Security Snares

RansomSnare

Stop Ransomware From Working. Full Stop.

With a proliferation of new variants, ransomware families, and vulnerabilities to exploit, traditional endpoint security and anti-malware tools have an increasingly difficult task in preventing the ransomware payload from getting on your network. With the need for constant updates to patch vulnerabilities or obtain the latest signatures, it's no wonder why ransomware has proliferated given an increasingly mobile workforce. The key is not to dump your current endpoint tool but augment it according to the threat.

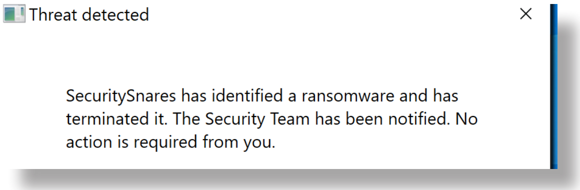
All forms of ransomware have the same thing in common; they all need to encrypt files. RansomSnare stops ransomware from working by suspending the process as it attempts to encrypt the very first file.

Because it works on the first file, RansomSnare does not need to reserve a block of space to roll back files like other products. Additionally, because it is so efficient, it uses an unnoticeable level of resources and maintains a tiny footprint unlike behavioral based detection.

RansomSnare also does not need to model a known good state as a baseline, therefore, it can be used in recovery as it stops reoccurrence after rollback from an attack. It also does all of this without signatures so it works offline and requires no updates to the core technology. In fact, the same core technology has stopped every ransomware strain over the last two years without update. This is critical for a mobile workforce.

How It Works

When ransomware gets on your device, it tries to encrypt files. When encryption is attempted on the first file, RansomSnare stops the process, alerts the user and sends the data to the security team.



Threat detected

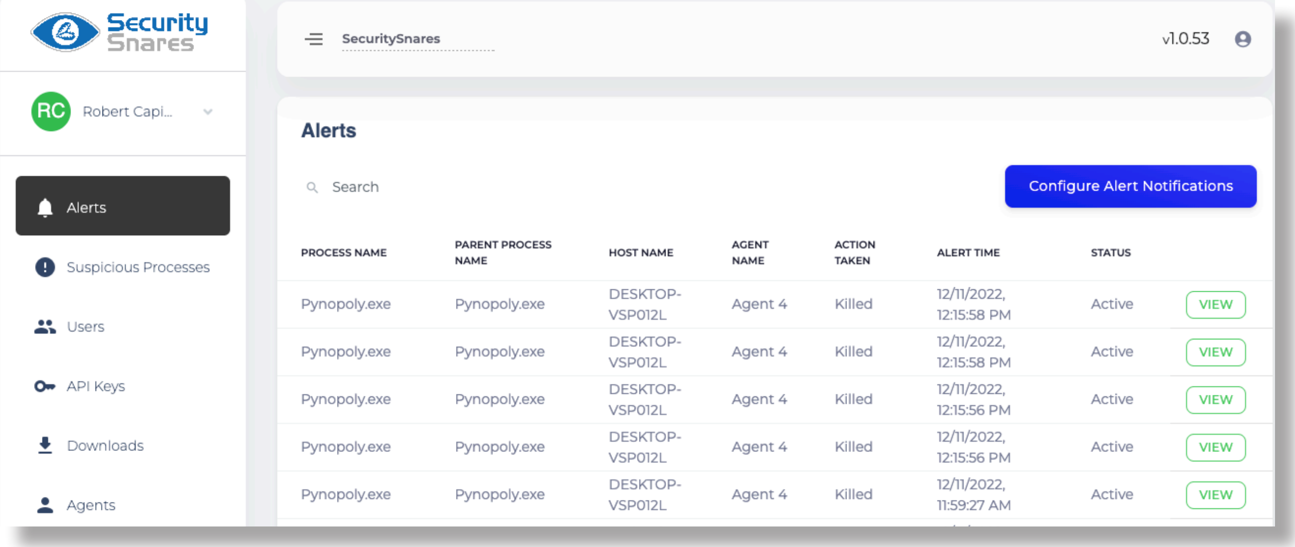
SecuritySnares has identified a ransomware and has terminated it. The Security Team has been notified. No action is required from you.

continued on next page

Stop ransomware from working by suspending the process as it attempts to encrypt the very first file.

This information is displayed via a management console. The console aggregates all the RansomSnare endpoints across the entire organization. The data can even be sent to the Security Information and Event Management (SIEM) tool of your choice.

Because the process was immediately suspended, the security team now has time to analyze the data and respond appropriately.



PROCESS NAME	PARENT PROCESS NAME	HOST NAME	AGENT NAME	ACTION TAKEN	ALERT TIME	STATUS	
Pynopoly.exe	Pynopoly.exe	DESKTOP-VSP012L	Agent 4	Killed	12/11/2022, 12:15:58 PM	Active	VIEW
Pynopoly.exe	Pynopoly.exe	DESKTOP-VSP012L	Agent 4	Killed	12/11/2022, 12:15:58 PM	Active	VIEW
Pynopoly.exe	Pynopoly.exe	DESKTOP-VSP012L	Agent 4	Killed	12/11/2022, 12:15:56 PM	Active	VIEW
Pynopoly.exe	Pynopoly.exe	DESKTOP-VSP012L	Agent 4	Killed	12/11/2022, 12:15:56 PM	Active	VIEW
Pynopoly.exe	Pynopoly.exe	DESKTOP-VSP012L	Agent 4	Killed	12/11/2022, 11:59:27 AM	Active	VIEW

To see RansomSnare in action contact info@ransomsnare.com