

[APT32]

攻击分析 报告

戎码翼龙NG-EDR **AI生成**

消耗的token数 **10200**

报告生成耗时 **3分02秒**



微信公众号
137-1769-9956



客服企业微信
kefu@rongma.com

生成时间：2024年2月9日 17:36
报告密级：内部查看



攻击概述

APT32



归属地
越南

目标国家
4（中国,柬埔寨,老挝,菲律宾）

目标行业
5（政府、科研院所、海事机构、海域建设、航运企业）

危险程度
高

受影响的主机
1台重要主机

检测时间
2024-02-08 18:18:50

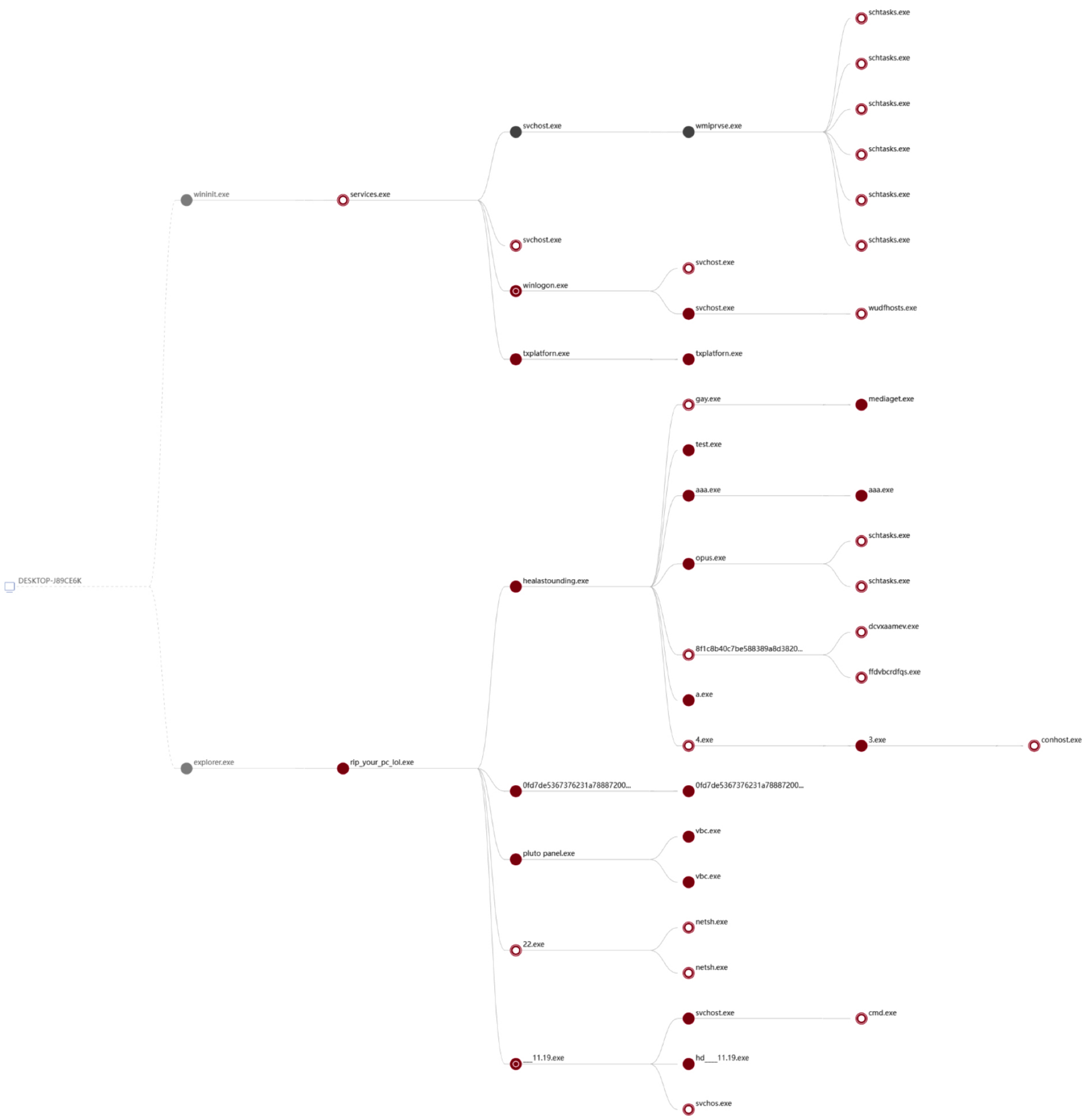
攻击复盘概述

攻击者运用了多种ATT&CK安全框架中提到的技战术，试图绕过安全防护措施，提升自身权限，并植入后门程序，企图择机运行恶意软件，通过加密文件对用户进行勒索。



攻击图谱

戎码翼龙对攻击过程进行还原，生成如下攻击图谱：



我被攻击了吗？

攻击类型

恶意软件传播

危险程度

高

检测时间

2024-02-08 18:18:50

安全GPT结论

该样本使用了多种战术和技术，试图绕过安全防护措施，提升自身权限，并植入后门程序。具体分析如下：

1. 样本利用Windows管理规范(WMI)执行程序，可能用于远程控制或信息收集。
2. 样本试图绕过用户账户控制(UAC)，以便在用户不知情的情况下执行恶意代码。
3. 样本通过进程注入技术，将恶意代码注入到正常进程中执行，以逃避安全软件的检测。
4. 样本劫持执行流程，修改进程入口点，从而控制程序的执行流程。
5. 样本利用内存代码加载技术，将恶意代码直接加载到内存中执行，避免留下文件痕迹。
6. 样本伪装成合法程序，以欺骗用户和防御系统。
7. 样本可能通过注册表设置自启动，实现持久化。
8. 样本试图禁用或修改系统防火墙，以降低系统的安全性。
9. 样本隐藏自身和相关的文件、目录，以逃避检测。
10. 样本可能窃取用户的各种凭据信息，包括浏览器凭据、密码等。
11. 样本可能通过屏幕捕获技术，窃取用户的敏感信息。
12. 样本可能利用Office应用程序的加载项功能，实现自启动。
13. 样本可能通过计划任务功能，实现定时执行。
14. 样本可能具有反虚拟机功能，以对抗虚拟化安全解决方案。
15. 样本可能具有反调试器功能，以对抗调试器分析。

综上所述，该样本具有多种恶意行为，可能是一个复杂的后门程序，目的可能是窃取用户信息、远程控制、持久化等。建议采取相应的安全措施进行防范和清除。



哪些主机受到了影响？

1台重要主机

DESKTOP-A4PH56B

主机ID
bd1af8f153e8483aa952d2f2ab15bea3

状态	重要性
在线	重要主机

最近检测时间	首次检测时间
