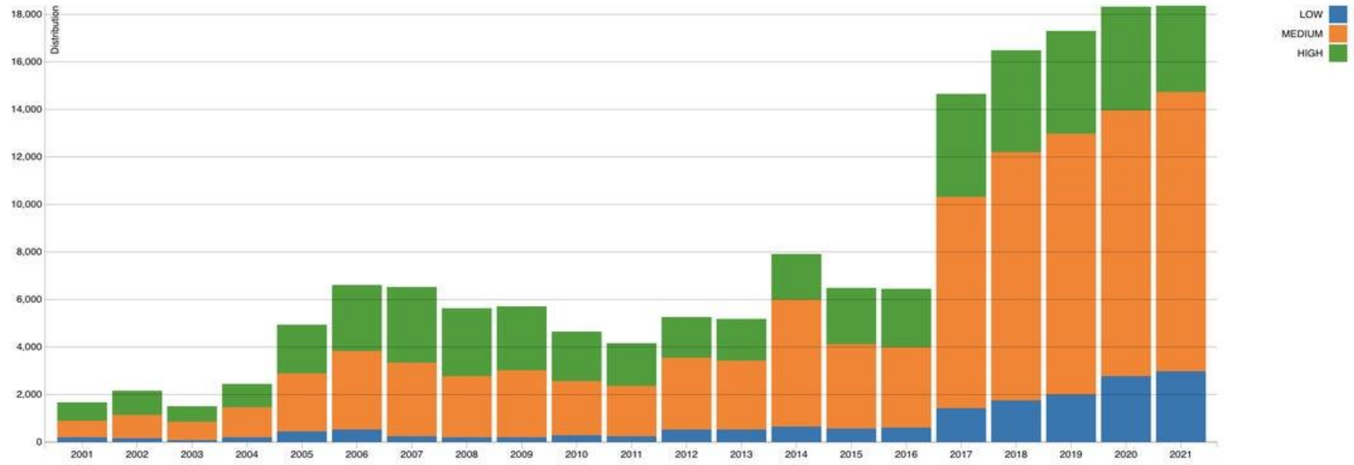
MEL CYBER TASK FORCE UPDATE

Be Cyber Alert: Active Threats and Vulnerabilities

- ✓ Multiple vulnerabilities found in VMware products, two being actively exploited, allowing infiltration
- ✓ Multiple vulnerabilities discovered in SonicWall products
- ✓ Multiple vulnerabilities discovered in Apple products allowing infiltration
- ✓ Credential-stealing malware identified in certain Microsoft Exchange servers
- ✓ High-severity vulnerabilities found in HP products, allowing infiltration
- ✓ New attack can hide malware in Windows event logs

WHEN DID ALL OF THESE HAPPEN?

These security threats are just a few of the many released in May. In fact, over 18,000 vulnerabilities were reported in 2021, according to the National Institute of Standards and Technology (NIST).



WHAT CAN WE LEARN?

Most of the vulnerabilities have a patch or a way of defending against the exposure, but you need to know about them to address them. This hits on two of our minimum cybersecurity recommendations:

1. **Cyber Memberships:** Join the NJ Cybersecurity and Communications Integrations Cell (NJCCIC) and Multi State Information Sharing and Analysis Center (MS-ISAC), both are free, to receive alerts and threat reports. Also consider joining relevant organizations, such as Cybersecurity and Infrastructure Security Agency (CISA), Water-ISAC, etc.

2. **Patch Management:** Implement a system of immediately identifying and implementing patches, there are many free and cheap services that can do this for you.

For details, contact the MEL Underwriting Manager or your local JIF Executive Director