在思科安全终端中创建高级自定义检测列表

目录

<u>简介</u> <u>背景信息</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>创建高级自定义检测列表</u> 相关信息

简介

本文档介绍在思科安全终端中创建高级自定义检测(ACD)的步骤。

背景信息

TALOS Intelligence于2020年1月14日发布了一篇博客,以回应Microsoft星期二补丁漏洞披露。

1月15日更新:为AMP添加了ACD签名,该签名可用于通过伪装成Microsoft ECC代码签名证书颁发 机构的欺骗证书来检测CVE-2020-0601的<u>利用。</u>

在TALOS BLOG中找到的要在ACD中使用的文件的签名:

- Win.Exploit.CVE_2020_0601:1:*:06072A8648CE3D020106*06072A8648CE3D020130
- <u>https://alln-extcloud-storage.cisco.com/blogs/1/2020/01/CVE-2020-0601.txt</u>

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 思科安全终端云门户
- ACD
- TALOS博客

本文档中的信息在特定实验室环境设备上创建。 所有使用的设备都以已清除(默认)的配置启动。 如果您的网络处于活动状态,请确保您了解任何命令的潜在影响。

创建高级自定义检测列表

现在,我们创建ACD以进行匹配。

步骤1.导航至Secure Endpoint Portal > Outbreak Control > Advanced Custom Detection,如图所示。

Outbreak Control V Mana
CUSTOM DETECTIONS
Simple
Advanced dhy
Android
APPLICATION CONTROL
Blocked Applications
Allowed Applications
NETWORK
IP Block & Allow Lists
ENDPOINT IOC
Initiate Scan
Installed Endpoint IOCs
Scan Summary

步骤2.以签名集CVE-2020-0601的名称开头,如图所示。

Custom Detections - Advanced					
		Create Signature Set			
Name	Ι	Save			

步骤3.接下来,**编辑**该新签名集,然后**添加签名**。 Win.Exploit.CVE_2020_0601:1:*:06072A8648CE3D020106*06072A8648CE3D020130。

Custom Detections - Advanced

O View All Changes

	Create Signature Set	CVE-2020-0601	Update Name
CVE-2020-0601 Created by Mustafa Shukur • 2020-01-22 12:19:38 CST Used in policies: Used in groups:		Created by Mustafa Shukur • 2020-01-22 12: Add Signature Build Database From Signatu ndb: Win.Exploit.CVE_2020_0601.UNOFFICIAL	19:38 CST ure Set
View Changes	🛓 Download 🕼 Edit 🛛 Delete		

步骤4.选择"**从签名集生成数**据库",数据库已生成。

步骤5.将新签名集应用于策略,单击Edit> Outbreak Control > Custom Detections > Advanced,如 图所示。

Modes and Engines	Custom Detections - Simple	None	~		
Exclusions 3 exclusion sets					
Proxy	Custom Detections - Advanced	CVE-2020-0601	~		
Outbreak Control		None CVE-2020-0601			
Product Updates	Application Control - Allowed	None	` ~		
Advanced Settings					
	Application Control - Blocked	None	~		
	Network - IP Block & Allow Lists	Clear Select Lis	ts v		
	None				
				Cancel	Save

步骤6.如图所示,在连接器UI上保存策略和同步。



步骤7.在目录C:\Program Files\Cisco\AMP\ClamAV中搜索当天创建的新签名文件夹,如图所示。

0.101.4.71	k	1/22/2020	12:30 PM	File folder	
📄 custom2522620200122121949.cud		1/22/2020 12:30 PM	CUD File	1 KB	
daily.cvd	~	5/24/2019 12:37 PM	CVD File	11 KB	
📄 freshclam.conf		1/22/2020 12:30 PM	CONF File	1 KB	
👼 freshclam.exe		12/20/2019 11:26 AM	Application	122 KB	
👼 freshclamwrap.exe		12/20/2019 11:26 AM	Application	65 KB	

相关信息

- •用于测试的生成是Windows 10 1909,不受每个MSKB的漏洞影响
- ; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601
- https://support.microsoft.com/en-us/help/4534273/windows-10-update-kb4534273
- 适用于:Windows 10、版本1809、Windows Server 1809、Windows Server 2019、所有版本
- <u>技术支持和文档 Cisco Systems</u>