Global Cyber Alliance Initiatives

Overview

The Global Cyber Alliance (GCA) is an international, cross-sector effort dedicated to reducing cyber risk and improving our connected world. We achieve our mission by uniting global communities, implementing concrete solutions, and measuring the effort of those solutions. GCA, a 501(c)(3) in the US and a nonprofit in the UK and Belgium, was founded in September 2015 by the Manhattan District Attorney's Office, the City of London Police, and the Center for Internet Security.

GCA's first major project – the protective Domain Name Service Quad9 – is a global success story that has reduced the number of anti-virus infections by 50% and reduced alerts from intrusion detection systems by about one-third, globally. On average, Quad9 blocks more than 60 million malicious domains on a daily basis, all while protecting the privacy of its users, and for a near-zero marginal cost.

Building on the success of Quad9, GCA has initiated a number of new projects that aim to have an equal or greater impact on cybersecurity worldwide.

Current Initiatives

Domain Trust (DT) brings together key stakeholders from the law enforcement, threat intelligence, domain registries/registrars and telecommunications communities. Through the use of DT these organizations will be able to share and collate data on criminal domains within the principles of the UK's Information Commissioner's Office "sharing data for good."

Through an intelligence-source taxonomy, DT will provide the necessary corroboration required by registries as a basis to suspend or even take down domains.

Foundation partners for this project are CentralNic, BT, ICANN, and the City of London Police. The project has been joined by APWG, Netcraft, PIR (.org) and EURid (.eu). Talks with Internet Service Providers and other registries and registrars are ongoing.

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is an international standard that is used to authenticate the sender of an email. It prevents criminals from sending emails using a legitimate email address, a leading method of carrying out phishing campaigns.

- GCA held two DMARC "Bootcamps" in 2020, training more than 2,150 registrants from more than 50 countries.
- GCA produced a DMARC guide that is available in 18 languages and has been accessed by more than 200 countries and 10,000 cities.
- GCA's advocacy of DMARC played an important role in the decision by the U.S. government to adopt DMARC as a government standard across all federal civilian agencies and likely influenced similar decisions by the governments of Australia and New Zealand.
- GCA co-hosted an event in October 2017 where the U.S. Department of Homeland Security (DHS) announced a directive to all U.S. civilian agencies to deploy DMARC; followed shortly by the U.S. Department of Defense issuing a similar mandate
- GCA advocated for and influenced the adoption of DMARC as a standard across all U.S. federal agencies.
- As of October 2018, use of DMARC likely reduced cybercrime losses as a result of Business Email Compromises (BEC) by $19 million per year.[1]

GCA provides an online setup guide alongside literature, bootcamps, and dedicated webinars to help promote global adoption.

GCA built and released the Automated IoT Defence Ecosystem (AIDE): a platform designed to help organizations protect Internet of Things (IoT) devices. AIDE collects data from a globe-spanning honey-farm with hundreds of nodes and records an average of 9.5 million attacks per day. It can also ingest data feeds from external organizations that may also use the platform. AIDE's 12 terabytes of IoT attack data can be made available, particularly for projects of mutual interest, to IoT device manufacturers, academics, security researchers, and policy-makers.

GCA has developed proxypot technology that allows for the rapid deployment of IoT honeypots of both emulated and real devices easier and more cost-effective than other approaches.

[1] https://www.globalcyberalliance.org/wpcontent/uploads/GCA-ROI-FULL- report 102618.pdf

GCA created a set of cybersecurity toolkits that are designed to improve the cyber hygiene of users in specific, high-risk communities. Each toolkit contains a collection of free-but-effective solutions from a variety of cybersecurity product and service companies that have been shown to reduce cyber risk by as much as 85%.

The three GCA toolkits are designed to support small businesses, organizations responsible for conducting elections, and journalists. The small business toolkit is available in English, French, German, Spanish, and Bahasa and is offered as a business resource by several organizations including Mastercard, Salesforce Trailhead, and the U.S. National Institute of Standards and Technology.

Projects Under Development

Routing Security

The GCA Routing Security project aims to provide network operators and policy makers with concrete data about the state of routing security for the Internet. GCA is a global, neutral party that can extract an objective picture while fostering discussion among the key players that need to collaborate and agree on a path forward for future improvements to routing security.

DMARC Intelligence

GCA has helped more than 10,800 businesses implement DMARC. As useful as this has been for discrete organizations, online criminals often target many organizations at the same time in a single malicious campaign. DMARC Intelligence will aggregate such data to deliver a broader and deeper view of malicious activity.

Law Enforcement Application

The Law Enforcement Application is a GCA-led effort to promulgate accessible knowledge about a wide-range of cybercrimes to frontline officers, enabling them to more rapidly and effectively interact with victims. It is a global capacity-building effort with the potential to reduce the impact of such crimes, stifle their proliferation, as well as increase the number of successful convictions of such crimes at the local, national, and international levels.

Exploratory

Ideas that have not been fully evaluated or approved, but are reflective of GCA's efforts to develop concrete solutions to systemic problems in cybersecurity.

Cyber Workforce 'Wonderlic'

The cybersecurity workforce shortage is real, but it is exacerbated by the organizations recruit and staff security positions. Aptitude testing can help identify individuals from any background or education level who have the potential to succeed in such careers, and the delivery of such testing through partners with strong ties to traditionally underrepresented communities can open up opportunities for large swaths of the workforce who might not otherwise be considered for such roles.

Help Reduce Cyber Risk

Cybersecurity issues have been a problem for more than 30 years. Success in combating malicious activity is only possible working together, at the right level, and at the proper scale. Support GCA and join a global network of like-minded organizations that are working to ensure that the Internet remains a net positive in our lives.