CASE STUDY_

todyl

DIRECTBUSINESS TECHNOLOGIES

Stopping a ransomware attack in it's tracks

On a Sunday afternoon, Justin Mirksy, Managing Partner at DBT, received a critical alert from Todyl's detection engineers for one of his clients. DBT was not utilizing Todyl's Managed eXtended Detection and Response (MXDR) or Endpoint Security (EDR+NGAV) modules in place at the time, however the MXDR team periodically reviews critical alerts for accuracy and immediately reached out to DBT as a courtesy due to the severity.

Todyl's detection engineers identified an unknown threat actor attempting to exfiltrate user credentials and data from DBT's client, which is an indication that ransomware was about to be deployed.

"It was clear that Todyl's MXDR was truly looking out for us 24/7. When I got the call from their detection engineers on a Sunday, I asked them to jump in and help us and they agreed right away."

Todyl's MXDR team immediately launched an investigation covering multiple areas of concern: logon activities, credential dumping, lateral movement, and the attempted loading of several malicious binaries. The team identified the compromised account by looking at a multitude of failed logon attempts, followed by a successful logon from the public internet in an IP block not used by the client.

Direct Business Technologies (DBT), an MSP based in Louisville, Kentucky, partnered with Todyl to provide security and networking services to their clients. For one of their clients in the healthcare industry, they leveraged multiple modules from Todyl's integrated networking and security platform, while another MSP provided services in a co-managed environment.

"Todyl's MXDR team's experience gave us crucial support through the entire process. They provided all the evidence, details, and notes to expedite investigations by a third-party incident response team we hired, which saved our client significant time and costs. They made us the hero.

Justin Mirsky
Managing Partner
DBT

The MXDR team then deployed Todyl's Endpoint Security (EDR+NGAV) module which blocked multiple attempts to load credential dumping utilities. The threat actor observed these tools being quarantined and attempted several techniques to dump credentials.

Based on the forensic analysis, Todyl's MXDR team discovered that the other MSP failed to decommission the VPN functionality and routing from a pre-existing appliance. This work was outside the scope of DBT's initial SASE and SIEM implementation.

As a result, the threat actor brute-forced an account, gaining access to the network. Todyl's Security Operations Center (SOC) analysts observed behaviors indicative of a ransomware attack, and inspected the malware binary, determining that it was related to the SunCrypt variant of ransomware.

Thanks to early detection, DBT immediately deployed Todyl's MXDR and Endpoint Security modules and caught the attack before SunCrypt could inflict significant damage to the organization. DBT, with Todyl's guidance, disconnected the domain controller and impacted systems from the Internet to stop the attack in its tracks. DBT then worked to remove the malware from the infected systems. Once confirmed that all systems were clean, DBT restored systems from known, safe backups.

The combination of Todyl's EDR, MXDR, SIEM, and SASE modules delivered maximum detection and response, immediately showing value by stopping a sophisticated attack. These modules also enable Todyl's MXDR team to vigilantly monitor the client environments for any other signs of compromise.

RESULTS BY THE NUMBERS_

85%
estimated cost savings by avoiding ransom payment

Zero
downtime for DBT's client

Learn more at **Todyl.com**