cisco

Ransomware:

An epidemic for the healthcare industry

Prevention is the best medicine.

Healthcare is a data goldmine. Criminals – and even insiders intent on selling data – are ready to take advantage of and exploit any vulnerability. Threats like WannaCry and SamSam are still rampant.

Healthcare organizations constituted 45%[1] of all ransomware attacks in 2017, and ransomware remains a top concern for 2018.[2]

In healthcare, **85% of malware attacks come from ransomware.**[3]

90% of healthcare organizations have experienced a **data breach since Q3 2016.**[4]

Healthcare data breaches cost organizations **$380 per record.**[5]

5.6 million patient records were **breached in 2017**, costing healthcare organizations billions.[6]

Training and security budgets need a boost

In 2017, more than **half of healthcare security breaches** came from **inside the organization.**[7]

Even more surprising: Among U.S. healthcare workers, **only 41% received training** on how to stay secure at work.[8]

Still, in this age of increasing threats and static budgets, **cybersecurity spending** is around **3% of total annual IT spending.**[9]

On the black market, **a social security number is worth 10 cents, a credit card number is worth 25 cents,** and an electronic medical health record **(EHR) could be worth hundreds or even thousands of dollars.**[10]

More devices = more risk

By 2020, it's expected IoMT devices will **increase to between 20 and 30 billion.**[11]

And ransomware attacks on **healthcare will quadruple.**[12]

The anatomy of an attack

01 Launch

Healthcare organization employee visits a compromised site or opens an infected email file

02 Exploit

Browser connects to an exploit kit which initiates a call back to malicious infrastructure or user initiates download of an exploit kit

03 Install

Ransomware variant is installed onto system

04 Callback

Data on the endpoint is encrypted when ransomware retrieves the private encryption keys

DNS: The first line of defense

Since **91% of malware uses DNS** for command and control callbacks, to exfiltrate data, or redirect web traffic, pointing your DNS to **Cisco Umbrella** will protect any device that joins your network, for security that's easy to deploy and simple to manage.

Internet threats
malware, phishing, C2 callbacks and shadow IT

Healthcare's first layer of defense against ransomware
for clinic and medical office locations & roaming devices anywhere over any port, on- or off-network

By implementing security at the DNS layer, Umbrella helps organizations:

- **Predict** ransomware threats before they happen
- **Prevent** ransomware from reaching the perimeter
- **Learn** where ransomware attacks are being staged
- **Provide** a critical layer of PHI/PII breach protection
- **Block** access to known cryptomining pools, to protect against emerging cryptojacking malware.
- **Pair** with Cisco Cloudlock, a cloud access security broker, to track how PHI data is shared, to protect data and help enforce compliance.

Ready to try Cisco Umbrella?

Sign up for a 14-day free trial today – and start blocking threats in minutes.

START FREE TRIAL

Protect yourself and your data against the next WannaCry or SamSam attack.

LEARN MORE

Sources

1. Verizon, "Healthcare Accounted for 45% of All Ransomware Attacks Last Year," Verizon Enterprise Blog, April 12, 2018.
2. 2018 HIMSS Cybersecurity Survey, HIMSS North America.
3. Healthcare's Cybersecurity Journey: Ransomware Protection, Duke University, Health Sector, April 17, 2018.
4. Black Book Survey of Healthcare Facility Breach Incidents Reveals 90% Have Experienced Data Breaches, Business Wire, Cision, September 6, 2017.
5. "Ponemon Institute Research Report," Ponemon Institute, December 2017.
6. "Cost of Data Breach Study: Global Overview," Ponemon Institute, June 2018.
7. "Verizon Data Breach Investigations Report," Verizon, 2018.
8. Black Book Survey of Healthcare Facility Breach Incidents Reveals 90% Have Experienced Data Breaches, Business Wire, Cision, September 6, 2017.
9. "Cost of Cybersecurity Study: Ponemon Institute," Ponemon Institute, June 2017.
10. "Ponemon Institute Research Report," Ponemon Institute, December 2017.
11. "Cisco VNI Forecast and Methodology, 2015–2020," Cisco, June 10, 2016.
12. "Cisco 2018 Annual Cybersecurity Report," Cisco, 2018.

cisco

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)