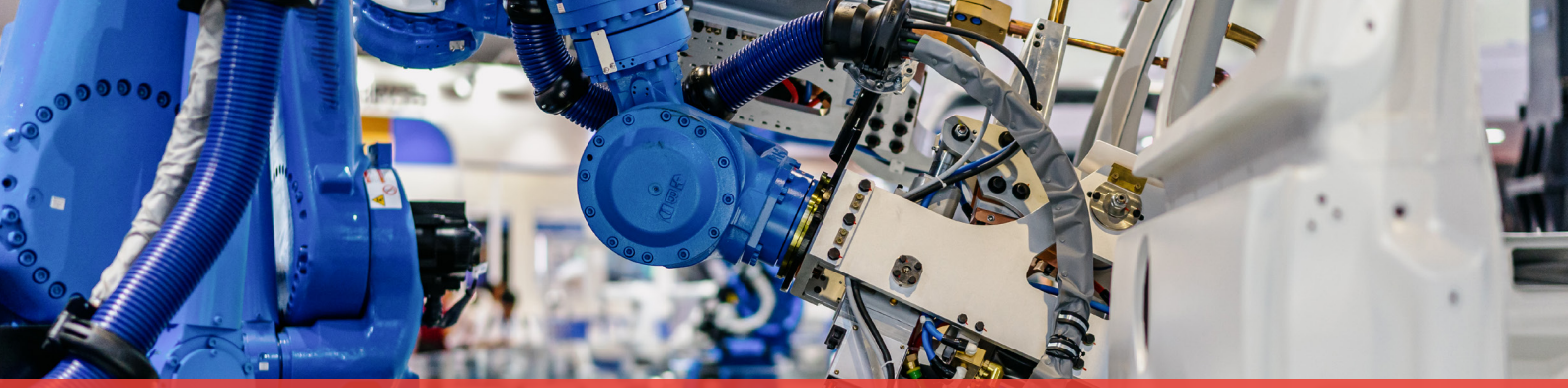

2020 REPORT ON THREATS AFFECTING ICS ENDPOINTS

As the interconnection between IT (information technology) and OT (operational technology) continues to grow, securing Industrial Control Systems (ICS) is becoming more important. In our paper "2020 Report on Threats Affecting ICS Endpoints", we share our latest findings on both old and new threats that hound industrial endpoints.

KEY FINDINGS

- Ransomware remains a concerning and rapidly evolving threat to ICS endpoints globally. Major ransomware families affect ICS endpoints, and the US is one of the most targeted countries for these attacks.
- Coinminers affect ICS mostly through unpatched operating systems. Since ICS endpoints are still vulnerable to the EternalBlue vulnerability, coinminers that were distributed through Equation Group tools exploiting this vulnerability is rampant in several countries, especially in India.
- Conficker is still propagating on ICS endpoints running newer operating systems. Conficker variants with the additional routine of brute-forcing admin shares can infect ICS endpoints even if they are running an OS that is not vulnerable to MS08-067, a Windows Server Service vulnerability that Conficker can use as an attack vector.
- Legacy malware continues to thrive in IT/OT networks. Despite being relatively older types of malware, worms such as Autorun, Gamarue, and Palevo that propagate through removable drives are still commonly detected in ICS endpoints.
- Malware detected on ICS endpoints varies between countries. By percentage, Japan had the least amount of ICS endpoints affected by malware or potentially risky software, while China has the most such detections (of the top 10 countries). As mentioned earlier, the US had the most ransomware infections, while India had the most coinminer infections.

RECOMMENDATIONS

ICS might be difficult to patch and update; however, patching is necessary to protect endpoints from threats. If patching is not an option, virtual patching can help fill in security gaps. It would also help to implement micro-segmentation in the network to enhance security by restricting network access and communications to the necessary devices and protocols.

Security solutions can also help. TXOne StellarProtect™ is an application control security software that only allows known benign executables and processes to execute in an endpoint. This solution delivers patternless protection against both known and unknown malware via machine learning and ICS root of trust.

Read more about ICS endpoint security in our research paper at http://bit.ly/ICSendpointthreats.

TREND MICRO | research