Fake Flash Update Targeting Sports Fans

By Sports Reporter on July 6, 2019 - No Comment
WHO WE ARE & HOW THIS BEGAN

- Sports-ISAO: Program Office of Cyber Resilience Institute (CRI)
- CRI: Nonprofit with a mission of building cyber capacity in communities
- ISAO and Pop-up SOC operations began in 2016 to demonstrate a crowdsourced cyber threat and information sharing operation; a key component was an internship of college students

- 2016 → Rio Olympics
- 2017 → IAAF World Championships
- 2018 → Winter Olympics PyeongChang
- 2018 → World Cup Russia
- 2019 → World Cup France
ANALYSTS FOR THE WORKFORCE – A PATHWAY

- Community Cyber Capacity
- Adversary Strategy
- Crowd-sourcing
- ISAO Programs
THE ELIXIR OF SPORT

• Students from over 40 universities – the CrowdWatch

• First college student club at UCCS

• Adversaries: Proving ground for new variants and TTP

Total TV ad spend: $1.5B
New spend quadrupled: $548M
Budweiser: $33.2M
Amazon: $27.5 million
THE ELIXIR OF SPORT

• Magnetism = Demand
• Translation: Workforce
US ‘CYBERSECURITY’ STRATEGY

• 2009 White House ‘Cyberspace’ Policy Review

• 2015 DOD Cyber Strategy: "The United States is committed to an open, secure, interoperable, and reliable Internet that enables prosperity, public safety, and the free flow of commerce and ideas."
ADVERSARY STRATEGY AND TACTICS

• Mueller Report: “Russia interfered in the 2016 presidential election in sweeping and systematic fashion”
• And China
• And …
Russian foreign minister: We're banned from Olympics because U.S. 'can't beat us fairly'
INCREASED USE OF CYBER IN STRATEGY

2015 Russian National Security Strategy

"increase the competitiveness and international prestige of the Russian Federation."

Russian view:
U.S. Doctrine and Strategy are anti-Russian.
RUSSIA

The Foundations of Geopolitics: The Geopolitical Future of Russia
Aleksandr Dugin

"the maximum task is the 'Finlandization' of all of Europe"

The United Kingdom should be cut off from Europe

Ukraine should be annexed by Russia because "Ukraine as a state has no geopolitical meaning"

"Moscow-Tehran axis": Iran is a key ally
The US narrative: Russia must spread Anti-Americanism everywhere: "the main 'scapegoat' will be precisely the U.S."

In the United States:
• Russia should use its special services within the borders of the United States to fuel instability and separatism, for instance, provoke "Afro-American racists".
• Russia should "introduce geopolitical disorder into internal American activity, encouraging all kinds of separatism and ethnic, social and racial conflicts, actively supporting all dissident movements – extremist, racist, and sectarian groups, thus destabilizing internal political processes in the U.S.
• It would also make sense simultaneously to support isolationist tendencies in American politics."
SOCIAL MEDIA TACTICS

**Bots:** One-third of tweets about Brexit came from just 1% of Brexit-related Twitter Accounts

- 54% Leave
- 20% Stay

Researchers say there has been a surge in the activity of Twitter bots ahead of Britain’s EU referendum on Thursday. They found just one per cent of 300,000 Twitter accounts posting about the referendum were responsible for a third of the activity, indicating they are automated accounts (such as @IVoteLeave pictured).
USE OF BOTS

FCC Net Neutrality Vote

Pew Research Center: >Half of comments from duplicate or temporary email addresses

Bots!
A FOCUS ON RUSSIA

Clinton Watts

Russian exploitation of social media
ATTACKING THE PUBLIC-PRIVATE GAP

Russian Internet Research Agency

aka
Troll Farm

St. Petersburg organization

100s of paid Kremlin Backers having a quota of posts/day
Jan 26 media reporting:
Dutch Intelligence monitored Fancy Bear – identifying the building and Kremlin-tied hackers – WHILE DNC hack was underway!!!

