Oregon email restored; official says hack fed scheme

June 22 2018, by Tom James

After a multi-day freeze triggered by a wave of spam messages, officials confirmed late Thursday that Oregon government emails could once again reach the public—and described the attack as part of a sophisticated scheme.

The freeze, initiated by providers at four popular email servers including Hotmail and Outlook, had blocked all messages from official Oregon.Gov email addresses from being delivered.

But the attack that led to the state's email service being temporarily blacklisted likely wasn't targeting government data. Instead, cyber-criminals sought to use state servers as a stepping stone, giving the appearance of authenticity to the subsequent wave of spam emails, said Dave McMorries, deputy chief information officer with the Oregon Department of Administrative Services. He is one of several administrators charged with overseeing computer security across the entire state government.

"This was a fairly sophisticated program that someone had put together," McMorries said. "We were only just a part of it."

The attack started when a state employee was tricked by an authentic-looking email into giving away login details.

But investigators so far haven't uncovered any evidence the attackers tried to use those digital credentials to access information held on state computers.

Instead, the attack appeared focused solely on accessing and exploiting an email address ending in .GOV, a designation tightly controlled by the federal government. Having the designator can boost emails past popular spam filters.

Once that was obtained, the attacker sent out roughly eight million official-looking messages, trying to trick unsuspecting residents into sharing their own personal information.

But at least some of the spam emails were recognized as fraudulent, leading Hotmail and Outlook, along with Live.com and MSN.com, to downgrade the state's "sender reputation score," according to a notice sent out last week.

Officials caught the attack June 11, but they were only able to get the state un-blocked by the email providers Tuesday, June 19, shortly media reports of the attack surfaced.

McMorries said he couldn't share specific details about the emails sent out using the compromised account, but that they looked convincing.

"For the majority of folks that would have received this, it would have appeared to be an official communication," McMorries said.

Attempts by cyber-criminals to fool state employees into giving up their credentials are fairly common, and they have succeeded before.

McMorries said at least four similar attempts have succeeded this year. While all were stopped before they could send out large numbers of messages, some resulted in smaller numbers of emails being sent out.

Together the attacks point to the growing sophistication of cybercriminals, and the need for email users to verify even sophisticated-looking messages, McMorries said.