**蜜点IP分析报告**

## 一、蜜点数据基本信息

蜜点数据基本信息如下：

IP地址：45.142.182.77  
 风险级别：高危  
 运营商：SkyLink Data Center BV  
 VT沙箱最近一次获取这个IP地址相关信息的日期：2023年10月20日  
 IP地址所在地：未知  
 IP地址相关信息最新修改日期：2023年11月02日  
   
 关联安全文件的数目：0个  
 关联危险文件的数目：1个  
 关联可疑文件的数目：0个  
 关联未能判断文件的数目：2个  
 关联超时没有结果的数目：0个

## 二、蜜点数据匹配结果

该ip地址45.142.182.77不存在于“重明”知识图谱中

## 三、蜜点数据推理

### 3.1 关联恶意样本

文件名：  
- SHA-1值：d92f13afe2baa19a7acc01cfff896be6d09ebb31  
- SHA-256值：65ac854d7a2c36e9c8202f75c653d93b52f705524990591183390ef7e2797a48  
- MD5值：a5c8704adc8652ca74d91c9151291c7e  
- 威胁标签：trojan.asf4t5g/ircbot

### 3.2 恶意样本行为分析

Malicious Sample SHA-256: 65ac854d7a2c36e9c8202f75c653d93b52f705524990591183390ef7e2797a48  
- Files Opened: 255  
- Files Written: 25  
- Files Deleted: 16  
- Files Attribute Changed: 1  
- Files Copied: 3  
- Files Dropped: 15  
- Processes Created: 0  
- Processes Terminated: 13  
- Processes Killed: 0  
- Processes Injected: 0  
- Services Opened: 1  
- Services Created: 0  
- Services Started: 0  
- Services Stopped: 0  
- Services Deleted: 0  
- Services Bound: 0  
- Windows Searched: 0  
- Windows Hidden: 0  
- Mutexes Opened: 4  
- Mutexes Created: 21  
- Registry Keys Opened: 408  
- Registry Keys Set: 160  
- Registry Keys Deleted: 2  
- Tls: 1  
- Dns Lookups: 11  
- Http Conversations: 0  
- Ip Traffic: 522  
  
---------------------------------

### 3.3推理结果

该样本集最有可能归属于以下APT组织（Top 3）：  
- APT-C-36: 75.19% 置信度  
- Kimsuky: 7.18% 置信度  
- Gamaredon Group: 4.18% 置信度  
  
---------------------------------  
该样本集对各APT组织的归属置信度为：  
- APT-C-36: 75.19% 置信度  
- Kimsuky: 7.18% 置信度  
- Gamaredon Group: 4.18% 置信度  
- The Gorgon Group: 3.06% 置信度  
- Higaisa: 1.86% 置信度  
- Unknown: 1.52% 置信度  
- OilRig: 1.12% 置信度  
- Leviathan: 1.03% 置信度  
- Putter Panda: 1.02% 置信度  
- Lazarus Group: 0.95% 置信度  
- ScarCruft: 0.93% 置信度  
- APT33: 0.93% 置信度  
- Ajax Security Team: 0.84% 置信度  
- APT17: 0.17% 置信度  
- Patchwork: 0.01% 置信度  
- APT32: 0.00% 置信度  
- MuddyWater: 0.00% 置信度  
- Silent Chollima: 0.00% 置信度  
- Machete: 0.00% 置信度  
- APT41: 0.00% 置信度  
- Mustang Panda: 0.00% 置信度  
- Evilnum: 0.00% 置信度  
- DragonOK: 0.00% 置信度  
- Energetic Bear: 0.00% 置信度  
- menuPass: 0.00% 置信度  
- DarkHydrus: 0.00% 置信度  
- Rocke: 0.00% 置信度  
- APT39: 0.00% 置信度  
- Leafminer: 0.00% 置信度  
- Orangeworm: 0.00% 置信度  
- FIN6: 0.00% 置信度  
- ZIRCONIUM: 0.00% 置信度  
- Group5: 0.00% 置信度  
- GCMAN: 0.00% 置信度  
- APT18: 0.00% 置信度  
- TA459: 0.00% 置信度  
- Sandworm Team: 0.00% 置信度  
- BackdoorDiplomacy: 0.00% 置信度  
- Suckfly: 0.00% 置信度  
- APT16: 0.00% 置信度  
- NEODYMIUM: 0.00% 置信度  
- FIN10: 0.00% 置信度  
- Scarlet Mimic: 0.00% 置信度  
- GALLIUM: 0.00% 置信度  
- TEMPER PANDA: 0.00% 置信度  
- beijing group: 0.00% 置信度  
- APT3: 0.00% 置信度  
- Gallmaker: 0.00% 置信度  
- SilverTerrier: 0.00% 置信度  
- Comment Crew: 0.00% 置信度  
- TeamSpy Crew: 0.00% 置信度  
- BlackTech: 0.00% 置信度  
- FIN5: 0.00% 置信度  
- Poseidon Group: 0.00% 置信度  
- DarkVishnya: 0.00% 置信度  
  
