MOVE OVER, RANSOMWARE – THERE'S A BIGGER VILLAIN IN TOWN

Meet Jack - Jackware to be formal

For organizations, individuals, and cyber carriers alike, ransomware has been a rampant cybersecurity risk that's only becoming more prevalent. It's been a problem that's dominated discussions on loss patterns and risk in the cyber insurance space, and it's not surprising to see why. Ransomware cost the world $20 billion in 2021, a number that experts expect will only continue to increase year over year.

With ransomware growing at such an alarming rate and posing such a viable threat to businesses and organizations globally, it's hard to imagine something that might be worse. This statement isn't meant to downplay ransomware, but more so to reiterate why it's imperative to have the right cybersecurity measures in place to protect your organization from malicious actors.

We hate to be the bearers of bad news, but unfortunately an even more dangerous type of malware is becoming more commonplace: JACKWARE.

WHAT THE HACK, JACK?!

Burnham | WGB
A BALDWIN RISK PARTNER

With ransomware, hackers want to take control of your data and make you pay to get it back. **Jackware attacks are focused on taking over your machines and making them do things you don't want them to do.** Here are some examples of jackware attacks that happened in the past:

German steel manufacturing facility: In 2014, malicious actors targeted a German steel mill's network. Attackers deployed booby-trapped emails to steal logins that gave them access to the plant's critical systems. Parts of the plant failed, and a blast furnace couldn't be shut down even at over 2,000 degrees. This caused massive damage to the steel mill and halted its operations.

Ukrainian power grid: In 2015, Russian hackers attacked the Ukrainian power grid using a multi-tiered strategy comprised of spear-phishing and harvesting worker credentials. This resulted in power outages for 230,000 consumers for one to six hours.

MRI and x-ray machines, globally: In 2018, the spyware Kwampirs was found on computers that support MRIs and x-rays, as well as devices that patients use to fill out consent forms. Experts believe that this was part of a cyber-espionage operation.

Though the Colonial Pipeline attack was technically a ransomware attack, this more recent event is worth mentioning because of the implications it holds for just how devastating a successful cyberattack that targets the infrastructure and machines that power the world we live in can be, which is what jackware can potentially do in a digitized, interconnected world.

In today's world, tiny computers are embedded in all types of machines used by countless people. The connectivity features that make our devices "smart" are also points of vulnerability. Embedded devices play a critical role in our infrastructure. Operating systems for cars, corporate enterprises, manufacturers, food processors, healthcare, mass transit, and our homes rely on this technology. The devices that power our world function more and more like computers, making them just as vulnerable to cyberattacks. Jackware can potentially shut down pipelines and sabotage airplanes, or even compromise your car or implanted medical devices.

This is why so many experts are concerned about jackware. A successful jackware attack can have direct, physical effects and consequences. It can compromise the embedded devices that power larger physical systems, bringing them to a halt. With supply chain issues already impacting the way the world operates, that last thing we need is more stress on an already fragile ecosystem.

SO, HOW DOES INSURANCE FIT INTO ALL OF THIS? THIS IS WHERE THINGS CAN GET A LITTLE TRICKY.

Though you might think that a cyber policy would respond to losses caused by jackware, cyber insurance isn't designed to cover injury and property damage. Even though a jackware attack is a cyber event, incidents that lead to bodily injury or property damage might not be covered by cyber insurance. A Commercial General Liability (CGL) policy might cover bodily injury and property damage that occur as a result of a jackware attack. Right now, it might be too early to determine which policy would cover jackware related losses. The most prudent thing to do would be to alert your broker immediately for guidance about reporting the claim.

Take the time now to review your cybersecurity posture and overall risk mitigation strategies with your broker. Be sure that you're doing your part to stop malicious actors from successfully infiltrating your organization's systems, and that you're covered with the right insurance so that you're protected should you experience a loss.

This material has been prepared for informational purposes only. BRP Group, Inc. and its affiliates, do not provide tax, legal or accounting advice. Please consult with your own tax, legal or accounting professionals before engaging in any transaction.

Powered by Baldwin Krystyn Sherman Partners Insurance Sales, LLC
DBA Burnham WGB Insurance Solutions
CA Insurance License 0F69771

This material has been prepared for informational purposes only. BRP Group, Inc. and its affiliates, do not provide tax, legal or accounting advice. Please consult with your own tax, legal or accounting professionals before engaging in any transaction.

Burnham | WGB
A BALDWIN RISK PARTNER

burnhamwgb.com