Case Study

Global Car Manufacturer
Incident Forensics and Response

Industry:

Automotive, Vehicle Manufacture

Business Challenge:

Risks of data and IP breach & theft through supply channel (contractor)

Environment:

Cloud Infrastructure (Amazon AWS)

Solution:

Immediate incident response and live remote Forensics and future IR program improvement

Results:

- Identification of the attackers
- Secured systems
- Improved IR response time
- Regained key shareholder and clienttrust

Background:

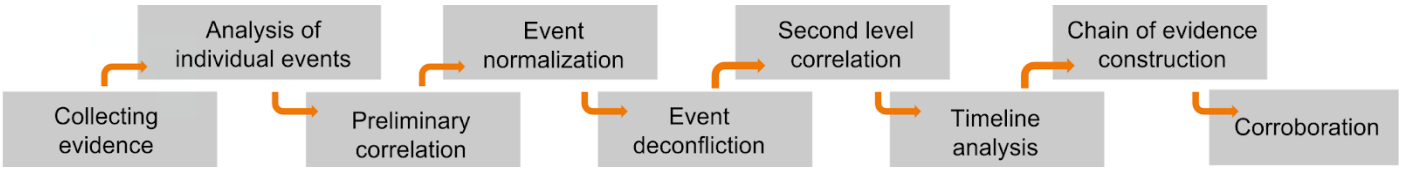
Our client is a global full-line vehicle manufacturer that sells more than 60 models under several brand names. In the last fiscal years, the company has sold over 5.63 million vehicles globally, generating revenue of 11.72 trillion yen. Our client engineers, manufactures and markets the world's best-selling all-electric vehicle in history, with its headquarters in Japan, and other operations in six regions around the globe. With an international workforce of 247,500 our client holds the world's largest automotive partnership with organizations like Renault and Mitsubishi, with combined annual sales of almost 10 million vehicles.

The Challenge:

Our client reported that a third party subcontractor they were working with had been hacked for a third time within a six-month period, experience multiple compromised instances and resulting in a large potential business risk of IP (Intellectual Property) being compromised and publicly distributed. Also IP might be used by competitors as well as attackers to compromise customers systems. The challenge was a multifaceted one, with our client requesting Incident Forensics on three different servers, as well as a Security Improvement plan and polishing existing IR plan for the organization.

People, Process, & Technology:

Spanning a total of three weeks our team lead by 2 Certified Incident Forensics Investigators initiated a cohesive plan with delegated tasks, providing real-time status for managing incidents to successful resolution. Giving our client the ability to manage the response more succinctly with greater control, higher efficacy, and decrease time between threat detection and elimination.



Taking a deep dive into the incidents we utilized the following tools in order to identify the key issues:

- Computer Aided Investigative Environment (CAIE)
- Amazon EC2, EC2,
- VMware vCenter, P2V
- Cent OS Linux
- WireShark

We were able to single out the attackers as a group from Romania, our investigations led us to understand that these hackers were breaking into the servers through vulnerable version of an Apache Tomcat server hosted in the client's Amazon EC2 environment, causing the loss and modification of information on the servers. After stealing passwords attackers tried to compromise the rest of infrastructure, and after failure utilizing compromised systems as DDoS botnet members. In order to minimize impact on the business, we isolated systems in order to preserve and collect evidence (for future training purposes).
Once forensics were complete we began our Incident Response by helping our client assess the level of the impact of the breach, educating them on which systems were compromised, identifying what data was stolen, accessed and removed, and estimated the potential impact for customers and partners.

The Result:

By improving visibility on the cyber incidents that occurred within the organization we were able to prepare with an actionable and detailed plan through a coordinated team response, allowing operations to return to normal. Reports to key stakeholders thus included:

- A detailed technical report with executive summary
- Forensic analysis of acquired data
- Forensic evidence for appropriate law enforcement or investigating government agency as requested by the customer (Systems preserved images, archive with events sorted by date, screenshots, extracted data files and logs)
- Identified vulnerabilities
- ISMS recommendations
- Recommendations on how to avoid security incidents in the future
- Incident response plan
- Collaboration initiatives with CISO/CTO/CIO/CEO to mitigate risks/consequences of data leakage or security breach

We helped our client to stop ongoing attacks and to mitigate future cyber threats immediately, during next three weeks we also worked to provide our client with insight on how the attack was conducted, by whom, when, and why. With this information we were able to assess the damage caused.

About UnderDefense:

We at UnderDefense are dedicated to supporting organizations around the world in planning, building, managing, and running successful security operations programs, meeting and maintaining compliance regulations and exceeding organizations abilities to run their businesses securely and confidently.
Our team of talented and professional cyber security experts partner with enterprise-class organizations to provide a full package of Cyber Security services and solutions including Security Assessments, Compliance Solutions, Product Advisory Services, Threat and Vulnerability management, Incident Response management, Network and Security architecture and implementation, and much more.

We don't just do;
we think, innovate, and create new security capabilities to combat tomorrow's threats today.

USA, New York
375 Park Avenue, Suite 2800, NY
Tel: +1.929.999.5101
email: help@underdefense.com

Poland (EU), Wrocław
Rzeźnicza str. 28-31, 50-130
Tel:+48 792-229-273
email: help@underdefense.com

Ukraine, Lviv
Heroiv UPA 73 k.38, Lviv, 79014
Tel: +38 063-11-357-66
email: help@underdefense.com