ICS MALWARE SANDBOX

Safe and Speedy Analysis of ICS-Specific Malware

Industrial Control System (ICS) and IIoT networks require specialized security capabilities because traditional IT sandboxes cannot "explode" or run ICS malware.

Traditional IT malware sandboxes provide an environment in which malware is allowed to roam free so that its behavior and payloads can be studied. VirusTotal, for example, has been around for years and provides a valuable resource by allowing analysts to upload suspected malware to a cloud-based environment, where they can then observe whether commercial anti-malware programs detect the malware, without suffering ill effects.

IT malware sandboxes, however, cannot be used for ICS-specific malware such as TRITON and Industroyer. That's because IT sandboxes don't simulate ICS-specific runtime components required for complete execution of the malware, such as ICS-specific libraries (TriStation, OPC, etc.), services, PLC communication, registry keys, DLLs, etc.

The CyberX ICS Malware Sandbox simulates real-world industrial networks, allowing ICS malware to execute and unpack, and then detects tell-tale malicious activities unique to ICS malware, such as OPC scanning or overwriting PLC configuration files.

The CyberX ICS Malware Sandbox simulates real-world industrial networks, allowing ICS malware to execute and unpack, and then detects tell-tale malicious activities unique to ICS malware, such as OPC scanning or overwriting PLC configuration files.
In other words, ICS-specific malware and payloads will typically not execute until and unless they find a particular PLC, DCS, engineering workstation, historian, or ICS protocol. The malicious payload remains dormant, and thus undetected, until it finds its victim. Because ICS environments are quite different from IT environments, with dozens of specialized protocols (MODBUS, DNP3, OPC, etc.) — in addition to standard IT protocols (HTTP, SMB, etc.) — it is especially difficult to create an ICS “sandbox” in which ICS-specific malware can be analyzed.

**Specifically Designed for ICS Malware**

Unique in the industry, CyberX’s subscription-based automated service is specifically designed for ICS malware and works even for ICS malware that has never been seen before (zero-day malware).

Leveraging CyberX’s extensive ICS expertise and deep understanding of ICS protocols, devices and applications, CyberX’s cloud-based sandbox creates a virtual ICS environment for executing suspected ICS malware and observing its behavior.

By virtualizing a complete OT environment, CyberX’s ICS Malware Sandbox can rapidly and automatically identify ICS-specific malware, pinpoint its IOCs, and enable threat intelligence sharing across the global ICS community.

CyberX’s ICS Malware Sandbox runs suspected malicious executables and gives them access to ICS-specific runtime components including processes, historians, and PLCs in order to analyze their behavior. It then identifies IOCs so you can proactively detect and hunt ICS-specific threats.
Rapidly Identify ICS-Specific IOCs

With a single click (or automated upload process), you can deliver suspicious files to our cloud-based service and immediately determine if the malware targets ICS assets — and exactly how they’re impacted — along with a list of network and host-based IOCs associated with the malware. An on-premises solution is also offered.

These IOCs can immediately be transferred to your existing security analytics solutions — such as IBM QRadar, Splunk, McAfee, and RSA NetWitness — to investigate incidents and halt the spread of malware in your ICS environment.

This approach enables your SOC team to easily embed ICS-specific malware analysis into their existing IR workflows — without hiring ICS malware experts or training your existing Tier 3 analysts to reverse-engineer ICS malware with homegrown scripts and traditional tools.

How it Works

CyberX customers use a variety of techniques to get suspicious files to the ICS Malware Sandbox for analysis. First, they can e-mail suspicious files directly to the ICS Malware Sandbox. Alternatively, they can use the CyberX API to automatically send quarantined and/or suspicious files from their endpoint security for OT networks to the ICS Malware Sandbox. Customers also choose to send suspicious files from endpoint scanning stations that are used to check laptops before connecting them to the OT network.

