Tip Sheet
ASIS IT Security Community

PROTECTING AGAINST RANSOMWARE

Tips to Protect Against Ransomware Attacks

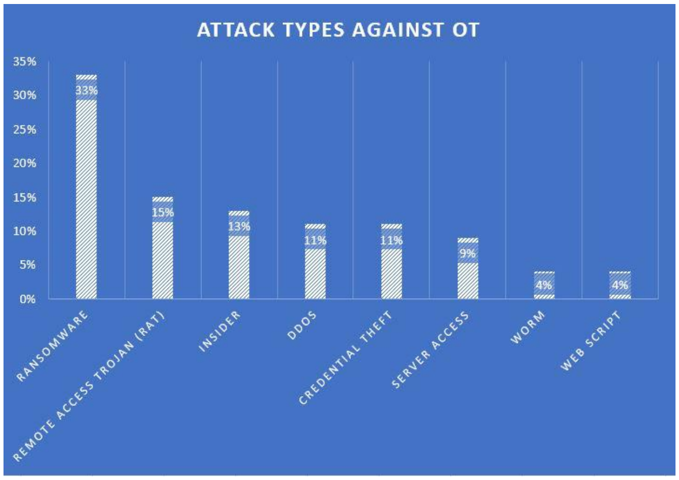
By Angel L. Hueca, PhD

What is Ransomware

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) describes Ransomware as "an ever-evolving form of malware designed to encrypt files on a device, rendering and files and the systems that rely on them unusable." Once ransomware has encrypted victims files, the malicious actors will demand a "ransom" in exchange for the decryption of the victim files. According to Berkeley University, ransomware is often spread through phishing emails that contain malicious attachments or drive-by downloading. Drive-by downloading occurs when users unknowingly visit malicious sites, or are redirected to a malicious site by the attacker.

One reason ransomware is so effective is that malicious exploit victim emotions, instilling fear and panic into their victims, which will cause the victim to click on a link or pay the ransom. Often the ransomware will display an intimidating message to further distress the victim.

As noted by the IBM X-Force Threat Intelligence Index 2020, Operational technology (OT) threats have the potential to lead to real-world incidents in the oil and gas sector, transportation sector, utilities and energy sector, as well as, events impacting the construction and mining areas. At 33% of all attacks on OT, ransomware attacks were the most common attacks on OT in 2020.



Percentage breakdown of attack types observed in 2020 against organizations with OT (Source: IBM Security X-Force)

What to do?

Some Considerations

- **Be Prepared**: Preparation is key to any type of cyber-attack. Create or update an incident response plan for your organization. Outline the incident response steps necessary or permitted within your industry, to assist analyst in the response process.
- **Stay Current**: Regularly patch and update software and OSs to the latest versions. Staying current also means, staying aware of what is happening "in the wild" to better protect your organization.
- **Conduct Regular Vulnerability Scanning**: Vulnerability scanning will help you identify and address vulnerabilities, especially those on internet facing devices to limit organizational attack surface.
- **Employ a Data Backup and Recovery Plan**: Include all critical information, perform and test regular backups to limit the impact of data or system loss to expedite the recover process.
- **Screen Emails and Don't Click Suspicious Links**: User awareness is one of the most important ways to protect your organization, since most ransomware is distributed through email. Users are the first line of defense, train them on safe computer usage.
- **Institute a Security Awareness Program**: Empower your employees by training them on how to prevent phishing attacks, how to identify malicious links, not to click on adverts, and how to stay vigilant
- **Make Sure Anti-Virus is up to Date**: While this may seem obvious, some organizations may overlook regularly updating anti-virus solutions. Many solutions now offer add-ons that help detect suspicious ransomware behavior such as file encryption and alert analysts to mitigate the threat.
- **Employ Two-factor Authentication**: An attacker tactic is to leverage stolen employee credentials to gain network entry. To reduce the likelihood of an attack, adopt two two-factor (2FA) authentication across all technology solutions.
- **Know Your Threat Landscape**: Understanding your IT infrastructure is one of the most important factors in defending your network. How will you know what to protect if you don't know what on your network? Adopt a Cybersecurity framework, and apply the methodology to your environment. The first function in the NIST Cyber Security Framework is Identify. Know what is on your network to help you develop an understanding of organizational risk.
- **Practice Good Cyber Hygiene**: Establish a cyber hygiene program, understand how attacks happen so that you can protect your organizations against them. Conduct regular audits of your cyber hygiene practices, identify gaps and remedy these gaps as soon as possible.