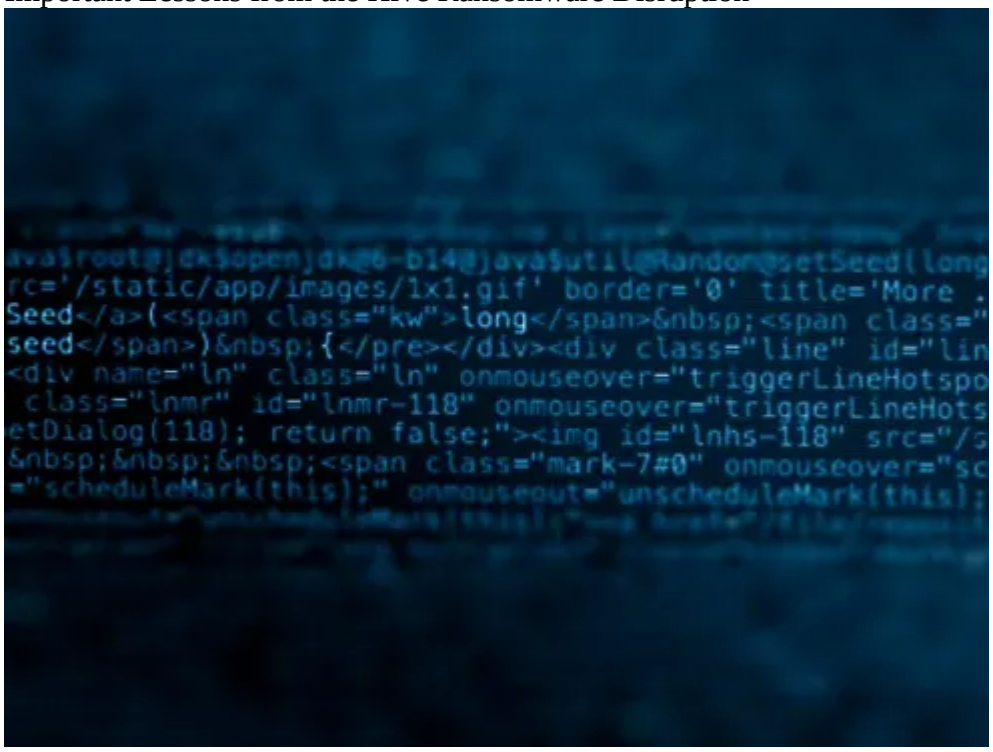
Blogs
February 08, 2023
Important Lessons from the Hive Ransomware Disruption



The recently announced disruption of the Hive ransomware network is a significant and welcome accomplishment. It cuts off bad actors from the gains they sought to extract from victims and makes their continued criminal activity more challenging. Raising the cost on malicious cyber actors is always a good way to deny them the inherent benefits of online crime, such as distance from target, anonymity, and freedom of operation.

The disruption has at least two additional important effects. First, it highlights in one case multiple ransomware themes that everyone should pay attention to:

- *Ransomware-as-a-Service (RaaS).* Sophisticated ransomware is available to online actors who are willing to pay for it. This is one reason the ransomware threat continues to grow, because it significantly lowers the barriers to conducting a ransomware campaign. It also means that actors who deploy ransomware may not be fully expert with the tools they are using.
- *Double extortion.* As potential victims have become better prepared to recover from the malicious encryption of their data, bad actors have correspondingly upped their game. Before encrypting a victim's data, online criminals will steal data (or collect enough information to make it look as though they stole data). Even if a victim does not want to, or have to, pay to decrypt their own data, they will face threats that their internal data will be revealed unless they pay a ransom. Be on the lookout for additional layers of extortion, such as bad actors reaching out to customers and vendors or adding denial-of-service attacks to dial up the pressure on ransomware victims.
- *Vulnerability of critical infrastructure*. Hive targeted, among other entities, hospitals and other critical infrastructure. These make attractive targets, because systems and defenses may be out of date and present broad attack surfaces. They also face a constant, daily pressure to maintain the continuity of their own options, because when critical services fail, the real-world effects can be immediate and disastrous. The importance of multi-layered security and contingency planning increase in proportion to the criticality of the service an entity provides.

The disruption also demonstrates the role of the Federal Bureau of Investigation (FBI) and other U.S. government agencies in preventing and remediating cyber crime – in other words, it highlights the benefits of engaging law enforcement. Among other measures, the FBI obtained Hive decryption keys and provided them to victims, which allowed victims to restore access to their data without paying ransoms. This was accomplished without compromising the confidentiality of a months-long operation and without preventing law enforcement from conducting the end-of-operation takedown. This cannot happen without productive, sustained engagement among government and private-sector entities, and presents good evidence that cooperating with law enforcement can not only enhance investigative efforts, but also benefit individual companies.

Authors

Explore more in

Privacy & Security Data Security Counseling and Breach Response