The bridge to possible

Automated Ransomware Recovery with Cisco XDR

The fastest, most comprehensive way to stop ransomware in its tracks

Bad guys don't land on high value assets. Don't get us wrong, they would love to directly attack your domain controller or your finance server in the data center, but they can't. So they start with a strike on an employee's device or internet-facing router on the edge of your network, exploit a vulnerability, establish persistence, escalate privileges, and begin moving laterally through your network.

To avoid early detection, today's sophisticated attacks leverage trusted operating system binaries like the MITRE ATT&CK Living Off the Land Binaries (LOLbins), and legitimate communication protocols like HTTPS, RDP, and SMB. They effectively masquerade as completely legitimate network traffic until they reach and encrypt your high value assets, and you often don't know they are there until the ransom demand arrives.

Until now.

Breaking the Chain

Automated Ransomware Recovery with Cisco XDR, in partnership with leading enterprise backup and recovery vendors, detects the earliest signs of a ransomware outbreak by identifying the attack chains that precede the malware. How? By focusing on the earliest indicators, like a PowerShell script spawned by a process that doesn't normally use PowerShell to create an abnormal network connection over HTTPS or SMB to an internal device. Usually a "low fidelity" event like this isn't enough signal to update a security policy without fear of a false positive that could disrupt network options. By applying proprietary telemetry and over a decade's worth of analytics development, Cisco XDR combines multiple low fidelity events occurring in close proximity to correctly identify the earliest signs of a ransomware outbreak so you can break the attack chain and protect your assets.

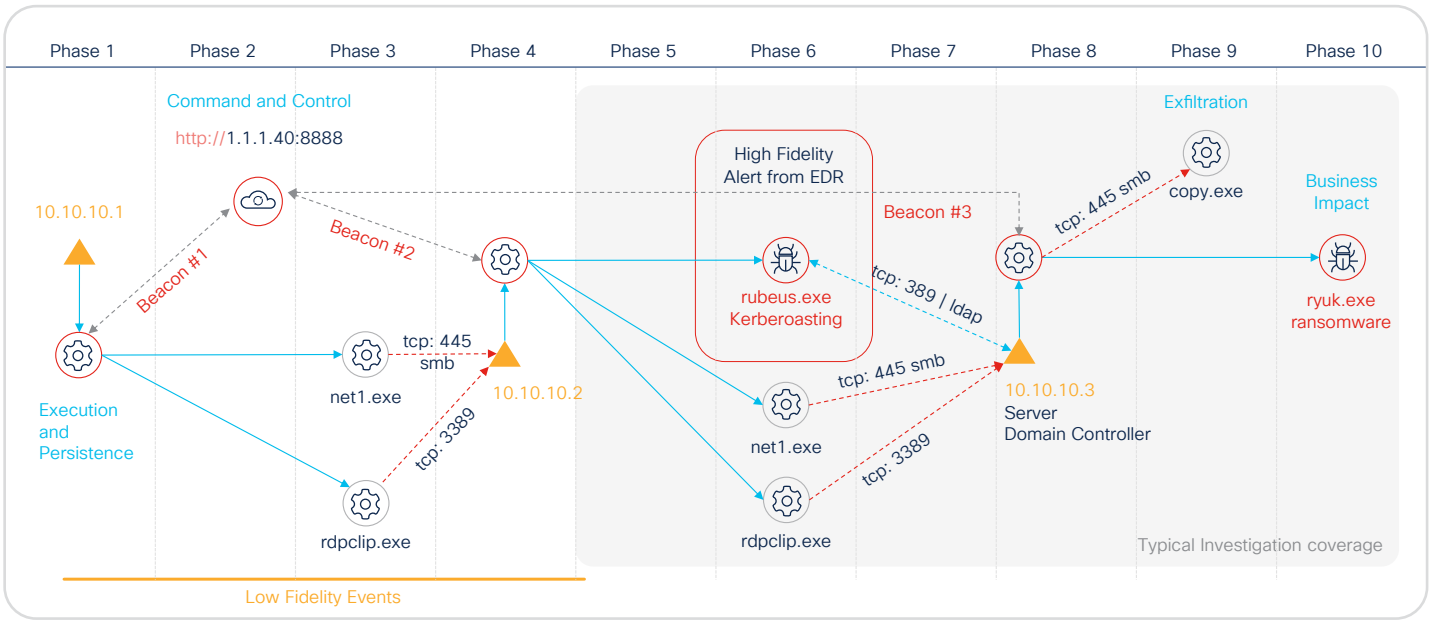

Figure 1. How a typical ransomware recovery investigation plays out without Cisco XDR Automated Ransomware Recovery. Ransomware attacks evade detection by even the best EDR solutions veiled as normal network traffic in search of your high-value assets.

