精译版

# Platinum 首次利用英特尔芯片管理功能

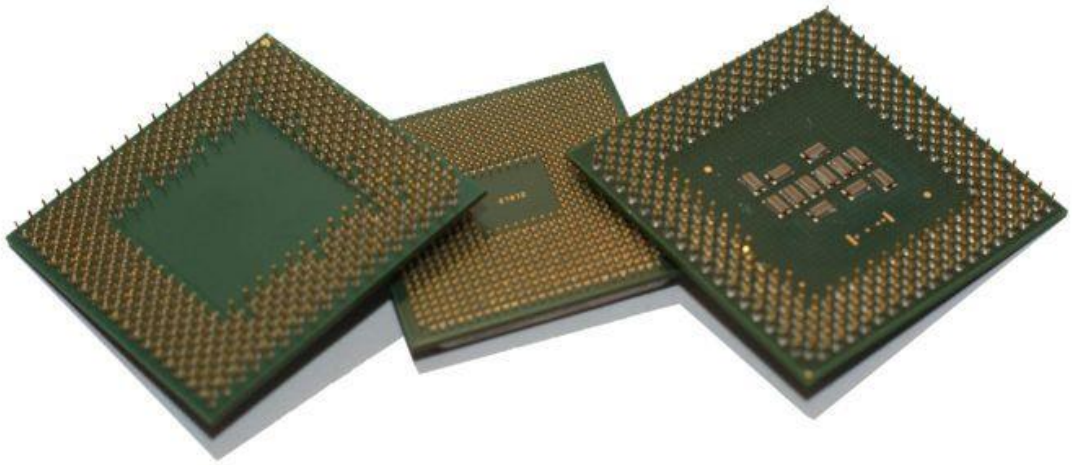
**非官方中文译文·安天技术公益翻译组 译注**

| 文档信息 | | | |
|---|---|---|---|
| 原文名称 | Platinum APT First to Abuse Intel Chip Management Feature | | |
| 原文作者 | Michael Mimoso | 原文发布日期 | 2017 年 6 月 9 日 |
| 作者简介 | Michael Mimoso 是 Threatpost 的编辑。https://www.linkedin.com/in/michaelmimoso/ | | |
| 原文发布单位 | Threatpost | | |
| 原文出处 | https://threatpost.com/platinum-apt-first-to-abuse-intel-chip-management-feature/126166/ | | |
| 译者 | 安天技术公益翻译组 | 校对者 | 安天技术公益翻译组 |
| 分享地址 | 请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块 | | |
| 免责声明 | • 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。<br>• 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。<br>• 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。<br>• 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。 | | |

# Platinum 首次利用英特尔芯片管理功能

Michael Mimoso

2017 年 6 月 9 日



在东南亚运作的 Platinum APT 组织利用英特尔芯片的功能，将恶意软件和漏洞加载到受感染的机器上。

上周四，微软发布了对 Platinum 组织的最新研究报告，该组织热衷于使用以前未开发的资源攻击计算机并规避检测。

在 2016 年 4 月，微软介绍了 Platinum 如何利用 Windows Server 2003（Windows 8 已经将其删除）引入的热补丁（hotpatching）功能，以便在运行的进程中注入恶意代码。Platinum 的目标主要是战略性的，包括政府机构、国防承包商和情报机构，以及电信等关键行业。

微软表示，Platinum 的一个文件传输工具能够利用英特尔主动管理技术（AMT），特别是其串行 LAN（Serial-over-LAN，简称 SOL）通信通道，在目标机器上运行恶意代码。微软和英特尔表示，这是 APT 组织首次以这种方式利用芯片组。

微软表示："该通道独立于操作系统，通过其上的任何通信不会被主机设备上运行的防

火墙和网络监控程序发现。在该事件之前，我们没有发现任何恶意软件利用 AMT SOL 功能进行通信。”

微软将调查结果告知了英特尔。两家公司表示，这不是 AMT 的漏洞，而是属于其功能的滥用。巧合的是，他们在 5 月初披露了一个严重的 AMT 提权漏洞，该漏洞允许攻击者远程访问和完全控制受感染的机器，但它与该事件无关。

微软在报告中表示，它仅在少数机器上发现了文件传输工具。

微软表示，该攻击有先决条件：因为 AMT 是默认关闭的，因此攻击者需要获得管理员权限。

微软表示：“目前尚不清楚，Platinum 能否配置工作站来使用其功能，或者搭载以前启用的工作站管理功能。无论哪种情况，在利用功能之前，Platinum 都需要在目标系统上获得管理员权限。”

AMT 功能存在于 Intel vPro 处理器和芯片上，用于远程管理。SOL 通过 TCP 公开一个虚拟串行设备，并独立于主机服务器上运行的操作系统和网络。只要主机设备以物理方式连接到网络，AMT 和 SOL 就能够利用英特尔管理引擎的网络堆栈进行通信。因为它绕过主机服务器的网络堆栈，因此不会被主机上的防火墙阻止。主机不会发现任何恶意流量，服务器上运行的任何杀毒软件或入侵检测软件也不会。

微软表示，Platinum 自 2009 年以来一直在亚洲活跃，并非常谨慎地保密其攻击工具，包括零日漏洞。

一年多前，研究人员披露 Platinum 利用 Windows 热补丁功能。他们利用该功能，将恶意代码注入到运行的进程中，而无需重启受感染的服务器。像 SOL 一样，热补丁功能需要管理员权限，这意味着攻击者必须首先感染机器。

与许多其他 APT 组织一样，该组织利用网络钓鱼活动在网络上创建据点。Platinum 使用受感染的 Office 文档 利用未修复和已知的漏洞将后门程序和其他代码安装到受感染的机器上。