Understanding and Preventing Zero-click Attacks

Many types of cyberattacks involve manipulating users into doing certain tasks—whether it's sharing login credentials, downloading dangerous attachments or clicking on harmful links—to help hackers compromise their systems or data. However, some incidents can be launched without these exchanges. In particular, zero-click attacks entail hackers leveraging software flaws in users' devices or applications to deploy malicious code (e.g., viruses, worms, spyware or ransomware), all without the need for any communication or activity from the users. Also known as zero-click exploits, these incidents require cybercriminals to deviate from typical attack patterns and utilize more stealthy techniques to quietly infiltrate users' technology. Such characteristics also make these attacks difficult to detect, often prompting prolonged and destructive incidents that generate serious consequences for affected users. As cyber incidents continue to become more sophisticated in nature, zero-click attacks are on the rise, ultimately representing a new frontier in security threats for businesses across industry lines. With this in mind, it's critical for businesses to better understand these exploits and how to prevent them. This article provides more information on zero-click attacks, outlines how they can impact businesses and highlights related mitigation tips.

Zero-click Attacks Explained

Unlike phishing scams and other social engineering tactics, zero-click attacks don't rely on interactions between cybercriminals and users to be successful. Rather, these incidents involve skilled hackers exploiting software vulnerabilities in users' devices (e.g., tablets, smartphones, laptops and desktop computers) or applications. Such exploitation typically stems from cybercriminals delivering specifically crafted data packets to unprotected systems and services without users' knowledge. Common targets for zero-click exploits include poorly secured Internet of Things (IoT) devices and mobile applications, particularly those with email, instant messaging, video-conferencing and voice-calling features. These applications frequently receive and analyze files from a range of external sources, making them vulnerable due to their ability to automatically process such content in different ways (e.g., generating previews of messages or media before users open them). What's more, these applications often have end-to-end encryption capabilities, meaning that the content of data packets sent through them remains unknown to all parties except the sender and receiver. Such capabilities can make it harder to identify attacks.

Because they leave little to no trace, zero-click exploits can go uncovered for extended periods, allowing cybercriminals to cause lasting damage to impacted users' systems and data. Complicating matters, hackers usually implement advanced strategies to install and delete these exploits, removing any evidence that they even took place. This can significantly hinder incident investigation and remediation efforts. Several high-profile cyberattacks involving zero-click exploits have occurred in recent years. One of the most prevalent is the Pegasus spyware incident, in which a foreign cyber intelligence firm used such exploits to conduct remote surveillance of journalists' and political figures' smartphones. The firm intruded on users' devices without their knowledge, bypassing standard security protocols and compromising a variety of sensitive government information.

How Zero-click Attacks Impact Businesses

Zero-click attacks can affect businesses in many ways, leading to the following ramifications:

- **Stolen funds and assets**—Through these attacks, cybercriminals can gain unauthorized access to confidential business records, private stakeholder information and intellectual property. This could enable hackers to commit corporate espionage and steal critical funds and assets, leaving businesses with considerable financial and reputational losses.
- **Damaged systems and technology**—Such exploits may also allow cybercriminals to leverage compromised devices to move laterally across corporate networks, escalate their privileges and infiltrate businesses' larger IT infrastructures, ultimately paving the way for more widespread damage and operational disruptions. As the number of remote workers and IoT devices continues to rise, these trends could expand possible attack surfaces for zero-click exploits, compounding related losses and creating opportunities for future incidents.

- **Regulatory and legal penalties**—When these attacks impact sensitive stakeholder information, businesses could be held liable for failing to properly protect such data, prompting costly lawsuits. Furthermore, businesses could face substantial regulatory penalties for breaching applicable international, federal and state data privacy laws.

Risk Mitigation Strategies

There are various risk management measures businesses can implement to help lower the likelihood of zero-click attacks and limit associated losses if these incidents do happen. Here are some mitigation strategies to consider:

- **Maintain updated software.** Businesses should make it a priority to regularly update all workplace devices, operating systems, applications and firmware to help patch known vulnerabilities and other security weaknesses, thereby blocking cybercriminals from exploiting this technology. Enabling automatic software updates and using patch management tools can simplify this process.
- **Utilize multilayered security solutions.** By equipping their devices with advanced threat identification systems, antivirus programs, firewalls and intrusion detection tools, businesses can ensure greater visibility of their entire IT infrastructures and watch for any abnormal activity. Such solutions can help stop cybercriminals in their tracks, addressing attacks before they cause more severe damage. Businesses should also consider using artificial intelligence and machine learning tools to monitor software patterns and swiftly identify suspicious anomalies that may indicate zero-click exploits.
- **Establish segmented networks and access controls.** To prevent cybercriminals from traveling laterally through their systems amid zero-click exploits and expanding attack surfaces, businesses should segment their networks. This way, hackers will only be able to compromise a small portion of corporate resources at a time, minimizing the risk of large-scale damage and disruptions. In addition, businesses should enforce strict access controls and uphold the principle of least privilege, only allowing employees to handle systems and data deemed necessary for their roles.
- **Promote proper cyber hygiene.** Although zero-click attacks don't stem from interactions between hackers and users, it's still important for businesses to educate their employees on this threat and encourage solid cyber hygiene through routine awareness training. Key topics to address include creating strong passwords, recognizing and reporting unusual network activity, and periodically reviewing and removing unnecessary applications.
- **Vet all vendors and applications.** Businesses should carefully evaluate all third-party software vendors and applications, especially niche or lesser-known providers, for possible security flaws before finalizing their contracts and purchases. In doing so, businesses can avoid introducing new vulnerabilities and offering further avenues for zero-click exploits.
- **Have a plan.** Creating cyber incident response plans can help businesses ensure necessary procedures are taken when attacks occur, keeping related losses at a minimum. These plans should be well documented, practiced on a regular basis and address a range of cyberattack scenarios (including zero-click exploits).

Conclusion

Zero-click attacks present numerous risks for businesses of all sizes and sectors. As these attacks become increasingly prevalent, it's vital for businesses to have proper safeguards in place. By maintaining awareness of zero-click exploits and taking sufficient steps to address them, businesses will be better equipped to navigate this evolving cybersecurity landscape and, in turn, prevent major losses. Contact us today for more risk management guidance.

BHC INSURANCE