Malware

July 5, 2023

Malware, or malicious software, is a blanket term for any kind of software created to cause harm. Hackers create it to make money, steal data, spy, blackmail, or even prank. It is a serious crime. The most common way to spread malware is through email (SPAM/phishing).

According to the SonicWall Cyber Threat Report, education is the number one target industry for malware attacks (2022) – this is up from number three (2021). The top 5 target industries (1-5) are: Education, Healthcare, Finance, Retail, and Government.

4 Common Types of Malware

Malware is categorized by how it spreads or what it does. Below are 4 common types:

- Trojan – tricks users into installing malware by posing as a valid program
- Virus – inserts hacker's own code in other programs
- Spyware – allows access to user's keystrokes, passwords and other sensitive information
- Ransomware – encrypts important files on user's computer and requires user to pay to decrypt

Fun Fact

The first virus, Creeper (named after a Scooby-Doo cartoon character) was created in 1971, by programmer Bob Thomas. This was as an experimental computer program – not harmful – and displayed the message, "I'm the creeper: catch me if you can".

New Threat

Credential harvesting, or password harvesting, is one of the newest threats. Hackers use a tool to collect (harvest) usernames and passwords (credentials).

A common source of credential harvesting is phishing emails. Other avenues include: malware viruses, cloned website links, the use of unsecure third-party vendors, and ransomware.

How it Works

1. **Hacker sends a phishing email.**
   The hacker takes great care to create a phishing email that seems real, even adding logos

and important titles. The subject seems applicable to the reader. Fear is used as a motivator – with subjects such as unpaid parking ticket, past due invoice, etc.

2. **You are encouraged to click on a link and perform a task.**
   You are encouraged to act quickly, and click on a link to resolve the issue.
3. **Link takes you to a web page.**
   Along with an elaborate phishing email, the hacker also makes a replica of a real website that looks legitimate. What appears to be a valid site is actually the hacker's server. The server detects and captures any secure information you type into the password fields.
4. **You are tricked into entering your email address and password.**
   You see a short message and are encouraged to sign-in, using your cloud-based company email and password.
5. **Hacker retrieves the password from their server.**
   The information you entered goes straight to the hacker.
6. **Hacker exploits harvested credentials.**
   Once the hacker has the credentials, they may be used in a number of ways – carry out more attacks, take over bank accounts or employer files, or sold on the dark web.

In the News

In early June 2023, Stephen F. Austin (SFA) State University was hit by a cyberattack. This attack is at least the 12th confirmed in Texas since March 2022, according to Comparitech.

Other recent cyberattacks, in Texas, include: The City of Dallas, Mansfield Independent School District, Rice University, the City of Tomball and the Dallas Central Appraisal District. Follow this link to view the full article from The Daily Sentinel.

With so many attacks, Highlanders must stay vigilant.

How to Prevent

STOP, LOOK and THINK, before you click.

Remember the PHISHING red flags we mentioned in the April IT Cybersecurity Newsletter:

- **FROM:** an email from an unknown sender; or, you know the sender, but the email looks funny
- **TO:** you were copied on an email, and you do not know the other individuals in the email
- **DATE:** you receive an email you would normally receive during business hours, but it was sent at 3am
- **SUBJECT:** the subject line does not make sense or does not match the message content; the email is about something you never requested, or a receipt for something you never purchased
- **CONTENT:** the sender is asking you to click on a link to open an attachment; you have an uncomfortable feeling, or it seems odd
- **ATTACHMENT:** any attachment you receive and were not expecting

- **HYPERLINKS:** misspellings in the link, hyperlinks asking you to take-action; you hover your cursor over the link, and the link address is for a different website

Revision #1
Created 6 February 2025 21:41:13 by Laura J. Crapps
Updated 26 February 2025 03:35:37 by Laura J. Crapps