Stopping a Ransomware Attack in its Tracks

Results by the numbers:

10x
Faster response time

85%
Estimated cost savings by avoiding ransom payment

Zero
Downtime for DBT's client

Mobilizing quickly to stop a ransomware attack

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 MXDR (Managed eXtended Detection and Response) 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."

Justin Mirsky
Managing Partner, Direct Business Technologies

Conducting a thorough investigation for complete remediation

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.

About DBT

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.

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 SOC (Security Operations Center) analysts observed behaviors indicative of a ransomware attack, and inspected the malware binary, determining that it was related to the SunCrypt variant of ransomware.

Saving time and money thanks to early detection

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.

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

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.

ABOUT THE
Todyl Security Platform

SASE Secure Access Service Edge
Empower your business with always-on security and frictionless connectivity

Managed Cloud SIEM Security Information and Event Management
Gain unprecedented visibility for real-time, correlated threat detection, investigation, and response.

MXDR Managed Extended Detection & Response
Extend your security operations with a 24x7 managed SOC and dedicated account manager helping across the security lifecycle

LZT LAN ZeroTrust
Stop lateral movement, APTs, and the spread of threats while securing internal networks

EDR+NGAV Endpoint Security
End attacks before they become a breach by unifying EDR+NGAV

GRC Governance, Risk, and Compliance
Take charge of compliance and identify opportunities to strengthen security postures with real-time visibility

Learn more at
www.todyl.com