GCA Founders

GLOBAL PARTNERS

Belgium: 1
China: 1
Egypt: 1
Finland: 1
France: 6
Georgia: 1
Germany: 2
India: 1
Ireland: 1
Israel: 1
Jamaica: 1
Japan: 1

Netherlands: 3
Nigeria: 1
Norway: 1
Oman: 1
Russia: 1
Spain: 1
Switzerland: 2
Uganda: 1
United Kingdom: 49
United States: 106

GLOBAL CYBER ALLIANCE

REMEMBER: CYBER CRIME IS JUST CRIME

STICK CRIME

GUN CRIME

CYBER CRIME

TIME CRIME

QUANTOM CRIME
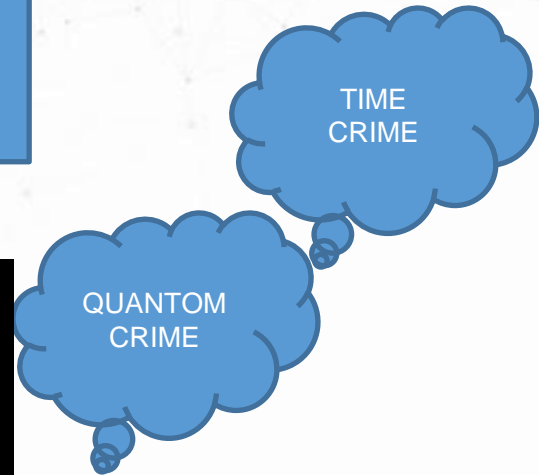
Addressing Systemic Cyber Risks

Systemic cyber risks affect more than one organization, are above the enterprise level, and are material

How was the internet formed?

"43.7 per cent of all statistics are made up on the spot."

Steven Wright

PHISING IS THE ROOT OF 80% OF CYBER CRIME

77% OF MAIL DOMAINS CAN BE SPOOFED

3% OF PEOPLE OPEN MARKETING EMAILS
7% OF PEOPLE OPEN PHISING MAILS

SOLUTION:

DMARC

A PROVEN WAY TO MITIGATE RISK

Domain-based Message Authentication, Reporting and Conformance (DMARC)
It's like an identity check for your organization's domain name.

The Power of DMARC: Aetna Case Study

Aetna followed leading banks and Internet Service Providers (ISPs) by implementing a trusted email program based on the DMARC standard in early 2015. This program was carefully planned and executed to include all third parties sending email on behalf of Aetna. Today, Aetna email subscribers do not receive SPAM or illegitimate email – including phishing attempts – from any email address associated with Aetna.
Each year, the program prevents approximately **60 million fraudulent email messages from being delivered**. The result is lower risk and better engagement: click-through rates on Aetna emails improve by 10 percent every year. DMARC adds a trust component to emails and is a core component to Aetna's trusted email program.

The Power of DMARC: UK HMRC Case Study

In one year we've stopped **300 million phishing emails that were fraudulently using our email address.** If we can do it anyone can! GCA is doing a great job helping organisations with practical solutions to loading DMARC.

– Ed Tucker, Head of Her Majesty's Revenue and Customs Cyber Security

Efficacy to Date

- Tool launched October 2016
- More than 9,400 users of the Setup Guide
- From more than 150 countries
- More than 3,100 cities
- Almost 10,000 unique domains tested
- More than 19% conversion rate (1,900+ domains)

B.I.M.I.
BRAND INDICATORS FOR MESSAGE IDENTIFICATION

https://authindicators.github.io/rfc-brand-indicators-for-message-identification/

