说说Windows10系统的安全机制

Windows一直是罪犯和安全研究人员钟爱的攻击目标，随着微软在 Windows 10 中加入用以摒除各类攻击的多种高级缓解措施，安全门槛已比过去抬高了很多。一旦发现有规避Windows防御的途径，微软就马上堵上这个安全漏洞。通过实现创新性安全技术来让攻击更难，多亏了这些新特性，Windows 10 才成为迄今为止最安全的Windows系统。

微软开发出了反恶意软件扫描接口(AMSI)工具，可以在内存中捕捉恶意脚本。任何应用程序都可以调用这个接口，任何注册反恶意软件引擎都能处理提交给AMSI的内容。Windows Defender 和AVG目前正在使用AMSI，这一接口应该被更广泛地采纳。AMSI是Windows系统上封锁脚本攻击的一大步。

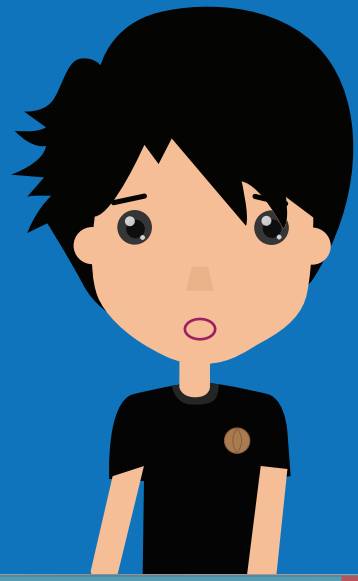
4

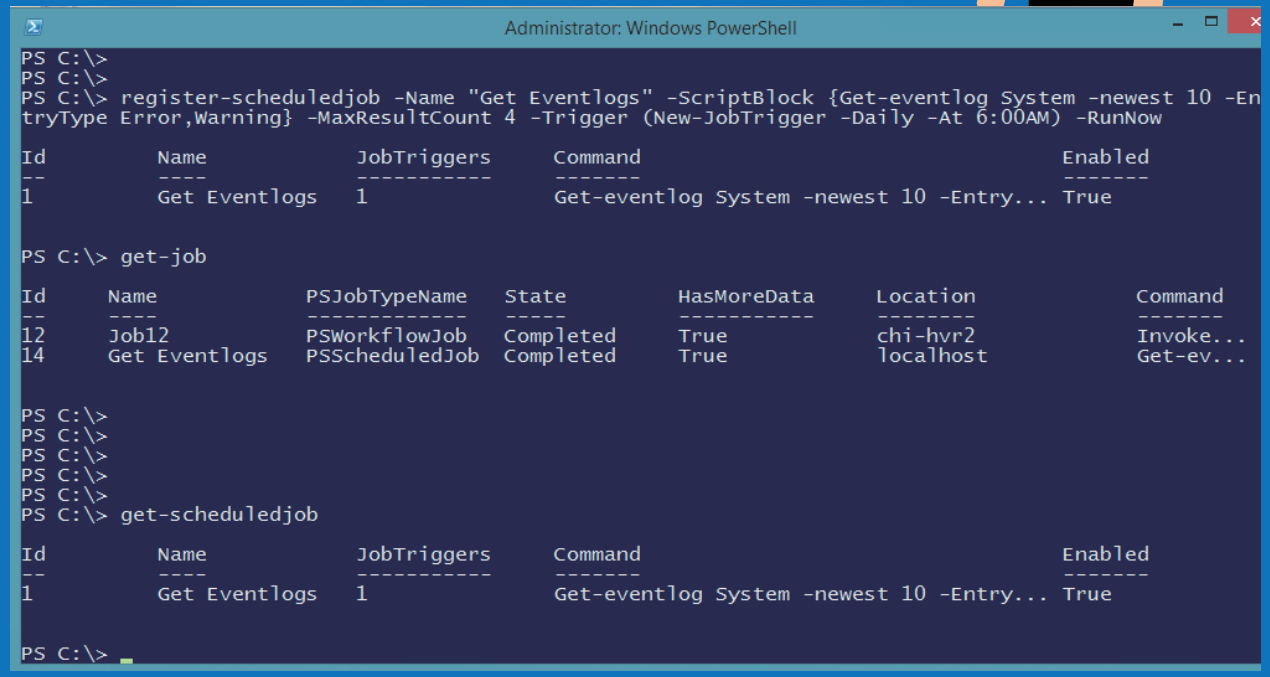
PowerShell

PowerShell

PowerShell

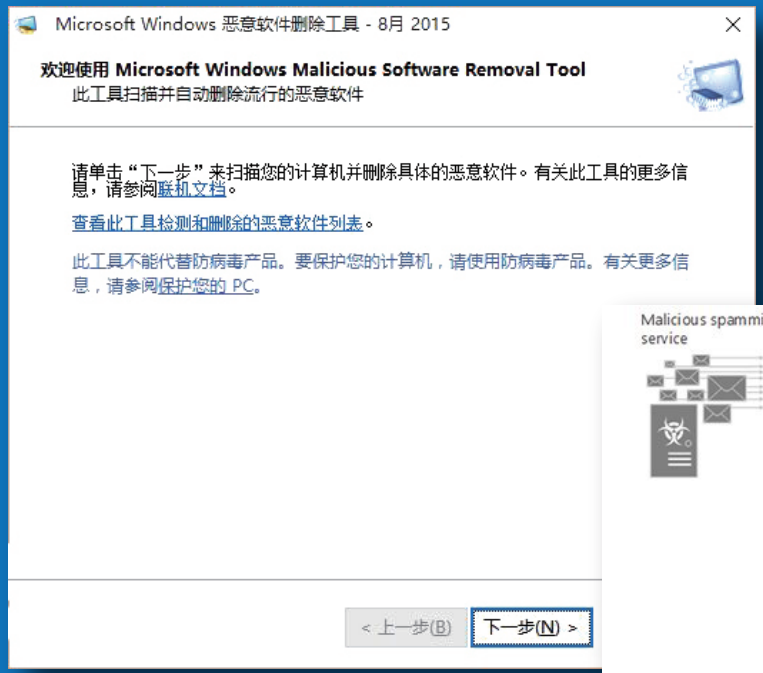
PowerShell

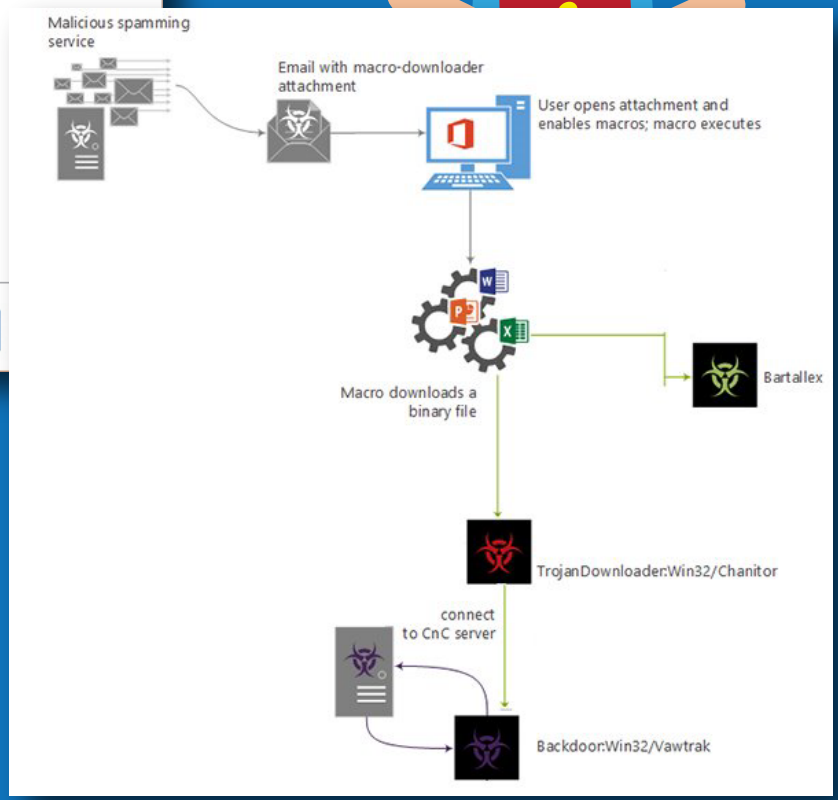


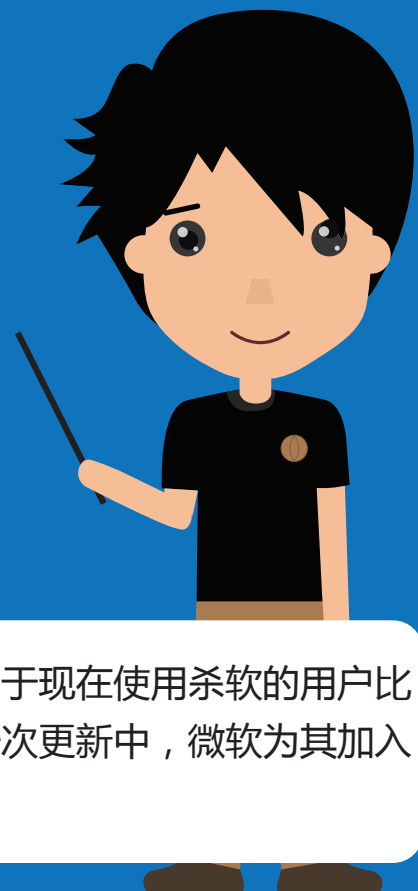


