REAQTA HIVE

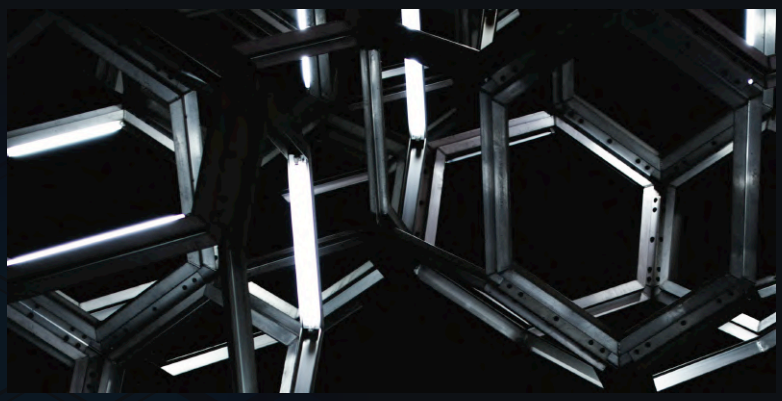
CASE STUDY
AUTOMOTIVE

File-less attack against Car manufacturer

INFO@REAQTA.COM

VISIT REAQTA.COM

File-less attack against Car Manufacturer



Case

A prestigious car manufacturer is attacked using a file-less vector. The attackers manage to gain initial entry but their malicious intent is quickly identified. ReaQta-Hive enables the security team to track and contain the attackers' movements until the security team decides to stop them to prevent data loss and potential damages.

Challenge

- No visibility over the endpoints.
- No threat hunting capabilities.
- Capable but undersized security team.
- Often targeted due to highly prestigious brand.

Solution

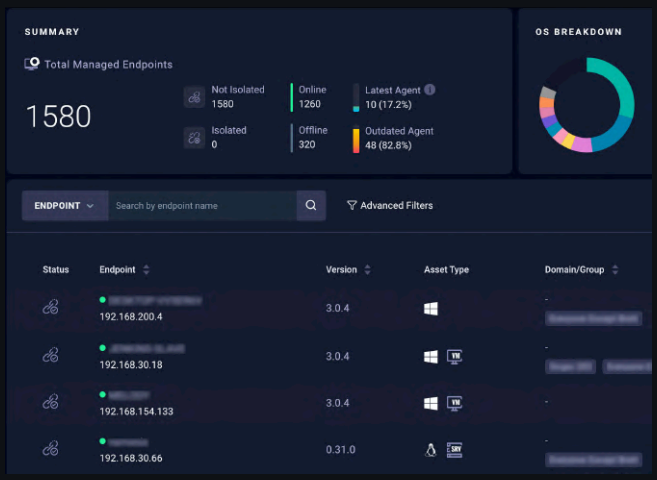
- ReaQta-Hive provides visibility over the endpoints, allowing security teams to explore and contain potentially malicious activities.
- ReaQta-Hive automation capabilities allow smaller teams to manage a large number of endpoints efficiently and to respond automatically to events.
- ReaQta-Hive threat hunting capabilities enable teams to confirm the complete removal of attackers in post-breach scenarios.

The Company

A well-known luxury car manufacturer serving high net-worth customers worldwide.

The Security Challenge

The company manages a sizable number of devices across different internal divisions, ranging from R&D to manufacturing. While there are several best practices adopted at the network level and an overall good security posture, visibility at the endpoint level has been established only recently and the internal security team is still getting accustomed to the new level of interaction and capabilities. Due to brand visibility, the company is often targeted for a variety of purposes, ranging from fraud attempts to direct interest in R&D data. The undersized team faces difficulties managing the large amount of attacks. If priority is given to contain a relatively high volume of fraud attempts, other families of attacks can slip through, with severe consequences.



The Process

ReaQta was adopted as the solution of choice to obtain visibility and protection capabilities on the endpoints. The team realized that the security investments were unbalanced toward a specific type of threats, leaving a gap for infrastructural attacks. At the time of the attack, ReaQta-Hive had already been running on the infrastructure for a month and the security team was capable of handling a variety of scenarios, but they never encountered a sophisticated attacker. The entry point was a Word document leveraging a 1-Day vulnerability that managed to grant an initial foothold to the attackers. The team was quick to identify the issue as severe and followed the attacker long enough to obtain all the necessary elements to initiate their response and containment plan before removing them completely.

