APT40公告

中华人民共和国国家安全部实操攻击手法

Australian Government

Australian Signals Directorate

National Cyber
Security Centre
a part of GCHQ

Communications
Security Establishment

**Canadian Centre
for Cyber Security**

Centre de la sécurité
des télécommunications

**Centre canadien
pour la cybersécurité**

目录

概述

背景

本公告由澳大利亚信号局的澳大利亚网络安全中心（ASD's ACSC）、美国网络安全与基础设施安全局（CISA）、美国国家安全局（NSA）、美国联邦调查局（FBI）、英国国家网络安全中心（NCSC-UK）、加拿大网络安全中心（CCCS）、新西兰国家网络安全中心（NCSC-NZ）、德国联邦情报局（BND）与联邦宪法保卫局（BfV）、韩国国家情报院（NIS）及韩国国家情报院的国家网络安全中心（NIS' National Cyber Security Center）、以及日本国家网络安全应急准备与战略中心（NISC）和警察厅（NPA）联合编制（以下统称为"编制机构"）。本公告概述了一个由中华人民共和国（PRC）政府支持的网络组织及其目前对澳大利亚网络所构成的威胁。本公告借鉴了各编制机构对该威胁的共识以及ASD's ACSC的事件响应调查。

该受中华人民共和国政府支持的网络组织此前曾针对澳大利亚和美国等多个国家的机构发起攻击。下文重点介绍的技术手法，也经常被全球的其他受中华人民共和国政府支持的行为者使用。因此，编制机构认为，该攻击团体及其类似技术仍对其国家的网络构成威胁。

编制机构评估认为，该组织是为中华人民共和国国家安全部（PRC Ministry of State Security，简称MSS）开展恶意网络行动的。其活动与技术与行业报告中追踪的"高级持续性威胁"（Advanced Persistent Threat，简称APT）40团体存在重叠（该组织在行业报告中亦被称为 Kryptonite Panda、GINGHAM TYPHOON、Leviathan 和 Bronze Mohawk）。据此前报道，该组织总部位于中华人民共和国海南省海口市，并接受中华人民共和国国家安全部海南省安全厅的任务指派。[2] 以下公告提供了两个受害网络的典型案例分析，展示该攻击者实际操作中的手法。这些案例分析对于网络安全从业者识别、预防和修复针对其自身网络的 APT40入侵至关重要。所选案例均已采取适当的补救措施，降低了该威胁行为者或其他行为者再次利用的风险。因此，这些案例发生时间相对较为久远，以确保相关组织有足够时间完成修复工作。

活动摘要

APT40已多次将澳大利亚网络以及该地区的政府和私营部门网络作为攻击目标，其对我们网络的威胁持续存在。本公告中描述的攻击手法已在澳大利亚网络中定期被观察到。

值得注意的是，APT40能够快速改造和调整新漏洞的概念验证（POC），并立即利用这些漏洞攻击拥有相关漏洞基础设施的目标网络。APT40定期对目标网络（包括本公告编制机构所在国家的网络）进行侦察，以寻找入侵目标网络的机会。这种定期侦察使该攻击团体能够识别目标网络上存在漏洞、寿命终止或已不再维护的设备，并快速部署漏洞利用程序。APT40早在2017年就不断成功利用漏洞。

APT40对新近公开的漏洞具有快速利用能力，目标涵盖广泛使用的软件，例如Log4j（CVE-2021-44228）、Atlassian Confluence（CVE-2021-31207、CVE-2021-26084）及Microsoft Exchange（CVE-2021-31207；CVE-2021-34523；CVE-2021-34473）。ASD's ACSC及编制机构预计，该攻击团体将在新出现的高危漏洞公开发布后的数小时或数天内继续利用POC进行攻击。

2 美国司法部（U.S. Department of Justice）。2021。《四名与国家安全部合作的中国公民因全球计算机入侵行动被起诉，该行动针对知识产权和机密商业信息，包括传染病研究》（Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research）。

图1.APT40 活动的 TTP（战术、技术与程序）流程图

该组织似乎更倾向于利用易受攻击的、面向公众的基础设施，而非需要用户交互的技术手段（例如网络钓鱼活动），并且高度重视获取有效凭证，以开展后续一系列活动。APT40经常使用Web Shell（网页壳层）脚本（T1505.003）来实现持续性，尤其是在入侵行为生命周期的早期阶段。通常，在成功进行初始访问后，APT40会专注于建立持续性机制，以维持对受害者环境的访问。然而，由于持续性的建立发生于入侵的早期阶段，因此无论入侵程度或采取的后续行为如何，在所有入侵事件中都更有可能被观察到。

值得注意的攻击手法

尽管APT40过去曾使用被入侵的澳大利亚网站作为其行动的指挥与控制（C2）主机，该攻击团体已对此技术手法进行了演化（T1594）。

APT40已顺应全球趋势，利用被入侵的设备（包括小型办公室/家庭办公室（SOHO）设备）作为其在澳大利亚开展行动的行动基础设施与末端跳转重定向器（T1584.008）。这使得编制机构能够更好地定性并追踪该组织的活动。

许多这类SOHO设备寿命已结束或未打补丁，为“N天漏洞利用”（N-day exploitation）提供了软目标。一旦被入侵，SOHO设备便成为攻击的跳板，其攻击流量被设计为混入正常流量中，从而对网络防御者构成挑战（T1001.003）。

此类技术也经常被全球其他受中华人民共和国政府支持的行为者使用，编制机构认为这构成一种共同威胁。更多信息，请参阅联合公告《中华人民共和国政府支持的网络行为者利用网络服务供应商与设备进行攻击行动》（People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices）以及《中华人民共和国政府支持的行为者入侵并持续访问美国关键基础设施》（PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure）。

APT40在其行动中，确实偶尔会使用采购或租赁的基础设施作为面向受害者的C2基础设施；然而，这一手法的使用似乎正呈现相对下降趋势。

攻击工具集

ASD's ACSC分享了在下列调查中发现的一些恶意文件。这些文件已上传至VirusTotal，以便更广泛的网络防御与网络安全社区更好地了解其所需防御的威胁。

案例分析

ASD's ACSC分享了两份匿名化的调查报告，以提升公众对行为者所使用工具与手法的认知。

MD5	文件名	附加信息
26a5a7e71a601be991073c78d513dee3	horizon.jsp	1 kB	Java源代码
87c88f06a7464db2534bc78ec2b915de	Index_jsp$ProxyEndpoint$Attach.class	597 B	Java字节码
6a9bc68c9bc5cefaf1880ae6ffb1d0ca	Index_jsp.class	5 kB	Java字节码
64454645a9a21510226ab29e01e76d39	Index_jsp.java	5 kB	Java源代码
e2175f91ce3da2e8d46b0639e941e13f	Index_jsp$ProxyEndpoint.class	4 kB	Java字节码
9f89f069466b8b5c9bf25c9374a4daf8	Index_jsp$ProxyEndpoint$1.class	3 kB	Java字节码
187d6f2ed2c80f805461d9119a5878ac	Index_jsp$ProxyEndpoint$2.class	1 kB	Java字节码
ed7178cec90ed21644e669378b3a97ec	Nova_jsp.class	7 kB	Java字节码
5bf7560d0a638e34035f85cd3788e258	Nova_jsp$TomcatListenerMemShellFromThread.class	8 kB	Java字节码
e02be0dc614523ddd7a28c9e9d500cff	Nova_jsp.java	15 kB	Java源代码

