Root Cause Analysis

The Root Cause Analysis (RCA) is a deep dive forensics examination of one or more endpoints with the associated network logs if available. The report of the analysis gives insight into what happened exactly and how it happened backed up with evidence items recovered from the breached infrastructure. These insights then trigger a whole series of recommendations on how to prevent the same thing from happening once over. There is synergy between an RCA and an CA (Compromise Assessment) as the RCA also leads to more case specific indicators that can be checked while doing a CA. Lastly an RCA report will fulfil most of the reporting requirements that official oversight bodies impose.

Aim: Finding out how an attacker got onto an endpoint and what he did there is the prime concern of a RCA. Once you know this, you might prevent it from happening again.

Deliverables: CPIRT delivers a comprehensive report from the RCA detailing the findings and showcasing the evidence to back up the findings.

Methodology: Triage- and full disk images of identified endpoints will be collected and together with relevant network logs transferred to CPIRT. After reception thereof our expert digital forensic analysts finish the investigation and write the report.

Benefits:

Know what happened: An RCA gives insight into what an attacker did while inside the network. It allows for a correct damage assessment and questions like: "*Are my customers at risk? Has data been exfiltrated, if so, what was exfiltrated, Did the attacker plant extra backdoors into my network? Was my intellectual property stolen?"* are answered.

Know how it happened: More importantly even is knowing how the attacker was able to breach the infrastructure. CPIRT tries not only to find the initial entry of the attacker but also focuses on identifying all elements of the kill chain: initial entry, lateral movement, privilege escalation, persistence, command and control, exfiltration and malware spreading.

Specific IoC: Identifying multiple steps of the attack chain leads to a larger collection of case specific Indicators of Compromise, this in turn helps possible compromise assessments to be more efficient in picking up other infected stations.

Don't have it happen again: Purging the attacker from the network is only a sound strategy if you remediate the way he came in in the first place. CPIRT dedicates sections of our report with recommendations to prevent and/or detect the adversaries' techniques that were proven to be in use. These recommendations will play a key role on preventing the same thing from happening ones over.

Reporting: Many countries have an official instance where breaches need to be reported, many of them ask for detailed information with regards to potentially exposed data and the techniques and attacker used to enter the network. A CPIRT provided RCA report will in most cases (depending on the data that is still available) contain enough detail to fulfil the legal reporting needs.