
***Issued 9/21/18***

## Hackers have Planted Credit Card Stealing Malware on Local Government Payment Sites

Security firm FireEye has confirmed that a widely used web payment portal used to pay for local government services, like utilities and permits, has been targeted by hackers. Hackers have broken into self-hosted Click2Gov servers operated by local governments across the US, likely using a vulnerability in the portal's web server that allowed the attacker to upload malware to siphon off payment card data over a period of "weeks to numerous months," Nick Richard, principal threat intelligence analyst at FireEye, told TechCrunch. Superion, a major technology provider that owns the web payment portal Click2Gov, said in June following a confirmed breach last year that there was "no evidence" that the portal was unsafe to use amid reports of suspicious activity by customers. Superion issued patches after several customers complained that their credit card information had been stolen, but said that it was largely up to local governments and municipalities to patch their servers. But since then, several more local government sites were identified as victims of the malware. FireEye's incident response arm Mandiant said the hacker used the server vulnerability to upload a tool, which it calls FIREALARM, to sift through server log data for credit card data, while another piece of malware it's calling SPOTLIGHT to intercept credit card data from unencrypted network traffic. Once collected, the data is encoded and exfiltrated by the hacker. Credit card numbers, expiration dates, and verification numbers, along with names and addresses were stolen by the malware, the security firm said.