Softcat Targeted Ransomware Battlecard

A two-page guide from Softcat Security Services detailing the before, during and after of combatting a targeted ransomware cyber attack

The 'Before' Stage

This is the best stage to operate in, it demonstrates thinking ahead of the scenario and allows the preparation of a preventative process. If you find yourself here, there are some steps you can take in advance to best manage this threat:

Firstly, **Assess the risk** in context of your wider risk register. Understanding how likely, how impactful and how well mitigated targeted ransomware is within your organisation will allow you to ensure addressing this is your main priority, and you are not missing a much more likely and impactful threat scenario.

Secondly, **understand your boundaries** – ensuring you have visibility of all network boundaries and ensuring all services and connections are validated and authenticated through multiple factors will limit the attacker's ability to obtain a foothold on the network.

Thirdly, **monitor for behaviours** – utilise intelligent tooling to actively look for unauthorised use of encryption and correlate systems to look for suspicious behaviour.

Finally, **plan ahead of time** – build out a robust and detailed incident response policy covering roles, responsibilities, and details of trusted third parties who can support in the event of a breach, have a ransomware playbook and IR partners who can help stress test these processes ahead of time.

The 'During' Stage

If you find yourself in this stage, Firstly, **Don't Panic**. This is where your pre-existing incident response policies kick in, and if you have trusted third party incident response services (such as Softcat's) these really come into their own. Whilst every incident is different and details often vary, we can broadly break down handling a targeted ransomware incident into the following stages:

Stop the Progress – one of the first steps has to be stopping the propagation of the threat. Easy to say, but in reality, difficult to do – without log analytics and behavioural monitoring it is difficult to understand how the malware is propagating, which is integral to stopping its progression. Looking for suspicious account activities (which are ideally baselined against a norm) is one example here, looking for privilege escalation attempts, failure to log onto administrative accounts and attempts to access deactivated/dormant accounts.

Full Removal and Restore – once we've stopped the threat from propagating, we then need to look at removing the offending malware and doing so fully before restoring. Depending on your available resource and toolsets this will either be relatively easy or a huge undertaking. Once sufficiently removed the restoration can begin which involves usually restoring from ideally not continually addressable back-ups.

The ‘After’ Stage

At this stage, you can let out a sigh of somewhat relief as this means you’ve drawn a line under during and means its relatively over. This is however where the real work begins. Some of the most valuable information regarding internal processes, strength of policies and performance of tooling can be truly ratified here. Again, each incident is individual and should be reviewed as such but again we can look at asking some broad questions to give insight:

What went wrong? – this question is to focus more on what enabled the attempt to be successful, and how this can be used to develop operating procedures in future. Understanding whether it was a simple error that a lack of process should have picked up or a sophisticated attack mechanism that wasn’t detected fast enough means two very different lessons learned.

What was the Impact? – here we look past the initial breach and data loss and look more to how this was communicated. Did the share price fall? Were there media articles etc? how was company facing communication received

So What? – if we get to this question, we lastly look at how this information can be actioned – after all if we arrive here and we change nothing we run the exact same risk (if not greater) as before the incident occurred. Whether its greater investment in information security, reviewing outdated/poorly functioning tooling or overhauling broken processes with more useful policies, this is the way to make the most of being breached.