APT32组织针对我国关基单位攻击活动分析

原创 伏影实验室 绿盟科技威胁情报 2022-08-06 10:00 发表于北京

一 事件背景

2022年5月，绿盟科技伏影实验室与运营能力中心梅花K战队共同于国家某关基单位发现异常外联IP，通过攻击活动中捕获的攻击流量分析，确认此次攻击活动是由境外APT组织APT32所发起。

绿盟科技伏影实验室与运营能力中心梅花K战队利用主机行为监控技术对攻击者攻击活动进行了全周期监控，并对其攻击活动进行阻断。在监控过程中，观察到攻击者活动持续至7月中下旬，时间长达2个月。攻击者针对关基单位负责重点课题的研究员发起APT定向攻击，瞄准文档类资料进行窃取，以窃取机密资料和重要文件为目标。如攻击者窃取成功，将造成严重损失。

通过流量分析，发现国内某核心制造业厂商也同样遭受该组织攻击，并持续处于活跃状态，经过处置，已成功阻断该组织攻击活动。

二 影响范围

在此次事件中，APT32组织选择了RemyRAT远程控制木马作为后门程序植入了国家关基单位，通过分析，此木马具备以下TTP：

Domain	ID		Name	Use
Enterprise	T1070	0.004	文件删除	从文件系统删除文件
Enterprise	T1095		基于 TCP 的 C&C 自定义通讯协议	利用 TCP 的私有通讯协议与 C&C 交互
Enterprise	T1012		查询注册表	查询注册表信息
Enterprise	T1082		系统信息查询	获取计算机名称
Enterprise	T1033		系统账户查询	获取计算机用户名
Enterprise	T1543		进程创建	执行新的恶意程序
Enterprise	T1046		网络服务发现	网络扫描，搜索开放端口、服务

表2.1 海莲花RemyRAT所使用技战术

通过RemyRAT的TTP能力实现，我们可以得出攻击者或具备以下意图：

1. 攻击者可以向受害者主机进一步投递恶意程序。在本次事件中，受害者为国家某关基单位研究员，APT32组织或靶向投递窃密程序以获取关键研究资料及技术成果，从而造成不可挽回的战略损失。

2. 通过进一步分析，发现某核心制造业厂商也遭受攻击，攻击者可能窃取生产资料、设计图纸等工业生产相关的机密信息，造成我国工业制造业核心技术泄露。

3. 攻击者能够通过失陷主机发起网络扫描以确定网络环境及资产分布。

4. 攻击者能够通过已探测网络拓扑，投递脆弱性嗅探程序，以攻陷更多的内网设备。

三 APT32组织简介

APT32组织，或称为海莲花、OceanLotus、SeaLotus、Cobalt Kitty、APT-C-00，是一个活跃于越南的攻击组织。该组织最早在2015年被发现，在2017年之后进入活跃期至今。一般认为，海莲花组织的主要目标为越南及相邻国家的政企工作人员，主要目的为窃取政府与商业情报，中国是该组织的主要攻击国家之一。

种种迹象表明，海莲花是一个多人分工合作的高效组织，该组织不断更新完善自己的攻击链条，并不断开发新的攻击方式和工具。目前，ATT&CK攻击矩阵显示海莲花使用的攻击工具超过10种，使用的攻击技术超过50种。

海莲花组织在突破边界并在内网中建立立足点后惯用Cobalt Strike进行横向移动。并通过Cobalt Strike扫描内网中存在的各类漏洞和配置问题，利用扫描结果进一步控制其它主机。最终窃取包括商业机密、机密谈话日志和进度计划等在内的各种资料，严重威胁制造、媒体、银行、酒店和基础设施的网络安全。

在后门植入方面，海莲花组织有着成熟应用且自主开发的后门，如DenisRAT，RemyRAT，SplinterRAT等。这些后门程序功能完备，一旦被植入，攻击者便可完全控制失陷主机。

RemyRAT在本次关基单位应急事件中被发现，作为海莲花组织的专有工具，屡次被用于后门植入，以完成下载执行，文件操作，端口扫描等功能。

四 攻击事件定性

通过流量还原技术，观察受害者IP与C&C的交互，发现出现单字节传输，通讯协议相似，固定长度心跳，上线交互一致等特征，通过与伏影实验室针对海莲花APT组织工具复盘特征的比对，将此流量定性为海莲花远程控制工具RemyRAT所产生。

