A study of the Port of Charleston evacuation and closure: How Live Action Role Play (LARP) Simulations create Cognitive Threat Vectors

June 2017

Dave Sweigert, M.Sci.

ABSTRACT

Examination of the Port of Charleston emergency evacuation and closure deliberately caused by anti-government social media "conspiracy theorists" is a harbinger of things to come. Role planning games that weaponize sensationalized "crowd-sourced" information represent a new emerging threat to critical infrastructure operators. Note: this paper is scholarly research and distributed for discussion purposes only.

Executive Summary

On June 15, 2017 two YouTube "conspiracy theorists", known as Jason Goodman and George Webb, created a sense of hysteria amongst LiveStream "crowd source" fans that the container ship Maersk Memphis was sailing into the Port of Charleston with a "dirty bomb" onboard.

These "online researchers" set events in motion that led to the evacuation of part of the port. A rigorous bomb sweep was conducted with nothing found.

The two apparently operate the web-site "CrowdSourceTheTruth", a Live Action Role Play (LARP) site, that seeks the help of fans to solve mysteries and conspiracy theories. The premise of this LARP is the distribution of "INTEL", in real-time, of information submitted by on-line fans. Webb/Goodman then form conclusions as to threats. The "threat" is broadcast to the LARP players with a soft inducement; a call to action is apparently inferred, and soon fans begin notifying authorities to warn of the threat.

Unfortunately, in the case of the Port of Charleston, dirty bomb warnings were received from multiple LARP players. Apparently, the intake of multiple sources of threat information demanded action, forcing the Port to be closed. Thankfully no was hurt during this bomb hoax.

Cognitive Threat Vector ("hack")

It is instructive to view the "crowdsource intelligence" and this LARP "fusion center game" in the context of cognitive threats to critical infrastructure.

A threat vector is a path or a tool that a threat actor uses to attack a target. Threat targets can be anything of value to the threat actors.

In this case it appears that participants within the LARP are lead to believe that actionable evidence exists of an urgent nature that requires action (e.g. notify Port Security of an incoming dirty bomb).

The "crowdsource" plot is advanced by the game controllers leading players to a call for action.

Potential for malicious use

This “fusion center game show” format purports to follow the process to source, validate and disseminate intelligence. This apparently legitimate process can be sensationalized by the game controllers to co-opt participants.

To be effective, LARP game controllers hold authority positions, such as reputable journalists or “internet researchers”. Webb/Goodman are fond of telling their LARP players that they are “internet researchers conducting an independent investigation” of current topics (ranging from who killed Seth Rich to human trafficking).

Viewers appear to be specifically vulnerable to inclusive roleplay which simulates real time espionage efforts through mock clandestine scenarios produced on video for dissemination through various social media platforms.

This message then becomes cognitively invasive, working exponentially, per viewer, with each comment further forming a directed opinion, adding validation to a fabricated scenario.

The exponential contamination of LARP players grows, regardless of viewer opinion. Negative and positive opinions build further accreditation for fabricated clandestine acts as viewers clash.

A cognitive worm is created which appears based on “crowdsourced data”. Debating amongst players, causes viral spread of cognitive worm, causing exponential viewers and mediums of dissemination. This eventually leads to player hysteria, angst or fear.

When critical mass is achieved and it appears the players have identified information requiring urgent action, then a call to action is inferred. Such calls to action could include botnet attacks, distributed denial of service (DDOS) attacks, public relations campaigns to disparage public officials, infrastructure operators, etc.

This type of threat vector can be added as an overlay to underlying cyber threats to create a multi-layer attack which critical infrastructure operators need to be aware of.

Urgent calls to action by unwitting players (port evacuation) can augment, amplify and mask other accompanying attacks. The fact that this new format of “crowdsourcing” represents a threat to owners and operators of critical infrastructure was clearly demonstrated in the case of the Port of Charleston.

Distribution of clandestine files

Two weeks prior to the Port of Charleston event, Webb/Goodman coordinated an on-line distribution of 1.1 Gb of files that they claimed were the property of the Democratic National Committee (DNC). The pair uploaded the files to a public document sharing site at the climax of two days of sensationalized on-line theatrical drama.

Then, in the early morning hours Webb/Goodman advised their audience it was crucial that they copy these files to their end-point computers to prevent forces working for the “deep state” from deleting these files.

Several hours after the mass download both Webb/Goodman announced that there was a possibility that beaconing malware may have been embedded in the files.

This is a troubling practice as the parties (Webb/Goodman) knew they were in possession of files they had no legitimate right to. Allegedly, these files contained Personal Identifiable Information (PII) of DNC donors; to include, names, home addresses, donations, etc.

These activities raises serious questions about LARP fans and devotees of Webb/Goodman that respond to their calls for action. This network, perhaps made up of unwitting participants, represents a type of cognitive botnet or DDOS-style attack ("beaconing" malware allegedly discovered after the mass download).

This demonstrates that with the right theatrical narrative, a network of LARP players can be induced into the potential commission of a federal or state crime.

Reputational damage to hospitals

Another disturbing tactic of this LARP style collaboration is the "investigation" into organ harvesting by American hospitals. Webb has distributed videos standing in front of hospitals while accusing the institution and staff of unethical organ transplants. In general terms, Webb classifies this under the category of "organ harvesting".

The potential for outraged LARP players to take action against such an institution should seem obvious.

"DOXing" of individuals

Another disturbing tactic used by the Webb/Goodman team is to reveal the PII of their enemies to their audience. Often times accompanied with a valid inducement that audience members should take some type of action against the dox'ed individual.

Doxing is the Internet-based practice of researching and broadcasting private or identifiable information (especially PII) about an individual or organization.

Summary

The totality of activities undertaken by the Webb/Goodman team should be troubling to healthcare institutions and critical infrastructure operators.

These activities (distribution of unauthorized software, crowdsourcing threat information that resulted in the closure of a major port, DOX'ing of individuals and inflicting reputational damage on institutions) should be taken very seriously.

These activities represent the future of a new kind of threat. The emerging trend towards such cognitive attack vectors should be understood and prepared for. Planners should consider that in the case of a multi-layer attack, such "soft" cognitive attacks can be used to mask and distract security personnel.

About the author

Unfortunately, George Webb Sweigert is the author's brother.