> **Without Todyl... we wouldn't have caught this nearly as quickly. Cases like this are just one reason why it's far easier to manage things with Todyl.**

Justin Smith
President, Midshore Technology Services

Acting Fast to Stop a Weekend Ransomware Attack

On call one Saturday afternoon, Justin Smith, President at Midshore Technology Services, received a Windows Defender Medium-severity alert about a suspicious Microsoft Activation script running on a client's endpoint. At the same time, Todyl MXDR also detected the activity, but deemed it a High-severity alert.

Within 15 minutes of confirming the initial alert, Smith sprang into action and deployed Todyl Endpoint Security to the device to investigate further. He was instantly alerted to another peculiarity: the application "CCleaner" being run out of the system's Music folder via the Anydesk remote access software. Todyl Endpoint immediately flagged the event as High severity and automatically prevented the application from running.

At this point, it was obvious that something was seriously amiss. Using Todyl Endpoint and SOAR modules, Smith and MXDR isolated the machine for fear of a potential ransomware infection, all in less than 20 minutes from the initial detection. As a result, Smith was able to prevent further compromise before the attacker's illegitimate CCleaner malware could begin deploying, saving the client from the dire potential of a ransomware attack.

Leveraging Todyl for Expediency and Efficiency

"Without Todyl, we would have undergone a manual investigation," Smith described, "And on a Saturday, on call by myself, with my kids in the background, we wouldn't haven't been able to catch it nearly as quickly." With the fake "CCleaner" being used to potentially deploy ransomware during the event, that extra time could have meant the difference between all clear and full-blown compromise.

On top of that, although it detected the initial scripts, Defender didn't actively block the malicious activity like Todyl Endpoint did. At that point, Todyl MXDR was already reaching out to Smith to discuss device isolation and next steps. On the topic, Smith remarked, "Cases like this are just one reason why it's far easier to manage things with Todyl."

Historically, Smith and the team at Midshore struggled to get this client's user to realize the value of cybersecurity despite having stopped other security events for them in the past. After this event, however, they were more than willing to prioritize cybersecurity as a core part of their relationship with Midshore.

<20 mins
To fully remediate the issue

14 mins
To remotely install Todyl Endpoint and prevent malicious activity

5 mins
To isolate the device through Todyl Endpoint Security & SOAR after deployment

MIDSHORE
TECHNOLOGY SERVICES

todyl

Preventing Ransomware in Under 20 Minutes

3:20pm EDT
Smith gets an alert from Windows Defender AV regarding Microsoft Activation Scripts. These are third-party activation tools for Microsoft product licenses that can be spoofed by bad actors. At the same time, Todyl SIEM detects the activity and MXDR begins investigating the case. MXDR notifies Smith and elevates the event to a High severity.

3:34pm EDT
Smith deploys Todyl Endpoint Security, which alerts to and prevents a fake "CCleaner" application from executing from the Music folder. The app's parent process was Anydesk, a free remote access software, which was later found to be a malware loader, but was completely stopped by Todyl Endpoint Security before anything could be downloaded.

3:37pm EDT
Windows Defender for Endpoint alerts on the same Microsoft Activation Scripts from earlier without alerting to the suspicious Anydesk activity or illegitimate CCleaner application.

3:39pm EDT
Todyl MXDR fully isolates the endpoint via SOAR playbooks and contacts Smith to notify him of the response action and discuss further investigation and remediation steps.

About Midshore Technology Services

Maryland-based Midshore Technology Services provides professional IT support and technology services for your business, performing proactive maintenance, monitoring, and backups. Built with security in mind from day one, they help companies of all sizes stay safe from cyberattacks.