2024-02-08 18:18:50	2024-02-08 18:18:50

操作系统版本	主机类型	互联网IP
Windows 10	Workstation	202.103.1.4

连接IP	客户端版本	用户
192.168.100.1	5.0.0.1181	UMFD-3

最近登录时间	备注
2024-02-08 18:18:50	123

攻击者
画像



是谁攻击的我？

APT32

OceanLotus,Cobalt Kitty,APT-C-00,
SeaLotus,Canvas Cyclone,BISMUTH

状态	归属地	
活跃	YUENAN	
目标国家	目标行业	
4（中国,柬埔寨,老挝,菲律宾）	5（政府、科研院所、海事机构、海域建设、航运企业）	
最后活跃日期	首次活跃日期	披露日期
2023年9月	2023年9月	2021
最后一次修改日期	攻击类型	攻击动机
2023年6月	eCrime	Criminal

APT组织描述:

该组织自2012年4月起，对中国政府、科研院所、海事机构、海域建设、航运企业等相关重要领域展开了有组织、有计划、有针对性的长时间攻击。海莲花组织除了攻击中国目标，还对柬埔寨、菲律宾、越南等东南亚国家目标实施攻击活动，其拥有一套功能完备的恶意代码，并结合商业工具实施攻击。2014年2月以后，海莲花组织进入攻击活跃期，并于2014年5月发动了最大规模的一轮鱼叉攻击，大量受害者因打开带毒的邮件附件而感染特种木马。一直至今该组织针对中国境内的攻击活动依然存在。

命中的情报:

HASH:
6C5C2692597B5BB0F2ECEE9C9F667134
DOMAIN:
VIDEO.CNHARDWARE.INFO
IP:
81.95.7.12
URL:
DLOAD01.S3.AMAZONAWS.COM/B89FDBF4-9F80-11E7-ABC4-2209CEC278B6B50A/
FIREFOXINSTALLER.EXE

攻击者怎么进来的？

ATT&CK-全景图

ATT&CK 技战术总结



- TA0002
 - T1204--用户执行
 - T1204.002-恶意文件
- TA0005
 - T1620---内存代码加载
- TA0011
 - T1071---应用层协议
 - T1071.001-Web 协议
- TA0004
 - T1548--滥用权限提升控制机制
 - T1548.002-绕过用户账户控制
- TA0005
 - T1548--滥用权限提升控制机制
 - T1548.002-绕过用户账户控制
- TA0002
 - T1106--通过本机API执行
- TA0010
 - T1041--通过C2通道的数据泄露
- TA0005
 - T1112---修改注册表
- TA0007
 - T1057--进程发现