Best Evidence Yet: Fancy Bear is Kremlin Run
- hacked cameras and captured video
The cyber landscape has
in just 15 – 20 years
transitioned from web defacement
To identity theft and credit card fraud
To permanent presence hacking for longer term exploitation
To state actor attacks on critical infrastructure that threaten public safety

To a state of asymmetric warfare that includes turning open democracies against one another through propaganda messages and distribution platforms
MAKING MONEY FROM SPORTS ADVERTISING

e.g. Methbot
Look-out For Android Ad Scams

The Sports-ISAO threat hunting teams have identified a series of Ad Scams that are currently targeting viewers of Women’s World Cup 2019 websites. One of the most sophisticated we have run across we are calling Shreembit. It is a fraud scheme where the threat actors promote alternative streaming video websites that serve as malware infection vectors for Android mobile devices and Windows-based operating systems.

USA W vs France W live streams
FRRREEEEE

livestreams.cf/2019/06/france...

#FIFAWWC #FRAUSA #OneNationOneTeam #FRAUSA #USWNT #USA_vs_France #FRAUSA #USAvFRA #FRAUSA #USAFA
The CrowdWatch network
CROWDWATCH USE CASES

ISAO enabler

Community Workforce Program

Outsourced Analysis
“Cybersecurity (and IT in general) are not the same as computer science. Traditional computer science can be helpful, but it's not the full story.”

But there's also all the knowledge needed about how current systems work, which computer science doesn't necessarily prepare you for.

Hiring practice is also all over the map. Generally, cybersecurity jobs (like this one for a U.S. Navy Cyberwarfare engineer) require 4-year college degrees. Many others require experience and industry standard certifications.
**KEY SKILLS & KNOWLEDGE**

- ISAOs and national efforts
- Legal & Policy issues in cyber threat intelligence
- Social media intelligence
- Automated cyber threat exchange – STIX/TAXII
- SOC Operations & Collection Management
- Actionable intelligence
- Report Writing
THE EXPERIENTIAL LEARNING COMPONENT

• Three Tracks
• Interdisciplinary Teams
• Mentor Oversight
• Capstone: Major Sport Event
ACHIEVING THE ISAO MISSION

THE CHASM BETWEEN CYBER POLICY ... AND REALITY

THE GAP: A BUSINESS MODEL TO MAKE POLICY HAPPEN

* Executive Order 13691

Share information ... in as close to real time as possible.

**

Quoted from a Community Cyber Program in a major US city

We are 100% volunteers.**

ISAOs are Part of the Solution

CrowdWatch enables ISAO Formation
JOBS, RESEARCH, AND STAFF AUGMENTATION

• PLACEMENT: 2016-19 INTERNS HIRED BY FIREEYE, USIC, SYMANTEC, BLUECOAT, FORENSICS COMPANY IN OHIO, ETC.

• OUTSOURCED RESEARCH AND STAFF AUGMENTATION TALKS: STATE, SPORT GROUPS, DHS

• HSIN SPORTS-ISAO COMMUNITY OF INTEREST

• GRIDEX 2019
PRIVATE-PUBLIC PARTNERSHIP

“PARTNERSHIP” – WHAT IT MEANS
TOKYO OLYMPICS

C-WATCH ENROLLMENT 2020
STATE DEPARTMENT TIER 1 RESPONSE
EMBASSY REPORTING/FBI CYWATCH/DHS NCCIC
CALL TO ACTION

• Grassroots petition for Community Cyber Capacity Building

• 20+ signatories so far

• Specific Outcome: to add “Community Cyber Capacity” to the DHS National Critical Function List of the National Risk Management Center
QUESTIONS

www.cyberresilienceinstitute.org

www.sports-isao.org

www.c-market.us

Doug.depeppe@cyberresilienceinstitute.org