Protecting Main Street from Malware:

A Cyber Briefing for Busy Leaders

Karen Arthur, GCFE

Cybersecurity Engineer, Northwestern Mutual
Incident Responder Volunteer, Wisconsin Cyber Response Team

What are we going to talk about?

1 What types of attacks are there? (TTPs)

2 What types of attackers are there?

3 Who is being attacked?

4 What can we do to prevent?

5 What to do if (when) it happens to you?

6 Questions?

What types of attacks are there? (TTPs)

1

Phishing

Vectors include:

- Email
- Text messages
- Phone calls:

2

Ransomware

Type of malware that:

- Encrypts files
- Blocks access
- Usually requires payment

3

Social Engineering

A tactic used by threat actors:

- No technical skill needed
- TA builds rapport with target
- Gets target to do something they normally wouldn't do

4

Denial of Service

Type of attack that:

- Causes high traffic (packet floods)
- Eventually servers can't withstand the traffic
- Knocks resources offline

What types of attackers are there?

1

Script Kiddies

- Less experienced
- Hack not always for damage, but to see what's possible
- Bad at covering their tracks

2

Hacktivists

- Not financially motivated, want to make a statement
- Can be motivated by revenge or other ideology
- Just because they don't steal money, doesn't mean they're not dangerous

3

State-Sponsored Hackers

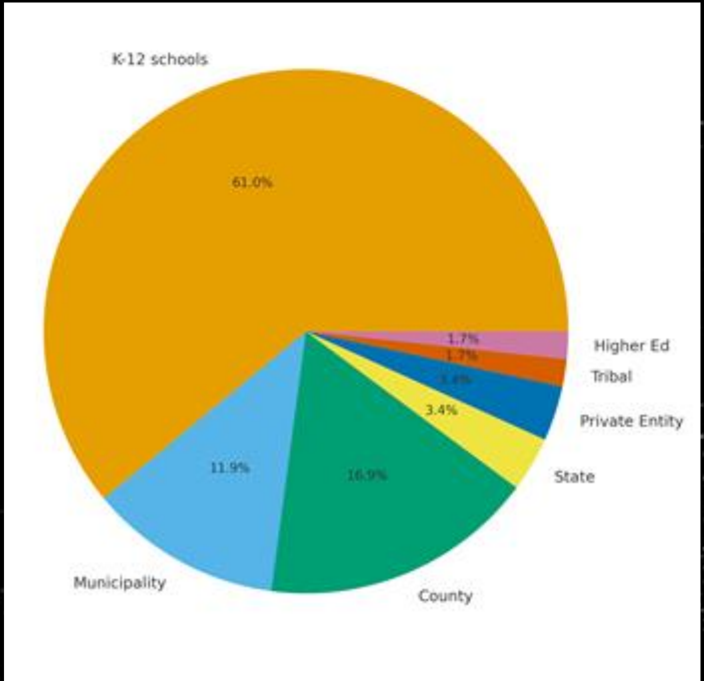
- Well resourced/very sophisticated
- Hack for strategic advantages
- Considered very dangerous
- Can exist in an environment undetected for some time due to advanced capabilities

4

Malicious Insider

- Individual with legitimate access
- Motivated by revenge, personal gain
- Bribery or coercion
- Especially dangerous because of their insider knowledge

Current Cyber Attacks in WI YTD



2025 Incidents

59

Volunteer Membership

Total Members: 293
Incident Responders: 156
Slack #general: 594

External Partners

-Cybersecurity & Infrastructure Security Agency (CISA)