---------------------------------

**APT组织APT-C-36相关信息:**

**描述**

该APT组织的描述如下：APT-C-36被认为是一支从2018年起就很活跃的南美洲间谍组织。该组织主要针对哥伦比亚政府机构以及金融行业、石油行业和专业制造行业的重要公司。

**TTP**

该APT组织使用过的TTP如下：T1204.002、T1027、CAPEC-267、T1105、T1053.005、T1036.004、T1588.002、T1059.005、T1571、T1566.001、CAPEC-163。

**工具**

该APT组织使用过的工具如下：Imminent Monitor、PowerShell。

**恶意软件**

该APT组织使用过的恶意软件如下：LimeRAT、WarzoneRAT、ProyectoRAT、BitRAT、njRAT、Remcos。

**漏洞**

无

**目标**

该APT组织攻击过的目标如下：农业银行、拜因顿、阿尔马维瓦、Sun Chemical、哥伦比亚国家盲人研究所、霍科尔、哥伦比亚国家石油公司、西方银行、哥伦比亚、巴拿马、西班牙、厄瓜多尔。

**APT组织Kimsuky相关信息:**

**描述**

该APT组织的描述如下：Kimsuky是自2012年以来活跃的一个位于朝鲜的网络间谍组织。该组织初始主要针对韩国政府机构,智库和各领域专家。后来扩大目标到美国、俄罗斯、欧洲和联合国。Kimsuky将情报收集的重点放在与朝鲜半岛、核政策和制裁相关的外交和国家安全问题上。

**TTP**

该APT组织使用过的TTP如下：T1593.001、T1189、T1134、CAPEC-633、T1001、T1025、T1548.002、T1573.001、T1020、T1113、CAPEC-648、T1185、T1083、CAPEC-127、CAPEC-497、T1071.003、T1583.006、T1218.011、T1176、T1012、CAPEC-647、T1591、T1587.001、T1218.010、T1562.001、CAPEC-578、T1218.005、T1553.002、T1005、T1564.003、T1204.001、T1098、T1036.005、CAPEC-177、T1534、T1204.002、T1557、CAPEC-94、T1566.002、CAPEC-163、T1583.001、CAPEC-630、T1550.002、CAPEC-644、T1041、T1589.002、T1016、CAPEC-309、T1133、CAPEC-555、T1190、T1071.002、T1584.001、T1057、CAPEC-573、T1594、T1059.005、T1608.001、T1593.002、T1074.001、T1059.001、T1059.006、T1003.001、T1543.003、CAPEC-478、CAPEC-550、CAPEC-551、T1070.004、T1585.001、T1547.001、CAPEC-270、T1114.002、T1588.005、T1586.002、T1567.002、T1078.003、T1566.001、CAPEC-163、T1587、T1564.002、T1588.002、T1114.003、T1036.004、T1055、CAPEC-640、T1111、T1112、CAPEC-203、T1059.003、T1546.001、CAPEC-556、T1598.003、T1102.002、T1053.005、T1552.001、CAPEC-639、T1555.003、T1136.001、T1585.002、T1007、CAPEC-574、T1071.001、T1219、T1040、CAPEC-158、T1583.004、T1082、CAPEC-312、T1105、T1070.006、T1560.001、T1140、T1589.003、T1562.004、T1056.001、CAPEC-568、T1027.002、CAPEC-570、T1505.003、CAPEC-650、T1027、CAPEC-267、T1036、CAPEC-177、T1518.001、CAPEC-581、T1059.007、T1055.012、T1021.001、CAPEC-555、T1560.003。

**工具**

该APT组织使用过的工具如下：Edge、Zoom、WinRAR、Chrome、Metasploit、PHProxy、Viking virus、PHPMailer、Firefox、Hancom Office、Nirsoft、KPortScan、UACMe、SendGrid、TightVNC、ProcDump、TeamViewer、Google Drive、QuasarRAT、PowerShell、schtasks、PsExec、Mimikatz、CSPY Downloader。

**恶意软件**

该APT组织使用过的恶意软件如下：MyDogs、FlowerPower、NavRAT、KimJongRat、PebbleDash、KONNI、Sanny、CARROTBAT、KGH\_SPY、Brave Prince、Gold Dragon、AppleSeed、BabyShark、NOKKI。

