CTI League

Playbook

April

Contents

Introduction

The Cyber Threat Intelligence (CTI) League is an online, global community of cyber threat intelligence researchers, infosec experts, CISOs, and other relevant people within the industry, whose goal is to neutralize cyber threats exploiting the current COVID-19 pandemic.

Our volunteers prioritize efforts on helping hospitals and healthcare facilities protect their infrastructures during the pandemic and creating an efficient channel to supply these services. With volunteers around the world, we can respond quickly during this emergency.

The CTI League is a cooperative of the people within the group and the managers welcome engagement and alignment by the volunteers. Please review the organizational information at cti-league.com and in the Administrative section of this document and contact the managers should you have need for additional information.

This document provides an overview of the CTI League activities and how you can participate to the fullest. As we continue to grow, we will continue to update the services we can provide. If you have ideas for improvements to our processes or the services we offer, please let us know. Thank you for joining us in this ongoing response.

As a reminder; using this data to advertise, market, engage in presales or cultivation of sales leads in any way for any commercial offering will result in immediate removal from CTI League. Uses where MSSPs and others have existing contracts to protect endpoint networks with their services and tooling are permitted. We strongly recommend that you check with the admins before sending notifications on your own. We have established contacts & official channels for contacting healthcare teams.

Activities

Cyber Threat Intelligence Community Sharing

General

The CTI League is a clearinghouse for data, connection network and a platform for facilitating those connections. These connections enable to its volunteers to find the best PoC for their need. We receive and concentrate data from three types of places using automated and manual methods in our Slack workspace:

1. CTI League monitoring streaming. Available streaming (updated 04/04/20):
    a. Medical infrastructure vulnerabilities in Shodan and Censys (Channel current name: medical-infra-vuln-streaming)
    b. Phishing attachments submitted to VT (Channel current name: phishing-attachments)
    c. Phishing domains and subdomains repositories (Channel current name: covid-phishing)
2. Feeds and external services
3. Information sharing by CTI League members

* The current keywords are in English. If you wish to add new keywords /systems, please review “Contact with the managers” chapter.

Sharing Information

The CTI League volunteers can share relevant data for the medical sector within the league’s relevant channel, whether they identified the information or tracked it in a feed (Channel current names: iocs, feeds).

With this data, we can achieve three purposes:

1. Create a repository of indicators relevant the current pandemic. The CTI League management team is providing the medical sector:
    a. GitHub dedicated to the medical sector, which in, we are creating a database of block lists, hunting queries and prevention methods.
    b. MISP integration – streaming information from the league to a dedicated MISP. **Tool in development.**
2. Enrich the league knowledge of trends and recent cyber-attacks regarding the current pandemic.
3. Prevent cyber-attacks.

Information Request

The CTI League volunteers can use the league to collect information about entities regarding their investigations and get help from other expert volunteers within the Request for Information (RFI) channels:

1. Information request:

    a. Using Jarvis, Main CTI-League Bot, with the slash command:

    /checkioc -- Checks IoCs on ThreatSTOP database

    b. Using D3P0, the RFI Ticket Bot - Requests for Information are managed through the D3.Intel Ticket backend. Associated Slash Commands are used for the management lifecycle of RFI Ticket Requests.

Available Slash Commands	
Query	Command
/rficlose	Close a request
/rficlosedcount <last x days>	Displays count of tickets closed in a period
/rficlosedlist <last x days>	List closed tickets over time
/rfinew	Submit a request for information
/rfiopenlist	Lists open and in progress tickets
/rfireply <ticket number>	Reply to a request
/rfisearch <search thing>	Fuzzy search for ticket description
/rfistatus <ticket number>	Status of one ticket

GitHub Project

The CTI League gives medical sector systems multiple options for receiving data from the league. One of these options is via our GitHub. The information in the Git repo can be divided into 2 sections:

1. Public release - Files vetted, and approved for the public, contains blocklists by hash, IP and domain. Vetted list of known bad actors. This option is open for publication for anyone in need. In this Git our volunteers can find:
    a. Vetted blocklists based on IP address, domains, and hash values for blocking.
    b. A PiHole feed for inclusion into the PiHole software as a blocklist that reflects the data in the domain blacklist.
    c. A compilation of links to information from the CDC and other sources containing information about health and safety.

