IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA

DONNA CURLING, an individual, et al. Plaintiffs, v. BRIAN P. KEMP, in his individual capacity and his official capacity as Secretary of State of Georgia and Chair of the STATE ELECTION BOARD, et al., Defendants.	)	CIVIL ACTION FILE NO.:

AFFIDAVIT OF LOGAN LAMB

County of Fulton)
) ss.
State of Georgia)

LOGAN LAMB ("Affiant"), being of lawful age and first duly sworn upon oath, deposes and states as follows:

1. I am a cybersecurity researcher based in Atlanta. I have a BS and MS in computer engineering from University of Tennessee, Knoxville. I have worked professionally in cybersecurity since 2010. I started at Oak Ridge National Lab in the Cyber and Information Security Research group. At CISR I specialized in static and symbolic analysis of binaries. I also worked with embedded systems security and conducting security assessments for the federal government. I left ORNL in 2014 and joined Bastille Networks, a local startup where I am still employed. At Bastille Networks I specialize in wireless security and applications of software defined radio.

2. On August 23, 2016 I went to 130 Peachtree Street in an attempt to meet the Fulton County election supervisor Richard Barron with the hope of gaining access to voting systems equipment so that I could conducting a wireless security

assessment as a research project. There I was told to contact Merle King at Kennesaw State University because all election equipment is managed by the Center for Election Systems at KSU.

3. On August 24, 2016 I intended to contact Merle King. Prior to doing so, I wanted to check the Center for Election Systems public website to see if there were any public documents that could give me background on CES and Merle King. I used the search "site:elections.kennesaw.edu inurl:pdf" at www.google.com and discovered what appeared to be files relating to voter registration cached by google.

4. After this discovery, I wrote a quick script to download what public files were available here: https://elections.kennesaw.edu/sites/ , at the time a publicly accessible site. After running the script to completion I had acquired multiple gigabytes of data. This data was comprised of many different files and formats, but among them were:
   - voter registration databases filled with personally identifiable information of voters (filename *PollData.db3*)
   - Election Management System GEMs databases (.gbf and .mdb extensions)
   - PDFs of election day supervisor passwords, for example:
     - *July 2016 Primary and NP Election Runoff Password Memo.pdf*
   - Windows executables and DLLs, for example:
     - *System.Data.SQLite.DLL*
     - *ExpDbCreate.exe*
     - *ExpReport.exe*

5. Besides leaking information, the server at elections.kennesaw.edu was running a version of Drupal vulnerable to an exploit called drupageddon. Using drupageddon, an attacker can fully compromise a vulnerable server with ease. A

public advisory for drupageddon was release in 2014, alerting users that attackers would be able to execute, create, modify, and delete anything on the server.

On August 28, 2016 I sent an email to Merle King notifying him of the vulnerabilities I found.

Hello Merle,

My name is Logan Lamb, and I'm a cybersecurity researcher who is a member of Bastille Threat Research Team. We work to secure devices against new and existing wireless threats: https://www.bastille.net/. This past Tuesday I went to Fulton County Government Center to speak with Rick Barron about securing voting machines against wireless threats. I was then directed to contact you and the center. I'd like to collaborate with you on securing our state's election systems infrastructure against wireless attacks.

While attempting to get more background information on the center prior to contacting you, I discovered serious vulnerabilities affecting elections.kennesaw.edu.

The following google searches reveal documents that shouldn't be indexed and appear to be critical to the elections process. In addition, the Drupal install needs to be immediately upgraded from the current version, 7.31:

"site:elections.kennesaw.edu inurl:pdf"
I generally use this type of search to find documents on websites that lack search functionality. This search revealed a completely open Drupal install. Assume any document that requires authorization has already been downloaded without authorization.

"site:elections.kennesaw.edu L&A"
The second search result appears to be for disseminating critical voting system software. This is especially concerning because, as the following article states, there's a strong probability that your site is already compromised.
https://www.drupal.org/project/drupalgeddon
https://www.drupal.org/SA-CORE-2014-005

If you have any questions or concerns please contact me. I'm able to come to the center this Monday for a more thorough discussion.

Take care,
Logan

6. After having a brief conversation with Mr. King on August 29, 2016 and being assured that the issues would be remediated, I dropped the issue.

7. In late February, 2017 I told my colleague Chris Grayson about what transpired in August. He quickly confirmed the leaking of information had not been appropriately remediated. I tweaked my script and checked to see if it worked as it had in August.

8. The script was able to download the publicly available information. The data downloaded included the same data from the previous collection and new information relating to recent elections including:
   - More recent GEMs database files
   - Files relating to the presidential election, e.g.
     - *November 2016 General Election Day Password Memo.pdf*
     - *November 2016 General Voter Lookup Password Memo.pdf*
   - Very recent files, e.g. *064 (1-10-2017).pdf*

9. Given the severity and ease with which an attacker can use drupageddon, an attacker would have easily been able to gain full control of the server at elections.kennesaw.edu had they so wanted.

10. Having gained control of the server, an attacker could modify files that are downloaded by the end users of the website, potentially spreading malware to everyone who downloaded files from the website.

11. In addition to the previously mentioned files on the server, there were multiple training videos. One of these training videos instructed users to first download files from the elections.kennesaw.edu website, put those files on a memory card, and insert that card into their local county voting systems.

12. Further Affiant sayeth not.

Logan Lamb