事件中DNS活动情况（Top5）

osuyet.net

事件中网络活动情况（Top5）

164.155.255.240

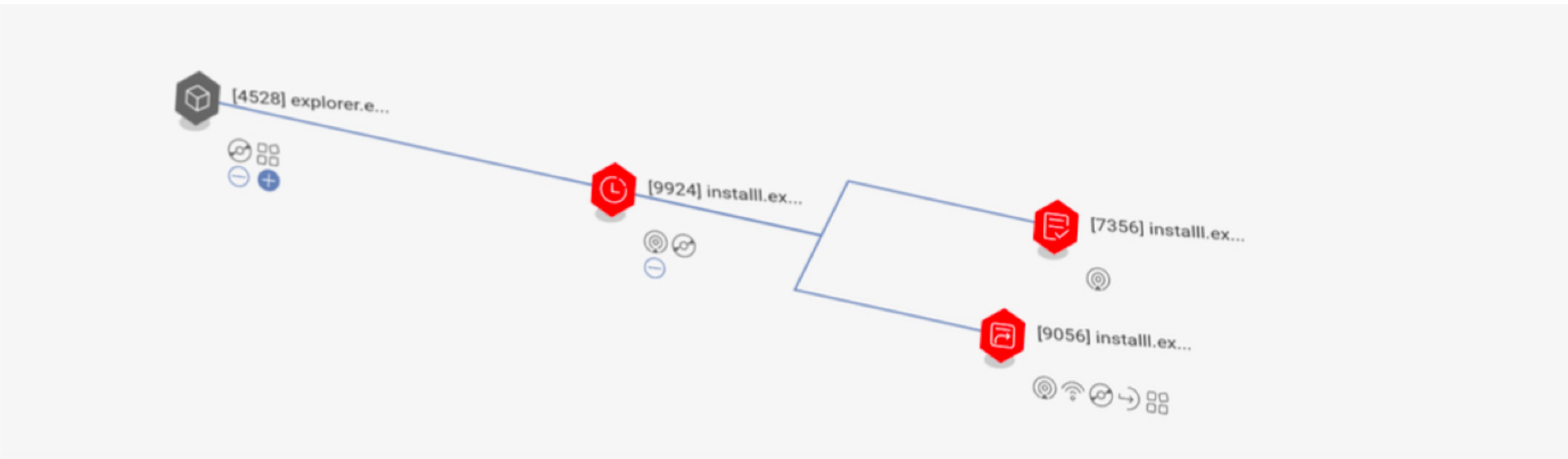
事件中进程的SHA1（Top5）

9E7FD3D5F6395B7B906DEE094BC09D1B69BAF9D17ED61C518F8CFF19D4A6A0F0DEB560537A4298
--

攻击溯源

攻击者是怎么进来的？（续）

- 攻击过程-进程链



攻击过程分析概要

该样本的进程链分析显示，攻击事件始于explorer.exe进程，该进程为Windows资源管理器，通常由用户手动启动。在此基础上，explorer.exe进程启动了名为test.exe的子进程，test.exe进一步执行了 4plo5w.exe。根据威胁分析，4plo5w.exe具有内存代码加载的行为，表明该样本采用了内存驻留技术以逃避检测。此外，test.exe与Web协议相关的命令和控制通信，表明该样本可能通过Web渠道接收攻击者的指令。综合分析，威胁来源可能为用户在不知情的情况下手动启动了恶意软件，导致整个攻击事件的发生。

告警中DNS活动情况（Top5）

osuyet.net

告警中网络活动情况（Top5）

164.155.255.240

告警中进程的SHA1（Top5）

9E7FD3D5F6395B7B906DEE094BC09D1B69BAF9D17ED61C51B8F8CFF19D4A6A0F0DEB5605B37A4298
--

攻击溯源

攻击者是怎么进来的？（续）

进程基本信息

[7836] explorer.exe

进程普通信息

进程名字：explorer.exe
进程路径：C:\windows\explorer.exe
进程命令行：C:\windows\Explorer.EXE
进程MD5：4BF8CF1A2379B0054860EC220CA329B9
进程SHA1：E94FC38810C097A64F7419960F2D21052D1CB2E7
进程安全性：安全
进程产品名字：Microsoft® windows®operating system
进程公司名字：Microsoft Corporation
进程签名：Microsoft windows,Microsoft corporation, Redmond,washington,us