案例分析1

为便于更广泛传播，本报告已匿名化。受影响的组织以下简称“该组织”。为保护受害者身份及 ASD's ACSC的事件响应方法，部分具体信息已被删除。

执行摘要

本报告详细介绍了 ASD's ACSC 针对2022年7月至9月期间该组织网络被成功入侵事件的调查结果。本调查报告已提交给该组织，旨在总结观察到的恶意行为并制定修复建议。调查结果表明，此次入侵是由 APT40 实施的。

八月中旬，ASD's ACSC 通知该组织，一台可能已被攻击团体控制的设备与该组织的网络进行了恶意交互。经该组织同意，ASD's ACSC于八月底在其网络中可能受影响的主机上部署了基于主机的传感器。这些传感器让ASD's ACSC 事件响应分析师能够进行全面的数字取证调查。利用现有的传感器数据，ASD's ACSC分析师成功地绘制出了该攻击团体的活动图谱，并创建了观察到的事件的详细时间线。

从七月到八月，ASD's ACSC 观察到的主要行为者活动包括：

- 主机枚举，使行为者能够构建自己的网络地图；
- 使用Web Shell，为行为者在网络上提供了初始立足点以及执行命令的能力；以及
- 部署行为者用于恶意目的的其他工具。

调查发现了大量敏感数据被访问的证据，且有证据表明行为者在网络中横向移动(T1021.002)。此次网络入侵之所以得以实施，主要是由于攻击团体在目标网络中建立了多个访问路径，该网络结构呈扁平化，并使用了可被任意上传文件的不安全的内部开发软件。被外泄的数据包括可供攻击团体登录使用的特权身份验证凭证，以及可让行为者在原始访问路径被阻止后重新获得未授权访问权限的网络信息。除最初被利用的主机外，未发现其他恶意工具；然而，该攻击团体已获取合法且具特权的认证凭证，因此无需额外的工具。调查结果表明，该机构很有可能是 APT40有意针对的目标，而非因公开漏洞而遭遇的偶发性攻击。

调查结果

2022年8月中旬，ASD's ACSC通知该组织，一个被确认的恶意IP地址（据信与一个受政府支持的网络团体有关联）至少在七月至八月期间与该组织的计算机网络发生过交互。被入侵的设备可能属于小型企业或家庭用户。

八月底，ASD's ACSC 在该组织网络中显示受入侵影响的主机上部署了一个基于主机的代理程序。

由于日志配置或网络架构设计的原因，一些本可支持调查工作的数据未能被获取。尽管如此，该组织积极提供所有可用数据，使ASD's ACSC能够开展全面分析，并了解APT40在其网络中可能进行的活动。

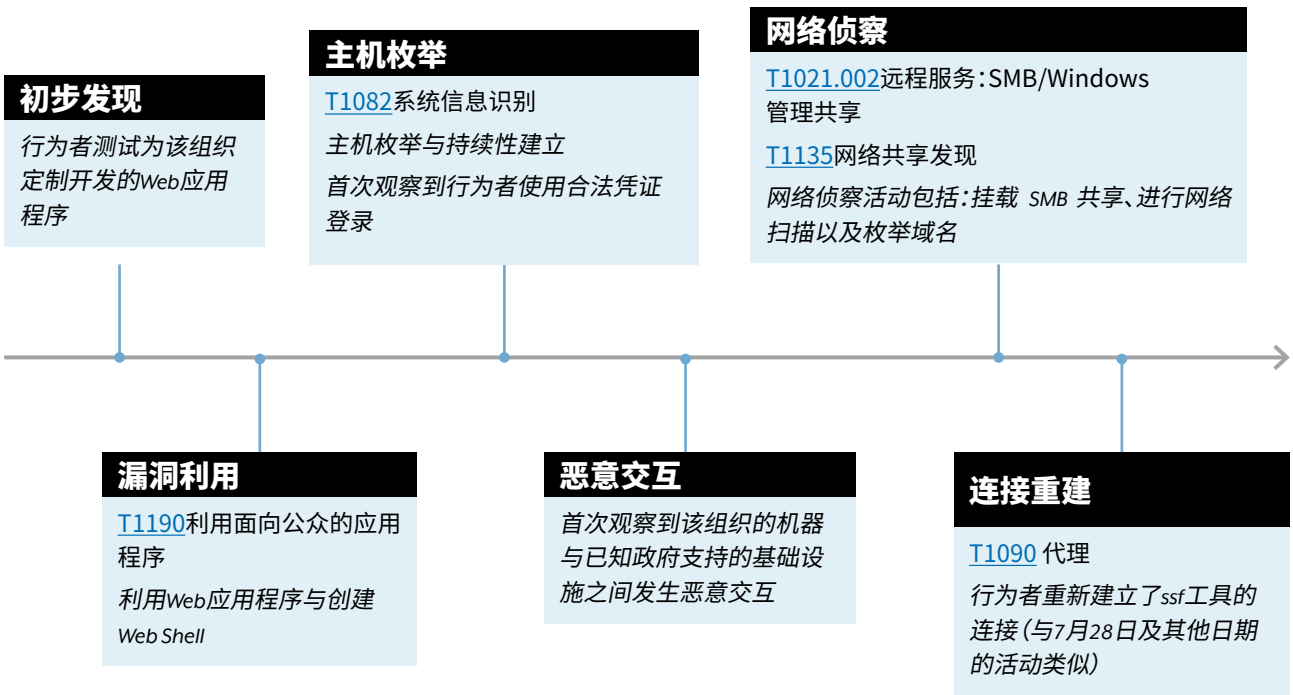
九月，在与ASD's ACSC协商后，该组织决定将初始通报中识别出的IP地址列入黑名单。十月，该组织启动了修复工作。

细节

自七月起，行为者开始测试并利用一款在`<webapp>2-ext`上运行的定制Web应用程序（T1190），使攻击团体得以在网络的非军事区（DMZ）建立立足点。行为者借此手段枚举了整个网络及所有可见域名。行为者利用已泄露的认证凭证（T1078.002）查询了 Active Directory（T1018），并通过在DMZ内的多台机器上挂载文件共享（T1039）实施数据外传。行为者执行了Kerberoasting攻击，以便从服务器（T1558.003）获取有效的网络凭据。未观察到该攻击团体在DMZ或内部网络中获取额外立足点。

