> **“Incidents like this prove that you are never too small to be a target for threat actors.”**

**Jack West**
CEO and President, West Computers

## A routine Chrome update goes wrong

SentinelOne's Vigilance MDR solution notified Jack West, CEO and President of West Computers, of a file run and execute event in a client's environment. The company is a small construction business that utilized the solution and trusted that they would protect them from any major security events.

West called to check in, and the client explained that they accidentally clicked on what appeared to be a Chrome update, which downloaded a suspicious file. SentinelOne's team communicated to West that they automatically remediated the file and rolled back changes, but West decided to bring in Todyl to conduct further due diligence and ensure his client was safe.

In 2023, across all of West's clients, Todyl has identified 15MM+ events, 124 alerts, and logged eight preventions, including over-watch activity for SentinelOne, so West had confidence that Todyl was the source of truth.

### Todyl's MXDR team responds in 5 minutes

Immediately after deploying Todyl's Security Information and Event Management (SIEM) West received an alert that a PowerShell script was running so he brought in Todyl's Managed eXtended Detection and Response (MXDR) team for additional expertise and support.

Within five minutes, the MXDR team alerted him that the file was malicious and guided him through remediation before it could destroy the customer environment.

### Intuition and fast response save West's client

After remediating the issue, the MXDR team analyzed the PowerShell script and attributed it to SocGholish malware utilized by multiple known threat actor groups that typically demand between $100,000-$200,000 in ransom. Todyl's Detection Engineering team built new detections into the Todyl Platform, helping West and his team fully understand the scope of the intrustion and protecting the full Todyl customer base from similar attacks.

**5 minute**
response time from Todyl's MXDR team

**Reputation Protection**
Of both West Computers and their client

**$100 to 200K**
estimated savings

**15MM+ events**
**124 alerts**
**8 preventions**
Logged and created by the Todyl Platform

todyl

# How West Computers and Todyl saved the day

## SentinelOne assured West that the threat had been contained

West's client utilized Sentinel One's Vigilance solution, and one day they notified him of a file run and execute event in the client's environment that they automatically remediated and rolled back changes.

## West's intuition told him something was off, so took a few steps to double-check the work

- He went into Vigilance and downloaded the file
- Put it into a sandbox
- Used a text editor and discovered heavy encoding

He immediately knew that his intuition was right, and this threat was more sophisticated than SentinelOne communicated.

## Todyl's SIEM solution and MXDR team confirm West's suspicions

West decided to bring in Todyl for additional support. Immediately after deploying Todyl's SIEM, West got an alert that a PowerShell script was running, and he noticed the same heavy encryption. Todyl's MXDR team jumped in and started manually reviewing a PowerShell script flagged by the rule "PowerShell Suspicious Payload Encoded and Compressed." Within minutes of investigating the script's contents, the team determined it was malicious based on its heavy and complex obfuscation and encryption.

## Todyl's MXDR team attributes the attack to a type of malware known as SocGholish

After supporting West with remediation recommendations so his client was safe, Todyl's team began reverse engineering the script and identified tactics, techniques, and procedures (TTPs) attributed to attributed to the SocGholish, a type of malware leveraged by several different threat actor groups. SocGholish is well known for its "drive-by" download method used to initially infect a device. The malware utilizes drive-by downloads to deliver a malicious JavaScript payload via a Zip file disguised as a browser update. In West's client's case, the malware was delivered via a fake Google Chrome update that they clicked on.

## "Drive-by download" techniques are particularly dangerous

Drive-by downloads quietly install malware on users' devices without their knowledge, exploiting vulnerabilities in web browsers or plugins. These techniques can rapidly infect numerous users through a single compromised website or malicious ad campaign, posing a widespread threat to security.

## West's client is spared from a ransomware attack

Thanks to West's intuition and Todyl's MXDR team's fast action, the company avoided a ransomware attack. After this incident, West's client sees the value in investing in full-stack security, regardless of how large a business is.

### About West Computers

West Computers

West Computers is the premier destination for computer services and support in the Laurel-Jones County areas. West transcends traditional computer sales and service, focusing on fortifying your digital landscape with advanced security measures.

Learn more at **Todyl.com**