进程IOA命中情况（Top5）

IOA名字：疑似进程下载文件 IOA描述：对手可能会通过现有的命令和控制（C2）通道窃取数据。被窃取的数据会使用与C2通信相同的协议编码到常规通信通道中。 ATT&CK TID: T1041 -----
IOA名字：创建进程快照 IOA描述：对手可能会尝试获取系统上正在运行的进程信息。获取的信息可用于了解网络中系统上常见的软件/应用程序。对手可能会利用进程发现期间获取的信息来进行自动化发现，并据此调整后续行为，包括是否完全感染目标或尝试特定操作。 ATT&CK TID: T1057 -----
IOA名字：PE文件ManualMap IOA描述：对手可能会反射性地将代码加载到进程中，以隐藏恶意负载的执行。反射性加载涉及在进程内存中直接分配和执行有效载荷，而不是通过磁盘上的文件路径创建线程或进程。反射性加载的有效载荷可以是编译后的二进制文件、仅存在于RAM中的匿名文件，或是无文件可执行代码的片段（例如：位置无关的shellcode）。 ATT&CK TID: T1620 -----
IOA名字：访问恶意ip IOA描述：对手可能会利用与网页流量相关的应用层协议进行通信，以此来避免被检测或网络过滤，通过混入现有流量中来掩盖行踪。发送至远程系统的指令，以及这些指令的执行结果，通常会被嵌入到客户端与服务器之间的协议流量中。这种方式使得恶意通信看起来像是正常的网页浏览活动，从而增加隐蔽性。 ATT&CK TID: T1071.001 -----
IOA名字：创建挂起进程 IOA描述：对手可能会与操作系统（OS）的本地应用程序编程接口（API）交互以执行各种行为。本地API提供了在内核中调用低级OS服务的一种受控方式，这些服务包括涉及硬件/设备、内存和进程等。操作系统在系统启动时（此时其他系统组件尚未初始化）以及在日常操作中执行任务和请求时，都会利用这些本地API。通过直接使用这些API，对手能够执行各种底层操作，包括隐藏活动、逃避检测、操控系统资源等，而这些操作可能较难通过传统的安全监控手段检测到。 ATT&CK TID: T1106

攻击溯源

攻击者是怎么进来的？（续）

进程网络操作（Top5）

本地IP： 192.168.220.167
远程IP： 20.24.121.134
端口： 443
网络协议： TCP

进程磁盘操作

文件读取（Top3）

C:\Program Files\rooma\rmroot\data\LICENSE.txt

C:\Users\%username%\AppData\Local\IconCache.db

新可执行文件写入（Top3）

C:\Windows\System32\drivers\rmkernel.sys

进程DNS请求

可疑的DNS请求（Top3）

暂无可疑的DNS请求

DNS请求（Top3）

域名： assets.msn.com

进程注册表操作

注册表值变更（Top3）

操作： 值新增
值名称： {e28f0235-8b2a-4b34-9e3c-7f38fd9cabf4}
注册表路径： \REGISTRY\MACHINE\BCD00000000\Description
注册表值： 0x1

操作： 值新增
值名称： {a3a94dc3-bf3c-47d1-8239-617e31a9d10b}
注册表路径：
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\BFE\Parameters\Policy\Persistent\Callout
注册表值： 0x1

操作： 值新增
值名称： {5bb254fc-9050-421a-9085-0c6a31e3bfa8}
注册表路径：
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\BFE\Parameters\Policy\Persistent\Filter
注册表值： 0x1

接下来 我该怎么办？

| 及时启动**应急预案**

应及时启动事先制定的应急预案，按照既定步骤进行细致处置。

| 隔离并及时**清理受影响主机**

首先，切断受影响主机的互联网连接及专线连接，避免在网间横向移动。
其次，严查受影响主机中的后门、木马等恶意程序，彻底清除该主机的所有恶意文件和驻留在内存中的恶意代码，确保主机中的恶意程序被彻底清理。若有必要，可重新安装操作系统并安装最新安全补丁。再次，对本次攻击涉及到的失陷账号进行密码重置，提升口令强度并启动多因素认证。

| 清理完成的**主机重新上线**

对清理完成的主机重新部署相关服务，配置相关网络，重新恢复上线。

我该如何避免再次发生？

重视安装安全补丁： 确保及时安装安全补丁和修复漏洞

建议所有操作系统、应用程序和网络设备等重要资产都及时安装安全补丁，以修复已知的漏洞和问题。

重视网络安全防护： 部署有效的网络安全检测防御产品

充分考虑边界安全、端点安全、数据安全、供应链安全等各方面，部署行之有效的检测与防御产品。选择网络安全产品时务必考察其攻防实战能力，并正确配置，避免遭受攻击时无法有效防御。

注重网管安全： 如网络分段、设置多因素认证与使用黑白名单

日常网络管理中，可将网络划分为多个隔离的区域，根据需要设置访问控制策略。这可以减少攻击者在网络中的横向移动能力。另外，设置多因素认证并强化密码和凭证管理，可以有效降低凭证被窃取的风险。使用应用程序的黑白名单机制也能有效降低攻击成功的概率。

强化员工安全意识： 培训员工，防范社会工程学攻击

对员工进行定期安全意识培训，避免点击不明邮件、文件或网络链接被攻击者实施钓鱼攻击。

制定数据备份和恢复策略： 定期备份关键数据

务必定期备份关键数据，并将备份数据存储在安全的离线位置。并提前测试和验证恢复过程，以确保在需要时能够快速恢复数据。