图示时间线

下方时间线概述了在该组织网络中所观察到恶意行为者的活动的关键阶段。



时间线详解

七月：行为者通过传输层安全协议（TLS）连接（T1102），建立了与该组织定制的Web应用程序（T1190）（以下简称“web 应用”或“*webapp*”）首页的初始连接。未观察到其他值得注意的活动。

七月：行为者开始枚举web应用网站，寻找端点[2]以进一步探查。

七月：行为者集中尝试利用某一特定端点。

七月：行为者成功向 Web 服务器发送POST请求，可能是通过在另一页面部署的 Web Shell 实现的。另一 IP 地址（可能为同一行为者所用）也开始向同一URL发送请求。行为者创建并测试了多个疑似Web Shell。

虽具体利用方法不明，但很明显是以特定端点为目标，以便在*<webapp>2*-ext上创建文件。

ASD's ACSC 认为两个 IP 地址的连接属同一次入侵事件，因其兴趣相同且初始连接仅相隔几分钟。

七月：攻击团体持续进行主机枚举，寻找权限提升机会，并部署了另一种 Web Shell。行为者使用窃取的*<firstname.surname>@<organisation domain>*凭据登录Web应用程序。

行为者的活动似乎并未成功实现*<webapp>2*-ext上的权限提升。行为者转而转向了基于网络的活动。

七月：该行为者测试了其所窃取的某个服务账户[3]的认证凭证，该凭证很可能是其在内部可访问的二进制文件中的硬编码信息中找到的。

七月：该行为者部署了开源工具Secure Socket Funnelling，用于连接至恶意基础设施。该连接被用于将来自行为者攻击机器的流量引导至组织内网。当行为者尝试使用服务账户凭证时，事件日志中暴露了其主机名。

八月：观察到行为者进行有限的活动，包括尝试使用服务账户建立连接但未成功。

八月：行为者执行了重要的网络与Active Directory枚举操作。随后，行为者使用另一个被入侵的的账户，在 DMZ区域的Windows 主机上挂载共享目录[4]，从而成功实施数据外传。

这似乎是行为者利用窃取的凭证在DMZ中可挂载的机器上伺机攻击。防火墙阻止了行为者利用类似活动攻击内部网络。

八月至九月：SSF工具重新建立了与恶意 IP 的连接。在其访问被阻止之前，未观察到该团体进行任何其他活动。

九月：该组织在其防火墙上将恶意IP列入黑名单，对其进行了阻断。

2 在本文中，“端点”指的是Web应用程序中的某项功能。
3 服务账户系指与服务绑定的账户，不与个人用户绑定。在微软（Microsoft）企业域名环境中，存在多种类型的账户。
4 挂载共享是指将文件系统结构中的文件设置为可供用户或用户组访问的过程。

行为者的战术与技术

MITRE ATT&CK 框架是一份记录了威胁行为者在网络空间中使用的战术和技术的文档集。该框架由美国非营利组织MITRE公司创建，旨在作为描述威胁行为者的行为的全球通用语言。

ASD's ACSC评估认为，以下技术与战术与该行为者的恶意活动相关：

侦察

T1594——搜索受害者拥有的网站

行为者枚举了定制Web应用程序的网站，以识别潜在的网络访问路径。

初始访问

T1190——利用面向公众的应用程序（利用定制Web应用程序）

T1078.002——有效账户：域名账户（使用已外泄的凭证登录）

行为者利用暴露于互联网的定制 Web 应用程序获得了初始访问点。行为者随后得以使用所窃取的凭证进一步扩展其在网络中的访问权限。

执行

T1059——命令和脚本解释器（通过Web Shell执行命令）

T1072——软件部署工具（行为者使用开源工具 Secure Socket Funnelling（SSF）连接至某一 IP）

持续性

T1505.003——服务器软件组件：Web Shell（利用Web Shell和SSF工具建立访问通道）

凭证访问

T1552.001——来自密码存储的凭证（与楼宇管理系统（BMS）相关的密码文件）

T1558.003——窃取或伪造 Kerberos 票据：Kerberoasting 技术（攻击获取网络凭证）

横向移动

T1021.002——远程服务：SMB 共享（行为者从多个设备上挂载SMB共享目录）

收集

T1213——来自信息库的数据（从BMS服务器上获取操作手册/文档）

数据外传

T1041——通过C2通道外传（行为者从Active Directory和挂载的共享目录中进行数据外传）

案例分析2

为便于更广泛传播，本报告已作匿名化处理。受影响的组织以下简称“该组织”。为保护受害者身份及 ASD's ACSC的事件响应方法，部分具体信息已被删除。

执行摘要

本报告详细介绍了 ASD's ACSC 对2022年4月该组织网络遭入侵既遂事件的调查结果。该调查报告已提交给该组织，旨在总结观察到的恶意活动并制定修复建议。调查结果表明，此次入侵是由 APT40 实施的。

2022年5月，ASD's ACSC通知某组织，其网络自2022年4月起可能遭受恶意活动影响。随后，该组织向ASD's ACSC报告称，在一台面向互联网的服务器上发现了恶意软件，该服务器用于提供该组织企业远程访问解决方案的登录门户。该服务器使用了一款远程访问登录与身份管理产品，本报告将其称为“遭入侵设备”。本报告详细介绍了ASD's ACSC的调查结果，以及由此为该组织制定的修复建议。

证据显示，至少自2022年4月起，该组织的部分网络已遭恶意网络行为者通过其远程访问登录门户入侵。该服务器可能被多个行为者入侵，并很可能受到在发生入侵时广泛公开的远程代码执行（RCE）漏洞影响。

ASD's ACSC观察到的主要行为者的活动包括：

- 主机枚举，使行为者能够构建自己的网络地图；
- 利用面向互联网的应用程序并使用Web Shell，为行为者在网络上提供了初始立足点以及执行命令的能力；
- 利用软件漏洞以提升权限；以及
- 收集凭证以实现横向移动

ASD's ACSC发现，一名恶意行为者于2022年4月在遭入侵设备上外传了数百组唯一的用户名与密码组合，以及若干与远程访问会话相关的多重身份验证代码与技术数据。经该组织审查，所泄露的密码均为真实有效。ASD's ACSC评估认为，行为者可能收集了这些技术数据，以合法用户身份劫持或创建远程登录会话，从而使用合法用户账户访问该组织的内部企业网络。

