Jackware Cyberattacks Explained

Author: Alliant

Ransomware incidents entail cybercriminals compromising their victims' computers or servers with malware and demanding large payments in order to restore the network (as well as any files or data stored on it). They are considered one of the most damaging cyberattack methods. While these incidents are certainly a significant concern, another emerging malware-based cyberattack method, known as jackware, has the potential to wreak even greater havoc on businesses of all sizes and sectors.

Rather than blocking access to important information, jackware incidents consist of cybercriminals hijacking victims' embedded systems via malware. These systems are comprised of specialized computing software that serves specific functions within larger machines. Embedded systems can be found within virtually all internet-connected devices (e.g., phones, laptops, tablets and smart cars and refrigerators), as well as advanced industrial machinery. After hijacking these systems, cybercriminals may cause their victims' compromised technology to malfunction or completely shut down, potentially creating business disruptions, inflicting major physical damage and even putting individuals' safety at risk. Similar to ransomware incidents, cybercriminals may require substantial payments amid jackware cyberattacks before restoring victims' devices.

As a growing number of businesses across industry lines rely on embedded systems to conduct critical operations, jackware incidents could become increasingly common and severe. With this in mind, it's crucial for businesses to understand and effectively address this attack vector. This article provides additional information on the potential implications of jackware cyberattacks, outlines the latest real-world examples of these incidents and offers prevention measures for businesses to consider.

Implications of Jackware Cyberattacks

Embedded systems play a key role in a wide range of critical business services and activities. These systems have been implemented within virtually all sectors through the use of smart technology and machine learning. Such systems are particularly prevalent within the critical infrastructure, health care and public transportation industries. Having these systems compromised by jackware cyberattacks can result in serious consequences for affected businesses.

Here's a breakdown of significant implications businesses could face from having their embedded systems compromised during jackware incidents:

- **Interruption issues**—Upon taking control of companies' embedded systems, cybercriminals may shut down certain devices or render them unusable, putting any operations that rely on this technology at complete standstills. For instance, a manufacturing business could be forced to halt its product assembly line if a crucial piece of machinery used during the assembly process ceases to work. These interruptions could

last for a few hours, or press on for multiple days. Without the ability to use critical technology for prolonged periods, businesses could experience major delays and lost income. If they are unable to recover hijacked devices, companies may even need to pay for technology repairs or replacements to stay operational.

- **Malfunction concerns**—Apart from shutting down embedded systems, cybercriminals may also intentionally cause companies' technology to malfunction or operate ineffectively amid jackware incidents. For example, a restaurant that utilizes smart refrigerators to store food at proper temperatures could encounter spoilage issues or inadvertently serve customers unsafe meals if its operational technology is altered. In addition to inflicting widespread physical damage, such malfunctions could negatively impact companies' productivity levels, increase their liability exposures, and possibly result in the need to issue product recalls.
- **Safety risks**—In some cases, cybercriminals may compromise companies' embedded systems in ways that threaten the safety of others. For instance, a hospital that leverages medical technology could end up providing incorrect diagnoses or improper treatment to patients if its devices become hijacked. Additionally, a transportation company that utilizes vehicles equipped with smart devices may face elevated accident risks on the road if its technology falls victim to jackware . These incidents could be particularly devastating, resulting in serious emotional harm, physical injuries, or fatalities.

Ultimately, the severe consequences associated with jackware attacks highlight just how crippling these incidents can be for impacted businesses. As a result, some cybersecurity experts have coined jackware as "ransomware's more dangerous cousin."

Examples of Jackware Incidents

Several notable jackware cyberattacks have occurred across the globe. Some of these incidents include:

- **The blast furnace incident**—In 2014, cybercriminals gained control of the embedded systems in a blast furnace at a steel manufacturing facility in Germany. In doing so, the cybercriminals caused the furnace to overheat and burn down a substantial portion of the facility. The incident forced the facility to close its doors permanently.

- **The vehicle hacking incident**—In 2015, cybersecurity researchers remotely hijacked the embedded systems within a Jeep Cherokee while it was on the road in the United States. Although this particular incident was merely a test carried out for informational purposes, it showcased the various ways in which cybercriminals could compromise vehicles equipped with smart devices. Such incidents could lead to damages as minor as a malfunctioning radio or as severe as disabled brakes.
- **The medical technology incident**—In 2018, cybercriminals targeted the embedded systems in various medical imaging devices (e.g., MRI and X-ray machines), temporarily taking control of this technology and compromising the operations of several global health care providers. The incident was widely considered an act of cyberespionage.

- **The Trickbot incident**—In 2020, cybersecurity researchers discovered that a well-known malware platform called Trickbot had started testing whether the embedded systems in PCs—namely, basic input or output system (BIOS) and unified extensible firmware interface (UEFI) software—were vulnerable to being hijacked. Looking ahead, cybercriminals could leverage this malware to remotely compromise the BIOSs or UEFI software in victims' PCs and ultimately take control of their devices.

Considering these incidents and their related ramifications, it's clear that businesses should implement measures to help prevent and reduce potential losses resulting from jackware cyberattacks.

Steps Businesses Can Take

Businesses should consider the following measures to effectively avoid and minimize damages stemming from jackware incidents:

- **Train employees**. Educate employees on what jackware is and what they can do to prevent these attacks. In particular, employees should be instructed to never click on suspicious links or download attachments from unknown senders on workplace devices, as doing so could trigger malware infections and allow cybercriminals to more easily execute jackware incidents.
- **Ensure effective authentication protocols**. Use the principle of "least privilege" by only allowing employees the minimum access to technology that they need to perform their job tasks. Further, require employees to use complex and unique passwords on all workplace devices, and leverage multifactor authentication capabilities whenever possible. These advanced authentication measures will make it increasingly difficult for cybercriminals to gain unwarranted access to and hijack company technology.
- **Utilize proper security software**. A variety of security software can be used to identify and prevent jackware cyberattacks. Examples of this software include endpoint detection tools, antivirus programs, and patch management services. Such software should be implemented on all workplace devices and updated as needed to ensure effectiveness. It's also important to establish firewalls and virtual private network (VPN) connections to promote network security and safe internet usage.
- **Have a plan**. Creating a cyber incident response plan can help ensure necessary procedures are taken when cyberattacks occur, thus keeping related damages at a minimum. This plan should be well documented, practiced regularly, and address a range of cyberattack scenarios (including jackware incidents).
- **Secure sufficient coverage**. It's critical to purchase adequate insurance to help protect against losses that may arise from jackware incidents. It's best to consult a trusted insurance professional to discuss specific coverage needs.

Conclusion

It's evident that jackware incidents are serious cyberthreats with the potential to result in major losses for impacted businesses—even greater than those caused by ransomware incidents. Yet,

by better understanding this cyberattack method and taking steps to prevent such incidents, businesses can reduce associated damages, therefore protecting their technology, operations, and the safety of others.