罪犯们开始采用PowerShell在内存中加载脚本，加载到内存中的恶意脚本根本就不会被检测到，所以AMSI试图在主机层级捕获脚本，也就是说，输入方式——无论是存在硬盘上，留在内存里，还是交互启动，无关紧要！

AMSI并不完美，经混淆编码的脚本，或者从WMI名字空间、注册表、事件日志等非常规位置加载的脚本，就不太会被AMSI检测出来。绕过AMSI的方法也有很多，比如修改脚本签名、使用 PowerShell 2 、或者禁用AMSI。





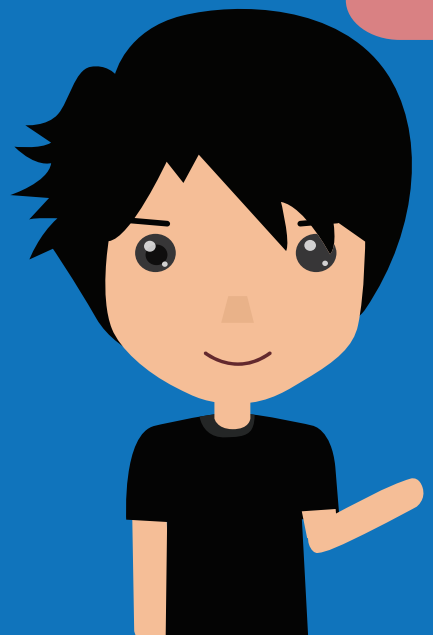


这款软件的作用就是在感染病毒等恶意软件后进行删除，微软每月都会对这款软件进行更新。由于现在使用杀软的用户比较多，因此这款删除工具比较“小众”。但微软并没有因此放弃对这款软件进行更新，在最近一次更新中，微软为其加入了Win32/Vawtrak、Win32/Critroni和Win32/Kasidet三类病毒的检测和杀除能力。

J6 C:\Windows\TEMP\b.exe

E	F	G	H	I	J
处理措施	事件	风险	程序	操作	目标
终止	文件系统	高	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershe	关闭	C:\Users\50219128\AppData\Local\Temp\b.exe
终止	文件系统	高	C:\Windows\System32\wscript.exe	关闭	C:\Users\50219128\AppData\Local\Temp\rad[illegible].tmp.exe
终止	文件系统	高	C:\Windows\System32\wscript.exe	关闭	C:\Users\50219128\AppData\Local\Temp\rad4D7C6.tmp.exe
终止	文件系统	高	C:\Windows\System32\wscript.exe	关闭	C:\Users\50219128\AppData\Local\Temp\rad[illegible].tmp.exe
终止	文件系统	高	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershe	关闭	C:\Windows\TEMP\b.exe

我们也在持续关注利用PowerShell执行脚本的攻击，经过研究分析，我们发现越来越多的勒索软件也在使用该种攻击方法，日前我们接到一起利用PowerShell执行脚本攻击案例，亚信安全OSCE行为检测功能将其成功拦截，上图为病毒日志截图：



亚信安全，棒棒哒！我们会更加努力维护您的安全！