- **归因依据-握手交互**

受控端发送02，控制端反馈03。与RemyRAT握手方式完全一致。

图 4.1 RemyRAT与C&C握手过程

- **归因依据-协议构成**

在交互流量存在单字节交互特征的前提下，我们也观察到其信息构成存在以下格式：

图 4.2 应急事件中RemyRAT上线信息结构

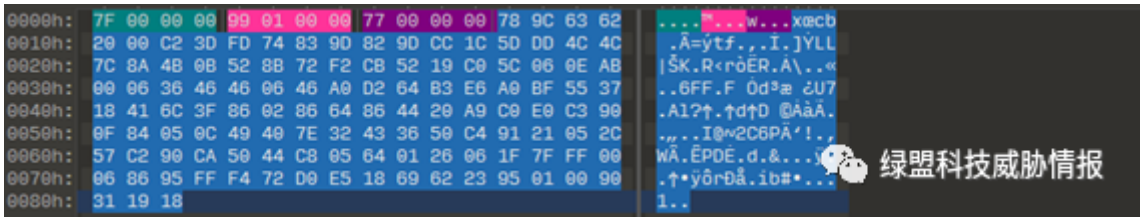

图4.3 伏影实验室海莲花复盘RemyRAT上线信息结构

通过以上可以看出，流量特征异曲同工。即为：

stream_size(4 bytes) + decompressed_data_size(4 bytes) + compressed_data_size(4 byets) + compressed_data(depends on compressed_data_size)

- **归因依据-固定心跳**

受害者与C&C存在固定长度及内容的心跳交互。心跳长度为8字节，且内容皆为00。

图 4.4 RemyRAT发送恒定心跳信息

- **归因依据-上线交互**

受害者会发出4字节长度，该长度代表即将发送的流长度，下一流将携带上线信息。

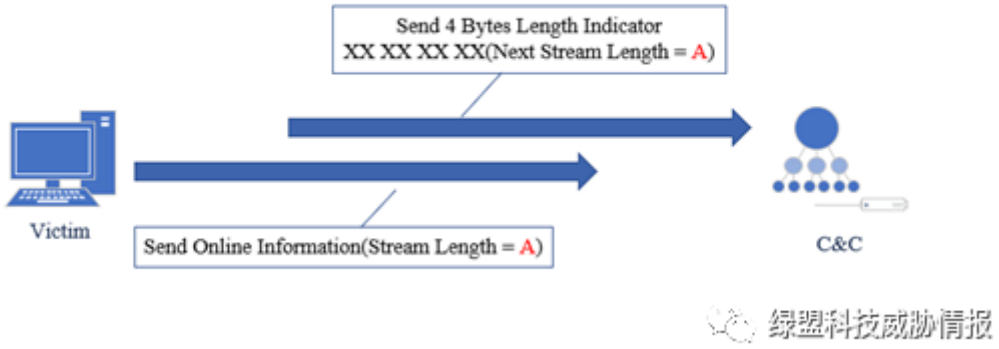

图 4.5 RemyRAT预上线交互

综上，根据握手交互，协议构成，固定心跳，上线交互特征的一致性，我们将此流量判定为RemyRAT所产生。

五 研判总结

APT32海莲花组织作为有国家背景支持的顶尖黑客团伙，在进入2019年后频繁攻击东南亚范围内的各类目标，后续针对中国境内的攻击活动扩展到几乎所有重要机构，包括政府部门、科研院所、境内高校，海事机构、海域建设、航运企业和金融投资机构。经研判分析，海莲花组织的攻击方式多样，攻击链条复杂，但使用的核心攻击技术与最终木马载荷较为固定。除此，海莲花组织会积极尝试使用各类热门漏洞和攻击技术，但多数未形成规模，只有最稳定且少数的攻击链实现了持久化。因此，鱼叉攻击、社工攻击、水坑攻击仍然是海莲花

组织最为成熟及有效的初始入侵手段。绿盟科技于2022年多起关基单位及核心制造业应急事件中发现，海莲花团伙攻击目标逐渐向科研机构，车辆制造及众多高新企业倾斜。其攻击意图逐渐由占领并监听上升为核心技术获取。因此，在未来一段时间内，科研院校，拥有自主技术的企业或成为其目标，应加强防范，避免发生无可挽回的战略损失。