调查结果

调查摘要

ASD's ACSC确认，行为者已入侵用于为组织员工提供远程登录会话的设备，并利用该入侵尝试开展进一步的活动。这些设备由三个负载均衡主机组成，在此发现了最早的入侵证据。在初始入侵发生后不久，该组织关闭了三台负载均衡主机中的两台。因此，所有后续活动均发生在一台主机上。与遭入侵设备相关的其他服务器也采用了类似的负载均衡方式。为便于理解，本报告的大部分内容将所有遭入侵设备统称为"单一设备"。

据信，行为者自2022年4月起利用已公开的漏洞，在遭入侵设备上部署了Web Shell。据评估，该攻击团体的威胁行为者已在该设备上获得了权限提升。由于日志记录不足，ASD's ACSC无法确定该活动的全部范围。然而，设备上的证据表明，行为者已完成以下操作：

- 收集数百个真实有效的用户名和密码组合；以及
- 收集可能允许恶意行为者以合法用户身份访问虚拟桌面基础设施（VDI）会话的技术数据。

ASD's ACSC评估认为，行为者可能曾试图进一步入侵该组织的网络。行为者外传的数据可能使其能够以合法用户身份（甚至以其选择的用户身份，包括管理员身份）劫持或发起虚拟桌面会话。行为者可能利用该访问路径进一步入侵该组织的服务，以实现持续性及其他目标。

该组织在托管服务供应商管理环境中的其他设备未发现遭入侵的证据。

访问权

遭入侵设备所在主机通过Active Directory 与 Web 服务器为连接虚拟桌面基础设施（VDI）会话的用户提供身份验证（T1021.001）。

地点	遭入侵设备主机名称（负载均衡）
数据中心1	主机1（HOST1）、主机2（HOST2）、主机3（HOST3）

该设备基础架构还包括访问网关主机，在用户获取并下载由设备生成的身份验证令牌后，为其提供通往VDI的隧道连接。

没有任何证据表明这些主机遭到入侵。然而，访问网关主机的日志显示与已知恶意 IP 地址存在大量交互。这些交互可能反映了该主机上发生的活动，或与威胁行为者基础设施的网络连接已延伸至该主机。现有证据无法确定该活动的性质，但表明了该攻击团体试图在该组织网络中实施横向移动（TA0008）。

内部主机

ASD's ACSC对该组织内部网络区域的有限数据进行了调查。已知影响该组织内部网络区域的未遂或既遂恶意活动包括：行为者访问VDI相关数据、抓取内部 SQL 服务器（T1505.001）、以及观察到来自已知恶意 IP 地址通过访问网关设备（TA0011）的不明流量。

攻击团体利用对遭入侵设备的访问权限，收集了真实有效的用户名、密码（T1003）、以及多因素认证（MFA）令牌值（T1111）。攻击团体还收集了用于创建虚拟桌面登录会话的JSON Web

Token (JWT) (T1528)。攻击团体可能利用这些伪证创建或劫持虚拟桌面会话(T1563.002),以合法用户身份访问组织的内部网络区域(T1078)。

此外,行为者还利用对遭入侵设备的访问权限抓取了位于组织内部网络中的 SQL 服务器(T1505.001)的数据。行为者很可能已经访问过这些数据。

访问网关主机提供的证据表明,该设备与已知恶意IP地址之间存在网络流量。如上所述,这可能表明恶意网络行为者已影响或利用该设备,并可能将其作为入侵内部网络的途径。

调查时间表

以下列表为调查中发现的关键活动的时间表。

时间	事件
2022年4月	已知恶意 IP 地址与访问网关主机HOST7发生交互。交互性质无法确定。
2022年4月	所有主机(HOST1、HOST2和HOST3)均遭恶意行为者入侵,并被植入 Web Shell。 在 HOST2 上创建或修改了一个日志文件。该文件包含可能由恶意行为者捕获的凭证材料。 HOST1和HOST3上的/etc/security/opasswd和/etc/shadow文件均被修改,表明密码已被更改。HOST1 上的证据表明,用户"sshuser"的密码已被更改。
2022年4月	该组织已将HOST2关闭。 在 HOST1 和 HOST3 上创建了额外的 Web Shell (T1505.003)。HOST1 遭受了来自 HOST3 的 SSH 暴力破解尝试。 HOST3 上的一个日志文件被修改 (T1070)。该文件包含可能由恶意行为者捕获的凭证材料 (T1078)。 JWT被捕获 (T1528) 并输出到 HOST3 上的一个文件中。 该组织将HOST3关闭。此后的所有活动均发生在 HOST1 上。
2022年4月	在 HOST1 (T1505.003)上创建了额外的Web Shell。JWT被捕获并输出到 HOST1 上的一个文件中。
2022年4月	在 HOST1 (T1505.003)上创建了额外的Web Shell,并且已知的恶意IP地址与主机 (TA0011) 发生交互。 已知恶意IP地址与访问网关主机HOST7发生交互。
2022年5月	已知恶意IP地址与访问网关主机HOST7 (TA0011) 发生交互。 在 HOST1 的日志中,某用户的身份验证事件与一个已知的恶意IP地址相关联。该主机上还创建了一个额外的 Web Shell (T1505.003)。
2022年5月	HOST1上的一个脚本被行为者修改(T1543)。该脚本包含从内部 SQL 服务器抓取数据的功能。
2022年5月	HOST1上的一个附加日志文件被修改 (T1070)。该文件包含该组织网络的用户名与密码组合,且被认为是真实有效的 (T1078)。
2022年5月	一个附加日志文件被修改 (T1070)。该文件包含从HOST1收集的JWT。
2022年5月	在HOST1上创建了额外的Web Shell (T1505.003)。当天,该组织向ASD's ACSC报告,发现一个创建日期为2022年4月的 Web Shell
2022年5月	在HOST1上创建了许多脚本,其中一个名为Log4jHotPatch.jar。
2022年5月	使用iptables-save命令为访问网关主机添加两个开放端口。这两个端口分别为9998和9999(T1572)。

行为者的战术与技术

以下突出说明调查过程中识别出的若干攻击战术与技术。

初始访问

T1190利用面向公众的应用程序

该团体可能利用远程访问登录与身份管理产品中的RCE、权限提升及身份验证绕过漏洞，以获取对网络的初始访问。

此种初始访问方式被认为是最为可能的，原因如下：

- 服务器在当时存在相关 CVE 漏洞；
- 已知行为者基础设施试图利用这些漏洞；以及
- 在漏洞利用尝试发生后不久即出现首个已知的内部恶意活动。

执行

T1059.004命令和脚本解释器：Unix Shell

成功利用上述漏洞的团体可能能够在受影响设备上的 Unix Shell 中运行命令。由于设备未记录这些命令，因此无法提供行为者所运行命令的完整详细信息。

持续性

T1505.003服务器软件组件：Web Shell

行为者在受影响的设备上部署了多个 Web Shell。可能有多个不同的行为者部署了Web Shell，但只有少数行为者使用这些 Web Shell开展了活动。这些Web Shell允许行为者在遭入侵设备上执行任意命令。

