.io/Documentation/Neuron/Agent.md

[3] How to download and install a Neuron®: https://neuro-foundation.io/Documentation/Neuron/InstallBroker.md

[4] Collections hosting Open Intelligence blocks include `RemoteEndpoints` and `OpenIntelligence`.

[5] https://cybercity.online/Documentation/Neuron/Agent.md

[6] https://lab.tagroot.io/Documentation/Neuron/Agent.md

[7] This is done using the `/Agent/Intelligence/CheckEndpoint` resource: http://cybercity.online/Documentation/Neuron/Agent/Intelligence/CheckEndpoint.md

[8] This is done using the `/Agent/Intelligence/Add` `/Agent/Intelligence/Delete` and `/Agent/Intelligence/Get` resources:
http://cybercity.online/Documentation/Neuron/Agent/Intelligence/Add.md
http://cybercity.online/Documentation/Neuron/Agent/Intelligence/Delete.md
http://cybercity.online/Documentation/Neuron/Agent/Intelligence/Get.md

[9] On legal identities: https://neuro-foundation.io/LegalIdentities.md

[10] For distributed SSO and MFA, see https://quicklog.in/

[11] The Neuro-Foundation: https://neuro-foundation.io/