PACKETVIPER®

Ransomware Defense for Converging Information Technology (IT) and Operational Technology (OT) Networks

A Deception-Based Approach To Strengthen Ransomware Defense

Use Case Overview

February 2021

THE RANSOMWARE THREAT TO OPERATIONAL TECHNOLOGY (OT) NETWORKS

Ransomware is one of the most potentially damaging threats facing businesses and critical infrastructure organizations today. It is a scheme intended to harm, leveraging malware that infiltrates a target network and prevents access to vital systems. The threat then extorts money from the target in exchange for control.

While ransomware has been a prominent IT threat for some time, cybercriminals are now increasingly targeting OT with ransomware. Packaging giant WestRock (NYSE: WRK)[1] was hit with ransomware, critical processes were hampered and the stock dropped more than 4% the day after the breach was disclosed.

OT is a ripe target is because the focus on process uptime tends to result in vulnerability. Since updating OT can result in unplanned downtime, OT isn't patched or updated as frequently as IT. Finally, OT and IT convergence increases the attack surface and paths in for threats.

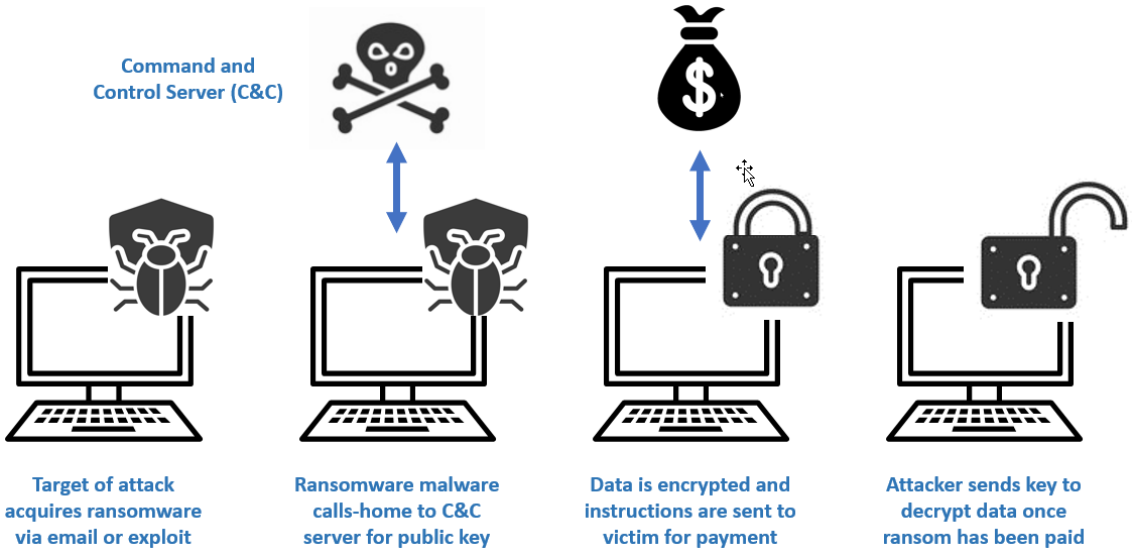
Fundamentals of Ransomware

Whether the attack is on an IT or OT network, the fundamentals are similar. The first stage of a ransomware attack is to infiltrate a network and deploy malware, typically through email. Often, this malware will reach back outside of the network and connect to the criminal's Command and Control (C&C) server. This connection is known as the ransomware 'call home' and typically uses standard port 80 and HTTP or port 443 and HTTPS protocols.

The attacker then uses the C&C server to evaluate where the malware has landed within the target. The threat is now assessing the best course of action to escalate access and move laterally to identify additional assets of value. Once the attacker has lingered long enough to identify the high value assets that are likely to maximize economic gain, the threat launches the attack.

Image 1 below illustrates a typical ransomware exploit:

Image 1:



[1] https://www.securityweek.com/packaging-giant-westrock-says-ransomware-attack-impacted-ot-systems

A PRACTICAL DEFENSE-IN-DEPTH APPROACH TO RANSOMWARE

Preventing ransomware requires a comprehensive approach. A layered, defense-in-depth approach will yield the best chance to defend against ransomware in combined IT/OT networks. Endpoint-based ransomware prevention tools are important but unpatched OT assets may not be well suited for advanced endpoint solutions. It remains important to protect the network against threats that manage to infiltrate and then seek to establish C&C communications.

Introducing Deception360™

PacketViper's Deception360 automates deception-based threat detection and attack prevention and can be a valuable addition to a layered approach to ransomware. Agentless, software-based deception artifacts provide active cyber threat detection, prevention and response. Deception360 supports secure IT/OT alignment, can evolve from mirror-mode to in-line security and doesn't threaten OT uptime.

Deception360 uses a combination of sensors, highly believable decoys with advanced capabilities, and OT Sirens™. Sirens are intended to be targets for threats passively listening to a network seeking services to exploit. Sirens are configured to emit network traffic as if it was a fully functioning system.

For threats performing more active reconnaissance scanning efforts, decoys are attractive targets. Decoys can authentically resemble systems and services that threats will try to exploit. Once decoys and sirens are touched by threats, a high-fidelity alert is generated and a variety of countermeasures can be taken.

Defending Against Ransomware.

