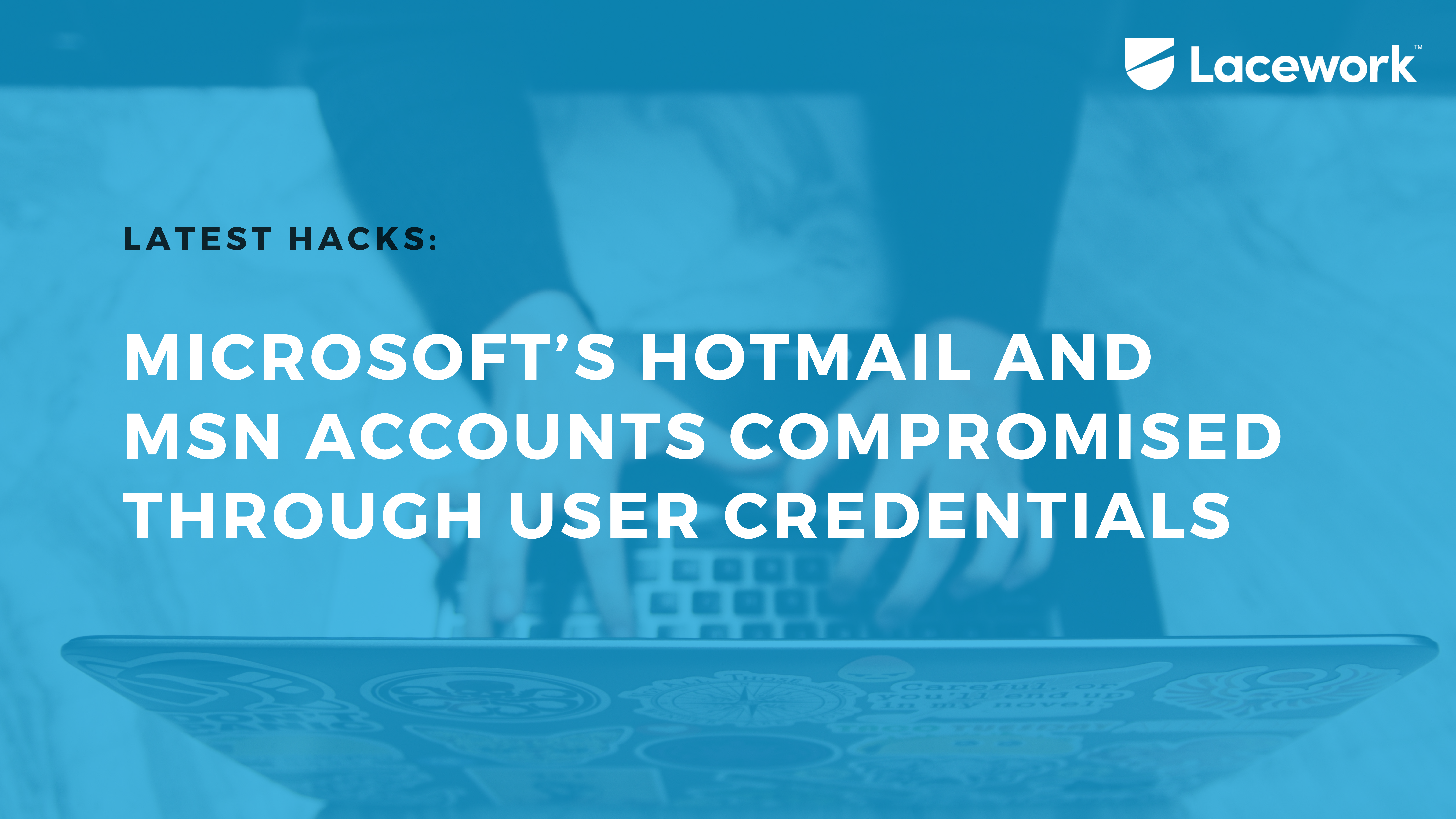
Lacework™

LATEST HACKS:

