



RevBits®

# Cyberbreaches Could Have Been Prevented on the World's Largest Oil and Gas Company

Solution Focus:  
RevBits Cyber Intelligence Platform

Report Date: May 2021

## Cyberbreaches could have been prevented on the world's largest oil and gas company

Cyberattacks on a country's infrastructure, whether by nation-state actors, or non-state actors, are as serious as it gets. Without proper security controls in place, and a unified security platform, the fallout from such attacks can have serious implications. The 2012 and 2017 Shamoon cyberattacks on Saudi Aramco could be an indication for more serious cyberattacks in the future, with implications for other companies.

Cyberattacks not only impact business operations, potential revenue loss, and public perception of the victimized company, they can have ramifications that affect customers and supply chain partners. In the Saudi Aramco case, the perpetrator group were highly likely to be nation-state actors in Iran. If true, mounting a defense without the necessary security platform would be like fighting a twenty-first century battle at sea using Galleon ships with cannons.

### Malware – a weapon of cyberwarfare

Malware, like Shamoon, can take over a computer's boot process, encrypt the entire disk, and erase all data on the drive. Shamoon is a modular computer virus that was discovered in 2012, when it wiped out Saudi Aramco's 30,000 computers and data. The virus was notable because of its destructive nature, and the cost associated with downtime and recovery time. Shamoon spreads from one infected machine to other computers on the network. Once a system is infected, the virus continues to compile a list of files from specific locations on the system, upload them to the attacker, and erase them. Finally, the virus overwrites the master boot record of the infected computers, making them unusable.

The virus has been used against oil companies including Saudi Arabia's Saudi Aramco, the world's largest oil producer. A hacker group named "Cutting Sword of

Justice" claimed responsibility for the Shamoon breach, causing the company to spend more than a week restoring computers and services. The attack was initiated within a phishing email that an IT employee clicked on, giving the group entry into the company's network. Days later, computer systems at RasGas were also taken offline by a virus that security experts also attribute to Shamoon. At the time, RasGas was the second-largest liquefied natural gas, or LNG, producer in Qatar. It has since merged with Qatargas, the largest LNG producer in the world.

If oil and gas companies don't act quickly, and implement broad security measures, they run the risk of potentially devastating future attacks. This is evidenced by the 2017 Shamoon attack on Saudi Aramco that was actually more advanced than the 2012 attack. We don't know for sure, but it's likely this hacker group has used the virus on other companies, using a different name to disguise the identity.

## Combating security threats with unified deception, detection and response

Security threats avoid detection by shrouding themselves between disjointed and siloed technologies and heterogeneous systems that create threat gaps. Without a unified security platform, organizations are in a losing battle of attempting to correlate and prioritize incongruent alerts, while investigating them with restrictive and inadequate hunt-and-peck approaches and limited visibility.

These investigations become a manually time-consuming effort for already strapped IT and security teams. When logs and alerts have no ability to share indicators, it's hard to know what to look for. When threats are found, it's difficult to map their path and impact across systems throughout the organization.

A unified umbrella approach to security automatically identifies, associates, correlates, connects, and creates fewer disassociated events, and provides the necessary visibility to prioritize alerts for fast and effective action.

By automating processes, IT and security teams can eliminate time-consuming and error-prone manual efforts. A rich set of data and unifying tools for analysis enables automated root cause analysis, and visibility to see attack timelines and paths across email, endpoints, servers, clouds, and networks. By assessing every element within the attack chain of events, they can quickly perform the required action.

Unified multi-layered defense, detection, and response improves threat detection rates and response times, that are measured and monitored as key performance metrics. These performance metrics help IT and security teams justify their technology investments, by helping the enterprise reduce business risk.

## RevBits uniquely prevents cyberattacks like Shmoon

RevBits takes a unified and consolidated approach to threat deception, detection and response. We collect and correlate data on threat activity across a multi-layered security stack of email, endpoints, servers, cloud workloads, and networks. By automatically coalescing analysis of rich heterogeneous data, IT and security teams can detect and prevent threats faster, conduct comprehensive investigations, and quickly take action. This provides the full context and visibility of the complete chain of events across a multi-layered security stack.

RevBits Cyber Intelligence Platform harnesses the power of ten different security modules, which are part of four unified functions, including email security, endpoint security, deception technology, and privileged access management (PAM). These are integrated into a single view within the user dashboard. Single sign-on enables system administrators to monitor, interact with, and control all security capabilities.

To have fully prevented the Shmoon virus breach at Saudi Aramco would have required a unified platform with endpoint security, PAM, and deception technology. That's not to say that the RevBits Endpoint Detection and Response, or EDR, capability would not have prevented the attack by itself. We are confident it would have, because of its unique ability to prevent security drivers from being loaded

without administrative verification. But, if the virus was undetected by the EDR, the unified capabilities of our EDR, PAM and deception technologies would have certainly protected the company. With cybersecurity, a platform approach is vastly more effective, because the whole is greater than the sum of its parts.