**漏洞**

该APT组织使用过的漏洞如下：CVE-2018-8174。

**目标**

该APT组织攻击过的目标如下： Hyundai Merchant Marine、朝鲜、北朝鲜、教育网络安全中心（ECSC）、韩国国防分析研究所（KIDA）、Ministry of Unification、韩国外交部、Sejong、大信证券。

**APT组织Gamaredon Group相关信息:**

**描述**

该APT组织的描述如下：Gamaredon Group组是一支怀疑为俄罗斯发起的网络间谍威胁组织。至少从2013年开始,该组织针对乌克兰的军事组织、非政府组织、司法部门、执法部门和非营利组织开展攻击。“Gamaredon”这个名称来源于该组织早期活动中对“Armageddon”一词的拼写错误。2021年11月,乌克兰政府公开指控Gamaredon Group归属于俄罗斯联邦安全服务中心。

**TTP**

该APT组织使用过的TTP如下：T1059.005、T1053.005、T1082、CAPEC-312、T1119、T1547.001、CAPEC-270、T1071.001、T1070.004、T1025、T1221、T1204.002、T1102、T1568、T1027、CAPEC-267、T1559.001、T1041、T1083、CAPEC-127、CAPEC-497、T1027.004、T1218.005、T1027.001、CAPEC-572、CAPEC-655、T1047、T1566.001、CAPEC-163、T1033、CAPEC-577、T1020、T1036.005、CAPEC-177、T1564.003、T1120、CAPEC-646、T1021.005、CAPEC-555、T1080、CAPEC-562、T1113、CAPEC-648、T1059.003、T1105、T1491.001、T1583.001、CAPEC-630、T1140、T1534、T1057、CAPEC-573、T1106、T1039、CAPEC-639、T1218.011、T1485、T1005、T1137、T1016.001、T1562.001、CAPEC-578、T1112、CAPEC-203、T1059.001、T1608.001。

**工具**

该APT组织使用过的工具如下：Ping。

**恶意软件**

该APT组织使用过的恶意软件如下：EvilGnome、RMS、Pteranodon、PowerPunch、QuietSieve。

**漏洞**

该APT组织使用过的漏洞如下：CVE-2017-0199、CVE-2018-20250。

**目标**

该APT组织攻击过的目标如下：伊朗，乌克兰。

## 四、处置建议

### 重明知识图谱推荐的防御策略

**针对APT组织APT-C-36“重明”推荐的防御策略如下：**

1.培训用户增强对访问或欺骗尝试的意识,降低成功钓鱼、社会工程和其他需要用户参与的技术风险。

2. 通过应用控制和/或脚本阻断阻止代码在系统上执行。

3.使用功能防止终端系统出现可疑行为模式,如可疑过程、文件、API调用等行为。

4.使用签名或启发式检测到恶意软件。

5.使用入侵检测签名在网络边界阻截流量。

6.对系统、权限、不安全软件、不安全配置等进行审计或扫描,发现潜在弱点。

7.管理与SYSTEM和root等特权账号相关的创建、修改、使用和权限。

8.管理与用户账号相关的创建、修改、使用和权限。

9.对操作系统或操作系统常见功能进行配置更改,加强系统防御技术。

10.此类别用于任何应用于初级访问前技术(例如侦察和资源开发技术)的适用缓解活动。

11.移除或拒绝访问可能存在漏洞的不必要且有潜在危险的软件,防止攻击者利用。

12.限制对某些网站的访问,阻断下载/附件,限制JavaScript,限制浏览器扩展等。

13.根据系统、函数或资源的关键性,将网络划分为不同区域。使用物理和逻辑隔离,防止访问潜在敏感系统和信息。使用DMZ隔离任何向互联网暴露的服务,不应从内部网络直接访问。为关键云系统配置独立的私有云(VPC)实例,实现隔离。

