AIRGAP

Garmin Down?

Airgap Network’s 7-Layer Defense

Background

Garmin, a fitness smartwatch firm, closed its connected services and call centers on 23 July after what the company called a massive failure. According to two sources with specific knowledge of what happened, a continuing global outage at sport and fitness tech company Garmin has been triggered by a ransomware attack. Security experts say the company was the target of an organized cyber-attack that leveraged WastedLocker ransomware to breach Garmin’s IT assets.

About WastedLocker Ransomware

WastedLocker has been tracked in the wild since April/May 2020. The name comes from the ‘wasted’ string which is appended to encrypted files upon infection. Similar to other ransomware families such as Maze and NetWalker, WastedLocker has been attacking high-value targets including several Fortune 500 companies. WastedLocker often works in tandem with SecGholish and CobaltStrike and likely to be the case in case of Garmin.

Anatomy of the attack

Step1:

The first victim is usually targeted by the cyber-criminals and the victim is convinced to download a payload using variety of known techniques such request for an update to the browser, phishing, or socially targeted campaign. SecGholish toolset is typically used in the campaign trail to achieve the objective of delivering CobaltStrike Payload.

Airgap Defense: Airgap filters known C&C sites which typically host the Malware/payload such as SecGholish and CobaltStrike so that the endpoints cannot connect and download the malicious payload.

Step2:

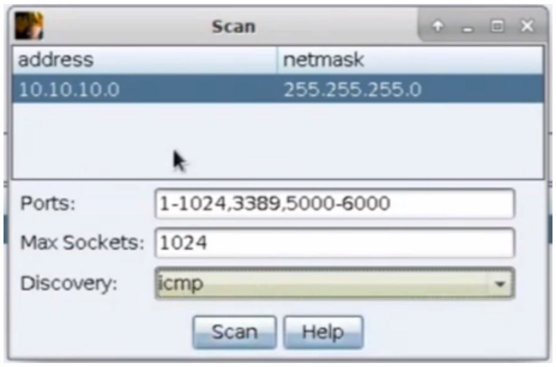
Once downloaded, CobaltStrike helps with lateral movement as well as gain additional profile data on the targeted hosts or environments. CobaltStrike also disables the Windows Defender feature rendering the host-based FW solutions defenseless. For lateral movement, CobaltStrike infiltrate the domain control by leveraging scanning tools such as NetBIOS, mDNS scanners

Airgap Defense: Airgap’s Zero Trust Isolation technology detects and blocks lateral and scans as well as scans originating from endpoints towards the datacenter.

Step3:

Once CobaltStrike compromises the domain controller, it obtains the list of members of the domain controller and then uses network tools such as nmap, port-scanning, ping etc to determine the member status in the network

Airgap Defense: Airgap’s Zero Trust Isolation technology blocks any lateral scanning attempt and presents the responses as if none of the members are present on the network



address	netmask
10.10.10.0	255.255.255.0

Ports: 1-1024,3389,5000-6000

Max Sockets: 1024

Discovery: icmp

Step4:

For detecting members/devices outside of the domain controller – such as Apple devices (MacOS, IoS) or Android devices, or IoTs, CobaltStrike uses popular IP port-scanning methods

Airgap Defense: Airgap’s Zero Trust Isolation technology blocks any lateral scanning attempt and presents the responses as if none of the members are present on the network

Step5:
Once the members have been identified on the network, CobaltStrike uses well known WMI port for lateral propagation.
Airgap Defense: Airgap's Zero Trust Isolation technology blocks all unauthorized lateral movement within the network

Step6:
Once CobaltStrike has infiltrated the endpoints, it moves to download WastedLocker payload (actual ransomware) that encrypts the data/information.
Airgap Defense: Airgap filters known C&C sites which typically host the Malware/payload such as WastedLocker so that the endpoints cannot connect and download the malicious payload

Step7:
The entire process usually takes a few minutes to propagate across the enterprise creating mass infection with little or no time to react to the cyber-breach of this kind. Worse part is, this attack can also penetrate through traditional VPN/remote-access solutions
Airgap Defense: Airgap's Zero Trust Isolation technology blocks lateral movement thereby limiting the exposure to one device in the network. Further, Airgap's modern remote access solution eliminates the need to provide network access to remote users preventing them from network-based attacks

About Airgap Networks

Airgap **predicts** potential cyber-breach by leveraging AI to perform deep device profiling and network vulnerabilities scans. Further, Airgap's network based agentless Zero Trust Isolation **prevents** lateral propagation of the threat in the network as well as filters known C&C sites **preventing** endpoints from downloading the payload. Further, Airgap **detects** internal reconnaissance attempts and lateral movement with high degree of accuracy and automates the **remediation** response by quarantining the compromised endpoints. Thus, Airgap's comprehensive Zero Trust Isolation platform is perfectly suited for protecting enterprise environments from variety of cyber threats.

Airgap Deployment Practices

- **Simple**: - installs in minutes, not hours or days
- **Easy**: No agents, no-APIs, no forklift upgrades, no design changes
- **Smart**: On-premise and Cloud deployments options

Contact Us

For questions or additional details, please contact us. We'd love to hear from you.

info@airgap.io
https://airgap.io