-Wisconsin Department of Justice

-Wisconsin Department of Administration

-Wisconsin Department of Public Instruction

-Wisconsin National Guard

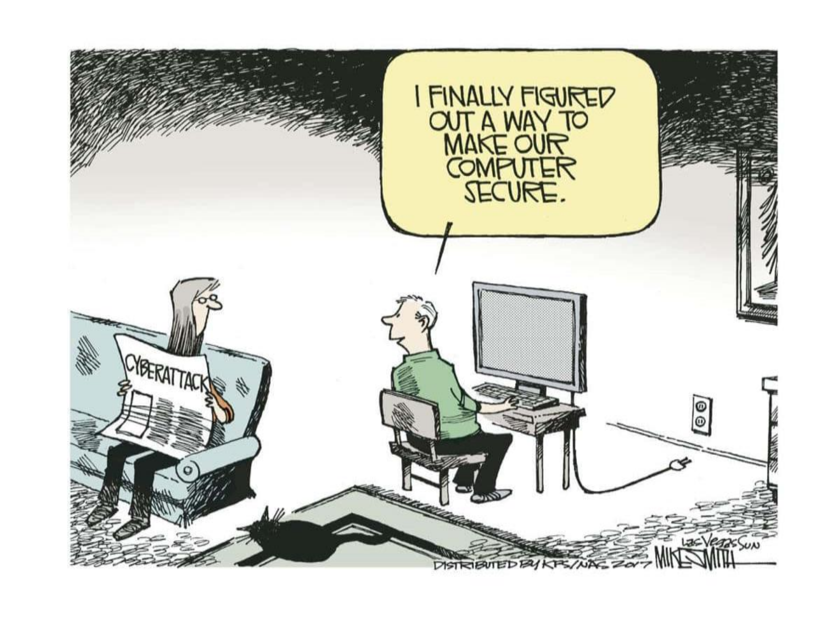
-University of Wisconsin-Whitewater

-Madison College

-Wisconsin Cyber Threat Response Alliance

Who is primarily being attacked?

- K-12 schools and other higher learning institutions
- Local governments/municipalities
- Healthcare
- Communications


I FINALLY FIGURED OUT A WAY TO MAKE OUR COMPUTER SECURE.
CYBERATTACK
DISTRIBUTED BY KPS/NAS 2017
MIKE SMITH
Las Vegas Sun

Why are these targets attractive to threat actors?

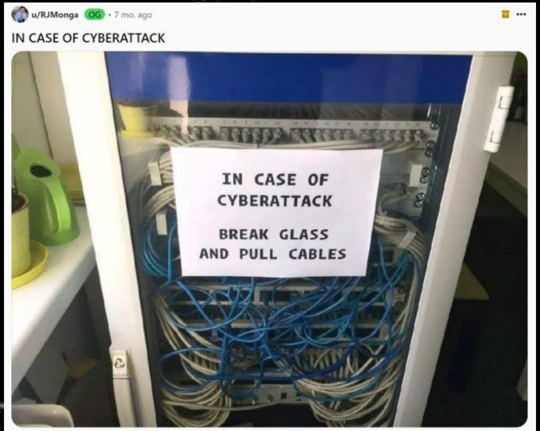
- Lack of funding for cybersecurity tools/management
- Lack of staff to detect/defend
- Financial gain
- Valuable information
- Pressure to pay quickly-can't afford downtime
- Public visibility/requirement to disclose

Things You Can Do Before

- Ensure systems are patched
- Conduct user awareness training
- Enable MFA
- Enforce a unique password policy
- Back up data "air gap" a copy
- Develop an incident response plan
- Have an inventory of all IT resources
- Consider a Zero Trust architecture
- Cloud resources, understand where they are residing/how they are accessed
- Email security software that evaluates for phishing/spoofing
- Enable non-technical controls to stop/slow down fraudulent change requests

What should you do during?

- Don't turn anything off/pull any plugs!
- Contact your IT Department
- Call your cyber insurance (if you have it!)
- Call the Cyber Response Team (1-800-943-0003, option 2)
- Contact IC3 to report the incident
- Try to write down what you observed and when (as close to exact timing as is possible)
- If the attackers leave a note or ask you to click on something, DON'T touch anything
- Wait for professional assistance before doing anything else on the affected machine



u/RJMonga OG • 7 mo. ago

IN CASE OF CYBERATTACK

Resources

1	https://www.schoolsafety.gov/	Safety resources for K-12 schools
2	https://www.ic3.gov/	Internet Crime Complaint Center
3	https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf	
4	https://wem.wi.gov/response-teams/#crt	Wisconsin Cyber Response Team
5	https://attack.mitre.org/	Mitre Attack Framework-Definitions and mitigations for TTPs
6	https://www.knowbe4.com/hubfs/Municipalities_Cybersecurity_Report.pdf	