    https://github.com/COVID-19-CTI-LEAGUE/PUBLIC_RELEASE

2. Limited (private) release- A reliable database of blocklists, vulnerabilities and sensitive information, that is presenting within GitHub for CTI League volunteers only. Following a list of the channels and a short explanation about each one:

    Private Block list: INTERNAL ONLY blocklist that have not been verified yet.

    https://github.com/COVID-19-CTI-LEAGUE/PRIVATE_BLACKLISTS

    Private Allow list: INTERNAL ONLY allow list that have not been verified yet.

    https://github.com/COVID-19-CTI-LEAGUE/PRIVATE_WHITELISTS

    Private Medical Infrastructure vulnerabilities: Enriched and by country separated list of IPs, taken from the vulnerabilities streaming. In this repository you can find lists from vulnerable hosts, attributed to medical/hospital-orgs, based on keywords in their hostnames or network-info. The lists are separated by country and generated for each day (these are not IOCs).

    https://github.com/COVID-19-CTI-LEAGUE/PRIVATE_Medical_infra_vuln

Cyber-Attack Neutralization

General

The CTI League's current goal is to neutralize cyber threats exploiting the current COVID-19 pandemic. Our volunteers can choose the best path to achieve this goal:

1. **Takedown** – CTI League volunteers can raise a takedown request for removal of a website, web page, or file from the Internet.
2. **Triage** – CTI League volunteers can help the medical sector with triage indicators. Triage definition: "high priority indicator of compromise to investigate in the medical sector networks and to block".
3. **Law enforcement escalations** – CTI League volunteers can escalate relevant cyber-attack, malicious activity, or critical vulnerabilities to law enforcement agencies and national CERTs.
    a. To submit takedown request - Use 3DP0 bot (see Takedown chapter).
    b. To receive data about requests, the Law enforcement members can check the law enforcements escalation channel.

Takedown

The CTI league wishes to remove any relevant threat from the internet. The CTI League options for take down IoCs:

- Helping with the takedown process, check "Takedown" channel.
- Using D3P0, our Ticket Bot – Take down requests are managed through the D3.Intel Ticket backend. Associated Slash Commands are used for the management lifecycle of Takedown Ticket Requests.

Available Slash Commands	
Query	Command
/takedownclose <ticket number>	Close a request
/takedownclosedlist <last x days>	List closed tickets
/takedownnew	Submit a request for a takedown
/takedownopenlist	Shows list of open and in-progress tickets
/takedownopencount	Shows count of open and in progress tickets
/takedownreply <ticket number>	Reply to a request

/takedownsearch <search string>	Fuzzy search for ticket description

Triage

The CTI League volunteers can triage any indicator or vulnerability to the medical sector using the triage channels. Moreover, our volunteers can use a simple workflow within the relevant feed's channel.

Law Enforcement Agencies Escalation

As the CTI League members receive reports of suspicious domains, compromised infrastructures, and other cyber-attacks by malicious actors, our 24/7 volunteer team triages these reports. Once verified, we work to take down or eliminate threats, escalating to CERTs and law enforcement agencies as necessary. Following example for relevant issues for escalation:

- Criminal activity in the cyber domain
- Threats against national security
- Takedown process would not be effective (in international campaigns for example)
- Urgent reporting to a medical facility
- Issues impacting government infrastructure
- Large scale information relevant to a specific country

Malware Analysis

The CTI League is a community of cyber threat intelligence experts. The league offers to its volunteers a platform for sharing information and consulting others regarding ongoing malware analysis researches. Our volunteers can find the following platforms:

- Windows malware analysis
- Mac malware analysis
- Linux malware analysis
- Android malware analysis

Further, we will start working on ransomwares when we get IR requests.

