CASE STUDY

Transforming security posture after state-sponsored cyberattack

When a state-sponsored threat actor attacked a financial services management firm, and its customers lost substantial funds, the company turned to Palo Alto Networks Unit 42™ Incident Response team to identify the point of entry and attack chain leveraged by the threat actor.

paloalto® NETWORKS

IN BRIEF

Customer
Large financial services management company

Industry
Financial services

Products and Services
Managing funds on cryptocurrency exchanges

Country
United States

Challenges

Following a state sponsored cyberattack resulting in hundreds of thousands of dollars in cryptocurrency being stolen, the client needed to understand who was responsible and how it happened.

Requirements

The company needed immediate incident response services help to identify the source of the attack, secure the environment, and provide an after-action report to help the company understand what had transpired. The organization's CISO also needed guidance on properly addressing board members' concerns about the incident and its resolution.

Solution

Unit 42 incident response experts identified how and where the breach occurred, guided the client to put the proper security controls in place, and provided post-event guidance to help the CISO effectively communicate what had happened and remedies put into place to ensure it doesn't happen again.

Introduction

We've seen a staggering amount of investment in cryptocurrencies in the last several years. Today, the space is no longer just the domain of technical enthusiasts. As cryptocurrency ownership has exploded, so has the number of attacks on cryptocurrency management firms. Unfortunately, many of these firms are ill-prepared to defend against skilled adversaries.

In this case, the North Korean-sponsored Lazarus Group utilized its fast-developing capability to spot and exploit infrastructure vulnerabilities. They used a combination of commercial and custom-developed tools and persistent mechanisms to find a single device that allowed them to breach the network to steal several hundred thousand dollars' worth of clients' crypto funds. The client realized they needed an experienced incident response team to find and fix the problem.

CHALLENGE

Cryptocurrency theft threats require proven expertise to find and fix the problem.

REQUIREMENTS

To immediately address and contain the threat—and harden their security posture to prevent future attacks—the cryptocurrency management firm needed the help of an experienced incident response firm that could:

- Identify the source of the breach.
- Determine the scope of the breach.
- Determine the identity of the threat actor.
- Contain the breach and ensure the threat actor has been completely removed from the environment.
- Provide the proper technology fit and recommend specific ways to mitigate the potential for future similar attacks.
- Consult with the CISO and other security leaders about how to address concerns and questions posed by key stakeholders, including board members.

The client needed an incident response team to immediately investigate, contain, and remediate the threat.

SOLUTION

The Palo Alto Networks Unit 42™ Incident Response team addressed the client's technical and business challenges.

The incident response services, combined with technical remedies, helped the management firm significantly harden its defenses both at the network's edge and within their security infrastructure.

The client chose to work with an experienced incident response team once they realized the scope and impact of the breach. Due to the extent and type of the threat, the IR team needed to be familiar with the specific technical challenges that are the hallmarks of an APT like the North Korea-backed Lazarus Group.

After consulting with their outside legal counsel, the financial services firm contacted Palo Alto Networks Unit 42 Incident Response team. The client's outside law firm recommended Unit 42 because of their rapid response capabilities, ability to leverage threat intelligence to accelerate their response and containment, industry-leading tools, and history of working closely with Unit 42.

CASE DETAILS

Unit 42 consultants quickly determined the chain of events that led to the currency theft:

- The threat actor targeted specific employees with a successful spear phishing campaign leading to installing a backdoor on their machine.
- The company had just completed a trial of EDR products which allowed them to remove the threat actor from the environment.
- However, several months later, the threat actor returned via the persistence mechanism left on a user's personal device where the EDR product was not deployed.
- The threat actor had performed reconnaissance on the environment during the first pass and knew exactly what to do when they came back.
- Once they returned, the threat actor initiated legitimate connections to the corporate VPN via the personal device and used multiple systems the user would typically use to harvest additional credentials.

- The attacker then pivoted to other corporate assets with the stolen credentials to get into the corporate email tenant using legitimate systems and credentials and removed users from distribution lists that would have been notified of any unauthorized financial transfers.
- They then used a stealthy, custom-written Trojan to harvest administrator credentials.
- Without detection, the threat actor then initiated multiple crypto transfers using a legitimate corporate system.
- Having exfiltrated several hundred thousand dollars' worth of funds, the threat actor exited the network, even cleaning up the malware used to move throughout the environment.

RESULTS

Determine the source and identity of the attack

Unit 42's consultants determined that the client was attacked using custom backdoors created by Lazarus Group, a North Korean-sponsored threat actor. This allowed Unit 42 to use its threat-informed approach and experience to determine the proper framework for tightening network access and credentialing based on the threat actor's past pattern of attack and data exfiltration.

Make focused recommendations to lock down systems against future similar attacks

The consultants recommended that the client not allow personal devices to operate on the corporate networks and install EDR/XDR tools to detect and protect the system from abnormal system behavior. These recommendations alone would make it far more difficult for adversaries to execute the malware found on the personal device.

Adopt EDR/XDR technology with the help of an experienced managed security service provider (MSSP)

Like many other organizations, the management firm was not very familiar with the benefits of EDR/XDR tools. Using an experienced MSSP allowed them to leverage their partners' knowledge and skills much faster and at a lower cost than trying to develop or hire resources for in-house security.

Position the CISO and security operations leaders as trusted advisors and forward-thinking professionals to C-suite executives and the board

Not surprisingly, being breached and losing clients' funds upset business leaders at the firm, especially board members. Unit 42's advisors coached the security leadership team on how best to present their findings, remedies, and go-forward plan to business leaders in a way that was credible and trustworthy.

CONCLUSION

Choosing the right security partner sets up the organization's future success and operational resilience.

As exciting and as potentially groundbreaking a business opportunity as cryptocurrency may be, it is clear that this emerging market is an inviting target for cybersecurity threat actors. More than one billion people will own cryptocurrency by the end of 2022.[1] Unfortunately, the industry's tenuous and halting stance toward regulations that protect individuals and management firms means that crypto thieves are already taking aim.

1. Henry Hon, et al., *Crypto Market Sizing*, Crypto.com, January 20, 2022, https://assets.ctfassets.net/hfgyig42jimx/5i8TeN1QYJDjn82pSuZB5S/85c-7c9393f3ee67e456ec780f9bf11e3/Cryptodotcom_Crypto_Market_Sizing_Jan2022.pdf.

The ever-evolving threat landscape means that organizations must be highly vigilant in understanding the nature of those risks and must put in place both the right technology and security best practices to protect crypto assets and the rest of their estate fully.

Doing so raises the bar for hackers and helps organizations have a more strategic view of their cybersecurity risks even beyond protecting their account holders' crypto assets.

ABOUT UNIT 42

Palo Alto Networks Unit 42 brings together world-renowned threat researchers with an elite team of incident responders and security consultants to create an intelligence-driven, response-ready organization passionate about helping customers more proactively manage cyber risk. With a deeply rooted reputation for delivering industry-leading threat intelligence, Unit 42 provides state-of-the-art incident response and cyber risk management services. Our consultants serve as your trusted advisor to assess and test your security controls against the right threats, transform your security strategy with a threat-informed approach, and respond to incidents in record time. Visit paloaltonetworks.com/unit42.

If you have been breached or have an urgent matter, please call the Unit 42 Incident Response team:

- North America Toll-Free: +1.866.486.4842 (+1.866.4.UNIT42)
- UK: +44.20.3743.3660
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

If you have cyber insurance or legal counsel, you can request for Unit 42 to serve as your Incident Response team. Unit 42 is on over 70 cyber insurance panels as a preferred vendor.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com