
RANSOMWARE ATTACK
ES ARE ENCRYPTED

RANSOMWARE 101

GENERAL INFORMATION ABOUT RANSOMWARE

HOW CAN I PROTECT AGAINST RANSOMWARE

I'VE BEEN HIT! WHAT TO DO

SOME SCARY STATS

WHAT IS RANSOMWARE

Ransomware is **a form of malware designed to encrypt files on a device**, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.

Many, if not most of ransomware attacks begin because of some human act:

- Clicking a link
- Downloading an attachment
- Logging into an unsafe site

MOVIE TIME

- CalTech, with sponsorship with state banking authorities, produced this video explaining how hackers can easily gain access and demand ransom.

- ANATOMY OF A CYBER ATTACK

KEY POINTS

Easiest way in – the human factor clicking a link

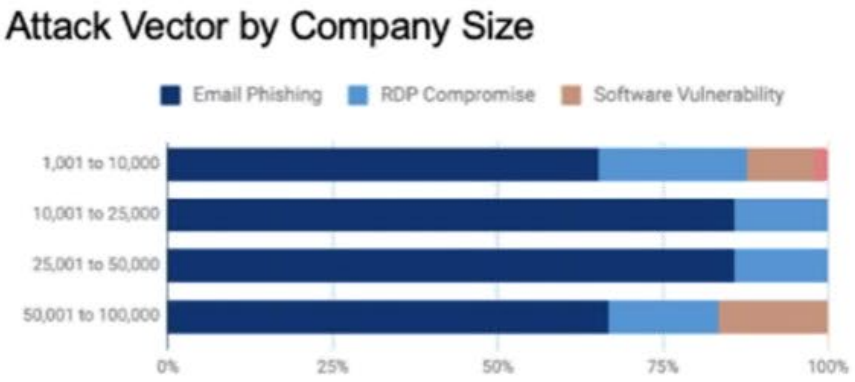
At UTHSC, our NetID and password gains access to many systems, not just email

Staging – bad actors can wait days, weeks or months before launching an attack while they search for our most critical data

A crisis ready organization is one that is cyber aware and trained, where plans are tested, key personnel have trained surrogates and have a business continuity plan

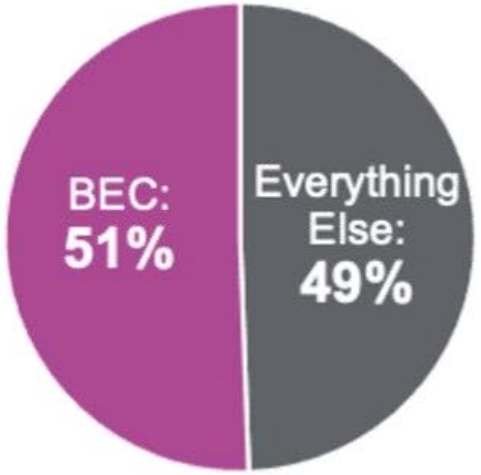
Ransomware Gets the Headlines, but…

Ransomware:
90% successful attacks via email



Source: Coveware Q4'20 Ransomware Report

BEC: Larger losses than all other threats *combined*



Source: FBI / IC3

Top enterprise risks are people centric

CAN WE PREVENT RANSOMWARE FROM HAPPENING TO US?

- First, assume that it will happen and be prepared for when it does
- Train everyone to spot the social engineers and phishers trying for the easy way in
  - If they fall for it, REPORT it!
- Segment networks so if they get in, they can’t get far
- Don’t give everyone the keys to the kingdom. Use the principle of least privilege
- Back up your data – test restoring from a backup

- Crisis management is not easy.
- Response is within our control.
- The damage may be beyond our control.

WE'VE BEEN HIT? WHAT DO WE DO?

Report it!

Response Checklist:

- Determine the systems impacted and isolate them
  - Is it one computer?
  - What applications did that device have access to?
  - Do you have to take the entire network offline?
- Communicate by "out-of-band" methods incase the bad actors are monitoring communications, i.e. emails.
- Power down devices ONLY if you cannot disconnect from the network
  - This can save potential evidence

WE'VE BEEN HIT? WHAT DO WE DO? (CONT.)