Support

The CTI League volunteers handle domains and network profiling for medical organizations. We offer the medical sector and the relevant organizations three types of support:

1. Medical sector support
2. Infrastructure support
3. Incident Response (IR) support

Medical Sector Support

The CTI League volunteers receive support applications from the medical sector. The information is transferred to the relevant channel via the following methods:

1. Formal application from a medical organization for support. The management team will publish cases we receive from the medical sector, and the league can help on these requests. In order to submit an official request, the medical sector can send an email to the following address: info@cti-league.com
2. Raising issues within the relevant channel by one of the CTI League volunteers – our volunteers receive reports on relevant support requests from the medical sector and share the request in the relevant channel. We encourage our volunteers to use the league for helping with medical sector support requests.
3. A call for support from national / medical sector CERTs. We encourage CERTs to raise a support requests for the medical organizations within their countries.

In the medical support relevant channel, our league can share methods and tools to help the medical sector. Handling domains and network profiling for the medical sector are the ongoing activities in the channel.

The CTI League creates a hunting queries database for the medical sector. The medical sector can receive the database for free and prevent attacks with it. CTI Volunteers are encouraged to share relevant hunting queries and rules via a workflow in hunting queries channel (current channel: hunting-queries-database).

Further, the hunting queries, such as Yara and sigma rules or queries for APT scanner, will be shared with the medical sector via our GitHub **(Tool in development).**

Infrastructure Support

The CTI League offers the medical sector and the relevant organizations infrastructure support to protect critical infrastructures, especially those found in medical or health-related organizations.

In the relevant channel, the CTI League creates discussions around availability and capacity, enriching the knowledge of the league about trends, vulnerabilities and capabilities.

Incident Response

The CTI League volunteers can help the medical sector with handling of ongoing events by incident response request. When medical sectors are under attack, our volunteers can help with the incident response process which include identification, analysis and responding to the specific threat.

CTI League experts are willing to help the medical sector with mitigating cyber-attacks.

Networking and Contact with Other Volunteers

General

CTI League encourages our volunteers to be an active, engaging, and respectful community. The CTI League is an online community connecting cybersecurity experts worldwide. With our power as a community, we can achieve our superior goal – preventing cyber-attacks. We encourage our volunteers to use the network for this goal. The league connects relevant people from various sectors and enables opportunities. Here are a few examples:

1. Use the relevant contact channel to connect with people from the group or ask the community to create the connection.
2. Share information about cyber-attacks and help to prevent and eliminate them.

Finding Contact

The CTI League volunteers can use Jarvis, the main CTI-League Bot, to find the relevant contact people they wish to contact with.

Available System Commands	
Query	Command
/add_contact <organization>	Add yourself as a contact for the specified organization
/del_org <organization>	Removes organization you are a member of
/leave_org <organization>	Remove yourself as a contact for an organization
/list_contacts <organization>	List contacts of specified organization
/list_org <search parameter>	List organizations who have contacts registered
/mod_org <exiting org>	Rename existing organization
/my_orgs	List the organizations you are contact for

Moreover, we encourage our volunteers to add the handle **"@ <relevant role / ability>** to their display name.

Disinformation

General

The CTI League is willing to neutralize any threat in the cyber domain regarding the current pandemic, including disinformation. The mission of this efforts is to find, analyze and coordinate responses to the current pandemic disinformation incidents as they happen, and where our specialist skills and connections are useful.

Our Efforts

After identifying a disinformation incident, the CTI League volunteers can use our incidents spreadsheet to report about the incident:

https://docs.google.com/spreadsheets/u/3/d/1PAfipi5e1oxb6tw_gSe-OZfpb_2b3un9ZTpYtqtF1TQ/edit#gid=0

After updating the spreadsheet, the volunteer should create a folder in the google drive INCIDENTS folder for notes and anything that won't fit into the DKAN

DKAN - https://data.cogsec-collab.org

Google Drive - https://drive.google.com/drive/u/2/folders/1MtsIfmYEAh9bH8A5OX9nb8xoZ6qCq2g_

Report on the rumor to the disinformation channel to receive help from the community and the report about it.