1. Root cause analysis

The entry point was quickly identified as ReaQta-Hive flagged a behavioral anomaly on Word. From that point onwards, the whole activity was fully tracked. The victim received an email that carried an attached Word document, as part of a back-and-forth email conversation, aimed at establishing direct contact between the soon-to-be victim and the attacker. After receiving the document, the victim promptly opened it, noticing, after a de-briefing interview, that the application closed just to reopen itself almost immediately.

The offending document was pulled from the endpoint and analysed. A malicious macro was expected, but the victim replied that no requests to activate the macro were ever issued. ReaQta-Hive confirmed that the document didn't contain a macro, but did contain an exploit for a recently-patched vulnerability. A quick Application Hunting run through ReaQta-Hive confirmed that the Word version in use by the victim (and the entire team) was still vulnerable at the time that the attack began.

2. Attack Reconstruction

The exploit payload was used to activate an in-memory RAT using Powershell. The attacker initially spent time running recon activities, to understand the network and identify potential targets of interest. A considerable amount of time was spent in understanding what kind of resources the victim was able to access and mapping the possible path towards other network segments. After several hours, the attackers managed to move to a second endpoint within the same network and quickly after that to a third endpoint. The team decided to stop the attack when they realized that a DC admin was also connected to that device and the attackers were about to extract credentials after a successful privilege escalation.

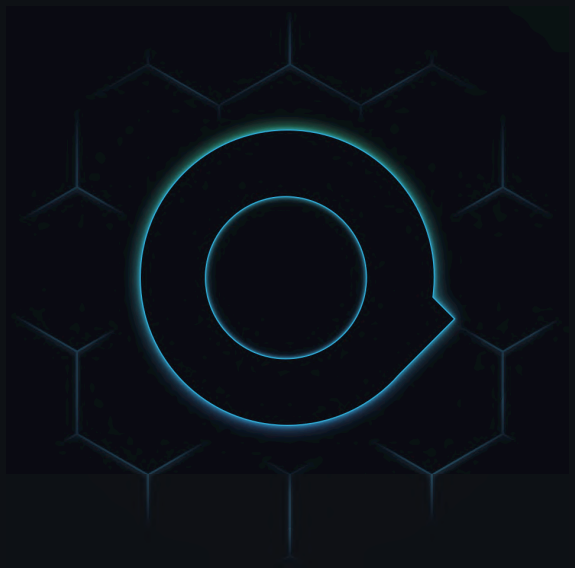
3. Response and Remediation

The team was immediately notified of the attack in progress, but they could respond only a few hours later. At that point the attackers managed to map the network and reach the second machine, at which point they were being actively observed. ReaQta-Hive helped to deploy a protection behavioral policy capable of preventing the exploitation of the vulnerability until the endpoints were updated. Once the infrastructure was secured, the tools and TTPs (Tactics, Techniques and Procedures) from the attack were collected and used to create additional detection and protection policies. The attackers failed to set persistence on any of the compromised machines, so the infection remained volatile and remediation was quick. Additional threat hunting campaigns were initiated on the entire infrastructure looking for the same TTPs on every network segment.

The Result

Time was of the essence in this scenario as the attackers were both skilled and lucky enough to face very favourable conditions, due to the lack of endpoint detection and monitoring capabilities, leading them to almost compromise the DC. The real-time nature of ReaQta-Hive allowed the security team to collect and assess data immediately, saving precious time and allowing the team to focus their attention at the right place at the right moment. A successful attack would have led to loss of Intellectual Property, causing extensive damage to the company. No data was exfiltrated and a subsequent attempt at compromising the infrastructure using the same methodology failed and was

ReaQta takes customers' confidentiality very seriously and while the individual incidents are presented as case studies, useful to understand how attackers operate against a specific industry, individual customers are never mentioned.



