CASE STUDY

Jolted by Ransomware Attack, Infrastructural Service Provider Emerges Strengthened With Insight and Improved Security Posture

An infrastructural services company with more than 1,000 employees experienced a ransomware attack that, theoretically, should never have succeeded. After all, the company had taken pains to deploy endpoint detection and response (EDR) and other security capabilities, had backed up all its data, and was doing its best to keep the network secure.

But when a phishing email came in with a spreadsheet attachment, a user opened it and enabled macros when prompted. This opened the door to the attackers, who took only three days to exfiltrate multiple gigabytes of company data with the intention of holding it for ransom, ultimately halting business operations.

The company urgently needed to stop further data exfiltration, determine if the attacker maintained persistence in the network, and if so, prevent any further exploitation. After containment, the company needed to go deeper to understand the chain of events—including the weaknesses in its security that led to every successful step of the compromise, and how to prevent it from recurring. It decided to call on the FortiGuard Incident Response (IR) Services.

Root-cause Discovery and Containment

Even though the company was not a Fortinet customer, the security team's decision to engage FortiGuard IR Services stemmed from its trust in Fortinet as a threat intelligence leader. After the kickoff debriefing with the security staff on the status of the attack and the existing security architecture, the FortiGuard IR team deployed forensics tools to assist in containment and analysis. Using a cloud-based FortiEDR instance, they identified currently infected hosts and threat activity, began blocking the threat actor requests to the network, and cleaned the compromised endpoints. Then they identified all other indicators of compromise (IOCs) across the threat's short but full lifecycle—from foothold, through command and control, lateral movement, ransomware deployment and encryption, to successful data exfiltration.

Next, the IR team analyzed the data gathered through the FortiEDR forensics tool. Using FortiEDR as a "black box" to play back the attackers' activity, they identified the initial compromised endpoint and followed the attack process chain, from the moment the unsuspecting employee opened the spreadsheet and enabled macros through all the activity that followed. It turned out that the attackers had used Cobalt Strike—a legitimate pen-testing (penetration testing) tool—as a means of remote access and lateral movement. With it, they scanned the network and identified other hosts, where they discovered the data that they ultimately exfiltrated and then encrypted.

The IR team also found that, although the company's existing EDR solution was up and running, it was not configured or tuned properly. So, while the system had been sending out alerts, it was not actually blocking any suspicious activity. And

The company had deployed EDR, backed up all its data, and was doing its best to keep the network secure. Yet, when a phishing email came in with a spreadsheet attachment, someone clicked on it. Within three days, attackers were able to exfiltrate multiple gigabytes of data.

Details

Industry: Infrastructural Service Provider

Location: Europe

Business Impact

- Rapid mitigation of business risk due to ransomware attack
- Improved protection against future attacks
- Increased cyber awareness among security staff

the security team, unable to keep up with the stream of alerts, did not recognize what was happening, so they did not take appropriate action.

By turning on and tuning the EDR protection policy, the IR team was able to contain the ransomware attack to avoid further damage. Then they turned their attention to preventing a recurrence of the attack, through an in-depth analysis of the attacker footprint. The analysis identified misconfigurations, a lack of processes that could have helped identify additional IOCs, and other gaps. The full engagement, including debriefing, containment, analysis, and a full report of remediation and best-practice guidance, was delivered over a period of five weeks.

Protocols to Boost Security Posture

The comprehensive guidance the IR team provided included both strategic and tactical recommendations. To start with, they said the team should ensure that all security tools are correctly configured and tuned soon after deployment. They should deploy appropriate prevention on all devices, not just those deemed operationally critical, because non-critical devices can easily become vectors to access critical hosts. In addition, the company can stay ahead of the rapidly evolving threat landscape by leveraging EDR technology that learns and prevents malicious behaviors such as ransomware-related file downloads, command-and-control, and lateral movement. The company should also ensure all such new tools are changed from simulation to prevention mode. Appropriate technology controls can not only block malicious files, they can also prevent dangerous user behavior such as macros enablement. The company should test the tools regularly and maintain an updated ransomware playbook.

To improve the detection of possible attacks, the company should implement a change control process to flag newly created accounts, especially those not authorized through the appropriate channels. It should also monitor changes or additions to files in sensitive directories, and flag and review large data transfers, especially those outside business hours. This, together with appropriate security technology controls and logging for suspicious behaviors, can reduce the efficacy of stolen credentials and lessen the likelihood of successful attack and attack discovery and response times.

Services

- FortiGuard Incident Response Services
- Fortinet Managed Detection and Response

Solutions

- FortiEDR

The company derived both immediate and long-term value from FortiGuard Incident Response (IR) Services. Rapid containment of the attack limited the impact on the company's revenues and reputation. Root-cause analysis and best-practices education have helped improve its security posture.

Policy changes, such as adopting least-privilege access and mandating multi-factor authentication (MFA), would limit the ability of an attacker to escalate privilege and perform privileged actions on the network.

Recognizing that all these steps would not completely preclude any further attacks, the company was advised to maintain an updated IR action plan. Putting this plan, or playbook, in place—and conducting regular tabletop exercises to test it—would put the company in a much better position to face the next cybersecurity incident.

Finally, the IR team's recommendations pointed to ongoing education for staff and awareness for employees. Although the company strives to conduct regular employee security awareness training, turnover can be high. The longer new hires are at the company before receiving security training, the higher the chance they can become the weakest link. The recommendation was to increase training frequency and to repeat the training at regular intervals to maintain awareness.

For the small security staff, the challenge was optimizing the use of their limited time and energy resources. Here, Fortinet recommended investing in staff development and training on security best practices and to get the most from their security tools by using them effectively. Because the team was small, it also made sense for the company to supplement their efforts with round-the-clock managed detection and response (MDR) services to monitor, review, and act on events or suspicious behavior.

A Learning Experience

As painful as the ransomware attack was, the company sees it as an eye-opening experience. It found it particularly insightful to recognize how unseen changes in the user base, the threat landscape, and the network underlines the need for regular security posture updates and processes and can otherwise converge to create very salient harm to the business.

On the other hand, this salience is helping the security team gain approval for investments in people, processes, and technology. For example, after seeing the multifaceted FortiEDR tool in action in the containment and analysis of the recent attack, the team is now leveraging FortiEDR for ongoing infrastructure protection.

The attack also brought into focus the way external expertise can augment a talented but overextended in-house team. Opting to have FortiGuard experts in threat hunting, incident response, and remediation manage its new FortiEDR technology, the company feels more confident it can get the greatest leverage from its investment and improve its security posture. As soon as they saw the suspicious activity, the team took their backup systems offline. This enabled them to restore their data and resume operations promptly after the containment process. Because containment happened so quickly, with the FortiGuard IR Services positively identifying the ransomware lifecycle and sources of compromise, the company was able to minimize the impact on its revenues and reputation.

September 3, 2022 2:20 AM
1732219-0-0-EN