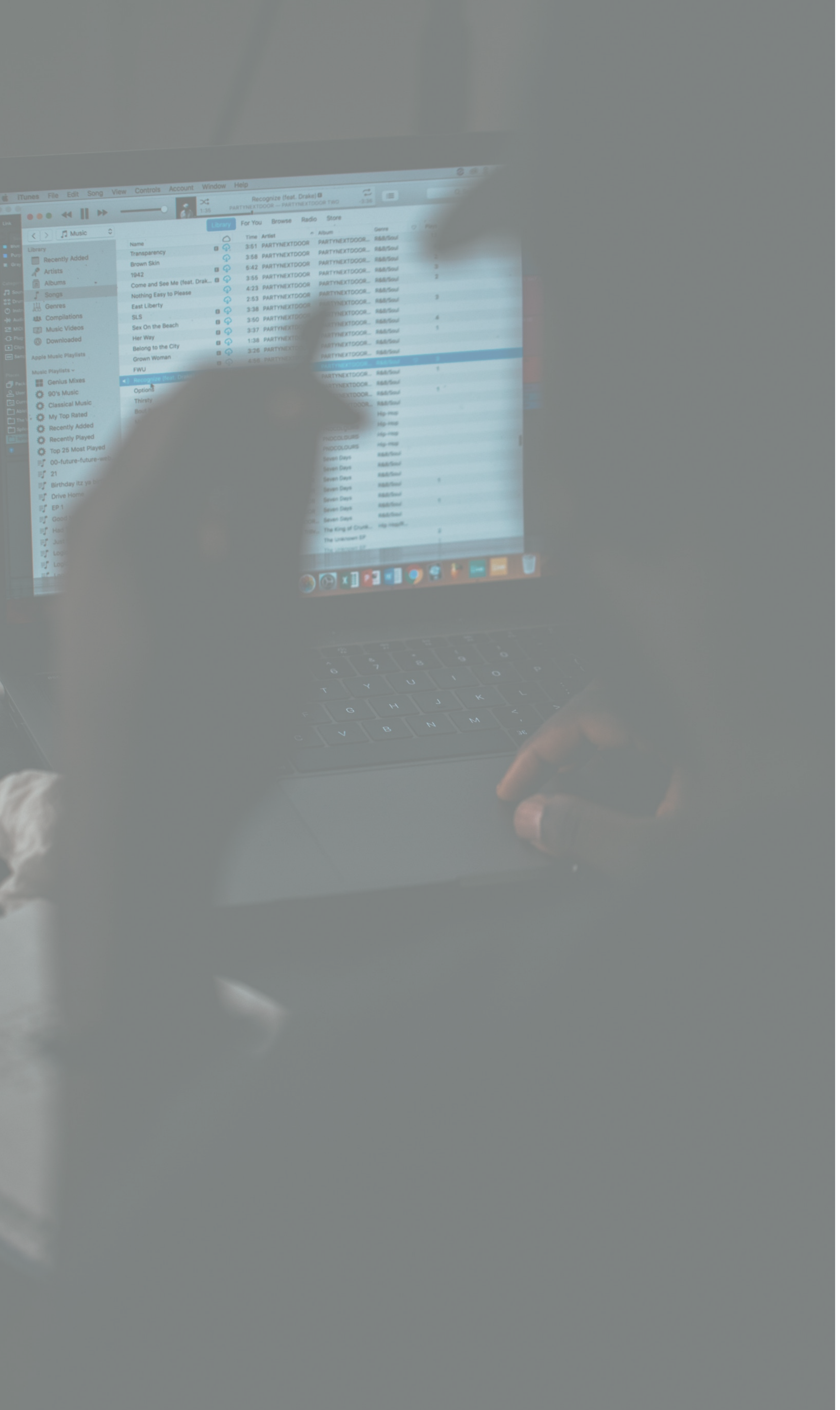
MICROSOFT’S HOTMAIL AND MSN ACCOUNTS COMPROMISED THROUGH USER CREDENTIALS



OVERVIEW

Microsoft has admitted that email accounts for MSN.com and Hotmail, both services owned and managed by Microsoft, have had their accounts compromised sometime between January 1 and March 28, 2019. It appears that attackers were able to identify user's email addresses, email folder names, email subject lines, and the email addresses of those with whom the account owner corresponded with. Microsoft was quick to point out that log-in credentials like passwords were not compromised.

The notice that Microsoft delivered to users said: "We have identified that a Microsoft support agent's credentials were compromised, enabling individuals outside Microsoft to access information within your Microsoft email account. Upon awareness of this issue, Microsoft immediately disabled the compromised credentials, prohibiting their use for any further unauthorized access."



CAUSE

Companies generally have policies around access in order to limit the number of users to specific resources. They also usually apply best practices like least privilege and demand MFA for users to create control around ID and access management.

Microsoft has not indicated whether or not MFA was enabled for this particular support rep, or if there were other security-related requirements that were or were not met. We also don’t know if any behavioral analytics tools were used to identify suspicious activity, although most agree that had there been, this issue would have been handled upon immediate alerting.

What we can surmise, however, is that because of an attacker impersonating or otherwise hacking a legitimate user, he or she was given wide access to sensitive data.

PREVENTION

As the Microsoft case indicates, if there is a vulnerability that allows an unauthorized user into your cloud services, that person has a much easier time of getting access to sensitive data. With that access, they can erase, steal, or otherwise do damage with. Best practices and configurations for services alone won't prevent this kind of thing. Organizations need context and behavioral analysis of activity in their environment to detect threats and understand anomalies that could signal a breach.

Learn how to use Lacework to prevent account compromises.