## Hackers took advantage of the company's EDR limitations

The strategic damaging maneuver in the Shmoon attack on Saudi Aramco was the hackers used an already signed driver to accomplish their breach. Code signing is the process of cryptographically authorizing software so the operating system and its users can verify its safety. When software is code-signed, it has an official cryptographic signature issued by a Certificate Authority, or CA. The certificate confirms the software is

**“RevBits EDR module is able to capture the driver and send it to the admin panel for approval. There is no other EDR, antivirus or anti-malware solution on the market capable of detecting and preventing hackers who have signed a legitimate driver with their own malicious code, using an official cryptographic signature.”**

legitimate and safe to use. Using their signed certificate, the driver gave them raw access to the disks. Using the code signed on the drivers, they were able to wipe the files, data and operating systems of 30,000 computers, rendering them unrecoverable.

The hackers took advantage of a license validation using a trial license. In order to make it work, they moved the system date and time back to when trial license was valid. This went undetected by the company's EDR solution. This is a very challenging area, because Microsoft has very specific protocols that must be followed when developing internal drivers, and administrators must follow the functions the SDK Microsoft provides.

The Microsoft SDK will not allow an administrator to prevent a legitimate driver that is signed from being loaded. They can prevent a process from being created, and can block a file from being written, but they can't block a legitimate driver that is signed from being loaded into the system.

However, RevBits Endpoint Security would have prevented this violation with its unique and patented technology that detects and prevents signed drivers from being loaded without first being vetted, or verified. RevBits EDR module is able to capture the driver and send it to the admin panel for approval. Upon thorough review by two or more admins, the driver is either approved or disapproved. There is no other EDR, antivirus or anti-malware solution on the market capable of detecting and preventing hackers who have signed a legitimate driver with their own malicious code, using an official cryptographic signature.

## Hackers thwarted the company's PAM tool

For a hacker to gain access to the driver, they would have had to obtain privileged access. In the Saudi Aramco case, hackers entered through a web server that required privileged access. They were able to escalate their privileged status to domain admin, with access

to the Active Directory admin account for all 30,000 computers. They accomplished this, even though the company had antivirus and PAM solutions in place. This clearly shows that without cross-functional and unified capabilities, it's nearly impossible to coalesce and correlate heterogeneous information among systems. This limitation, and the lack of their EDR to capture the driver, expanded the company's cybersecurity weaknesses that created security gaps that hackers exploited. This is where RevBits unified platform

would have greatly helped the company.

**"The unified capabilities of our EDR, PAM and deception technologies would have certainly protected the company. With cybersecurity, a platform approach is vastly more effective, because the whole is greater than the sum of its parts."**

### RevBits Cyber Intelligence Platform

RevBits Cyber Intelligence Platform includes endpoint security with AI, machine learning, and vetted driver requirements. Privileged access management (PAM) escalates privileges that prevent changes to a policy, with approval that requires two admins in order to allow a driver to be whitelisted. Our deception technology would have detected the hackers, by deploying honeypots into the network, automatically trapping and quarantining them, while notifying IT and security teams.

While the hackers didn't phish with email, RevBits Email Security module would have analyzed emails at the endpoint with over fifty algorithms to detect the most sophisticated phishing emails. RevBits delegates email analysis to email clients, and detects sophisticated and previously undetected credential harvesting via fake

login pages - page impersonation. Again, this is where a unified security platform approach has the greatest impact, and shows the real value of the whole being greater than the sum of its parts.

## About RevBits

RevBits provides a unified security platform that simplifies and secures enterprise digital infrastructure. RevBits Cyber Intelligence Platform delivers a broad set of security deception, detection, and response capabilities via the cloud and on-premises for protecting corporate systems and data assets. The Cyber Intelligence Platform can be deployed as an extremely efficient and differentiated managed security service offering.

RevBits addresses the operational and business challenges associated with cybersecurity incidents within traditional and modern networks when users, wherever they are, access applications and services. In addition to our Cyber Intelligence Platform, RevBits offers a full range of professional services along with advanced security solutions, including incident management, malware forensic analysis, penetration testing, IoT/hardware/firmware analysis, and code analysis. For more information, call **844-473-8248**, email us at **info@revbits.com**, or visit us at **revbits.com**.

To get more technical details on the Saudi Aramco Shamoon breach, [click here](#) to access the **RevBits Cyber Security Solutions "Operations Saudi" intelligence brief**.

# Keep Your Enterprise Protected. Get a Demo or Free Evaluation.

To learn more, visit [www.revbits.com](http://www.revbits.com)



34 Willis Avenue • Mineola, NY 11501 • 844-4REVBIT (844-473-8248) • [www.revbits.com](http://www.revbits.com)

© 2023 RevBits, LLC. All rights reserved. This material is provided by RevBits, LLC. Further distribution is prohibited. **RB-EB-CIP\_(01/2023) 051**