权限提升

T1068利用漏洞提升权限

现有证据并未描述行为者获得的权限级别。然而，行为者使用Web Shell获得的权限级别与遭入侵设备上的Web服务器相当。据信遭入侵设备上存在的漏洞可能使行为者能够获得root权限。

凭证访问

T1056.003输入捕获：Web 门户捕获

遭入侵设备上的证据显示，行为者已捕获数百组明文用户名与密码组合，这些密码组合被认为是真实有效的。这些凭证很有可能是通过对真实身份验证流程的进行某种修改而捕获的，该过程会将凭证输出至文件。

T1111多重身份验证拦截

行为者还获取了与合法登录对应的 MFA 令牌值。这些令牌值很可能是通过修改真实身份验证流程，使其将令牌值输出至文件的方式捕获的。用于存储MFA安全令牌唯一值的“密钥服务器”未发现遭入侵的证据。

T1040网络嗅探

据信，行为者通过捕获遭入侵设备上的HTTP流量来获取 JWT。有证据表明，行为者在遭入侵设备上执行了tcpdump工具，这可能是行为者获取这些JWT的方式。

T1539窃取 Web 会话 Cookie

如前所述，行为者捕获JWT，它类似于Web会话Cookie。行为者可能通过重用这些JWT来建立进一步的访问权限。

发现

T1046网络服务发现

有证据表明，行为者在遭入侵设备上执行了网络扫描工具nmap，以扫描同一网络区域中的其他设备。行为者可能利用该工具来发现其他可访问的网络服务，从而寻找横向移动的机会。

收集

现有证据未能揭示行为者如何收集数据，亦无法明确其从遭入侵设备或其他系统中具体收集了哪些信息。然而，行为者很可能已访问遭入侵设备上的全部文件，包括捕获的凭证（T1003）、MFA令牌值（T1111）以及上述JWT。

命令与控制

T1071.001应用层协议：Web协议

行为者使用 Web Shell 实现命令与控制。Web Shell命令可能通过设备上现有的Web服务器，以HTTPS协议传输(T1572)。

T1001.003数据混淆：协议伪装

行为者利用遭入侵设备作为攻击跳板，发起旨在与合法流量混淆的攻击活动。

检测与缓解建议

ASD's ACSC强烈建议实施 ASD 的 "基本八项"(Essential Eight)控制措施及相关的"网络安全事件缓解策略"(Strategies to Mitigate Cyber Security Incidents)。以下为建议采取的网络安全措施,用于检测并防止 APT40 的入侵行为,随后将列出表格1中总结的四项关键TTP(战术、技术与程序)的具体缓解措施。

检测

上述部分文件被投放至C:\Users\Public* 和C:\Windows\Temp*等位置。这些位置通常具有全局可写权限,即所有已注册的Windows用户账户均可访问这些目录及其子目录。通常,任何用户随后均可访问这些文件,从而为横向移动、防御规避、低权限执行以及数据外传的预部署操作等提供了机会。

以下Sigma规则可用于检测来自可疑位置的执行,以作为异常活动的指标。在所有情况下,仍需进一步调查以确认恶意行为及归因。

标题:全局可写执行检测—— Temp(临时目录)

ID: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

描述:检测从C:\Windows\Temp目录发起的进程执行。

背景:

本规则专门用于识别从 C:\Windows\Temp* 目录发起的执行。由于 Temp 目录更广泛地为合法应用程序所用,因此作为恶意活动指标,其置信度比从其他 C:\Windows中的全局可写子目录发起的执行更低。

若排除由系统(SYSTEM)或网络服务(NETWORK SERVICE)用户执行的应用程序,可显著减少该规则所选择的合法活动数量。

这意味着该规则可能无法检测到更高权限级别(如 SYSTEM)的恶意执行,因此建议使用其他规则来判断用户是否试图将权限提升至 SYSTEM。

调查:

1. 检查与该文件执行直接相关的信息,例如用户上下文、执行完整性级别、即时后续活动及该文件加载的图像。
2. 调查主机上的上下文进程、网络、文件及其他辅助数据,以帮助评估活动是否恶意。
3. 如有必要,尝试收集该文件副本以进行逆向工程分析,从而判断其是否合法。

参考文献:

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

作者: ASD's ACSC

日期: 2024年6月19日

状态:实验性

标签:

- tlp.green
- classification.au.official
- attack.execution

日志来源:

```
category: process_creation
product: windows
```

检测:

```
临时目录(temp):
    Image|startswith:'C:\\Windows\\Temp\\'
common_temp_path:
    Image|re|ignorecase:'C:\\Windows\\Temp\\\
    {[a-fA-F0-9]{8}-([a-fA-F0-9]{4}-){3}[a-fA-F0-9]
    {12}\}\\'
system_user:
    用户(User):
    - 'SYSTEM'
    - 'NETWORK SERVICE'
```

dismhost:

Image|endswith: 'dismhost.exe'

known_parent:

ParentImage|endswith:

- '\\esif_uf.exe'
- '\\vmtoolsd.exe'
- '\\cwainstaller.exe'
- '\\trolleyexpress.exe'

条件(condition):temp and not (common_temp_path or system_user or dismhost or known_parent)

误报:

- 已观察到允许列表中的审计类应用程序从 Temp 目录运行可执行文件。
- Temp 目录会存在一系列合法的安装应用程序与启动器,因此在部署该规则之前,不妨考虑此类行为在受监控网络中的普遍性(并考虑是否可将其加入允许列表)。

级别:低

标题:全局可写执行-非临时系统子目录

ID:5b187157-e892-4fc9-84fc-aa48aff9f997

描述:检测从 Windows 操作系统安装路径的子目录中全局可写位置发起的进程执行。

背景:

本规则专门用于识别从 C:\ 目录下,尤其是 C:\Windows* 路径中的全局可写目录发起的执行。其中排除了 C:\Windows\Temp 目录(因为该目录被大量合法应用程序使用,因此作为恶意活动指标的置信度较低)。

如果文件以 SYSTEM 身份运行,则 AppData 文件夹将被排除在外——这是许多临时应用程序文件的一种良性执行方式。

在完成初始网络基线评估并识别出从这些位置发出的已知合法执行后,该规则应极少触发。

调查:

1. 检查与该文件执行直接相关的信息,例如用户上下文、执行完整性级别、即时后续活动及该文件加载的图像。
2. 同时调查主机上的上下文进程、网络、文件及其他辅助数据,以帮助评估活动是否恶意。
3. 如有必要,尝试收集该文件副本以进行逆向工程分析,从而判断其是否合法。