Internet Immune System
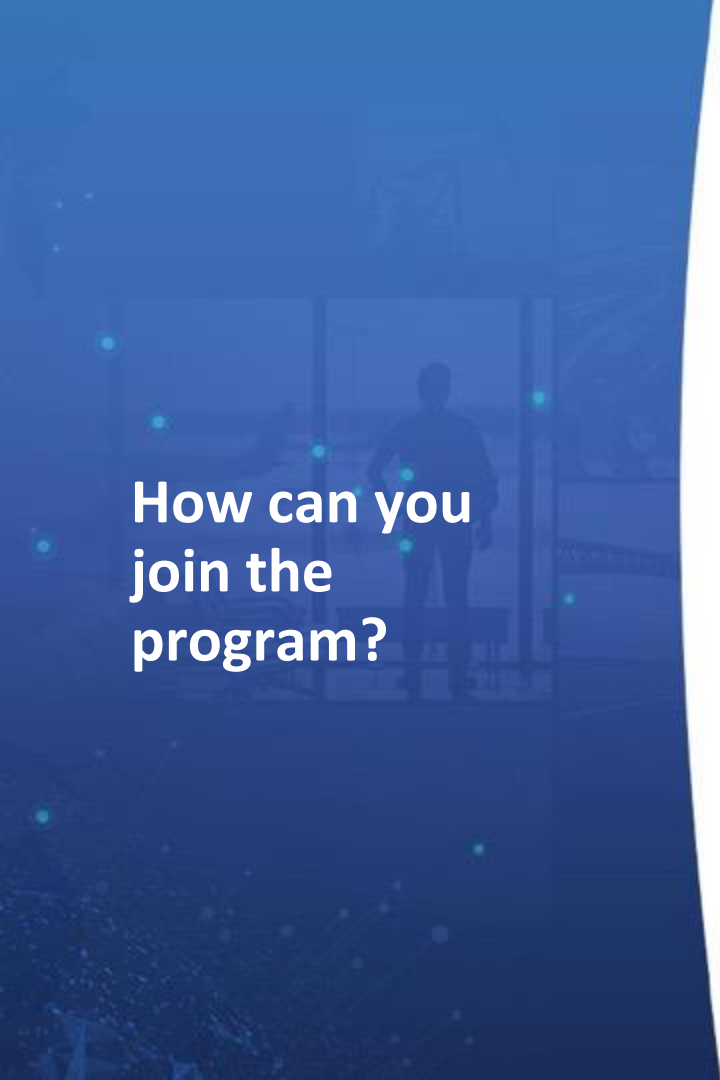## Protecting Users and Networks via DNS

How Our DNS Project is Different

- Focus on "operationalizing" Threat Intel that is "at rest" in a DNS filtering sense from security vendors
- A strong focus on preserving privacy for users
- **We do not provide individualized reports/reporting**
- We focus on malware c2 domains, exploit kit domains, phishing domains, etc.
- Platform is populated by crowdsourcing threat intel from many providers (commercial and non-commercial)
- Creates a compound view of the threat landscape!

Efficacy to Date

- Average of 60-120M queries a day

- Peak of 1M blocks a day

- Average up to 30K a day

- 1M domains in list (varies)

- 18 threat intelligence feeds

- Deployed on 5 continents

- One adopter saw 50% decrease in AV alerts, and 30% decrease in IDS alerts

- 35 resolvers

How can you join the program?

WE LAUNCH ON 16TH NOVEMBER 2017

TUNE IN !!

gca-dns@globalcyberalliance.org

@andycyberbates

150,000,000?

45,000 LISTED

INTERNET
PROVDIERS
1000 ?

GLOBAL ISP
* 100 ?

EVERYONE HAS AN INTERNET CONNECTION

INCLUDING THE BAD GUYS

SO THAT'S ALWAYS A GOOD PLACE TO START THE CLEANUP

WHERE NEXT ?

IOT, IOT & IOT

GDPR

COMMON CYBER RANGE

INTEL SHARING

BETTER REPORTING

THE BAD GUYS SHARE INTEL BUT THE GOOD GUYS FIND THIS DIFFICULT,
SO WHO IS SMARTER ?

THE BAD GUYS ARE AN INTERNATIONAL STATELESS FORCE

SO AM IN ? ARE YOU ?

WHAT NEXT

- WE BUILD THINGS TO MAKE THE INTERNET SAFER

- WE GIVE THEM AWAY

- BRING US YOUR IDEAS

- YOU ARE NOT ALONE

- WE WILL WORK WITH YOU TO BUILD COMMON SOLUTIONS TO GLOBAL PROBLEMS

24

MACHINES BUILD CARS BUT PEOPLE WRITE CODE??????

PEOPLE ARE FALLIBLE SO HACKERS GET THROUGH VULNERABILITIES

CODE IS EXPENSIVE SO WE COPY IT MILLIONS OF TIMES

SO WHY DON'T MACHINES WRITE CODE??

H.P.R.A.D.

10,000,000,000 reduction in attack surface

DON'T SWITCH THIS OFF WHEN YOU SWITCH TECHNOLOGY ON

BUT
DO <u>AUGMENT</u> IT WITH AI AND MACHINE LEARNING

Thank You!

www.GlobalCyberAlliance.org

abates@GlobalCyberAlliance.org

@GlobalCyberAlln

@andycyberbates