CTI League Inaugural Report March 2020

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.

In this first report, we provide an overview of the CTI League activities including how membership has grown over a short period, the crucial projects that our volunteers are working on, and information on how to engage with us. In the first chapter, we examine the membership growth and the distribution of the volunteers (more than 1400 from 77 countries). In the second chapter, we provide stats regarding CTI League efforts neutralizing cyberattacks on three different matters: takedown from the internet, triage the information to the medical sector and escalation of information to the Law enforcement agencies and national CERTs. The third chapter will provide information about the support that CTI League supplied to the medical sector to protect their organizations and their infrastructure within its first month, including vulnerabilities alerts, IoCs identifying and explanation about our information streaming services.

This is an unprecedented global emergency. Those of us in the cyber security community have come together to protect those on the front lines who are fighting for us. As we continue to grow, we will continue to provide regular reports about our efforts.

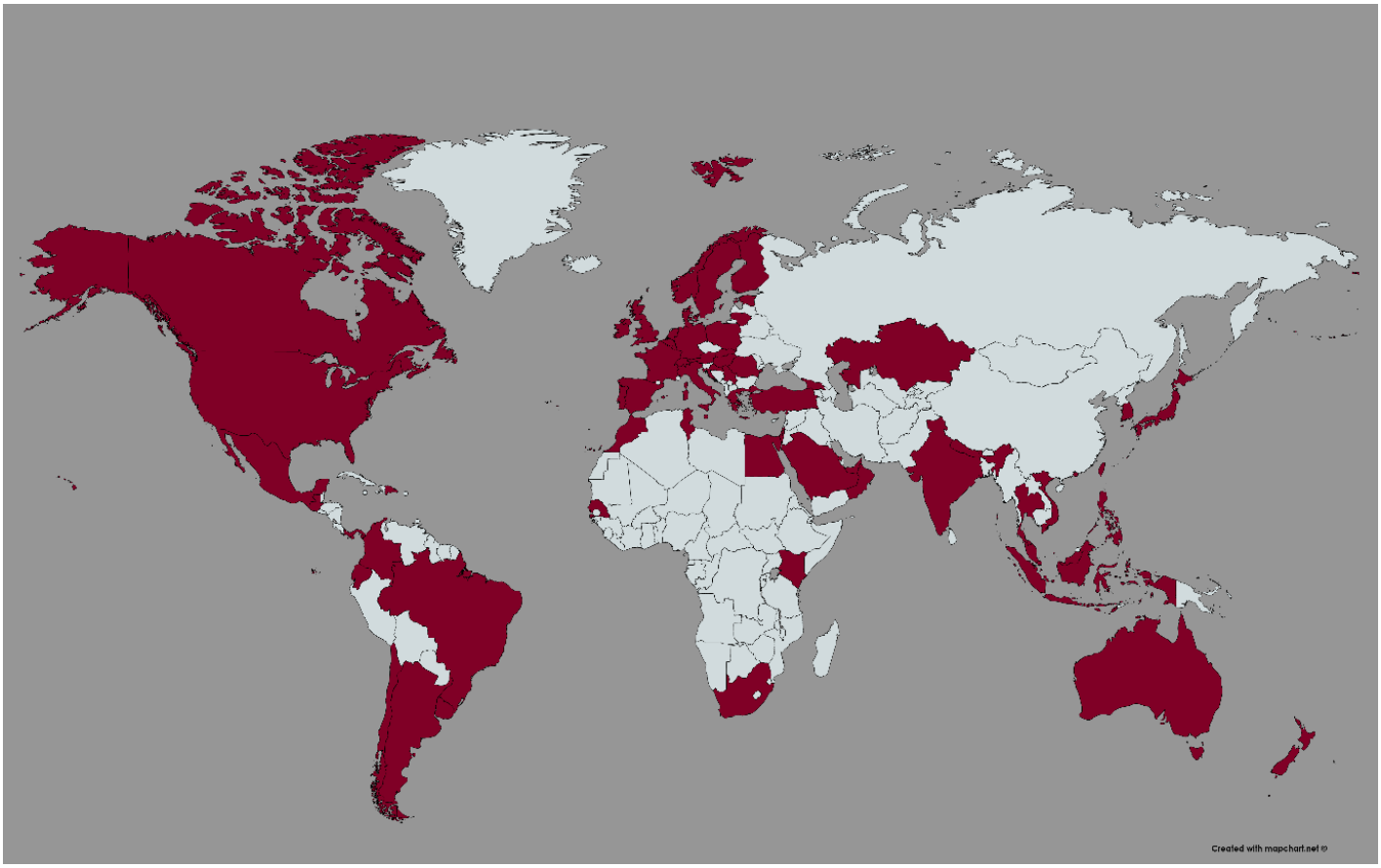
About CTI League Volunteers

Membership Growth

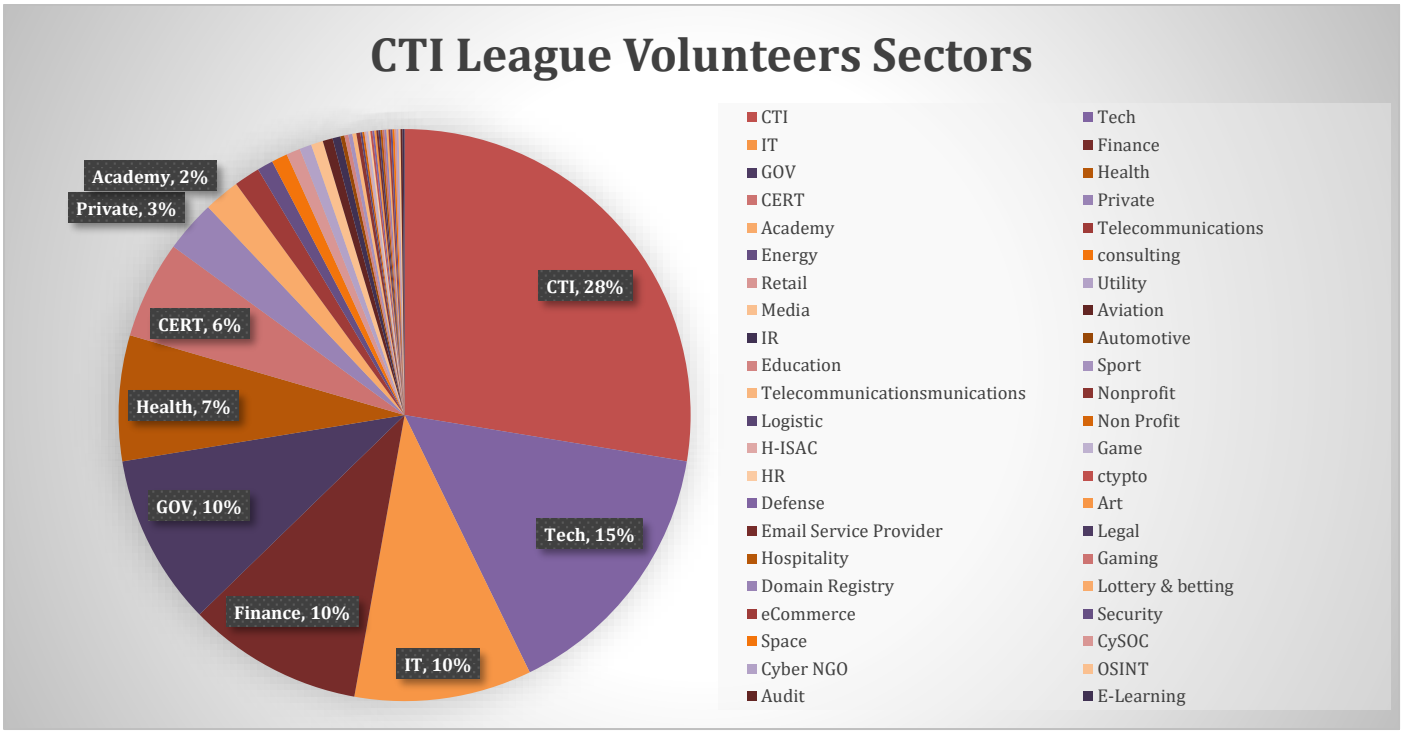
Established on the 14th March 2020, the CTI League grew from 2 users to over 100 volunteers in only one week. In 20 days, over 1000 new volunteers joined the league. Today, there are more than 1400 volunteers from almost 80 countries within the league.

