The Silent Danger Of USB-Borne Malware

Honeywell's Global Analysis, Research and Defense (GARD) team has been analyzing USB-borne malware and publishing their findings in an annual report for six years now. The report is based on telemetry from deployments of Honeywell's Secure Media Exchange (SMX) product, which is designed to use a variety of methods to enforce access controls on USB media and to prevent access to unwanted files. It could be a simple policy decision – your organization simply doesn't allow certain files in their facilities – or it could be because a file is infected.

If a file is malicious, Honeywell wants to know more about it. The GARD team is typically focused mainly on two areas: how did it get there, and what is it capable of? But Honeywell wanted to expand the focus, so this year the GARD team did something extra.

From years of engagement with customers, it is clear that the majority of active infections found in industrial areas were introduced via USB. Once Honeywell SMX began deployment, there was a new lens available for the first time, allowing a closer look into this very specific threat vector.

In Honeywell SMX's first year, a surprising amount of malware detected was spyware, PUAs (potentially unwanted applications), adware and various forms of junkware. Yes, USBs were compromised, but there wasn't much discernable intent. The malware found was also, for the most part, less dangerous. Still, there were indications that more was going on.

High-profile malware attributed to large adversarial groups and nation-backed actors were found. Stuxnet, even though already nearly a decade old at that time, popped up. The Mirai botnet was highly prevalent, as was NotPetya. It was only in the second year that things began to get intriguing. Of the malware analyzed – specifically, malware that was detected and blocked while attempting to enter an OT facility – the amount that posed an actual risk to industrial operations effectively doubled.

The next year, it happened again. In 2022 and 2023, the growth continued to slow. Now, that growth seems to be holding steady – albeit at dangerous levels, with 80% of the malware analyzed being capable of causing loss of view or loss of control of an industrial process. The samples now included new variants of just about every prevalent industrial threat of the day, including Trisis.

Year after year, the same thing is prevalent: malware seems to be targeted; the malware found on USBs seems to be there because it's intentionally propagating via USB; it can cause LOC; and it seems to be disproportionately slanted toward providing remote access and command-and-control.

This is why the GARD team started tracking a few additional details, and why they looked more closely into specific tactics and techniques.

Targeted cyber-physical attacks aren't about zero-day exploits anymore. They're about silent residency and "living off the land" techniques – knowing how to use the system to do their dirty work and waiting for the right time to do so.

It's no surprise that this year Honeywell saw a huge focus on observational tactics (discovery, collection and exfiltration), evasion and persistence. When zooming in on ICS-specific tactics, the team found nothing but execution and escalation tactics, using techniques that leverage the inherent capabilities of the target system.

If you're interested in reading more about what the Honeywell GARD team discovered this year, check out the 2024 USB Threat Report and see what you can do to better prepare for attacks and threats against your operations.

2024 USB THREAT REPORT

REQUEST A CONSULTATION →

RELATED CONTENT

7 Tips To Improve OT Cybersecurity

Feedback