CASE STUDY

Attivo NETWORKS

HEALTHCARE CUSTOMER DETECTS INFECTED IOT DEVICES

HIGHLIGHT

Attivo Solution detected malware spreading from IoT medical device that bypassed all existing security controls.

Company Profile

- Company in the Healthcare industry
- Large Enterprise: 15,000+ employees

Attivo Deployment

- Attivo network deception solutions deployed in production
- Default services and VMs

Detection

- Brand new patient monitoring devices observed dropping malware on decoys
- Customer traced infected system and remediated infection before it spread to other systems

S.NO	SEVERITY	TIMESTAMP	ATTACKER IP	TARGET HOST	TARGET IP	TARGET OS	VLAN	ATTACK DESRCIPTION	ATTACK DETAILS
1	MEDIUM	"2017-09-14T23:25:23.5712"	[redacted]	""	[redacted]	""	"650"	"ARP FLOOD"	"VLAN-ID=650 SRC-IP= [redacted]
2	MEDIUM	"2017-09-14T17:46:55.8582"	[redacted]	"WINDOWS7-1"	[redacted]	"WINDOWS 7"	"2520"	"DROPPED FILE PROCESS EXIT"	"SUSPECT PROCESS [\DEVICE\HARDDISKVOLUME2\
3	MEDIUM	"2017-09-14T15:26:34.9672"	[redacted]	"WINDOWS7-1"	[redacted]	"WINDOWS 7"	"1830"	"DROPPED FILE PROCESS EXIT"	"SUSPECT PROCESS [\DEVICE\HARDDISKVOLUME2\
4	MEDIUM	"2017-09-14T12:50:37.1082"	[redacted]	"WINDOWS7-1"	[redacted]	"WINDOWS 7"	"2520"	"DROPPED FILE PROCESS EXIT"	"SUSPECT PROCESS [\DEVICE\HARDDISKVOLUME2\
5	MEDIUM	"2017-09-14T12:50:36.9392"	[redacted]	"WINDOWS7-1"	[redacted]	"WINDOWS 7"	"2520"	"DROPPED FILE PROCESS START"	"THREAD [804.3132] STARTED SUSPECT PROCESS [2
6	HIGH	"2017-09-14T12:49:36.9352"	[redacted]	"WINDOWS7-1"	[redacted]	"WINDOWS 7"	"2520"	"UNSIGNED EXECUTABLE FILE DROP"	"PROCESS [C:\WINDOWS\MSSECSVC.EXE] WITH
7	HIGH	"2017-09-14T11:36:01.2152"	[redacted]	"WINDOWS7-1"	[redacted]	"WINDOWS 7"	"960"	"UNSIGNED EXECUTABLE FILE DROP"	"PROCESS [C:\WINDOWS\MSSECSVC.EXE] WITH
8	MEDIUM	"2017-09-14T11:34:26.6962"	[redacted]	"WINDOWS7-1"	[redacted]	"WINDOWS 7"	"960"	"DROPPED FILE PROCESS EXIT"	"SUSPECT PROCESS [\DEVICE\HARDDISKVOLUME2\
9	MEDIUM	"2017-09-14T11:34:26.3302"	[redacted]	"WINDOWS7-1"	[redacted]	"WINDOWS 7"	"960"	"DROPPED FILE PROCESS START"	"THREAD [804.3132] STARTED SUSPECT PROCESS [2