Release Notes

Early Access Program (July) Intercept X
Sophos Intercept X Endpoint
C:\Program Files (x86)\HitmanPro.Alert\hmpalert.exe (build 713)

As of July 24 2017

Executive Summary

The Early Access Program for Intercept X includes a new endpoint agent that can be deployed on select machines participating in the early access program. A list of core features and known issues are described below.

Supported Platforms

Windows 7 and above desktops

Supported new features

Feature		Description
Credential theft protection		Preventing theft of authentication passwords and hash information from memory, registry, and off the hard disk.
Process protection	Code cave utilization	Detects the presence of code deployed into another application, often used for persistence and antivirus avoidance.
	Malicious process migration	This detects a remote reflective DLL injection used by adversaries to move laterally between processes running on the system.
	Process privilege	This prevents a low-privilege process from being escalated to a higher privilege, often used by an active adversary to gain system access rights. This feature is not enabled in the EAP at this time
	APC protection (AtomBombing)	This detects abuse of application procedure calls often used as part of the new (2016) AtomBombing exploit technique. Adversaries use this to make another process to execute their code.
New registry protections	Sticky key protection	Intercept X prevents replacement of the sticky key executable by an adversary, which is often used for persistence.
	Application verifier protection	Intercept X prevents the replacement of application verifier DLLs that would allow the adversary to circumvent antivirus and other normal process start-up behavior.
Improved process lockdown	Browser behavior lockdown	Intercept X prevents the malicious use of PowerShell from browsers as a basic behavior lockdown.
	HTA application lockdown	HTML applications loaded by the browser will have the lockdown mitigations applied as if they were a browser.

Known Issues

Red Security Health State Integration with Synchronized Security to place the endpoint into a red security health state until the admin indicates the issues has been resolved is not included in the early access program.

Code Cave – Process termination for applications with a detected code cave are not always terminated when the code caved application is launched from inside a metrepeter shell.

Application Verifier – When an application verifier registry modification is detected the application being verified may terminate as opposed to simply being restricted to the authorized Microsoft verification dlls.

Download Reputation + Web Control – These features are not working correctly in Edge for current Windows 10 desktop build

Install of EAP endpoint with Symantec – With Symantec endpoint protection the install of the service for Malicious Traffic Detection can be blocked as a low reputation file. Rebooting and re-install of Intercept X EAP appears to resolve the conflict.

EAP working with 'Paused Updates' – Sophos central's support for 'paused updates' can conflict with the EAP agent. If using paused updates, then endpoints selected for the EAP program will need to have tamper protection turned off if they are removed from the EAP program so that updates can resume correctly. After the successful update you can re enable tamper protection.