REAQTA HIVE

CASE STUDY
FINANCIAL INSTITUTION

Preventing Data and Revenue loss to leading Financial Institution

INFO@REAQTA.COM

VISIT REAQTA.COM

Preventing Data and Revenue loss to leading Financial Institution

Case

A leading multinational Financial Institution is targeted by a cyber-crime organization specialising in financial fraud. Attackers manage to obtain initial access via a spear-phishing email and then try to acquire access to personal and financial data belonging to high-profile individuals.

Challenge

- Geographically distributed offices with limited visibility across endpoints and infrastructure.
- Lack of detection and hunting capabilities for modern day malware and file-less threats.
- Security teams assigned almost exclusively to business services, leaving endpoints underserved.
- Zero downtime tolerance due to high transaction volume.

Solution

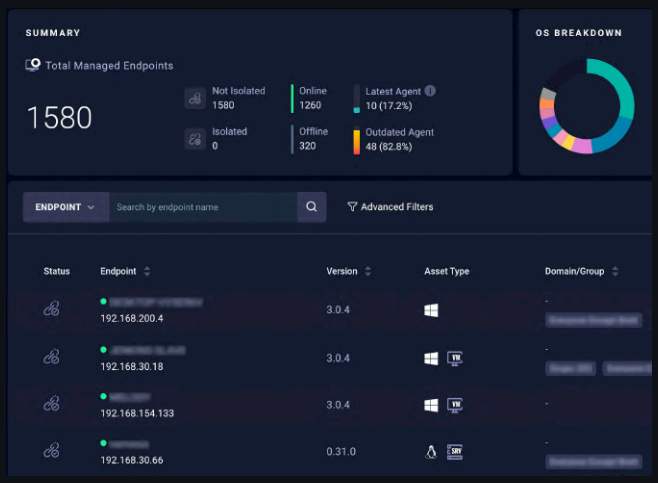
- ReaQta-Hive platform uses the world's first NanoOS to provide an unprecedented level of visibility across endpoints and infrastructure.
- ReaQta-Hive platform allows organisations to search for IOC, binaries and behaviours in real-time. Automated data mining/threat-hunting enables the discovery of dormant threats.
- ReaQta-Hive's interface enables organisations to respond to threats in minutes. There's no need for additional security personnel–the analysis workflow is simple and streamlined, with zero downtime and business continuity ensured.

The Company

A leading Asian investment management firm engaged in managing investment strategies across public and private markets globally. The organisation was ranked Top-50 by Bloomberg Magazine Top-Performing Funds and Top-10 in Asia by size of managed assets.

The Security Challenge

Like all financial institutions, the organisation had a labyrinth of offices spread across the globe working in different time zones, each with its own decentralized management. This posed a unique security challenge as their present security solutions (that included a leading AV solution) offered limited visibility over their varied and vast infrastructure. There was no monitoring in place on the enormous number of disjointed endpoints behaviours to detect any anomalies or suspicious user activity. Their solutions also lacked the capability to hunt for dormant and latent threats on the infrastructure. Furthermore, in case of active threats, their security teams had to invest a considerable amount of time analysing and responding manually, diverting resources from the institution's critical services.



The Process

ReaQta was commissioned to run on all servers, desktops and laptops across all offices in the organisation to detect, hunt and remediate suspected attacks. Using its inbuilt dual A.I. engines and detailed behavioural analysis, ReaQta's NanoOS provided full visibility over the infrastructure, allowing real-time queries to the endpoints, extended searches for both IOCs and behavioral indicators, together with advanced data-mining for the discovery of dormant threats. The single lightweight agent detected the initial breach in real-time and the team remediated remotely within the first 2 hours, after gathering initial intelligence on the attackers and their activities. The AntiVirus solution in use failed to identify any malicious activity. Without ReaQta-Hive, the attackers would have managed to reach their objectives undetected.

1. Detect

ReaQta-Hive platform detected an unknown malware on an endpoint belonging to a management staff member. A script originated from a spear-phishing email activated the A.I. engines on the user's endpoint. ReaQta-Hive managed to track the attackers' entry-point and every action initiated after the initial breach. The malicious software adopted a series of bypass techniques that allowed attackers to execute their plan undetected by the Antivirus solution in use.