Membership distribution

The CTI League is a community based on volunteers. In only one month, more than **1400 volunteers** joined the league. As the COVID-19 pandemic is a global problem, the CTI-League must be a global initiative. Our volunteers are based in 76 countries covering **22 time zones**. The CTI League has at least one representative from almost every continent (still looking for that recruit from Antarctica). The CTI League is a trusted community, which each one of the contacts is vetted by the managers with a validation process. Following is a map of our volunteers' locations.



All CTI League volunteers work in the cyber security domain and across **45 different sectors**. Most of the volunteers work within the cyber threat intelligence sector (28%). One quarter (25%) of the people work in Information Security for the IT and Tech sectors.



The CTI League welcomes collaboration with Computer Emergency Readiness Teams (CERTs) and Law Enforcement agencies. Within the group, 10% of the people are from governmental organizations worldwide, 6% of the volunteers are from national CERTs, and 7% of the people work directly in the medical and health sectors. We believe this direct collaboration between the security industry, government, and law enforcement is at the heart of what makes it so successful.

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. We define triage as high priority indicator of compromise (IoC) 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.

Takedowns

CTI League volunteers requested takedowns of 2,833 IoCs from the internet in the past month. Most of the indicators requested for takedown were malicious domains (2818, 99.4%). Here are examples of governmental institution impersonation takedowns:

Impersonators subject (Institutions)	Amount
By territory	
United States	4
United Kingdom	2
Canada	4
Denmark	1
Morocco	1
Brazil	1
By organization	
UN	1
WHO	3
CDC	1
HHS	4

Furthermore, the CTI League handled a few takedowns of specific attacks that were reported to the relevant organization for the takedown. Examples of this activity:

1. DDoS attack against governmental organization (notification to Amazon)
2. Malicious email notifications to Google's CyberCrime Investigation Group (CCIG)
3. Compromised companies for notification/remediation to FBI

Triage

CTI League volunteers can triage any indicator or vulnerability for the medical sector using the triage channels. Moreover, our volunteers can use a simple workflow within the relevant feed's channel. We launched this service on the 31st of March; thus, the information reflects only one week of data.

Medical vulnerabilities triaged:

Country	Amount
United States	24
Poland	1
Swiss	1

Law Enforcement Agency Escalations

As 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. The following are examples of relevant issues for escalation:

- Criminal activity in the cyber domain
- Threats against national security
- Ineffective takedown process (in international campaigns for example)
- Urgent reporting to a medical facility
- Issues impacting government infrastructure
- Large scale information relevant to a specific country

Support

General

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

1. CTI League monitoring streaming:
    a. Medical infrastructure vulnerabilities
    b. Malicious files
    c. Malicious domains and subdomains
2. External feeds and services collaborate with the CTI League
3. Information sharing by CTI League members

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

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 info@cti-league.com
2. Raising issues within the relevant channel by one of CTI League volunteers. Or volunteers receive reports on relevant support requests from the medical sector and share these requests 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 medical organizations within their countries.

In the medical support channel, our League volunteers 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 utilize it to prevent attacks.

Infrastructure Support

The CTI League offers support to protect critical infrastructure, especially those running in medical institutions, healthcare providers and their supporting organizations (testing laboratories, equipment suppliers, infrastructure providers etc.).

The CTI League creates discussions around availability and capacity, enriching the knowledge of League volunteers about trends, vulnerabilities, and capabilities.

The CTI League provides the medical sector and relevant organizations (such as national CERTs) 24/7 streaming of infrastructure vulnerabilities in organizations important to our mission. Each day, we identify thousands of vulnerable servers within relevant organizations, vet them within our systems, and engage the appropriate partners to notify the affected parties. Currently, we are searching information with 6 languages and working on adding more. In this section, we will examine our findings in March 2020. Within the streaming group, more than 10% of the messages are organic (made by League volunteers).

The CTI League discovered more than **2000 vulnerabilities** (136.07 vulnerabilities per day in average) in hospitals, healthcare facilities, and their supporting organizations. These organizations are in more than **80 countries** world-wide, some of which are not taking an active part in the CTI League. For example, this is a list of vulnerable servers reported to the law enforcement agencies within the first week of the CTI League:

- Pulse VPN (CVE-2019-11510): **22**
- Citrix Netscaler (CVE-2019-19781): **21**
- BlueKeep vulnerability (CVE-2019-0708): **2**
- SMBGhost vulnerability (CVE-2020-0796: **2**
- Less prioritized CVE vulnerabilities: **5**
- exposed Xero Universal Viewer instances: **3**

Within all the issues, several issues were so severe that the vulnerable entities were directly contacted by CTI League collaborators. 10 global organizations escalated vulnerabilities to the law enforcement agencies and helped with the outreach.

