solis

THWARTED THREAT

A machinery manufacturer nearly falls victim to malicious software

Case study

When people think about insurance, they typically assume that it is just a piece of paper that promises to pay valid claims. While in some areas this may be true, cyber insurance is actually much more than that.

Not only do cyber insurance policies indemnify policyholders for losses stemming from cyber events, but they also provide a service to policyholders by helping and advising them when things go wrong. This includes access to a whole range of partners and experts who are effectively on retainer to the policyholder through their purchasing of a cyber policy, which many small businesses might not otherwise be able to afford.

However, some cyber insurers are going beyond purely providing reactive services in response to cyber events that have already happened and are looking to provide proactive risk management services to clients to prevent incidents from happening in the first place.

After all, a lot can change during the course of a policy year and a policyholder's cyber security posture is rarely static: new software applications might be adopted, networks might be expanded to incorporate newly acquired entities, and staff might shift towards remote working, to list just a few examples. Likewise, the cyber threat landscape is always evolving, with criminals constantly looking for new vulnerabilities to exploit.

Solis is a strong proponent of proactive risk management. That's why we have invested heavily in our incident response and threat intelligence teams as well as utilising CFC's Response mobile app. This allow us to proactively alert policyholders to critical threats to their business in the hope that we can remedy issues before cybercriminals look to take advantage.

Our business at Solis is proactive risk management and one business that has benefitted from this is a manufacturing company that specializes in the manufacture of tools and machinery, with an annual revenue just short of $15 million.

MICROSOFT VULNERABILITY ENABLES ATTACK

The incident began with cyber criminals looking to exploit the Microsoft Exchange Server vulnerabilities which were first discovered in January 2021 and first publicly identified by Microsoft in March 2021, collectively known as “ProxyLogon”.

Microsoft Exchange Server is Microsoft’s email, calendaring and collaboration platform for business use. In January, four new vulnerabilities were discovered which allowed cyber criminals to gain access to Microsoft Exchange Servers. In March, Microsoft released updates to patch the vulnerabilities, but many organizations had been compromised prior to this or were unable to patch before the cybercriminals found them.

This is precisely what happened in this instance.

Since Microsoft Exchange Servers are web-facing servers and are visible on the internet, cybercriminals are able to quickly locate servers exposed to any new vulnerabilities by using scanning tools. The threat actor was able to locate the manufacturer’s exchange server using a scanning tool, and as the manufacturer had not made the necessary patch that Microsoft had released to fix this security issue, the threat actor was able to exploit the vulnerabilities to gain access to our businesses server.

Since Microsoft Exchange Servers are web-facing servers and are visible on the internet, cybercriminals are able to quickly locate servers exposed to any new vulnerabilities by using scanning tools.

EXPLOITATION THROUGH MALICIOUS CODE

The threat actor's first step was to exploit a vulnerability that allowed them to falsely authenticate as the most privileged account on the server. With these administrator privileges at their disposal, they were able to exploit two further vulnerabilities which allowed them to install what is known as a web shell.

Essentially, a web shell is a piece of malicious code that allows criminals to remotely access web servers and execute commands on them, including commands to exfiltrate data or install malware or ransomware.

One of the benefits for cybercriminals of installing a web shell is that patching the server against the vulnerabilities does not automatically remove it, thus allowing threat actors to attach web shells to as many vulnerable servers as possible to act as a beachhead which they can then return to later (assuming the server remains on and the web shell isn't removed).

In this case, this meant that although the manufacturer eventually implemented the patches rolled out by Microsoft to remove the vulnerabilities, the web shell installed by the threat actor remained in place, allowing for continued remote access to the server.

With the web shell acting as a backdoor into the organization, the threat actor then looked to take the next step: installing ransomware onto the manufacturer's computer systems. In order to do so, they downloaded a common type of precursor malware that is used to deliver ransomware onto computer systems and begin the encryption process.

Essentially, a web shell is a piece of malicious code that allows criminals to remotely access web servers and execute commands on them, including commands to exfiltrate data or install malware or ransomware.

CFC THREAT ALERT WARNS BUSINESS OF INTRUDER

Fortunately, however, it was at this point that Solis' proactive threat intelligence team entered the picture. At Solis, we work with CFC to utilize a range of internal and external resources that allow us to scan our their internet presence for potential vulnerabilities and signs of compromise, including the presence of web shells and common precursor malware used in ransomware attacks.

Following one of these scans, we were able to detect both the presence of the web shell and the precursor malware on the manufacturer's computer systems. As soon as our threat intelligence team were aware of this, we got in touch with the insured and alerted them to the issue, stressing the point that a ransomware attack was likely to hit them imminently.

Having been notified of the issue and its urgency, a member of our threat intelligence team jumped on a call with a member of the manufacturer's IT team, talking them through the issue and explaining how to delete the malware and remove the web shell. With these actions, the threat actor was removed from the manufacturer's server and the ransomware attack was foiled without any costs being incurred by the insured.

Had our threat intelligence team not intervened at this critical moment, it is almost certain that the manufacturer would have been laid low by a ransomware attack, with all the financial costs and operational disruption that this entails.

As soon as our threat intelligence team were aware of this, we got in touch with the insured and alerted them to the issue, stressing the point that a ransomware attack was likely to hit them imminently.

THE IMPORTANCE OF PATCHES AND MORE

This incident highlights a few key points.

Firstly, it highlights the importance of making security patches and updating computer systems as promptly as possible. Cybercriminals are constantly on the lookout for new vulnerabilities that they can exploit in order to gain access to organizations' computer systems. It is therefore imperative that businesses make any security patches as soon as is feasible.

Secondly, it highlights the value of proactive threat intelligence in the world of cyber insurance. In a threat landscape that is constantly evolving with cybercriminals always on the look-out for new vulnerabilities to exploit and new tactics to employ, it's vital that organizations are alert to any new threats that may arise.

Solis' proactive threat intelligence team is staffed by cyber security experts who are solely dedicated to identifying new threats and making our businesses aware of them.

By working with our team, businesses can keep up to date with the latest security issues and hopefully reduce the chances of a cyber event impacting their business. In this instance, by promptly acting on our alert and working with a member of our threat intelligence team, the insured was successfully able to avoid a costly ransomware attack.

And finally, this illustrates the value of cyber insurance. When this policyholder purchased their cyber insurance policy with CFC, they weren't simply buying a piece of paper that promised to pay valid claims. They were also buying access to a whole range of services which they might otherwise have been unable to afford. And although cyber insurance is still there to provide a valuable safety net in the event that the worst should happen, a good cyber insurance provider should be able to offer a range of risk management tools and services that can help reduce the likelihood of a claim happening in the first place.

Solis' proactive threat intelligence team is staffed by cyber security experts who are solely dedicated to identifying new threats and making our businesses aware of them.


solis