Healthcare Service Provider Prevents Ransomware Attack with Saner Endpoint Security

Case Study

Overview

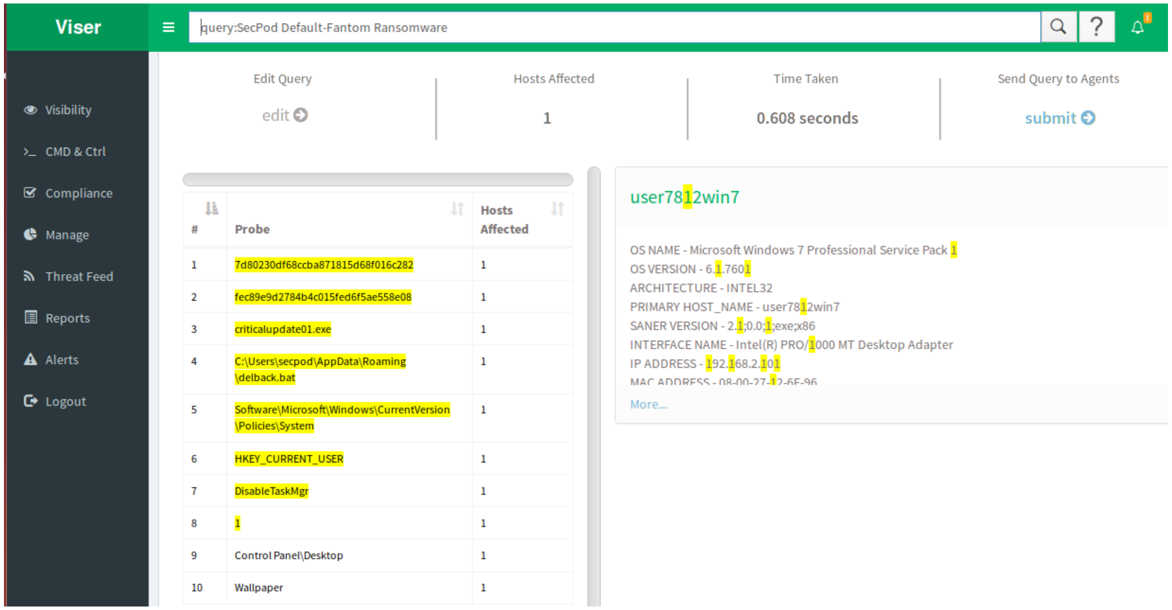
An employee of a large healthcare institute was working on his system as usual. The IT admin was notified of a malicious behavior in that system. With Saner, he detected a ransomware and quickly took necessary actions to avoid any damage to the system and the network. The timely Saner updates helped the IT admin to proactively detect and remediate the threat. The system user was unaffected and was able to work as usual.

What Happened?

What displayed on the employee's screen was a fake Windows updates screen. It pretended that Windows is installing a new critical update. This fake update is a ransomware variant known as Fantom. The cyber criminals use this technique trusting that employees will download the ransomware. Users think that the upgrade prompt is legitimate and download it. Fantom tries to update Windows system with critical patch/update, by displaying a fake UI. This alert was a wakeup call to every employee in the organization.

If the employee had clicked on the update, the desktop would have gone into a full-screen mode. The file encryption would've taken place in the background. But with Saner, the security team could watch the client machine and observe each file that the ransomware was reading and writing in real-time. Consecutively, they were able to isolate infected endpoints and stop the attack from progressing.

The Fantom ransomware indicators detected by Saner endpoint security have been highlighted in fig 1.



query:SecPod Default-Fantom Ransomware

Edit Query: edit

Hosts Affected: 1

Time Taken: 0.608 seconds

Send Query to Agents: submit

#	Probe	Hosts Affected
1	7d80230df68ccba871815d68f016c282	1
2	fec89e9d2784b4c015fed6f5ae558e08	1
3	criticalupdate01.exe	1
4	C:\Users\secpod\AppData\Roaming\delback.bat	1
5	Software\Microsoft\Windows\CurrentVersion\Policies\System	1
6	HKEY_CURRENT_USER	1
7	DisableTaskMgr	1
8	1	1
9	Control Panel\Desktop	1
10	Wallpaper	1

user7812win7

OS NAME - Microsoft Windows 7 Professional Service Pack 1
OS VERSION - 6.1.7601
ARCHITECTURE - INTEL32
PRIMARY HOST_NAME - user7812win7
SANER VERSION - 2.1;0.0;1;exe;x86
INTERFACE NAME - Intel(R) PRO/1000 MT Desktop Adapter
IP ADDRESS - 192.168.2.101
MAC ADDRESS - 08-00-27-12-6E-96

More...

fig 1

How Can Saner Endpoint Security Solution Help?

Saner solution's expanded visibility helped to detect ransomware in real-time at an early stage. Saner helped to expand the depth and quality of data to prevent security events.

Benefits

- Detected the breach early.
- Quickly killed the process stopping the dissemination of the ransomware.
- Created alerts on anomalous file activity to rapidly detect and prevent future attacks.

Potential Consequences

If infected, the consequences of the ransomware on the healthcare institute could've been critical. It could have lead to:

- Loss of patient information
- No access to patient's medical records which could impact patient's diagnosis
- Delayed lab orders
- Legal costs
- Damage to brand and reputation

To learn more about the SecPod MSP Partner Program, visit http://www.secpod.com/msp-endpoint-security-service.html

To learn more about us, visit www.secpod.com.

For a Saner 2.2 demo, contact SecPod at info@secpod.com.

To submit a support request, email SecPod at support@secpod.com.