CTI League volunteers share data about tens of thousands of vulnerable and compromised servers from the dark web. The information is triaged as high priority and provided to the law enforcement agencies and national CERTs.

Compromised credentials program

CTI League volunteers identify compromised credentials relevant to the medical and other related sectors within the internet and the dark web. These credentials can be used for hacking the compromised organization, blackmailing, or as a platform for future attacks by the threat actor. We launched this service on the 31st of March.

A large amount of the credentials reported by CTI League volunteers was stolen from breached sites, which we see hundreds each week. For example, in the first week of April, data regarding more than 400 websites was streamed to a dedicated channel, examined by CTI League volunteers, and reported directly to the breached organization or the appropriate CERT for reporting.

This program takes lists of stolen credentials and processes them. When we find a match on either Microsoft Account (consumer) or Azure Active Directory (Commercial), we place those users into a compromised account workflow.

Malware and Phishing Streaming

The CTI League investigates files and messages identified by several external public sources. These malicious items are then triaged two different ways. The league's automated analysis engines ran malicious files reported from public malware repositories through Antivirus scanning engines. These files were then scored in terms of how many different AV scanners were able to detect them. The result of that analysis is listed below.

A total of 587 files was reported to the CTI League. These were assigned 3 different levels of Antivirus detections:

- Well detected for items that were flagged by most Antivirus engines = 198
- Poor detection for things that were only detected by a few Antivirus engines = 374
- Low/Undetected for files that were not detected by any of the public Antivirus engines = 15

The undetected files were subsequently triaged and flagged for antivirus analysis.

Phishing domains are identified by scanners in repositories of domains. More than 20,000 phishing domains were identified and reported to the CTI League, and 2584 confirmed phishing messages.

Confirmed phishing messages are analyzed for IoCs such as domains which are then fed into the IoC triage process or the domain takedown process. IP addresses exhibiting malicious behavior are reported to the relevant ISP or registrar that is responsible for them.

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 repository can be divided into 2 sections:

1. Public release - Files vetted and approved for the public contains blocklists (by hash, IP, and domain) and, a list of known bad actors. This option is open for publication for anyone in need. In this GitHub, our volunteers can find:
    a. Vetted blocklists based on IP address (19), URLs (2308), domains (6067), and hash values (2503) 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 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 presented within GitHub for CTI League volunteers only.

Incident Response

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

Disinformation

General

The CTI League neutralizes any threat in the cyber domain regarding the current pandemic, including disinformation. The mission of this effort is to find, analyze, and coordinate responses to the current pandemic disinformation incidents as they happen, and where our specialist skills and connections are most useful. Disinformation is a new workstream within the league. Formed Wednesday 8th April, it has already hit the ground and is tracking several major disinformation campaigns.

Campaigns investigated

These are examples of some of the campaigns investigated by the CTI League:

Campaign	Purpose	Vector
COVID-5G	Associate COVID-19 spread with the distribution of 5G equipment	Spreading via multiple vectors - Youtube videos, Facebook Groups and images, Twitter images and more.
WeWontStayHome	Encourage citizens to break quarantine	Primarily an Image seen on Facebook "no more lockdowns" with hashtags #wewontstayhome #alljobsareessential
Texasffrally	Incite “Texas Freedom Force” rallies	Image seen on Twitter 1st & 2nd amendment rally at The Alamo, April 25th, 2020, hosted by this is Texas Freedom Force and Open Carry Texas, posted by @thisistexasff
OperationGridlocck	Started in Michigan but spreading, an attempt to incite vehicular based rallies to cause noise and ultimately gridlock streets.	Image seen on Twitter of Facebook "operation gridlock" pages

CTI League General

Code of Conduct

Please review the 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/

CTI League Services

Please review the CTI League services statement:

https://cti-league.com/services/

OPEN LETTER FOR THE MEDICAL SECTOR

Please review the CTI League open letter for the medical sector:

https://cti-league.com/open-letter/