5 lessons we learned from our ransomware attack

By Mark Hughes, Senior Vice President, DXC Technology

Time is of the essence in a ransomware attack, as one of the real impacts is downtime.

It's well documented that ransomware attacks are on the rise, and they can have serious consequences that impact all parts of a business including customers, operations, brand, and even boards of directors.

As part of my role at DXC Technology, I oversee our security business, and I frequently deal with attacks on our customers. But on Saturday, July 4, 2020, as I was stepping out of the car to start my family vacation, the company became the target of a ransomware attack.

The incident involved Xchanging, a subsidiary based in the United Kingdom, which provides technology-enabled business services to the commercial insurance industry. The attacker sent an often-used image of a beloved cartoon character making an obscene hand gesture with this message: "We have your data. We've encrypted your files. If you want to negotiate, we can talk on a secure tool or chat session."

While the network used by the Xchanging business was segregated from DXC's much larger IT environment, we were nonetheless concerned about whether the incident would have operational impacts to Xchanging customers when London insurance offices opened on Monday.

Time is of the essence in a ransomware attack, as one of the real impacts is downtime. The average attack takes critical systems down for 16 days, according to Emsisoft, which predicts overall ransomware costs could hit $170 billion worldwide in 2020.

In the Xchanging instance, the hacker had gained initial access just two days earlier. Only a handful of systems were accessed, and we were able to quickly isolate and neutralize the threat. No data was stolen, and we did not pay the ransom. We immediately engaged our customers and authorities. On Sunday, July 5, we cleaned and restored the impacted environment. By Monday morning, Xchanging was able to process insurance policies.

Tips for staying safe

The criminal investigation is ongoing, and we are taking every opportunity to review our controls and procedures. Nearly everything worked as planned. But that, sadly, is not the case for many organizations.

We analyzed what went right, what did not, and what we can do better.

Here are five key takeaways:

Know your infrastructure. Focus on basic software-patching hygiene, and ensure all networks and firewalls have enterprise security tools in place to detect malicious behavior. The attackers began by using a publicly available security testing tool referred to as "grayware." Grayware is not malicious in its own right but in this case was used to create a backdoor to exploit Microsoft Windows and deploy a new variant of encryption malware. While we had not prevented the attack, we were alerted that something was not quite right, and we were able to quickly identify where the network was compromised when the attack was underway.

Involve senior leadership from the start. Our global crisis team met to assess the situation, which was key for us because we directly involved senior leaders so that critical decisions could be made quickly. For example, we needed to shut off remote access, so I made the decision to sever all connectivity to the Xchanging systems. While that sounds easy, it required urgent action from our IT teams in both the United Kingdom and India, and engaging leadership from those teams allowed the shutoff to happen quickly and efficiently. Throughout the response, members of our leadership team — including our CEO, Mike Salvino — were involved in evaluating the situation and making key decisions. Good governance is crucial in these times. If you lack accountability or clarity on who's doing what, you're wasting precious minutes that attackers will exploit.

Authorities strongly advise against paying ransoms. In fact, the United States and United Kingdom are moving to enforce civil and even criminal penalties for making ransom payments.

Engage authorities and experts early. Law enforcement and security experts can provide invaluable insight on how to counter an attack and enable fast legal intervention. For example, the ransomware was set to send Xchanging data to website domains in the United States, so I contacted law enforcement officials working on the holiday weekend. That evening, we obtained a court order to take control of the attackers' internet domains.

Gain as much leverage as you can — and don't pay. Authorities strongly advise against paying ransoms. In fact, the United States and United Kingdom are moving to enforce civil and even criminal penalties for making ransom payments. In our case, the attackers didn't ask for money upfront. They wanted to negotiate. We knew we had cut off the attack, we knew they didn't have our data, and we knew we had backups. We were in a strong position, so we didn't need to negotiate. If you do choose to negotiate with cybercriminals, don't go it alone. Find and retain an experienced ransom broker — preferably as part of your incident response preparation, before you've been attacked.

Be transparent. You don't have to reveal all the facts, but openness is generally a good practice. We shared the attacker's indicators of compromise (IOCs) with hundreds of customers. While there certainly may be information that you cannot release (e.g., when subject to customer confidentiality restrictions or as directed by law enforcement), sharing information when you can do so not only helps keep others safe, but it can also help you enlist the aid of a large body of your colleagues, authorities, and the security community. We issued a news release on Sunday, July 5, to make public markets aware, and we followed up with another release a few weeks later to confirm containment.

The law enforcement officials I spoke with that weekend were surprised that our attack was already contained. Most of the calls they receive come from the CEO, because the IT and security teams are frantically busy, and the company is usually on its third or fourth day of shutdown with no end in sight.

We know our July 4 attack could have been much worse. A combination of rapid incident response, security controls and governance, and utilizing technical tools and industry practices gave us an advantage.

The "new DXC" showed up strong to address the challenge and keep our customers top of mind at all times.

And that's how I spent my summer vacation.

Stay on top of the latest threats. Subscribe to DXC's Security Threat Intelligence Report at **www.dxc.technology/threats_HBR**.

About the author

Mark Hughes is senior vice president of offerings and strategic partners at DXC Technology, responsible for DXC's global security organization and offerings, including cyber defense, secured infrastructure, digital identity, and data protection. He previously served as chief executive at BT Security.

Get the insights that matter.
www.dxc.technology/optin

About DXC Technology
DXC Technology (NYSE: DXC) helps global companies run their mission critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. With decades of driving innovation, the world's largest companies trust DXC to deploy our enterprise technology stack to deliver new levels of performance, competitiveness and customer experiences. Learn more about the DXC story and our focus on people, customers and operational execution at **www.dxc.technology**.

© 2020 DXC Technology Company. All rights reserved.