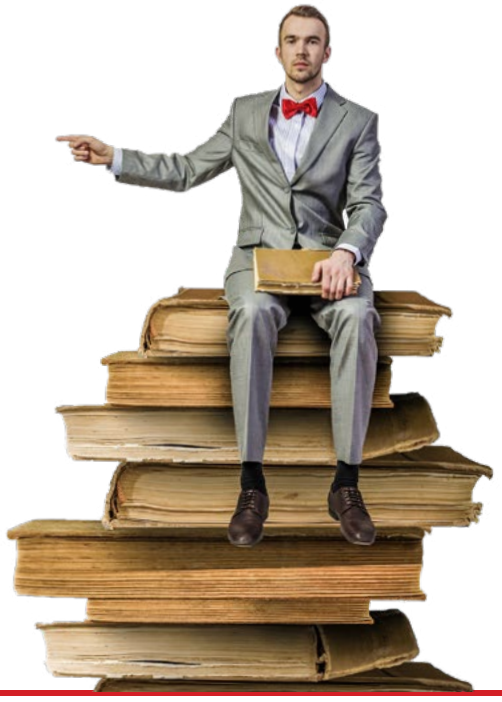
ReaQta was founded by an elite team of offensive and defensive cyber security experts as well as machine learning researchers. Combining these varied expertise, our team has built a powerful Active Defense Intelligent Platform.

Our solution provide clients with advanced detection and response capabilities, without requiring additional or highly skilled personnel. This innovative approach applies the latest A.I. algorithms to automate and simplify the process of detecting and handling new threats.

On this single, highly integrated active intelligence platform, our clients gain flexibility and speed in performing complex an alyses that were only possible with large and highly specialized teams. It is a dynamic approach that doesn't just protect organisatio ns in the here and now, but also far into the future.

With ReaQta, businesses are empowered to pursue growth and ambition fearlessly.

Bedankt voor uw interesse in ReaQta!



Hopelijk heeft dit document u de benodigde informatie en inzicht gegeven waar u op zoek naar was.

Hier vindt u meer whitepapers over ReaQta.

Weten wat ReaQta kost? Gebruik onze prijscalculator.

Andere tools die uw organisatie weerbaarder maken

ProteQtor IT Security is niet alleen reseller partner van ReaQta, maar biedt nog meer cybersecurity tools aan om uw organisatie zo weerbaar mogelijk te maken.

Hieronder tools die wellicht interessant zijn ter bescherming van uw organisatie:

- Beveilig uw e-mail met **Proofpoint email security**
- Train uw medewerkers met laagdrempelige **Wizer security awareness trainingen**
- Bescherm het inloggen met **Watchguard Authpoint multi-factor authenticatie**
- Voorkom bezoeken aan ongewenste websites met **NSOC360 Safeweb webfiltering**
- Krijg inzicht in de veiligheid van uw netwerk met **Guardian360 scans**
- Herstel verloren data met **NSOC360 Safedata online backup**

ProteQtor
Next-Gen IT Security

Laat hackers uw bedrijfscontinuïteit niet in gevaar brengen!

Cyberaanvallen bedreigen privacy, bedrijfskritische data, de reputatie en andere 'kroonjuwelen' die cruciaal zijn voor de continuïteit van uw organisatie. De vraag is allang niet meer 'of' uw organisatie aangevallen wordt, maar 'wanneer' uw organisatie (weer) aangevallen wordt. Het is essentieel om cyberaanvallen te voorkomen en de gevolgen van cyberaanvallen tot een minimum te beperken. Het feit dat u deze pdf leest, toont dat u dat belang inziet.

Vanwege de grootte, de complexiteit en de diversiteit van moderne cyberaanvallen is een multidisciplinaire aanpak nodig. We helpen u graag met praktische adviezen en effectieve oplossingen om deze aanpak te realiseren.

Met de juiste trainingen, tools en support helpen wij u hackers het hoofd te bieden en er voor te zorgen dat alles wat voor uw organisatie van waarde is, beschermd blijft.

Hulp nodig? Bel 088-0660770 of plan een afspraak in

ProteQtor
Next-Gen IT Security

Telefoon : +31 (0)88 066 0770
E-mail : contact@proteqtor.nl
Website : proteqtor.nl