The bridge to possible

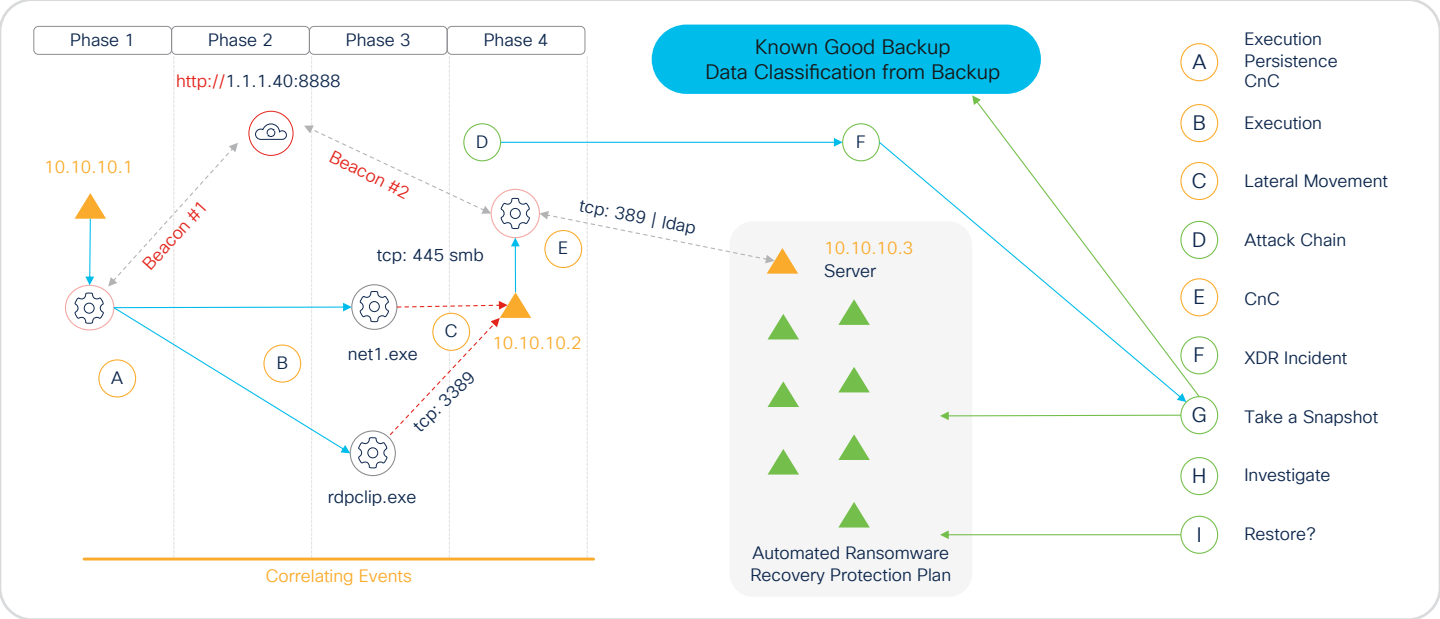

Figure 2. Early and proactive Automated Ransomware Recovery with Cisco XDR. When indications of a ransomware attack are detected, Cisco XDR triggers a snapshot request of the targeted assets, ensuring you have a clean and current backup.

The Cisco XDR Automated Ransomware Recovery workflows trigger a request to your enterprise backup and recovery solution to automatically back up your organization's high value assets before an infection occurs. Cisco XDR initiates the backup at the earliest signs of an attack, unlike the hours or days it can take a traditional Endpoint Detection and Response (EDR) tool to identify the attack and trigger a request.

Peace of Mind and Reduced Downtime

By creating snapshots in real-time, Cisco XDR and the integrated backup recovery solution can reduce the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) to near zero. So, you no longer need to worry about the loss of business-critical data since your last backup, typically 24- or 48-hours preceding the event. Cisco XDR will restore your last known good configuration, getting your organization back up and running with as little downtime as possible, and without having to pay a huge ransom. And what about false positives? Cisco XDR eliminates these, and if it turns out the low fidelity signals were completely benign the integrated recovery solution will delete the backups and free up space on your server.

That's security resilience. That's Automated Ransomware Recovery with Cisco XDR.

How to get started

Automated Ransomware Recovery is available with Cisco XDR at the Advantage and Premier license tiers and requires an integration with a certified backup and recovery solution (not included in the Cisco XDR license).

View a demo of Automated Ransomware Recovery with Cisco XDR and one of our backup recovery partners.

For more information, contact your Cisco sales representative or visit the Cisco XDR webpage at cisco.com/go/xdr.