参考文献

https://gist.github.com/mattifestation/5f9de750470c9e0e1f9c9c33f0ec3e56

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

作者:ASD's ACSC

日期:2024年6月19日
状态:实验性

标签:

- tlp.green
- classification.au.official
- attack.execution

日志来源:

类别:process_creation
产品:windows

检测:

writable_path:

Image|contains:

- ':\\$Recycle.Bin\\'
- ':\\AMD\\Temp\\'
- ':\\Intel\\'
- ':\\PerfLogs\\'
- ':\\Windows\\addins\\'
- ':\\Windows\\appcompat\\'
- ':\\Windows\\apppatch\\'
- ':\\Windows\\AppReadiness\\'
- ':\\Windows\\bcastdvr\\'
- ':\\Windows\\Boot\\'
- ':\\Windows\\Branding\\'
- ':\\Windows\\CbsTemp\\'
- ':\\Windows\\Containers\\'
- ':\\Windows\\csc\\'
- ':\\Windows\\Cursors\\'
- ':\\Windows\\debug\\'
- ':\\Windows\\diagnostics\\'
- ':\\Windows\\DigitalLocker\\'
- ':\\Windows\\dot3svc\\'
- ':\\Windows\\en-US\\'
- ':\\Windows\\Fonts\\'
- ':\\Windows\\Globalization\\'
- ':\\Windows\\Help\\'
- ':\\Windows\\IdentityCRL\\'
- ':\\Windows\\IME\\'
- ':\\Windows\\ImmersiveControlPanel\\'

- ':\\Windows\\INF\\'
- ':\\Windows\\intel\\'
- ':\\Windows\\L2Schemas\\'
- ':\\Windows\\LiveKernelReports\\'
- ':\\Windows\\Logs\\'
- ':\\Windows\\media\\'
- ':\\Windows\\Migration\\'
- ':\\Windows\\ModemLogs\\'
- ':\\Windows\\ms\\'
- ':\\Windows\\OCR\\'
- ':\\Windows\\panther\\'
- ':\\Windows\\Performance\\'
- ':\\Windows\\PLA\\'
- ':\\Windows\\PolicyDefinitions\\'
- ':\\Windows\\Prefetch\\'
- ':\\Windows\\PrintDialog\\'
- ':\\Windows\\Provisioning\\'
- ':\\Windows\\Registration\\CRMLog\\'
- ':\\Windows\\RemotePackages\\'
- ':\\Windows\\rescache\\'
- ':\\Windows\\Resources\\'
- ':\\Windows\\SchCache\\'
- ':\\Windows\\schemas\\'
- ':\\Windows\\security\\'
- ':\\Windows\\ServiceState\\'
- ':\\Windows\\servicing\\'
- ':\\Windows\\Setup\\'
- ':\\Windows\\ShellComponents\\'
- ':\\Windows\\ShellExperiences\\'
- ':\\Windows\\SKB\\'
- ':\\Windows\\TAPI\\'
- ':\\Windows\\Tasks\\'
- ':\\Windows\\TextInput\\'
- ':\\Windows\\tracing\\'
- ':\\Windows\\Vss\\'
- ':\\Windows\\WaaS\\'
- ':\\Windows\\Web\\'
- ':\\Windows\\wlansvc\\'
- ':\\Windows\\System32\\Com\\dmp\\'
- ':\\Windows\\System32\\FxsTmp\\'
- ':\\Windows\\System32\\Microsoft\\Crypto\\RSA\\MachineKeys\\'
- ':\\Windows\\System32\\Speech\\'
- ':\\Windows\\System32\\spool\\drivers\\color\\'
- ':\\Windows\\System32\\spool\\PRINTERS\\'
- ':\\Windows\\System32\\spool\\SERVERS\\'
- ':\\Windows\\System32\\Tasks_Migrated\\Microsoft\\Windows\\PLA\\System\\'
- ':\\Windows\\System32\\Tasks\\'
- ':\\Windows\\SysWOW64\\Com\\dmp\\'
- ':\\Windows\\SysWOW64\\FxsTmp\\'
- ':\\Windows\\SysWOW64\\Tasks\\'

应用程序数据(appdata):

Image|contains: '\\AppData\\'
用户(User):'SYSTEM'

条件(condition): writable_path and not appdata

误报:

已观察到允许列表审计应用程序从这些目录运行可执行文件。

受监控环境中使用的一些脚本和管理工具可能位于这些目录之一,应逐案处理。

级别: 高

标题:全局可写执行 - 用户

ID: 6dda3843-182a-4214-9263-925a80b4c634

描述:检测来自 C:\Users\Public* 以及 Users 目录中其他全局可写文件夹的进程执行。

背景:

如果文件以 SYSTEM 身份运行,则 AppData 文件夹将被排除在外——这是许多临时应用程序文件的一种良性执行方式。

调查:

1. 检查与此文件执行直接相关的信息,例如用户上下文、执行完整性级别、即时后续活动以及该文件加载的图像。
2. 调查主机上的上下文进程、网络、文件和其他支持数据,以帮助评估活动是否恶意。
3. 如有必要,尝试收集该文件副本以进行逆向工程分析,从而判断其是否合法。

参考文献:

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

作者:ASD's ACSC

日期:2024年6月19日

状态: 实验性

标签:

- tlp.green
- classification.au.official
- attack.execution

日志来源:

类别: process_creation
产品: windows

检测：

用户：

Image|contains:

- ':\\Users\\All Users\\'
- ':\\Users\\Contacts\\'
- ':\\Users\\Default\\'
- ':\\Users\\Public\\'
- ':\\Users\\Searches\\'

应用程序数据：

Image|contains: '\\AppData\\'
用户：'SYSTEM'

条件：用户且非应用程序数据

误报：

– 受监控环境中使用的脚本和管理工具可能位于 Public 目录或其子目录中，应逐案处理。

级别： 中

缓解措施

日志记录

在ASD's ACSC的调查中，一个常见问题是，在包括 Web 服务器请求日志、Windows 事件日志和互联网代理日志的多个领域，均缺乏全面和历史性的日志信息，这降低了调查工作的有效性和速度。

ASD's ACSC建议审查并实施其关于《Windows 事件日志记录和转发的指南》(Windows Event Logging and Forwarding)，包括《Windows 事件日志记录存储库》(Windows Event Logging Repository)中的配置文件和脚本，以及《信息安全手册》(Information Security Manual)中的《系统监控指南》(Guidelines for System Monitoring)，以实现日志集中化并在适当期限内保留日志。

补丁管理

及时为所有暴露在互联网上的设备和服务，包括 Web 服务器、Web 应用程序和远程访问网关打补丁。考虑实施集中式补丁管理系统，以实现该流程的自动化与提速。ASD's ACSC建议实施《信息安全手册》(ISM)中的《系统管理指南》(Guidelines for System Management)，特别是适用的系统补丁控制措施。

