Global ransomware damage costs predicted to exceed $5 billion in 2017, up from $325 million in 2015.

Ransomware damages up 15X in 2 years, expected to worsen; Ransomware attacks on healthcare organizations will quadruple by 2020.

MENLO PARK, CA, UNITED STATES, May 26, 2017 /EINPresswire.com/ -- Ransomware — a malware that infects computers and restricts their access to files, often threatening permanent data destruction unless a ransom is paid — has reached epidemic proportions globally.

Ransomware accounted for roughly $325 million in damages in 2015, according to Microsoft.

According to the Cisco 2017 Annual Cybersecurity Report, ransomware is growing at a yearly rate of 350%.

“This is the new business model and it is growing at an extraordinary rate,” says Marc van Zadelhoff, General Manager, IBM Security. “Our X-Force security researchers have tracked email spam trends – and discovered a huge increase in ransomware. In 2016, an average of 40 percent of spam emails contained malware links to ransomware, an increase of 6,000 percent over 2015, when less than one percent contained ransomware.”

> The estimated damage caused by WannaCry in just the initial 4 days would exceed a billion dollars”
> *Stu Sjouwerman, founder and CEO at KnowBe4*

“Ransomware allows criminals to monetize a breach instantly with Bitcoin” says van Zadelhoff. “We expect a long cycle of businesses needing to improve basics like patching, as well as adopting advanced capabilities like cognitive security tools to detect attacks faster and with greater precision.”

Cybersecurity Venturees predicts that Ransomware damage costs will exceed $5 billion in 2017, up more than 15X from 2015.

The costs include damage and destruction (or loss) of data, downtime, lost productivity, post-attack

disruption to the normal course of business, forensic investigation, restoration and deletion of hostage data and systems, reputational harm, and employee training in direct response to the ransomware attacks.

While the percentage of ransom victims who pay bitcoin to hackers in hopes of reclaiming their data appears to be on the decline, the total damage costs in connection to ransomware attacks is skyrocketing. Rransom payouts are the least of all damage cost contributors.

The massive WannaCrypt (a.k.a. WannaCry) attack damage is partially responsible for the 2017 prediction.

“The WannaCry ransomware attack is the largest we’ve ever seen of its kind, demonstrating in real time that ransomware continues to escalate as a global problem and a lucrative business for cyber criminals” says Mike Fey, President and COO of Symantec, a global leader in cybersecurity.

“In the last year alone, Symantec identified a 36 percent spike in ransomware attacks” says Fey. “The ‘clean up’ for companies who were impacted by WannaCry will be enormous, including months of recovery time for IT departments and multi-millions in cost for the victims. In terms of the hit to an individuals’ wallet, Symantec researchers have found the average ransom per victim grew 266 percent to over $1,077, up from $294 in 2015.”

One industry expert suggests that WannaCrypt could be responsible for as much as 20% of total ransomware damage costs in 2017.

“The estimated damage caused by WannaCry in just the initial 4 days would exceed a billion dollars, looking at the massive downtime caused for large organizations worldwide” says Stu Sjouwerman, founder and CEO at KnowBe4, a company that specializes in training employees on how to detect and respond to ransomware attacks.

“WannaCrypt is a sign of the times” says Steve Morgan, founder and Editor-In-Chief at Cybersecurity Ventures. "There’s been a gradual buildup of ransomware attacks, one more severe than the next. There was the recent Google Docs attack where a million workstations were infected within hours. At the end of last year an infection called HDDCryptor compromised the IT network of San Francisco Municipal Transit Agency, paralyzing the company’s critical services for several days."

The Locky strain of ransomware hit Hollywood Presbyterian Hospital in Los Angeles last year – which led to the shutdown of its computer systems and a $17,000 ransomware payout. There have been dozens of ransomware attacks on the healthcare industry in 2016 and 2017.

Cybersecurity Ventures predicts ransomware attacks on healthcare organizations will quadruple by 2020. “Hospitals are the number one target for cybercriminals, and they are particularly vulnerable to ransomware” says Morgan.

Ransomware targets all industries, and more than just computer data. Motion pictures and anything digital are now at risk.

Days after the WannaCrypt outbreak, Deadline Hollywood reported that Disney CEO Bob Iger has gone to the FBI, rather than pay a huge amount of Bitcoins to the ransomware hackers to recover the latest Pirates of the Caribbean sequel. The first several episodes generated $3.75 billion at the box office.

“Ransomware doesn’t discriminate” says Robert Herjavec, founder and CEO of Herjavec Group, a

leading global information security and advisory firm, and a ‘Shark’ on ABC’s TV show Shark Tank. “Hackers aren’t just after financial information anymore, it’s personal. We’ve seen movies held captive, healthcare data, financial data. Data is being used as a weapon – full stop. We can’t bend or break in this world of cyberwarfare – we need to be resilient. We have to be resilient with better defenses, better planning and better training for our employees.”

For now, a cybersecurity visionary sums up the state of ransomware.

“Ransomware is a game changer in the world of cybercrime” says Marc Goodman, author of the New York Times best-selling book Future Crimes, founder of the Future Crimes Institute and the Chair for Policy, Law and Ethics at Silicon Valley’s Singularity University. “It allows criminals to fully automate their attacks. Automation of crime is driving exponential growth in both the pain felt by businesses and individuals around the world, as well as in the profits of international organized crime syndicates.”

Cybersecurity Ventures predicts cybercrime will cost the world in excess of $6 trillion annually by 2021, up from $3 trillion in 2015. Ransomware is expected to worsen and make up a proportionately larger share of total cybercrime by 2021. Training employees is the big variable, and the potential big gainer in cutting down ransomware damage costs.

A report from Cybersecurity Ventures, due out in November 2017, will provide ransomware damage cost predictions for the 5 year period from 2017 to 2021.

Editor-In-Chief
Cybersecurity Ventures
631-680-8660
email us here
