Fighting cybercrime in the retail sector with Rapid Response Retainer

Use Case

The retail business is changing at warp speed to meet industry challenges that have been accelerated by the sudden change in consumer behavior triggered, in part, by the pandemic. But hackers thrive in times of uncertainty and change, taking advantage of vulnerabilities in systems that were installed hurriedly. All too often, the results are system breaches that compromise stores' internal systems and expose customers' personal and financial data.

The situation

A large regional apparel retailer first learned something was wrong when law enforcement authorities informed them that personal information belonging to customers had been released on the dark web. Earlier in the year, the retailer had been rushing to rebuild its web infrastructure, reinforce and streamline vendor supply chains and roll out a refreshed smartphone app.

Web application servers are the most common hacker targets, but retailers typically fix only about half of known vulnerabilities within 90 days after patches become available.[i]

As with many retailers, this chain was forced to close store locations for months while business moved almost entirely online. To respond to new retailing realities, it moved urgently to rebuild its website and app to accommodate new types of inventory, new lines of business and new modes of shopping like curbside delivery.

With so much change happening so quickly, it is easy to make security secondary to execution, even in sophisticated IT environments. Virtually all retail sector attacks have a financial motive, with hackers looking for payment data and other associated personal information. In addition, larger retailers have integrated supply chain systems that connect inventory, ordering and payment processes with their suppliers. A major breach that compromises consumer data is unwelcome headline news—news that too often comes to light only, as in this case, when the authorities call to report that customer data has already been found online.

Investigation and response

With a Rapid Response Retainer, a response starts well before emergencies arise. It typically starts with an onboarding call, where the customer has an in-depth conversation with a Verizon Threat Research Advisory Center (VTRAC) investigation liaison. When trouble comes, VTRAC is just a phone call away, 24 hours a day.

When this retailer had been onboarded—as with all Rapid Response Retainer clients—the VTRAC team conducted upfront discovery audits and assessments; available options include an executive breach simulation, a cybersecurity first responder training course, an incident response plan assessment or a network health check. These assessments help bolster cyber defenses and incident response capabilities while helping the VTRAC team familiarize itself with their new Rapid Response Retainer customer.

And because every plan works better when it's practiced ahead of time, the retailer asked for VTRAC to lead breach simulation exercises and workshops envisioning a range of scenarios. When the response was no longer a drill, everyone knew what to do.

In this case, with all the new technology and operational changes being rolled out in a hurry, some security details got overlooked, leaving the retailer vulnerable. The retailer had a sophisticated security practice, but it was moving so fast that some doors were accidentally left ajar.

verizon

Very often, threat actors will upload software that scans systems to discover where payment data is stored, then harvest financial information and encrypt it so a subsequent download won't trigger alarms.

It turned out that his retailer's vulnerability was lower tech; it was in the way the retailer managed credentials for new hires and trainees. Retailing is a high-turnover business, so control over credentials and access to shared devices is particularly important. Industrywide, about 45% of data breaches involve the use of stolen credentials.[1] When an employee left the business, the retailer was rigorous about cutting off access. But new employees, hired in a rush, were given their own logins immediately instead of sharing credentials with a training partner until they were known to be trustworthy. One of those logins had gone astray. The credentials apparently fell into the hands of a bad actor, who used them to get into the system, escalate privileges, extract payment and personal data, package it and dump it on the dark web.

As part of its response, the VTRAC team followed its protocols for securing digital forensic data, which may typically include malware, output files, disk images, volatile data, network traffic and log data. VTRAC investigators and lab technicians are experts in PCI forensic investigation. They routinely handle evidence and manage chains of custody to store evidence that may be needed for litigation, insurance purposes or in criminal prosecutions.

Lessons learned

Financial information at risk is not just payment information like credit card numbers. Retailers can also hold personally identifiable information (PII) such as birth dates and Social Security numbers. Although financially motivated criminals may be looking primarily for card numbers they can exploit quickly, they will happily take anything they find and resell it on the dark web.

The risk to retailers goes beyond the security of data. Retailers are particularly public-facing enterprises; the reputational risk of a major security breach is significant, and the best kind of public relations damage control is the kind that never has to happen in the first place.

The core of Rapid Response Retainer includes SLAs for phone and onsite support, flexible annual assessment options, weekly threat intelligence summaries and a mobile application. But the latest version of the retainer goes beyond that, offering add-on VTRAC capabilities including network telemetry analysis, endpoint telemetry analysis and dark web hunting. We can detect issues and help you get a jump on your response efforts before the authorities or someone else outside your organization tells you there's a problem

Stay ready

The time to prepare for an attack is long before it begins. You need an experienced team on your side to help make sure that there are no surprises lurking in your network, that all doors are secured and that there's a well-crafted action plan in place should something go wrong. Being ready reduces the very real risk to your reputation and your business.

Learn more:

Contact your Verizon Business Account Manager at 877.297.7816 or visit enterprise.verizon.com/products/security/incidentresponse to learn more.

verizon

1 *2020 Data Breach Investigations Report,* Retail Industry Report.

Network details & coverage maps at vzw.com. © 2020 Verizon.