Checklist continued:

- Triage impacted systems for restoration and recovery
  - Prioritize based on criticality
  - Review backups and run antivirus / antimalware scans on the backups to see if they are infected

Personal devices

- Disconnect or power down
- On a non-infected device, do an online search to determine the kind of ransomware and see if a decryption key is already available
- Report the crime!

VIDEO TIME

- I'll stop talking again and have someone else reinforce what we've talked about. Let's watch another video that highlights some of this year's most notable attacks.

- Ransomware attacks, explained

STATISTICS THAT PACK A PUNCH!

A ransomware attack occurs every 11 seconds

The average cost to remediate a ransomware attack doubled in one year – from $761,106 in 2020 to $1.85 million in 2021

The average ransom payment in Q1 2021 was $220,298, which was 43% higher than the previous quarter

Ransomware results in an average of 23 days of downtime

STATISTICS THAT PACK A PUNCH!

Over 73% of ransomware victims have 1,000 employees or less

1,681 schools, colleges and universities were victims of ransomware in 2020

34% of healthcare organizations were hit by ransomware in the last year.

The most targeted sector in 2021 was government

Local government is the sector where organizations are most likely to have their data encrypted in a ransomware attack (69%)

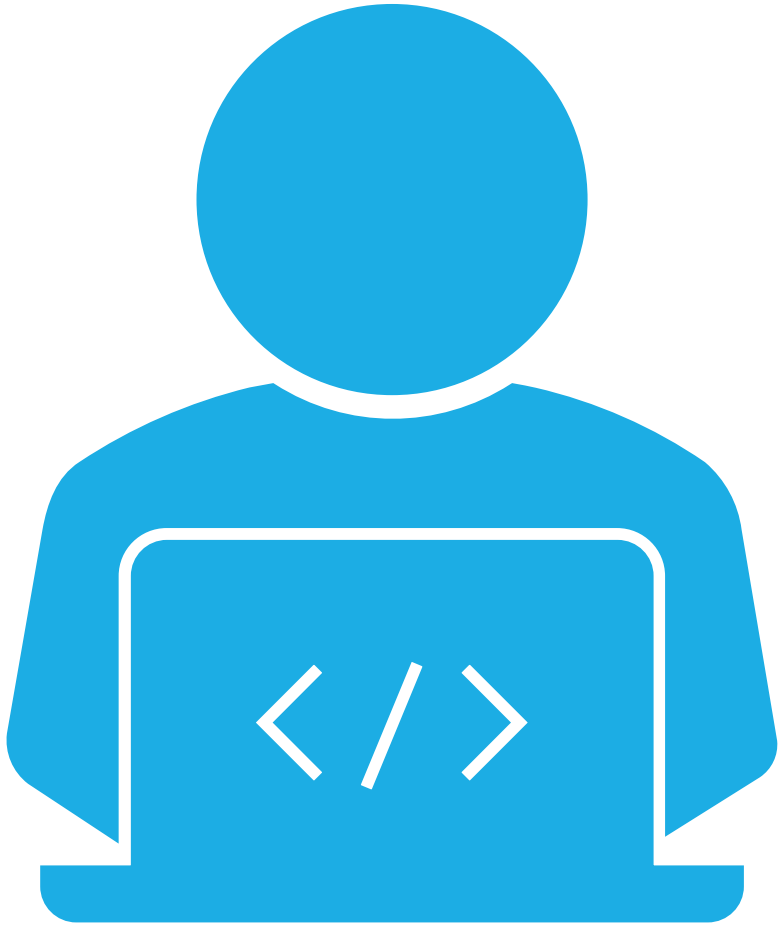
Global Ransomware Damage Costs*

- **2015: $325 Million**
- **2017: $5 Billion**
- **2021: $20 Billion**
- **2024: $42 Billion**
- **2026: $71.5 Billion**
- **2028: $157 Billion**
- **2031: $265 Billion**

Ransomware is expected to attack a business, consumer, or device every 2 seconds by 2031, up from every 11 seconds in 2021.

CYBERSECURITY VENTURES

* SOURCE: CYBERSECURITY VENTURES



CONTACT INFORMATION

Chris Madeksho – Cybersecurity Analyst

mmadeksh@uthsc.edu

901.448.1579

Office of Cybersecurity

itsecurity@uthsc.edu

901.448.1860

https://uthsc.edu/its/cybersecurity/


QUESTIONS?