Creating a

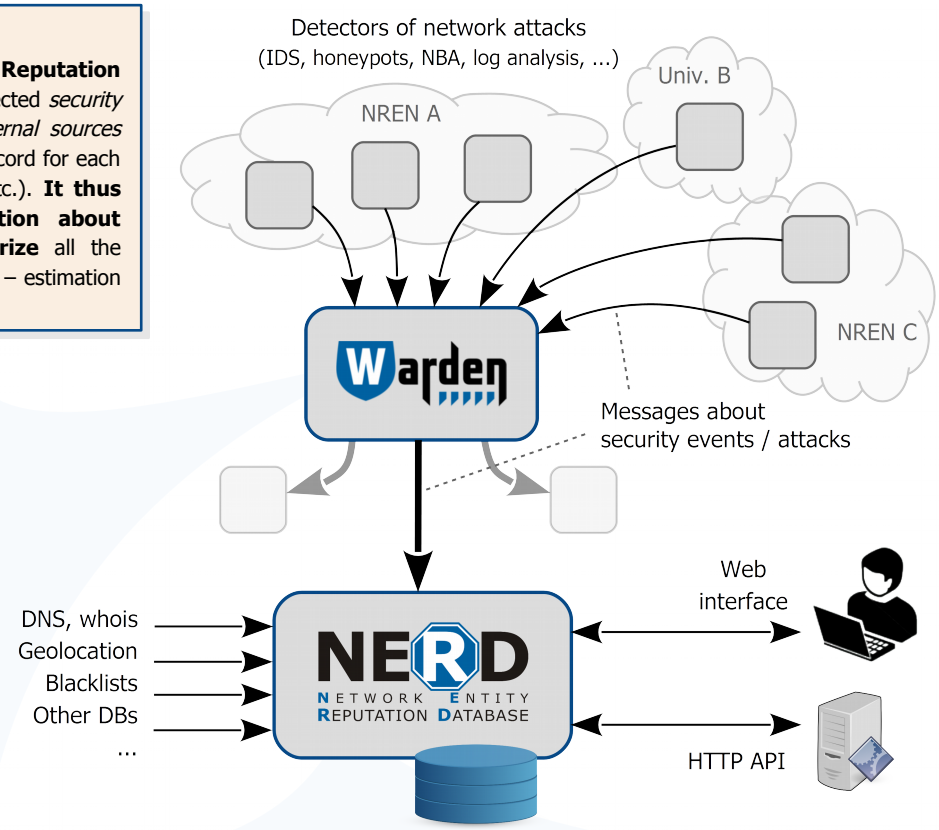
Network Reputation Database

"A list of bad actors on the internet & everything we know about them."

Václav Bartoš <bartos@cesnet.cz>

Summary

We are working on a system called **"Network Entity Reputation Database" (NERD)**. It receives messages about detected *security events*, combines them with data from various *external sources* (e.g. blacklists), and stores all that information as a record for each reported *entity* (i.e. IP address, network, domain, etc.). **It thus keeps all available security-related information about network entities** at one place. It also **summarize** all the information about an entity into its ***reputation score*** – estimation of the level of threat the entity poses.



Warden – alert sharing

- Detectors of malicious traffic deployed in different networks (senders) report their results to the central hub (Warden server).
- The hub distributes the messages to all subscribed receviers.
- Reciprocity – anyone sending data to Warden is allowed to receive all data sent by others.
- Common data format – IDEA [1]
- Developed and operated by CESNET.
  - Currently >20 senders
  - 1.5 million alerts per day
- We are looking for more participants ...
- **Join the sharing community now!**
  - Share data from your detectors
  - Get data from all others
  - Get access to NERD

Reputation database (NERD)

- Keeps all known security-related information about network entities – IP addresses, networks, domains and others.
- Main data source – **alerts from Warden** (or other similar systems, e.g. MISP [2])
  - Information about all detected malicious activities related to an entity.
- Data from various **other sources** added
  - Blacklists, other databases, geolocation, ... (see left)
- Summary of all the information – ***reputation score***.
  - Ranking of entites by level of threat they pose.
  - Formally – probability of future attacks combined with their expected severity. (Predicted by machine learning.)

An IP address record contains:

- Time added, last updated
- All reported **events**
- Hostname (rev. DNS)
- Country, city
- ASN, abuse contact
- List of blacklists the address is present on
- Amplifier (open DNS, NTP, ...)
- TOR exit node
- VirusTotal
- Shodan info (e.g. open ports)
- Static / dynamic address (guessed)
- Device type (guessed)
- *... many other information ...*

(some with history and/or probability)

- **Reputation score** (summary of all above)
- Manually added notes

Access:

- Via a **web interface** or **HTTP-based API**.
- **CSIRT teams** and **security researchers** can request access to NERD.
- Anyone sending data to **Warden** gets full access automatically → start sharing!
- Limited access for public

Use-cases:

- "NERD, what do you know about IP x.y.z.a?"
  - "It is a known spammer."
  - "It often tries to break into SSH by guessing passwords".
  - "It was scanning ports a week ago, no report since then."
  - "It is a botnet C&C server according to blacklist 'X'."
  - "Unknown – probably benign."
- "NERD, give me a list of all malicious IP addresses in my network (x.y.z.0/22)."
- "NERD, give me all open DNS resolvers known to be used in DNS amplification attacks."
- *... and many more ...*

Useful for:

- Incident handling
- Block lists
- Security research
- Statistics, visualization
- ...

More information

http://nerd.cesnet.cz
bartos@cesnet.cz

http://warden.cesnet.cz
warden-info@cesnet.cz

Acknowledgments:

This work is supported by the Security Research Programme of the Czech Republic 2015 - 2020 (BV III / 1 VS) granted by the Ministry of the Interior of the Czech Republic under No. VI20162019029 The Sharing and analysis of security events in the Czech Republic.
It is also partially supported by the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1) and 731122 (GN4-2).

References:

[1] IDEA – Intrusion Detection Extensible Alert. https://idea.cesnet.cz/
[2] MISP – Malware Information Sharing Platform. http://www.misp-project.org/