The threat established immediate persistence, in order to survive machine reboots and unwanted terminations. The threat itself was a full-fledged in-memory RAT (Remote Access Trojan) having the capabilities of capturing screenshots, keystrokes, sensitive data and potentially any other kind of activity, structured in a modular fashion to allow the operators to add various functionalities after the initial infection.

From the detection to the response and eradication, the malware activity was closely monitored and immediately stopped after the security team acquired enough information about the attackers' motivation and objectives. ReaQta-Hive prevented the leak of sensitive information and it was used to activate an automated response plan aimed at protecting the entire infrastructure from similar attacks.

2. Threat hunting

ReaQta worked in concert with the organisation's cyber security team to resolve the issue immediately, without any impact to the infrastructure, data and ultimately to the user involved. ReaQta also ran a comprehensive threat analysis listing out the detailed end-to-end journey of the attack vector. ReaQta identified a scheduled task that was used to start the malicious script that in turn took advantage of powershell to execute its functions as a powershell in-memory backdoor. The backdoor leverages on lolbins (Living-Off-The-Land binaries) techniques in order to remain under the radar and to avoid detection from antivirus products. The components abused by LOLbins attacks are part of any Windows installation, so no other malicious or external components were necessary for the backdoor to function.

3. Root cause analysis

After the initial detection, ReaQta decided to initiate a threat hunting session, aimed at identifying the prevalence of the initial vector on the entire infrastructure. The first phase of the hunt was focused on identifying the first occurrence of the malicious script and the system components responsible for executing the first stage payload. All events related to the malware incident were identified, and as a final step, the hunting team established the starting point of the infection process. ReaQta-Hive was used to reconstruct the complete flow of the incident, provide details on the behavioral tree and track if any kind of sensitive information was accessed by the attackers.

4. Response and Remediation

As part of the response stage, the malicious powershell instance was suspended for further analysis and a behavioral blacklist created and deployed to stop any malicious script and to avoid further infections. This step automatically propagated the containment instructions to every device in the infrastructure, immediately preventing further malicious instances from running. The next step involved the remote remediation of the affected device and the automated removal of every artifact produced by the attackers.

The incident was successfully closed without any loss of data.

The Result

Without ReaQta-Hive, the initial breach and the deployment of the in-memory RAT would have gone completely undetected, almost certainly leading to the loss of sensitive information belonging to high-profile individuals. The time needed to identify and mitigate the attack, without ReaQta-Hive, would have meant letting the attackers free to operate within the infrastructure for longer, eventually leading to a prolonged downtime in order to clean up the infrastructure. The downtime would have interrupted business services, with significant loss of revenues and additional expenses incurred on specialised security resources.

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.

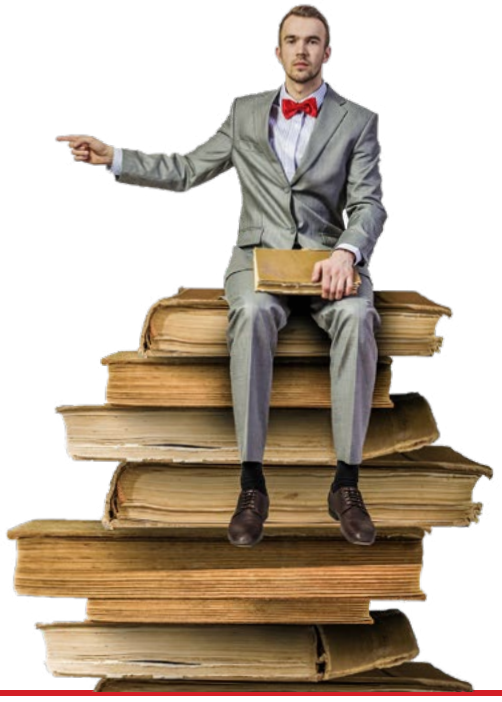
ReaQta was founded by an elite team of offensive and defensive cyber security experts as well as machine learning researchers. Combining these varied expertise, our team has built a powerful Active Defense Intelligent Platform.

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