BURR FORMAN LLP

Hacking the Hive: How It Can Help Businesses

Article
02.15.2023

Businesses can breathe a little easier now that one of the world's top five ransomware networks, the Hive, has been infiltrated and disbanded by the FBI.

The Hive ransomware group targeted more than 1,500 businesses around the world, including many health care businesses, and received over $100 million in ransom payments. Hive used a ransomware-as-a-service (RaaS) model, where developers created ransomware and marketed it to fellow criminals as a franchise opportunity of sorts. Hive customers, or affiliates, used the ransomware as an off-the-shelf product to attack victims, and they earned a percentage of the spoils. The Hive ransomware encrypts and steals data. Attackers demand a ransom for both the decryption key and their (unenforceable) promise not to publish stolen data. After a victim pays, the affiliates and developers split the ransom 80/20. Hive publishes the data of victims who refuse to pay on the Hive Leak Site.

Hive affiliates exploit access points, such as using stolen single-factor logins via Remote Desktop Protocol (RDP), virtual private networks (VPNs), and other remote network connection protocols. They exploited FortiToken (which acts as a security token) and Microsoft vulnerabilities and sent phishing emails with malicious attachments. Prior to encryption, Hive ransomware removed virus definitions and disabled all portions of Windows Defender and other common antivirus programs in the system registry.

RELATED PROFESSIONALS

Elizabeth B. Shirley, CIPP/US, CIPM

RELATED CAPABILITIES

Cybersecurity & Data Privacy

Hacking the Hive: How It Can Help Businesses

What Did the FBI Do?

The FBI penetrated Hive's computer networks, captured its decryption keys, and offered the keys to Hive ransomware victims worldwide, preventing them from having to pay $130 million in demanded ransom. It also distributed over 1,000 additional decryption keys to previous Hive victims. The FBI announced it seized control of the servers and websites Hive uses to communicate with its members, thereby disrupting Hive's ability to attack and extort additional victims. The FBI did this in coordination with German law enforcement (the German Federal Criminal Police and Reutlingen Police Headquarters-CID Esslingen) and the Netherlands National High Tech Crime Unit.

Why Does This Matter to My Business?

The effects of a ransomware attack can be devastating, particularly for health care providers. From January 2016 to December 2021, the ePHI (electronic personal health information) of nearly 42 million patients was exposed in 374 ransomware attacks on U.S. health care organizations. Keep in mind that ransomware attacks are under-reported. Attacks more than doubled from 2016 to 2021. Studies have shown only 20% of attacked health care organizations were able to restore data from backups. Around 16% of attacks included evidence that ePHI was made public – posted on the dark web and for sale to other criminals. Significantly, health care delivery was disrupted in around 45% of the cases, and close to 10% of those disruptions lasted over 2 weeks (Neprash 1). Additionally, ransomware attacks can result in reputational harm to businesses, regulatory fines, and class action lawsuits.

What Can My Business Do to Help Protect Itself?

Ensuring data privacy not only helps businesses comply with HIPAA and other recent U.S. state data privacy laws, but also it can help prevent data breaches. The following steps to protect data privacy and secure information can help:

Identify threats and vulnerabilities to electronic information, including ePHI and personal information (PI).

- Personal information includes:
  - Name;
  - Email address;
  - Phone number;
  - Mailing address;
  - SSN;
  - DL and passport #;
  - IP address;
  - Unique personal or online identifier;

  - Account name;
  - Records of products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
  - Browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement;
  - Geolocation information;
  - Professional or employment-related information;
  - Biometric information;
  - Educational information; and
  - Inferences drawn from any of the above to create a profile about a consumer.
- Do not retain PI for longer than necessary. When the business no longer needs the PI, securely and permanently delete it.
- Do not allow employees to maintain ePHI and PI on their individual workstations, separate from the company's operating systems.
- If employees are allowed to use personal devices for work, ensure they have the same security as work-based workstations.
- Do not allow employees to use personal email accounts for work purposes.
- Implement procedures to detect and prevent against malicious software.
- Train employees who have access to ePHI and PI on cybersecurity threats and ways to protect data privacy.
- Push out routine, unannounced phishing campaigns to identify employee weak links.
- Train employees on what to do and who to contact if they think they have clicked on a malicious link or attachment.
- Implement access controls to limit access to only those persons and software programs that require access to ePHI and PI.
- Maintain separate, secure, and regular backups of electronic data. Test back-ups regularly. Consider offline backups and multiple backups.
- Have a disaster recovery plan that accounts for possible data breaches. Keep it updated.
- Obtain cyber insurance.
- Maintain legal counsel on retainer in the event of a potential data incident.
- Designate a group of employees from management, IT, human resources, legal, the privacy office (if one exists), and marketing to form an incident response team (IRT) to respond to possible data breaches.
- Consult with data privacy legal counsel to establish privacy controls and procedures for the business.

Hacking the Hive: How It Can Help Businesses

Burr & Forman's Cybersecurity & Data Privacy Team can help. You may reach the author at bshirley@burr.com, or her direct line at (205) 458-5186.

Sources: Neprash, Hannah T, PhD, et al., JAMA Health Forum, "Trends in Ransomware Attacks on US Hospitals, Clinics, and other Health Care Delivery Organizations, 2016-2021," 12/29/2022
Office for Civil Rights, U.S. Department of Health and Human Services, "Ransomware and HIPAA,"
U.S. DOJ, "U.S. Department of Justice Disrupts Hive Ransomware Variant," 1/26/2023