Within the ICS Malware Sandbox environment, threats are executed and intelligence is extracted. The simulated ICS environment in which the malware executes includes all essential run-time components such as ICS-specific libraries, services, connected PLCs, registry keys, DLLs, etc. system.

It then instruments the malware during execution — when it’s detonated in the sandbox — to comprehensively analyze its behavior and document the IOCs it creates.

CyberX’s ICS Malware Sandbox efficiently spots ICS-specific malware and can simulate the types of traffic to and from a PLC, for example, as its honeypot function. That allows the malware to execute in a safe space while unpacking and uncovering its functions and matching them with other known or unknown variants. The CyberX ICS Malware Sandbox includes ICS software, virtualized ICS processes and files, and an ICS network. The ICS network serves as a honeypot.

A technical presentation about the CyberX ICS Malware Sandbox is available here.

Operational related Alerts

<table>
<thead>
<tr>
<th>Name</th>
<th>Severity</th>
<th>Alerts</th>
<th>Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>The checksum of the pe is not verified</td>
<td>1</td>
<td>1999be595d90cf46f4c480beed8033f0fd7738e40af20</td>
<td>generic</td>
</tr>
<tr>
<td>Queries information on disks, possibly for anti-</td>
<td>3</td>
<td>Process ‘killdisk’(PID: 3260)</td>
<td>anti-vm</td>
</tr>
<tr>
<td>virtualization</td>
<td></td>
<td>sec_service.exe</td>
<td></td>
</tr>
<tr>
<td>Expresses interest in specific running processes</td>
<td>2</td>
<td>killdisk tried to sleep 146 seconds, actually delayed analysis time by 26 seconds</td>
<td>anti-sandbox</td>
</tr>
<tr>
<td>A process attempted to delay the analysis task.</td>
<td>2</td>
<td>VCS, Microsoft Corporation</td>
<td></td>
</tr>
<tr>
<td>This executable probably uses a packer</td>
<td>1</td>
<td>Detected attempt to access the file: C:\Program Files (x86)\ASEM\Ubiquity\Runtime\32\sec_service.exe(3idelimiter Programs: Asem Ubiquity) By the PID: 3260</td>
<td>ics</td>
</tr>
<tr>
<td>Access to ics simulator files</td>
<td>3</td>
<td>Installed Bootkit</td>
<td>rootkit</td>
</tr>
<tr>
<td>Likely installs a bootkit via raw harddisk modifications</td>
<td>3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Killdisk malware investigation with ICS Malware Sandbox showing access to OT-specific “sec-service” used by serial-to-ethernet controllers manufactured by ASEM Ubiquity.
We know what it takes.

CyberX delivers the only industrial cybersecurity platform built by blue-team experts with a track record defending critical national infrastructure. That difference is the foundation for the most widely-deployed platform for continuously reducing IIoT and ICS risk and preventing costly production outages, safety failures, environmental incidents, and theft of sensitive intellectual property.

CyberX delivers the only IIoT & ICS security platform addressing all five requirements of the NIST CSF and all four requirements of Gartner’s Adaptive Security Architecture. CyberX is also the only IIoT & ICS security company to have been awarded a patent for its ICS-aware threat analytics and machine learning technology.

Notable CyberX customers include 2 of the top 5 US energy providers; a top 5 US chemical company; a top 5 global pharmaceutical company; and national electric and gas utilities across Europe and Asia-Pacific. Strategic partners include industry leaders such as Palo Alto Networks, IBM Security, Splunk, McAfee, Optiv Security, DXC Technology, and Deutsche-Telekom/T-Systems.

Customers choose CyberX because it’s the simplest, most mature, and most interoperable solution for auto-discovering their assets, identifying critical vulnerabilities and attack vectors, and continuously monitoring their ICS networks for malware and targeted attacks. What’s more, CyberX provides the most seamless integration with existing SOC workflows for unified IT/OT security governance.

For more information, visit CyberX.io or follow @CyberX_Labs.

ABOUT CYBERX