VARONIS

How Varonis Helped a Large Services Company Eliminate a Massive Malware Infection

CASE STUDY

> “In terms of solutions, Varonis Edge was our MVP. Edge directed us to computers with suspicious DNS requests, correlated them with specific users, and showed us the addresses we needed to block.”

ABOUT THIS CASE STUDY:

Our client is a large services company. We have happily accommodated their request to anonymize all sensitive information, including individual names, company name, and industry.

HIGHLIGHTS

CHALLENGES

- Getting to the bottom of why their network was slower than usual
- Understanding the full extent of their malware infection
- Eliminating cryptomining malware that had infected almost every server and workstation

SOLUTION

The most robust data security platform:

- **DatAdvantage** for Active Directory and Azure
- **DatAlert** for threat detection and prevention
- **Edge** to root out perimeter threats, including cryptomining malware

RESULTS

- Malware infection successfully eliminated
- More visibility and protection to prevent future attacks
- Peace of mind that comes with a proven security platform and support

Challenges

Detecting and stopping a cryptomining attack

The signs of the attack were subtle: computers running a little slower, unstable applications, and general network slowdowns.

But it was enough that the security engineers for a large services company (who requested anonymity), knew something was wrong.

They decided to install Varonis DatAlert and Edge to get to the bottom of the problem. What they found was shocking.

> “We knew there was an issue, but we wouldn’t have known how devastating it was without Varonis.”

With Varonis, they discovered that nearly every server and workstation was infected with cryptomining malware.

> “Varonis helped us find the full extent of the situation—and it was more surprising than we thought it would be.”

Rather than build mining rigs and pay the electric bill themselves, attackers use cryptomining malware to piggyback off other people's resources. By pooling the resources of multiple infected devices, cybercriminals are able to create massive mining networks of hundreds or even thousands of devices.

Cryptominers mean big paydays for criminals. According to a recent industry report, $175M in Monero (5% of all Monero currently in circulation) has been mined illegally using cryptomining malware. But, given the prevalence of Bitcoin and other cryptocurrencies, the total amount is likely much higher.

Unlike blatant ransomware attacks, cryptojacking is difficult to detect. Hackers disguise the cryptomining malware as regular network traffic. As a result, infection rates were up over 4,000% in 2018, according to McAfee, and a lot of companies may be infected without even realizing it.

Varonis not only helped this client detect this threat, it helped them eliminate the malware and protect against future attacks.

> "We knew there was an issue, but we wouldn't have known how devastating it was without Varonis."

Solution

Discovering the extent of the malware infection

The company's security engineers had two main reasons for choosing Varonis over other security solutions:

1. They'd seen it in action and knew how effective it was at detecting and eliminating potential threats.
2. They appreciated the open and honest approach of Varonis' team, both pre- trial and as a client.

> "A lot of vendors just wanted to sell us something. They'd say, 'we've seen it all' or 'we can solve that problem' without investigating further. But when we showed the problem to the Varonis team, they said, 'We've never seen that before.'"

To figure out what the threat was and how to stop it, the Varonis Security Research Team collaborated with security engineers to investigate the extent of the infection.

> "Varonis' team didn't offer any kneejerk solutions—they listened, took notes, did some homework, and came back with informed suggestions that actually helped us solve our problem. That approach was so refreshing."

Analysis of the collected malware samples revealed a new variant, which the team dubbed "Norman." Because it was a new variant, Norman was able to slip past their antivirus, endpoint detection and response (EDR), and firewalls—effectively avoiding discovery on their network.

In other words, even though the company had numerous safeguards in place, the malware was able to infect almost every device at the company before it was caught.

Using Varonis products to eliminate the threat

Three Varonis products were instrumental in helping the client's security engineers find and fix their malware infection: DatAdvantage, DatAlert, and Edge.

DatAdvantage gave the client more visibility into what's going on in their servers and in the cloud. It made it easy to see when and where changes were taking place and who was making them.

> "Every organization should have DatAdvantage. The dashboard displays information in almost real-time and insights we were missing. With it, we can monitor file shares and directory services, as well as Office 365 and Azure."

When combined with the DatAlert Suite, the engineers were able to track potential threats to their source. The extra context it provided enabled the security team to understand the problem and take swift and decisive action.

> "We use DatAlert every day. It alerts us to suspicious activity and lets us drill down to the root of the problem—the username or computer the issue occurred on, the IP address that caused the problem, if the attacker is geo-hopping, etc."

And, for detecting and dealing with the cryptomining malware, Edge was invaluable. By analyzing activity on perimeter devices combined with data access activity, Edge was able to detect this almost invisible threat—and stop it from escalating any further.

Results

Cleaned up infrastructure & clear audit trails

There had been malicious activity going on undetected within the company's environment for months. With Varonis' help, security engineers were able to understand the activity, find the source of the problem, and eliminate the malware infection from every device.

> "Varonis showed us the full extent of the problem and played a big role in helping us eliminate it."

Now, Varonis is helping them on a day-to-day basis with data protection, threat detection and response, and compliance.

> "Varonis makes it easy to pinpoint information you can't normally find. In minutes, we can see exactly who's accessed a file share or make informed decisions about suspicious activity."

They like the fact that even though Varonis' offers granular insights, the dashboard prioritizes the most important information, making it easy to understand and actionable.

> "It's easy to pick up. Learning the basics and how to generate reports is very accessible. And the dashboard is topnotch for knowing what's going on within your network."

And the company has since tried—and enthusiastically endorses—every product in the Varonis suite of solutions.

> "We've viewed every product Varonis has to offer and, if we had an unlimited budget, we would buy them all. They all provide so much value."

"Varonis showed us the full extent of the problem and played a big role in helping us eliminate it."

VARONIS

Don’t let malware sneak through your defenses.

Simplify security investigations, get all the insights you need, and protect your network and its perimeter from threats.

REQUEST A DEMO