恶意行为者利用的大多数漏洞都是公开的，并且有可用的补丁或缓解措施。组织应确保48小时内将安全补丁或缓解措施应用于面向互联网的基础设施，并在可能的情况下，使用最新版本的软件和操作系统。

网络分段

网络分段可以显著增加对手定位和获得访问组织敏感数据权限的难度。对网络进行分段，通过拒绝计算机之间的流量（除非必要）来限制或阻止横向移动。Active Directory和其他身份验证服务器等重要服务器应只能从数量有限的中间服务器或"跳板服务器"进行管理。这些服务器应受到严密监控，严格保护，并对于哪些用户和设备可以连接到它们做出限制。

无论是否检测到横向移动被阻止的实例，额外的网络分段都可以进一步限制行为者可访问和提取的数据量。

额外缓解措施

编制机构还建议采取以下缓解措施，以应对APT40 和其他组织使用以下TTP 。

- 禁用未使用或不必要的网络服务、端口和协议。
- 使用经过良好调校的 Web 应用程序防火墙 (WAF) 来保护 Web 服务器和应用程序。
- 强制执行最小权限原则，以限制对服务器、文件共享和其他资源的访问。
- 使用多重身份验证 (MFA) 和受管理的服务账户，使凭据更难被破解和重复使用。MFA 应被应用于所有可从互联网访问的远程访问服务，包括：
  - 基于 Web 和云的电子邮件
  - 协作平台
  - 虚拟专用网络连接
  - 远程桌面服务
- 更换生命周期终点设备。

表1：缓解策略/技术

TTP	基本八项缓解策略	ISM控制
初始访问 T1190 利用面向公众的应用程序	为应用程序打补丁 为操作系统打补丁 多重身份验证 应用程序控制	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
执行 T1059 命令与脚本编译器	应用程序控制 限制Microsoft Office宏 限制管理员权限	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
持久性 T1505.003 服务器软件组件Web Shell	应用程序控制 限制管理员权限	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
初始访问/权限提升/持续性 T1078 有效账户	为操作系统打补丁 多重身份验证 限制管理员权限 应用程序控制 用户应用程序强化	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

有关更多通用检测和缓解建议，请查阅本公告末尾 MITRE ATT&CK技术网页上的缓解措施和检测部分，该部分列明了MITRE ATT&CK 摘要中识别的每项技术。

免责声明

本报告中的信息“按现状”提供，仅供参考。本公告编制机构不对任何商业实体、产品、公司或服务表示认可，包括本文件链接中的任何商业实体、产品、公司或服务。任何通过服务标志、商标、制造商或其他方式提及特定商业实体、产品、流程或服务，均不构成或暗示编制机构的认可、推荐或偏袒。

本文档标记为 TLP:CLEAR。披露不受限制。来源可根据适用的公开规则和程序，在信息误用风险极小或可预见风险为零时使用 TLP:CLEAR。在符合标准版权规则的前提下，TLP:CLEAR 信息可不受限制地分发。有关红绿灯协议的更多信息，请参阅 cisa.gov/tlp

MITRE ATT&CK - 历史上值得关注的APT40攻击手法

侦察 (TA0043)	
搜索受害者拥有的网站 (T1594)	收集受害者身份信息：凭据 (T1589.001)
主动扫描：漏洞扫描 (T1595.002)	收集受害者主机信息 (T1592)
搜索公开网站/域名：搜索引擎(T1593.002)	收集受害者网络信息域名属性(T1590.001)
收集受害者身份信息：电子邮箱地址(T1589.002)	

资源开发(TA0042)	
获取基础设施：域名(T1583.001)	获取基础设施(T1583)
获取基础设施：DNS服务器(T1583.002)	入侵账户(T1586)
开发能力：代码签名证书(T1587.002)	入侵基础设施(T1584)
开发能力：数字证书(T1587.003)	开发能力：恶意软件(T1587.001)
获取能力：代码签名证书(T1588.003)	建立帐户：云账户(T1585.003)
入侵基础设施：网络设备(T1584.008)	获取能力：数字证书(T1588.004)

初始访问(TA0001)	
有效账户(T1078)	网络钓鱼(T1566)
有效账户：默认账户(T1078.001)	网络钓鱼：鱼叉式网络钓鱼附件 (T1566.001)
有效账户：域名账户(T1078.002)	网络钓鱼：鱼叉式网络钓鱼链接 (T1566.002)
外部远程服务(T1133)	利用面向公众的应用程序(T1190)
路过式入侵 (T1189)	

执行(TA0002)	
Windows 管理规范 (T1047)	命令和脚本编译器：Python (T1059.006)
计划任务/作业：At 命令 (T1053.002)	命令和脚本编译器：JavaScript (T1059.007)
计划任务/作业：计划任务(T1053.005)	本机 API (T1106)
命令和脚本编译器(T1059)	进程间通信 (T1559)

执行(TA0002)	
命令和脚本编译器：Windows Command Shell (T1059.003)	系统服务：服务执行(T1569.002)
命令和脚本编译器：PowerShell (T1059.001)	利用客户端执行 (T1203)
命令和脚本编译器：Visual Basic (T1059.005)	用户执行：恶意文件(T1204.002)
命令和脚本编译器：Unix Shell (T1059.004)	命令和脚本编译器：Apple Script (T1059.002)
计划任务/作业：Cron (T1053.003)	软件部署工具(T1072)

持续性(TA0003)	
有效账户(T1078)	服务器软件组件：Web Shell (T1505.003)
Office 应用程序启动：Office 模板宏 (T1137.001)	创建或修改系统进程：Windows 服务 (T1543.003)
计划任务/作业：At 命令 (T1053.002)	启动或登录自动启动执行：注册表运行键/启动文件夹 (T1547.001)
计划任务/作业：计划任务(T1053.005)	启动或登录自动启动执行：快捷方式修改 (T1547.009)
外部远程服务(T1133)	劫持执行流：DLL 搜索顺序劫持 (T1574.001)
计划任务/作业：Cron (T1053.003)	劫持执行流：DLL 侧加载 (T1574.002)
账户操纵(T1098)	有效账户：云账户(T1078.004)
有效账户：域名账户(T1078.002)	

权限提升 (TA0004)	
计划任务/作业：At 命令 (T1053.002)	创建或修改系统进程：Windows 服务 (T1543.003)
计划任务/作业：计划任务(T1053.005)	启动或登录自动启动执行：注册表运行键/启动文件夹 (T1547.001)
进程注入：线程执行劫持 (T1055.003)	启动或登录自动启动执行：快捷方式修改 (T1547.009)
进程注入：进程镂空(T1055.012)	劫持执行流：DLL 搜索顺序劫持 (T1574.001)