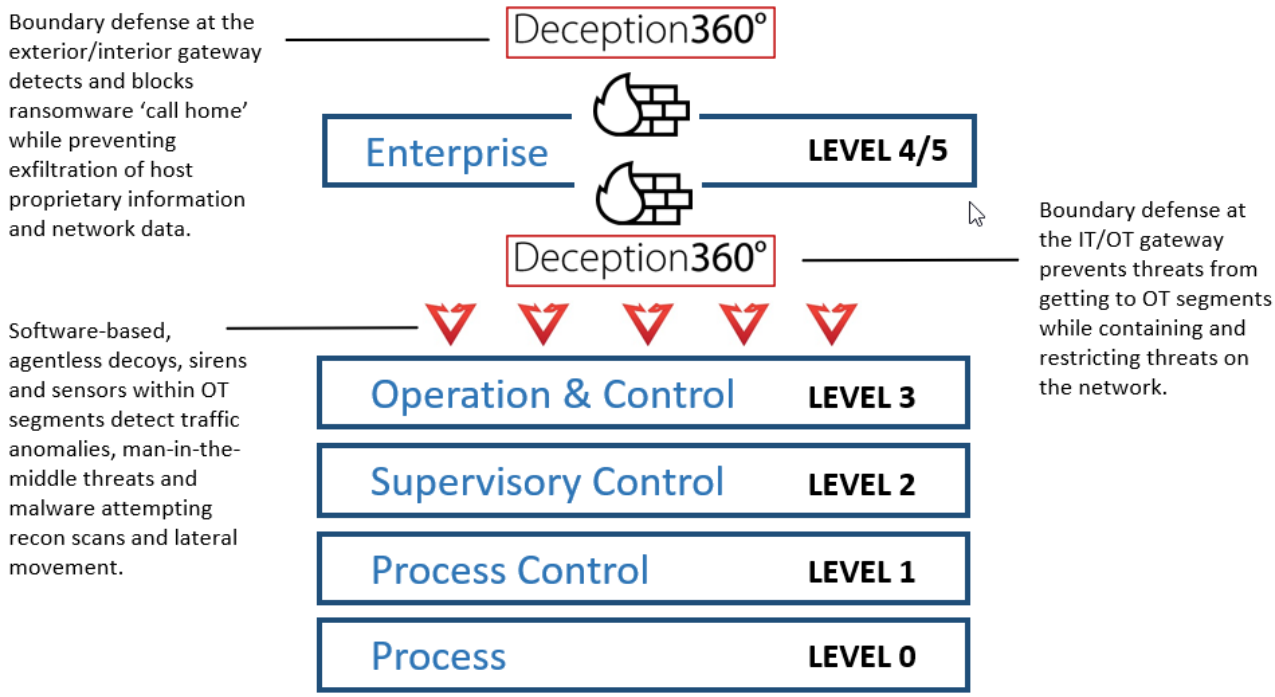
Once deployed, Deception360 decoys and sensors passively monitor the network without scanning. This improves visibility while gathering intelligence on internal network threats performing reconnaissance and moving laterally. The solution can reduce dwell time when deployed in-line by responding to attacks at wire speeds, both within a segment or across an enterprise.

Boundary protection is an important feature of Deception360 that helps contain ransomware regardless of source. A comprehensive set of rules can be easily deployed to detect anomalous outbound traffic and automatically block the C&C 'call home'. This stops ransomware from accessing the internet, preventing host data exfiltration or leakage of proprietary information.

Deception360 works earlier in the cyber kill chain, allowing for more effective threat response and ultimately resulting in less risk for the organization. All of this can be accomplished straight from Deception360 and without complex orchestrations.

Security teams can easily and affordably saturate the network with software-based, agentless deception artifacts. Ideally deception should be spread across all network segments, as well as at the IT/OT boundary, and any external/internal boundary (Image 2).

Image 2:



And with compliance increasingly becoming a part of comprehensive cybersecurity programs, teams find comfort in how Deception360 supports key security controls (Image 3).

Image 3:

NIST Framework for Critical Infrastructure Cybersecurity *Identify (ID) Protect (PR) Detect (DE) Respond (RS) Recover (RC)*	**NIST 800-53 Security and Privacy Controls for Information Systems and Organizations**
PR.DS.2: Data in transit is protected	**RA-10:** Threat hunting
PR.DS.5: Protections against data leaks are implemented	**SC-5(3):** Detection and monitoring
PR.IP.7: Protection processes are continuously improved	**SC-7:** Boundary protection
DE.CM.1: The network is monitored to detect potential cyber events	**SC-7(9):** Restrict threatening outgoing communications traffic
DE.CM.7: Monitoring for unauthorized personal, connections, devices and software is performed	**SC-7(10):** Prevent exfiltration
DE.DP: Detection Processes	**SC-30:** Concealment and misdirection
RS.MI.1: Incidents are contained	**SI-4(1):** Systemwide intrusion detection
RS.MI.2: Incidents are mitigated	**SI-4(5):** System generated alerts
	SR-3(2): Limitation of harm

This deception-based approach to ransomware provides new and innovative ways to address the threat earlier while minimizing risk and mitigating loss.

ABOUT PACKETVIPER

PacketViper has transformative and trusted cybersecurity solutions for organizations seeking better security performance, reliability and results across their converging OT & IT networks. Deception360 solution automates deception-based attack prevention from both external and internal threats. PacketViper customers cover multiple public and private sector industries.

For more information visit www.packetviper.com.