Center for Elections System Incident – 03/01/2017

Incident background:

Stephen Gay (KSU CISO) was contacted by Professor [redacted] (KSU [redacted] Professor) regarding a 3rd-party report he had received from an "Atlanta based security firm". This initial call was at 9:29pm on Wednesday March 1st and alleged that through the use of [redacted] for counties across the State of Georgia. Stephen immediately activated the UITS incident response team to validate the vulnerability, which was confirmed by the senior engineer. Stephen notified Lectra Lawhorne (KSU CIO), at 11:00pm regarding the notice and vulnerability. At 11:20pm, [redacted]

b6
b7C
b7E

Potential Impact:

High. The discovered vulnerability is challenging to recreate, requiring [redacted]

b7E

Current progress:

Members of the UITS Information Security Office [redacted] met with members of the Center for Election Systems (Merle King, [redacted] and Michael Barnes) on 03/02/17 to discuss the incident, extract the logs for analysis, and begin aligning resources toward the hardening of the elections.kennesaw.edu servers. The Center Director, Mr. King, informed all parties that he would need to keep the Georgia Secretary of State "in the loop" since he (The Secretary of State) was the data custodian for the Center of Elections data. Mr. King further advised that he had been in contact with him regarding the incident and that the Secretary of State was "ok" with our investigation although he requested to receive regular updates.

b6
b7C
b7E

Stephen Gay briefed the CIO regarding the incident and notified the USG HelpDesk regarding this incident, per KSU Incident Response Procedures (USG Ticket number USG-INC0014152). At 11:00am on 3/2/17, UITS began [redacted] elections.kennesaw.edu [redacted] extend back to February 16th, 2017 due to system configuration and initial examination identified a single database file which contained 6.7 million records of what appears to the voter data. At 3:24pm, log review determined that:

- 40 IP Addresses accessed 1 or more database files
- 17 IP Addresses accessed 1 or more zip archives

At 4:30pm 3/2/17, a conference call was held with KSU Representatives, The Georgia Secretary of State's Office, The Center for Election Systems, KSU Legal Affairs, and others. The call was to bring all parties up to speed and discuss next steps. Under the direction of the KSU CIO, at 7:00pm 03/03/17, UITS staff members [redacted] met with Merle King and seized the center for elections system [redacted] (KSU Tag 103019). A chain of evidence form was completed for the transaction and the server locked in UITS ISO Secure Storage (Pilcher 109A) which is behind auditable locks.

b6
b7C
b7E

The initial incident reporter [redacted] provided the following activity from the security researcher at 8:00pm 3/3/17

- Wednesday 02/22/17 - 6:00PM - 12:00AM EST - traffic originated from an Atlanta IP address and an IP address from Switzerland
- Friday 02/24/17 - 12:00PM - 8:00PM EST - traffic originated from an Atlanta IP address
- Tuesday 02/28/17 - 5:00PM - 12:00AM EST - traffic originated from an Atlanta IP address
- Wednesday 03/01/17 - 7:00PM - 10:00PM EST - traffic originated from an Atlanta IP address

UITS ISO Staff are currently working to use this additional data to correlate events to actors.

From: Stephen C. Gay
Sent: Tuesday, March 21, 2017 4:15 PM
To: AT) (FBI)
Subject:
Attachments:

Agent

b6
b7C
b7E

Following up on the CD you provided Friday, a member of the team in a new spreadsheet (attached) which denotes any additional information we may have on I'm passing along in hopes that it will ultimately help you in determining whether there are

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director Information Security Office University Information Technology Services (UITS) Kennesaw State University Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050