权限提升(TA0004)	
有效账户：域名账户(T1078.002)	利用权限提升 (T1068)
访问令牌操控：令牌模拟/窃取 (T1134.001)	事件触发执行：Unix Shell 配置修改 (T1546.004)
进程注入：动态链接库注入 (T1055.001)	有效账户：域名账户(T1078.002)
有效账户：本地账户(T1078.003)	

防御规避 (TA0005)	
Rootkit (T1014)	间接命令执行 (T1202)
混淆文件或信息 (T1027)	系统二进制代理执行：Mshta (T1218.005)
混淆文件或信息：软件打包 (T1027.002)	系统二进制代理执行：Regsvr32 (T1218.010)
混淆文件或信息：隐写术 (T1027.003)	颠覆信任控制：代码签名 (T1553.002)
混淆文件或信息：交付后编译 (T1027.004)	文件和目录权限修改：Linux 和 Mac 文件和目录权限修改 (T1222.002)
伪装：匹配合法名称或位置 (T1036.005)	虚拟机/沙盒规避：系统检查 (T1497.001)
进程注入：线程执行劫持 (T1055.003)	伪装 (T1036)
反射式代码加载 (T1620)	削弱防御：禁用或修改系统防火墙 (T1562.004)
进程注入：进程镂空(T1055.012)	隐藏工件：隐藏文件和目录 (T1564.001)
指标移除：文件删除 (T1070.004)	隐藏工件：隐藏窗口 (T1564.003)
指标移除：时间戳修改 (T1070.006)	劫持执行流：DLL 搜索顺序劫持 (T1574.001)
指标移除：清除 Windows 事件日志 (T1070.001)	劫持执行流：DLL 侧加载 (T1574.002)
修改注册表 (T1112)	Web 服务 (T1102)
反混淆/解码文件或信息 (T1140)	伪装：伪装任务或服务 (T1036.004)
削弱防御 (T1562)	

凭据访问 (TA0006)	
操作系统凭据转储：LSASS 内存 (T1003.001)	未受保护的凭据：文件中的凭据 (T1552.001)
操作系统凭据转储：NTDS (T1003.003)	暴力破解：密码猜测 (T1110.001)
网络嗅探 (T1040)	强制身份验证 (T1187)
从密码存储中获取凭据：钥匙串 (T1555.001)	窃取或伪造 Kerberos 票据：Kerberoasting (T1558.003)

凭据访问 (TA0006)	
输入捕获：键盘记录 (T1056.001)	多重身份验证拦截 (T1111)
窃取 Web 会话 Cookie (T1539)	窃取应用程序访问令牌 (T1528)
利用凭据访问 (T1212)	暴力破解：密码破解 (T1110.002)
输入捕获：Web 门户捕获 (T1056.003)	操作系统凭据转储：DCSync (T1003.006)
从密码存储中获取凭据(T1555)	从密码存储中获取凭据：从浏览器获取凭据 (T1555.003)

发现 (TA0007)	
系统服务发现 (T1007)	系统信息发现 (T1082)
应用程序窗口发现 (T1010)	账户发现：本地账户 (T1087.001)
查询注册表 (T1012)	系统信息发现，技术 T1082 - 企业版 | MITRE ATT&CK®
文件和目录发现 (T1083)	系统时间发现 (T1124)
网络服务发现 (T1046)	系统所有者/用户发现 (T1033)
远程系统发现 (T1018)	域名信任发现 (T1482)
账户发现：电子邮件账户 (T1087.003)	账户发现：域名账户 (T1087.002)
系统网络连接发现 (T1049)	虚拟机/沙盒规避：系统检查 (T1497.001)
进程发现 (T1057)	软件发现 (T1518)
权限组发现：域名组 (T1069.002)	网络共享发现，技术 T1135-企业版 | MITRE ATT&CK®
系统网络配置发现：互联网连接发现 (T1016.001)	

横向移动 (TA0008)	
远程服务：远程桌面协议 (T1021.001)	远程服务 (T1021)
远程服务：SMB/Windows 管理共享 (T1021.002)	使用替代身份验证材料：票据传递 (T1550.003)
远程服务：Windows 远程管理 (T1021.006)	横向工具传输 (T1570)

收集 (TA0009)	
来自本地系统的数据 (T1005)	归档收集数据：通过库归档 (T1560.002)
来自网络共享驱动器的数据 (T1039)	电子邮件收集：远程电子邮件收集 (T1114.002)

收集 (TA0009)	
输入捕获：键盘记录 (T1056.001)	剪贴板数据 (T1115)
自动化收集 (T1119)	来自信息存储库的数据 (T1213)
输入捕获：Web 门户捕获 (T1056.003)	数据暂存：远程数据暂存 (T1074.002)
数据暂存：本地数据暂存 (T1074.001)	归档收集数据 (T1560)
电子邮件收集 (T1114)	

数据外传 (TA0010)	
通过 C2 信道外传 (T1041)	通过替代协议外传：通过非对称加密的非 C2 协议外传 (T1048.002)
通过替代协议外传 (T1048)	通过 Web 服务外传：外传到云存储 (T1567.002)

命令与控制 (TA0011)	
数据混淆：协议伪装 (T1001.003)	Web 服务：固定情报解析器 (Dead Drop Resolver) (T1102.001)
常用端口 (T1043)	Web 服务：单向通信 (T1102.003)
应用层协议：Web 协议 (T1071.001)	入口工具转移 (T1105)
应用层协议：文件传输协议 (T1071.002)	代理：内部代理 (T1090.001)
代理：外部代理 (T1090.002)	非标准端口 (T1571)
代理：多跳代理 (T1090.003)	协议隧道 (T1572)
Web 服务：双向通信 (T1102.002)	加密通道 (T1573)
加密通道：非对称加密 (T1573.002)	入口工具转移 (T1105)
代理，技术 T1090 - 企业版	MITRE ATT&CK®	

影响 (TA0040)	
服务停止 (T1489)	磁盘擦除 (T1561)
系统关机/重启 (T1529)	资源劫持 (T1496)

注释

免责声明

本指南中的材料具有一般性，不应被视为法律建议或在任何特定情况或紧急情况下可依赖的帮助材料。在任何重要事项上，您都应该根据自己的情况寻求恰当的独立专业建议。

对于因依赖本指南中包含的信息而导致的任何损害、损失或费用，联邦政府不承担任何责任或义务。

版权所有

国徽的使用

国徽的使用条款详见总理及内阁部网站《联邦国徽信息和指南》Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au.

如需了解更多信息或报告网络安全事件，请联系我们：

cyber.gov.au | 1300 CYBER1 (1300 292 371)

该号码仅可在澳大利亚境内拨打。

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre