

Forum:[Hack Forums](#)

Thread: [University of Toronto detects SMTP & VPN phish](#)

Hackers - January 29, 2025, 5:02 am

<https://utcc.utoronto.ca/~cks/space/blog/spam/WellPreparedPhishSpammer>

This is a story about how University of Toronto almost fell victim to a phish.

Quote:Yesterday evening, we were hit by a run of phish spam that I would call 'vaguely customized' for us, for example the display name in the From: header was "U of T | CS Dept" (but then the actual email address was that of the compromised account elsewhere that was used to send the phish spam). The destination addresses here weren't particularly well chosen, and some of them didn't even exist. So far, so normal. One person here fell for the phish spam that evening but realized it almost immediately and promptly changed their password. Today that person got in touch with us because they'd started receiving email bounces for (spam) email that they hadn't sent. Investigation showed that the messages were being sent through us, but in an alarmingly clever way.

We have a local VPN service for people, and this VPN service requires a different password from your regular (Unix and IMAP and etc) password. People connecting through our VPN have access to an internal-only SMTP gateway machine that doesn't require SMTP authentication. As far as we can tell, in the quite short interval between when the person fell for the phish and then changed their password, the phish spam attacker used the main password they'd just stolen to register the person for our VPN and obtain a VPN password (which we don't reset on Unix password changes). They then connected to the VPN using their stolen credentials and used the VPN to send spam email through our internal-only SMTP gateway (initially last evening and then again today, at which point they were detected).

Based on some log evidence, I think that the phish spammer first tried to use authenticated SMTP but failed due to the password change, then fell back on the VPN access. Even if VPN access hadn't been their primary plan, they worked very fast to secure themselves an additional access method. It seems extremely likely that the attacker had already researched our mail and VPN environment before they sent their initial phish spam, since they knew exactly where to go and what to do.

If phish spammers are increasingly going to be this well prepared and clever, we're going to have to be prepared for that on our side. Until now, we hadn't really thought about the possibility of phish spammers gaining VPN access; previous phish spammers have exploited some combination of webmail and authenticated SMTP.

(We're also going to need to be more concerned about other methods of obtaining persistent account access, such as adding new SSH authorized keys to the Unix login. This attacker didn't attempt any sort of SSH access.)

BiNBo - January 29, 2025, 6:45 am

An absolutely fascinating read, Great share! Definitely gives me some thoughts on improving my own environment.

Hackers - January 29, 2025, 6:54 am

(Jan 29, 2025 07:45 AM)BiNBo Wrote: [\[CITE\]](#) An absolutely fascinating read, Great share! Definitely gives me some thoughts on improving my own environment.

glad you liked it. I think the comment about their VPN passwords not syncing with Unix password resets is interesting. It definitely makes me think about how if someone's account is compromised, they often just reset that 1 account... even if they use the same email/password combo on other services.

Flan. - *January 29, 2025, 6:36 pm*

Wow, that's a pretty clever tactic by the phish spammer. It's definitely a wake-up call to be more vigilant about account security and anticipate different attack methods. Good thing you caught it in time!