Ransomware Attacks Are Closer Than You Think

August 5, 2021

By Wes Stillman

Phishing email scams and unprompted or suspicious requests for login credentials are real. Both have the potential to devastate businesses and individuals in very short order. For this Tech Trends post, I wanted to share a real-life example of how quickly bad actors can move and the type of response that's needed to address it.

A massive business failure for our client was avoided because we understood the sophistication level of the bad actors and flagged their activity, ultimately containing their actions and thwarting their intentions within minutes.

Here's What Happened

As part of our ongoing and active monitoring protocols, our team recently spotted suspicious activity occurring inside a client's private server. It appeared as if an employee had logged on from an unusual IP address and their behavior was outside of their normal usage patterns.

Within 60 seconds, our AI-enabled technology identified the aberrant, atypical actions, allowing our experts to assess what was going on and act immediately. Within minutes, our experts verified this was a bad actor using stolen credentials that were not protected by multifactor authentication (MFA). MFA requires at least two forms of identity verification to get access to a system.

Once the suspicious activity was discovered and confirmed, our team contained the attack by isolating our client's server and taking it offline.

For the next 60 minutes, the multi-step process of containment, removal, and recovery kicked into overdrive.

Only after we were fully satisfied that the client's systems were 'clean' did we re-enable access to the server so that the client could continue access as usual. All users at this client were urged to change all of their passwords to all of their accounts immediately.

The Takeaway

Even though this client had not engaged us to manage their end devices and did not have MFA in place, we were able to save the firm by taking the client's server offline for a few hours during their business day to address this attempted attack.

True, the disruption may have seemed inconvenient at the time. But in this case, it was a necessary and critical part of the remediation process that included salvaging and protecting the client’s systems, and restoring them back to their pre-intrusion state.

That said, with end device management and MFA in place, the employee’s ID credentials would not have been compromised and this situation would not have happened.

Some Final Thoughts on Staying Secure:

- Implement MFA and end device management – used in combination, these tools can prevent most cybersecurity attacks.
- Don’t click on any links or attachments inside phishing emails. Doing so instantly compromises the email account and puts the firm’s IT network into the hands of a criminal or criminal network.
- Never upload or offer your credentials unless you are expecting to access a known system. When in doubt, don’t enter anything in and call your IT support team.
- Pay attention to the senders of inbound emails. “Spoofed” email addresses look similar enough to a legitimate address and can trick the unsuspecting receiver into giving away access or information to a cyberthief.
- Have your IT support team implement a cybersecurity training and testing program for your entire organization on data protection and cybersecurity protocols.

# # #