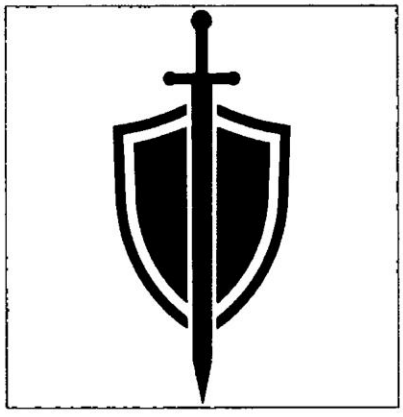

Sword and Shield
Digital Security, LLC

Cuyahoga County Email Bomb DOS...After Action Report

Easton Horner
CTO at Millennial Realty and Investments/White Hat Hacker SSDS
Published Sep 2, 2022

+ Follow

"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."

A free press is generally associated with the ability of people to speak their minds through writing, deliver news in newspapers, or on the air through open broadcast. This is indeed the primary meaning of the "free press" in the First Amendment.

But there is a second, less commonly used meaning. We as citizens enjoy the freedom of the press, as in the physical machine which uses movable block letter type to mass produce written communications. We have the right as citizens to buy one of these presses, print what we want, as much as we want, and paper the town.

PLAINTIFF'S EXHIBIT
BB

The modern equivalent of that movable block letter type press is an email server, and on Sept. 1st 2022, I used the protections afforded me under the First Amendment to launch a **#whitehat** "email bomb" DOS attack on the Cuyahoga County Courthouse in **#peacefulprotest** to their obscene practices. *(Full details can be found at www.Rights4Fathers.com, but that is another story.)* This document serves as an after-action report to those actions so the Cuyahoga County Courthouse may improve their systems.

Now before I go any further, let's clarify what an email bomb is so non-cybersecurity readers don't think there was real explosives being sent to a courthouse. An email bomb DOS is one of the oldest and most benign denial of service (**#DOS**) attacks an organization may face.

Simply put, a hacker sends so many emails to a target email server he crashes it. In the email bomb I used against the Cuyahoga County Courthouse for example, I sent ~12K+ copies of 1) The Holy **#Bible** 2) The **#Quaran** 3) The **#Torah** 4) The Works of **#Budda** and 5) The first 1000 lines of human chromosome 1 to Judge Tonya R. Jones and her staff attorney.

The purpose of the email bomb was to lock down both targets' emails and create a hectic morning for Judge Jones and Ms. Ross trying to solve IT problems which would force them to have to reschedule our 10:45a "Trial". The trial itself was the item being peacefully protested and Affidavit of Disqualification against Judge Jones and the Cuyahoga County Courthouse has already been sent to the Chief Justice of the Ohio Supreme Court, Honorable Chief Justice O'Conner.

If we were to imagine the email bomb performed by an old school press, the attack equates to delivering 12K+ copies of the referenced texts and blocking the doorway to the courthouse with them to prevent trial from being held. This action is clearly protected under the 1st Amendment to the US Constitution thus completing the "White Hat" criteria of the exercise. Our approach was just more **#ecofriendly** .

As a White Hat, my job is to not only break machines and systems but to diagnose how they were broken and most importantly how quickly they were fixed. In this case, the attack began at ~11pm on 8/31/2022. By design the attack started when both targets still had 7-8 hours before they would begin opening their email. This gave the bomb many hours to do its damage before being detected by their human targets.

The first indications of resistance by the targets was detected at ~10:15a. Target 1, Jones, had established a previous firewall against one of the three attacking servers. While technically cutting the bomb's yield by 1/3, in practicality 8K+ copies of the above referenced text is more than enough to accomplish the objective. The bomb was executed in triplicate from three separate locations to precisely overcome such a contingency. Sufficient yield was present to crash the email account.

The defended server was then re-directed to Target 3, the chief stenographer for the court. The previously established firewall was Jones and server specific. Once rediverted, successful bombardment on all three targets resumed from all three bombarding servers.

At 10:45a a broad-spectrum email blast to the entire Cuyahoga County Courthouse was sent to confirm my not being sent an invite link to the trail and the need to reschedule. This confirmed accomplishment of the primary objective of the email bomb. Email from the bombarding server was getting through the firewall.

The broad-spectrum email blast also served a secondary objective to notify the IT department of the bomb's source. The broad-spectrum email was sent from a different domain which tracked back to the same server the bomb was being launched from providing the opponent the opportunity to triangulate its bombarding server's position. Our goal with the white hat **#hack** was to force a rescheduling of the trial. Once accomplished, hints to help the opponent recover are appropriate white hat actions.

recover are appropriate white hat actions.

The bomb was rendered inert at approximately 1:30p with all members of the cuyahogacounty.us domain protected. Total time to stop the attack was approximately 14.5 hours.

Good Faith Suggestions for Improvement from Attacking White Hat:

- Stacking incoming bandwidth limits on a per email address, domain, and server basis. Certainly, there is an average amount of email the entire courthouse gets from a single person, firm, or email server a day. Go X% above that and the servers stop receiving email from the sender.

- Incoming bandwidth limits on a receiving @cuyahogacounty.us email address. Certainly, a Judge, staff attorney, and stenographer get an average amount of incoming email a day. They receive X% above that and it trips a circuit breaker which shunts/quarantines all additional incoming email to a secondary server to keep the primary up and running. This prevents coming into a production crash in the morning.

- Automated bandwidth threshold notifications to IT personnel so the IT person knew they were under attack at 1am instead of walking into it that morning with the job having run for 9 hours. Has an obvious manpower tradeoff which might not be worth it.

- Incorporate strong(er) data command screening logic. The CRON job deployed builds emails around programmatic/HTML commands which are easily identifiable from human generated email. They also mask the administrative emails for the server with the "senders" email peacefulprotest@xxxxx.tech. Spam filtering technology is well established to identify and nullify these telltale data command and email masking bomb signs.