Providing Cybersecurity Support For the State of California

Chris Tharratt
Tharratt@umd.edu
Science Discovery and the Universe
Computer Science

Introduction

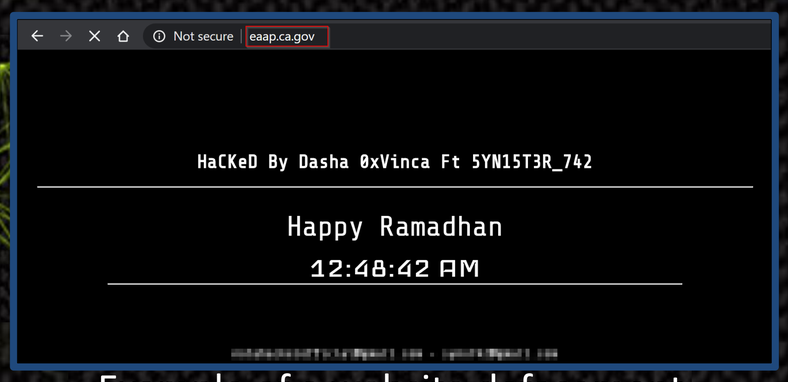
During the summer I interned at the California Cybersecurity Integration Center (CSIC). CSIC provides cybersecurity infrastructure for all entities in California. CSIC maintains the state cybersecurity strategy, provides up to date information on the latest cyber threats, and handles incident response across California.

@state.gov	_9KzuWd8
@dfeh.ca.gov	003437
@dss.ca.gov	bear1
@vcgcb.ca.gov	1995
@doj.ca.gov	doras1
@state.ca.gov	canyouhear
@.ca.gov	password
@lc.ca.gov	ddfxRBJiz
@ctc.ca.gov	NlbUoFs5M

A censored example of a password dump.
Source: Author

What was Done

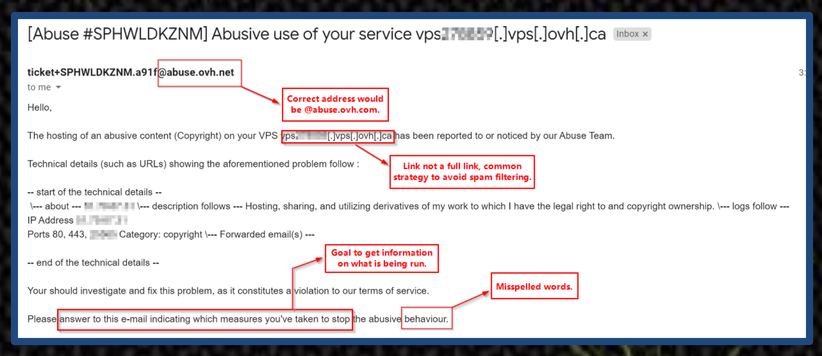
One of my main responsibilities at CSIC was taking public password dumps like the image above that are posted online and informing relevant parties about the leak. The most attacked target were California based universities and schools, due to a high likelihood of misconfigured networks combined with demands from students for high speed connections. Additionally I helped create vulnerability reports on the latest new malware, reporting on what the malware does, and how to mitigate the effects.



Example of a website defacement.
Source: Zone-H

Protection and Mitigation

The attack surface that hackers can exploit is large. Hackers may penetrate a network through a phishing email, or a misconfigured server on a network. You are only as strong as your weakest link, so it is vital to have strong password policies, and training to ensure you do not give accidental access to unauthorized users.



Example of a Phishing Email.
Source: Author

Impact

During my internship, I was able to inform more than 50 organizations of over 300 leaked credentials. Additionally, I helped create tools to better streamline vulnerability report generation. I gained valuable skills in attack and defend methodologies for large networks, and how intelligence analysis is done.

The entrance to CSIC.
Source: Author

Future Work

I enjoyed my time working at CSIC. I will continue to advance my Cybsersecurity knowledge through future internships, but likely not at CSIC. I want to pursue other opportunities in cybersecurity in other locations, and to experience different aspects of cybersecurity like penetration testing that other internships may provide.

Special thanks to Dr. Alan Peel from SDU and Darin Bournstein from the California Cybersecurity Integration Center