Protecting the finance industry with Rapid Response Retainer.

Use case

Cybersecurity remains at the forefront of concern for banks, insurers and the rest of the financial industry–especially in today's digital age. This use case is based on work we performed for a previous client and informed by both our global footprint and our extensive experience helping financial organizations protect their assets.

Thirty-one percent of consumers say they discontinued their relationship with a company that had a data breach.[1]

The situation

A CISO of a national retail and investment bank received a call from law enforcement. The law enforcement officer informed the CISO that certain systems on the bank network were likely compromised—they had been observed contacting a known malicious IP address.

The CISO immediately understood how serious this could be. Modern customers were leaving banks without hesitation after a data breach. New fintech competitors were stealing market share, which increased the danger of reputational risk. Even minor damage to the bank's reputation could lead customers to turn elsewhere.

The CISO had already begun to prepare for this moment. The bank had embraced mobility and cloud-based solutions to good effect, but its security teams were often stretched thin; 10% of all breaches occur in the financial industry, and the bank was feeling its share.[2] Because finding, affording and retaining more security experts was an enormous challenge, the CISO had instead invested in Verizon Rapid Response Retainer, which was powered by the Verizon Threat Research and Advisory Center (VTRAC).

With a much larger attack surface due to cloud and mobility, and a rapidly vanishing insurance buffer as more and more real-time payment transactions cleared in seconds, the CISO had looked to Rapid Response Retainer as a proactive solution that could help respond to incidents fast. This would be its test.

The investigation

The bank's initial network review revealed two systems—one in California, one in Virginia—communicating with the malicious IP address. The bank's security team quickly determined the systems contained customer financial data that absolutely could not be exposed. The CISO triggered Rapid Response Retainer.

VTRAC investigators began remote investigation immediately. Using leads provided by the bank's security team, the VTRAC investigators identified an active open-source remote access Trojan (RAT). Malware analysis of the RAT revealed domain names resolving to the malicious IP address.

Leveraging Verizon's global IP network—the world's largest—and its expansive view of worldwide cyberthreat activity, the VTRAC cyberthreat intelligence team was able to associate the RAT with a known advanced persistent threat. This armed the VTRAC team with a list of indicators of compromise (IoCs) to hunt for.

Along with the bank's security team, the Verizon responders quickly and methodically scanned the bank's network for other potentially compromised systems. The scans identified multiple infected systems, some that had been compromised for some time.

The VTRAC threat hunting efforts found the commodity malware right away. These were backdoor tools used by the attackers to maintain persistence on the network. Deeper-dive

verizon

analysis also found multiple compromised user accounts, including administrator accounts. The threat actors were observed accessing the bank network via an IP address associated with the bank's cloud managed service provider. The CISO had been right to be concerned about a larger attack surface brought about by the cloud.

With evidence of a sophisticated attack, particularly over such an extended period of time, the CISO knew it was highly possible other critical systems and user credentials were at risk. Most importantly, it was possible that attackers had already stolen customer financial data.

The response

The CISO and VTRAC team had already set up the war room and convened a running meeting with the incident response (IR) stakeholders. These IR stakeholders ranged from highly technical infosec response managers to legal counsel, human resources and corporate communications individuals, among others. Everyone involved knew their roles, responsibilities and authorities, as before this incident, Rapid Response Retainer had helped the CISO refine the bank's response plan. This made setting up the war room a matter of process, not panic, and helped the teams involved inform the right audiences and take steps toward crafting legal and PR responses if necessary.

The bank set about identifying and then rebuilding all affected systems. Certain areas of the network had been lacking in adequate visibility. The CISO made a note to expand monitoring capabilities as soon as the crisis was over.

The IR group realized that understanding every detail of the threat actors' actions in the network would be very resource intensive—another point the CISO would have to address later. Instead the bank committed to determining if data exfiltration had occurred and if the attackers had gotten away with customer data.

Ultimately the bank's containment, eradication and remediation efforts succeeded, in part due to the rapid action of the CISO and VTRAC teams. The bank observed no additional threat actor activity on the network, and found no evidence that data had been stolen.

What could have been a major issue with significant financial and reputational damages had been avoided thanks to quick action and the bank's investment in Rapid Response Retainer.

The CISO had been right to be concerned about a larger attack surface brought about by the cloud.

Getting ahead of the next attack

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.[3] But the latest version of the retainer goes beyond that to offer add-on VTRAC capabilities that would have allowed the bank to add capabilities that suited its needs, such as:

- Prepaid service hours
- Backbone NetFlow Collection
- Dark web hunting
- Network telemetry analysis
- Endpoint telemetry analysis
- Additional assessments

As the CISO learned, identifying the path the threat actors blazed through the bank's network was easier said than done. Network telemetry analysis would have made this much faster. And that was just one example of the way these add-on capabilities could reduce much of the heavy lifting and speed up the response effort.

Although the bank's investigation uncovered no evidence of data exfiltration, the latest version of Rapid Response Retainer would have given the CISO a way to double-check this result. With dark web hunting, VTRAC can monitor the dark web, deep web and clear web to see if any of the bank's data ends up for sale or if the threat actors brag about the breach.

Stay ready with proactive capabilities.

The CISO in this use case learned the value of having seasoned cybersecurity expertise on call. But there was one other lesson as well: A little preparation indeed does go a long way. Whether it's a well-crafted IR plan or predeployed capabilities like network or endpoint telemetry analysis, preparation can help financial organizations protect their customer data, their reputation and the health of their business.

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

verizon

1 https://www.centrify.com/media/4737054/ponemon_data_breach_impact_study.pdf

2 *Verizon 2019 Data Breach Investigations Report* (DBIR)

3 Coming soon.

Network details & coverage maps at vzw.com. © 2020 Verizon. UC9000620