We will add an incident to the MISP instance for the rumor:

https://covid-19.iglocska.eu

Please check the readme:

https://docs.google.com/document/d/1XimTUfZlxfZBBgka-_DQYsXTEgz-GuFfym5MHdva-5g/edit?usp=sharing

Administrative

General

The CTI League community encourages its volunteers to take active part in advancing the league's ability to help the medical sector. The managers suggestion box is open 24/7; we kindly welcome them.

To submit a suggestion for the managers, use the workflow in general channel. If you have any administration process improvement, if you want to develop some service for helping the medical sector, if you want to help us - We are here for you!

If you want to help the CTI League managers with missions we have as a league, please check new volunteer positions in CTI League board (current channel - # 1-volunteering-board).

The CTI League volunteers can use the command /jarvis_help to receive information for Jarvis bot. Following, a list of available commands:

/jarvis_help dev

/jarvis_help vulnerabilities

/jarvis_help takedowns

/jarvis_help supporting medical

/jarvis_help supporting infrastructure

/jarvis_help triage

/jarvis_help law enforcement escalations

/jarvis_help requests for info

/jarvis_help malware analysis

/jarvis_help contact info

/jarvis_help hunting queries

/jarvis_help iocs

/jarvis_help incident response

/jarvis_help phishing

Adding People

The CTI League welcomes cyber threat intelligence experts from all around the world. To add a new member for the league, please fill the form in our website:

cti-league.com

The CTI League managers review the requests, validate potential volunteers, and accept qualified people.

Admins

The CTI League managers work with admins and lead researchers within the community. The admins are divided into four teams:

1. Administrative team
    a. Community and channels managing
    b. Graphic designing and content writing
    c. Operations response
2. Technical team
    a. DevOps
    b. Bots
    c. Streaming and publishing
3. Research team
    a. Malware Analysis
    b. Hunting queries
    c. Darknet
    d. Indicator of Compromise
4. Support team
    a. Medical sector support
    b. Infrastructure support

Code of Conduct

Please review CTI League code of conduct. All volunteers are held accountable to this code.

https://cti-league.com/code-of-conduct/

Privacy Statement

Please review the CTI League privacy statement:

https://cti-league.com/cti-league/privacy-policy/

Slack Channel Reference

#1-announcements – a read only channel of announcements from the volunteer admins

#1-general – Company-wide announcements and work-based matters. Please use the :zap: button at the top of the channel to submit workflow requests.

#1-introduction – Check out our code of conduct listed here: https://cti-league.com/code-of-conduct/. Please use your real name here & include a note about your affiliation or skills you bring to the group in your nickname. Thanks & welcome to CTI League!

#2-covid-phishing – Suspicious domain names [Scam / Malicious / Phishing] related to COVID-19 captured from live streaming and pasted "as is" by the bot. There could be FP. To suggest keywords or improvements, contact @Emanuele De Lucia

#2-ioc-triage

#2-medical-infra-vuln-strea -Stream of vulnerable infrastructure likely linked to medical/health related organizations.

#2-medical-vuln-triage

#2-phishing-attachments

#3-contacts-at- Ask here to find contacts at other orgs

#3-hunting-queries-database

#3-infrastructure-support- Discussion around availability and capacity. Telecoms, SaaS, Hosters, etc.

#3-medical-sector-supporting- This channel handles domain & network profiling for medical organizations. BinaryEdge/Censys/Shodan/Shadowserver scans, etc. Please read the pinned notes, and welcome!

#4-darknet

#4-help-requests- General help requests from the community regarding investigations and helping the medical sector

#4-hunting-queries

#4-iocs- IOCs shared are TLP:WHITE unless stated otherwise by author

#4-ir-requests

#4-law-enforcement-escalations

#4-network-monitoring

#4-request-for-information

#4-takedown-requests- Request that orgs take down Bad Stuff. Please tag the org name where you're expecting action.

#5-android-malware-analysis

#5-feeds

#5-linux-malware-analysis

#5-mac-malware-analysis

#5-windows-malware-analysis

#6-news-covid19

#6-random- Non-work banter and water cooler conversation

Version History

Version	Date	Change Summary
1.0	4/13/2020	Initial release