14.对软件(不是操作系统)实现配置修改,缓解与软件操作相关的安全风险。

**针对APT组织Kimsuky“重明”推荐的防御策略如下：**

1、此类别用于任何应用于初级访问前技术(例如侦察和资源开发技术)的适用缓解活动。

2、定期进行软件更新,缓解利用风险。

3、限制对某些网站的访问,阻断下载/附件,限制JavaScript,限制浏览器扩展等。

4、使用功能检测并阻断可能导致或表现出软件漏洞利用的条件。

5、将代码执行限制在终端系统上的虚拟环境中或在传输到终端系统时。

6、管理与SYSTEM和root等特权账号相关的创建、修改、使用和权限。

7、管理与用户账号相关的创建、修改、使用和权限。

8、使用入侵检测签名在网络边界阻截流量。

9、使用数据丢失防护(DLP)策略来分类敏感数据,识别个人身份信息(PII)的数据格式,并限制敏感数据外泄。

10、对系统、权限、不安全软件、不安全配置等进行审计或扫描,发现潜在弱点。

11、配置Windows用户账号控制(UAC),减轻攻击者获得提升访问的风险。

12、培训用户增强对访问或欺骗尝试的意识,降低成功钓鱼、社会工程和其他需要用户参与的技术风险。

13、阻止用户或组安装未批准的软件。

14、通过应用控制和/或脚本阻断阻止代码在系统上执行。

15、通过设置目录和文件权限限制访问,但不基于用户或特权账号。

16、移除或拒绝访问可能存在漏洞的不必要且有潜在危险的软件,防止攻击者利用。

17、使用两个或更多的认证因素来验证系统访问,例如用户名密码结合物理智能卡或令牌生成器产生的令牌。

18、根据系统、函数或资源的关键性,将网络划分为不同区域。使用物理和逻辑隔离,防止访问潜在敏感系统和信息。使用DMZ隔离任何向互联网暴露的服务,不应从内部网络直接访问。为关键云系统配置独立的私有云(VPC)实例,实现隔离。

19、对操作系统或操作系统常见功能进行配置更改,加强系统防御技术。

20、使用数字签名验证强制执行二进制文件和应用程序的完整性,防止未经信任的代码执行。

21、使用功能防止终端系统出现可疑行为模式,如可疑过程、文件、API调用等行为。

22、使用网络设备过滤入站或出站流量,并进行基于协议的过滤。在终端配置软件过滤网络流量。

23、防止访问文件共享,远程访问系统以及不必要的服务。限制访问机制可包括使用网络集中器、RDP网关等。

24、使用强密码加密保护敏感信息。

25、对软件(不是操作系统)实现配置修改,缓解与软件操作相关的安全风险。

26、漏洞扫描用于查找潜在可利用的软件漏洞以进行整改。

27、使用签名或启发式检测到恶意软件。

28、为账号设置并实施强密码策略。

29、使用功能防止攻击者成功访问凭据,包括阻止凭据抓取形式。

30、使用保护进程等机制保护与关键系统组件交互的高特权进程,防止进程注入攻击。

**针对APT组织Gamaredon Group“重明”推荐的防御策略如下：**

1.通过应用程序控制和/或脚本阻止来阻止系统上代码的执行。

2.删除或拒绝访问不必要的和可能易受攻击的软件，以防止对手滥用。

3.限制使用某些网站、阻止下载/附件、限制浏览器扩展等。

4. 使用功能防止端点系统上出现可疑行为模式。 这可能包括可疑的进程、文件、API 调用等行为。

5.使用签名或启发式方法来检测恶意软件。

6.对系统、权限、不安全软件、不安全配置等进行审核或扫描，以识别潜在的弱点。

7.管理特权帐户（包括SYSTEM和root）的创建、修改、使用和权限。

8.管理与用户帐户关联的创建、修改、使用和权限。

9. 进行与操作系统或操作系统常见功能相关的配置更改，从而导致系统针对技术进行强化。

10.使用远程安全日志和敏感文件存储，可以更好地控制访问，防止入侵检测日志数据或敏感信息泄露。

11.通过强加密保护敏感信息。

12.使用入侵检测签名来阻止网络边界的流量。

13.使用数据丢失防护（DLP）策略对敏感数据进行分类，识别表明个人身份信息（PII）的数据格式，并限制敏感数据的泄露。

14. 培训用户了解对手的访问或操纵尝试，以降低鱼叉式网络钓鱼、社会工程和其他涉及用户交互的技术成功的风险。

15.将代码的执行限制在端点系统上或传输到端点系统的虚拟环境中。

16.对软件（操作系统除外）进行配置更改，以减轻与软件运行方式相关的安全风险。

17.通过设置不特定于用户或特权帐户的目录和文件权限来限制访问。

18.通过数字签名验证强制执行二进制和应用程序完整性，以防止执行不受信任的代码。

19.阻止用户或组安装未经批准的软件。

20.使用网络设备过滤入口或出口流量并执行基于协议的过滤。在端点上配置软件以过滤网络流量。

21.使用功能来检测和阻止可能导致或表明发生软件漏洞的情况。

22.从最终用户系统和关键服务器获取并存储数据备份。确保备份和存储系统得到强化并与公司网络分开，以防止泄露。

23. 此类别用于任何适用的缓解活动，这些活动适用于对手获得初始访问权限之前发生的技术，例如侦察和资源开发技术。

24.定期进行软件更新以降低利用风险。

25.限制修改Windows注册表中某些配置单元或键的能力。