

APT-C-28（ScarCruft）利用MiradorShell发起网络攻击的安全预警

ctfiot.com/297233.html

APT-C-28 ScarCruft

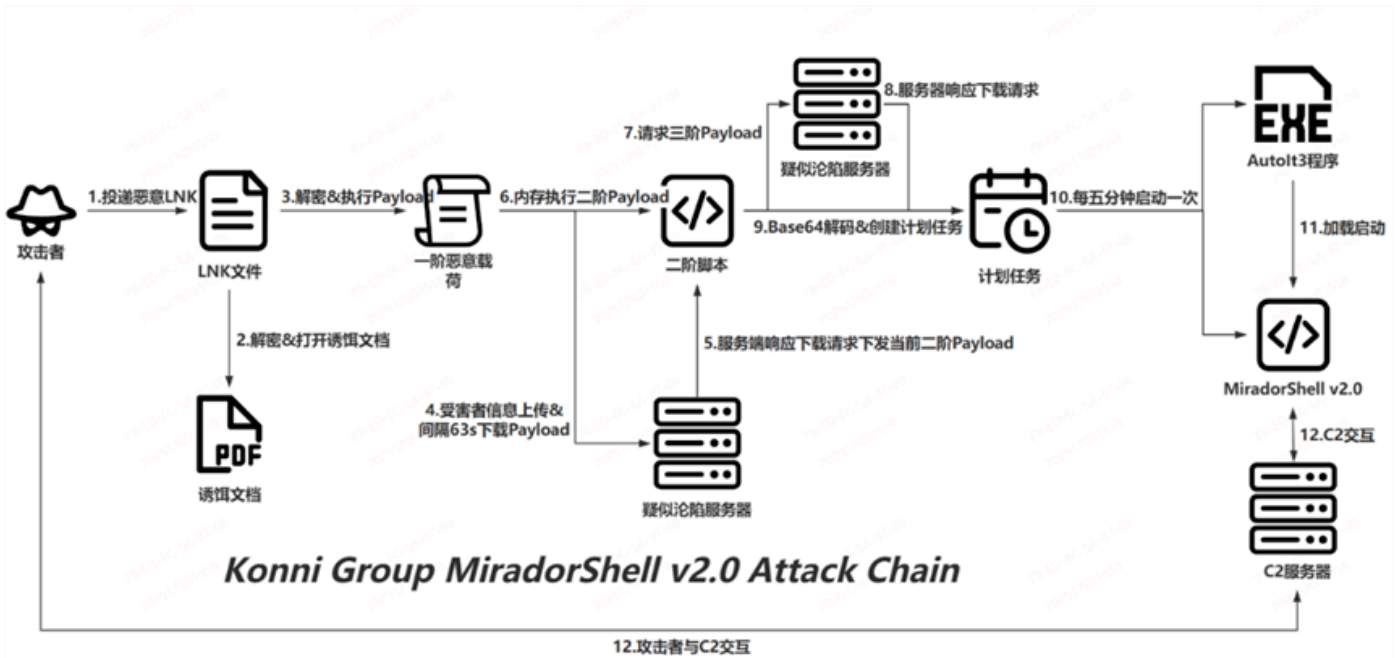
APT-C-28（ScarCruft），又称Konni，是一个长期活跃于朝鲜半岛的APT组织，其攻击活动最早可追溯至2014年，主要针对周边国家地区的政府机构实施网络间谍活动，以窃取敏感信息为核心目标。近年来，该组织频繁被国内外安全团队追踪并披露，活动呈现持续升级势头。

一、概述

近期在360高级威胁研究院在日常APT组织追踪分析过程中，发现Konni组织将攻击目标扩展至加密货币行业，通过伪装成PDF的LNK文件实施鱼叉式钓鱼攻击，诱饵文档精心设计了100万至300万美元的投资金额，精准针对Web3初创公司及DeFi开发者的融资需求，既保持足够吸引力又避免引起怀疑。当用户执行文件后，会触发多阶段Payload加载，最终部署MiradorShell v2.0获取系统控制权。鉴于MiradorShell这类载荷还未完整披露过，因此本文将对这一新型攻击的完整执行过程进行技术剖析，以帮助潜在受害者及时识别威胁并采取防护措施，避免重要数据泄露和资产损失。

二、攻击活动分析

1. 攻击流程分析



Konni组织使用恶意压缩包进行鱼叉钓鱼，一旦用户执行压缩包中伪装成PDF的LNK文件，便会进行层层下载并解密，最终执行MiradorShell载荷，并创建计划任务，达到持有驻留的目的。需要特别说明的是，攻击者在下发最终载荷之前，会检查用户上传的信息，若信息不符合，则不会下发后续组件。

2. 恶意载体分析

Konni组织在近期的定向攻击中主要使用的是恶意ZIP压缩包，以下是最近捕获到的攻击样本，其基本信息如下：

MD5	ca1237bd33f61f77990d76a3df130ef5
文件大小	119.44 KB (122307 bytes)
文件类型	ZIP

该压缩包打开后，有两个文件，一个是伪装内容，名为“Soft Commitment Letter.docx”，一个是伪装成PDF的恶意LNK文件，该文件名（“Investor Profile (Korea-based) – JiHoon Jeong”）与诱导文档名相呼应，让其用户以为这是承诺函相关附近，从而点击恶意LNK文件。

分析该LNK文件，发现文件命令部分存在混淆的CMD/Batch、[C#多种语言代码](#)，如下图所示：

将混淆的代码格式化后，发现该LNK运行后首先通过递归搜索系统目录(`dir /b /s %windir%system32*wers*.l.?x? > %temp%PJoaEy.TiU`)定位PowerShell.exe路径并保存到临时文件，随后调用该路径执行恶意PS1脚本。

接着，PS1脚本会动态编译[C#解密函数](#)，其解密算法如下：

最后，搜索原始LNK文件并从中解密出内存加载的第一阶段Payload，同时释放诱饵文档并清理痕迹，最终实现无文件攻击。释放的PDF诱饵文档与Soft Commitment Letter.docx有相似之处。

第一阶段Payload经过[C#解密函数处理过后](#)，发现功能主要包括了三个部分：沙箱/虚拟机检测、受害者信息收集和加载二阶载荷。解密后的载荷内容如下：

沙箱/虚拟机检测功能描述

一阶恶意载荷会通过执行SystemInfo并检查系统信息中是否包含“Google Compute Engine”，如果是GCE(云服务器/沙箱)则只进行受害者信息收集&上传，不进行后续二阶载荷下载执行。

受害者信息收集功能描述

一阶载荷会收集三个部分的信息：系统信息(SystemInfo)、收集进程列表(tasklist)、收集文件列表(桌面、文档、下载、最近访问、开始菜单、程序目录)。收集完成后构建POST请求发送至二阶服务器(`https[:]//techcross-wne[.]com/include/plugin/snoopy/board/register.php?id={hostname}&sn={请求数}`)。

加载二阶载荷功能描述

如果当前运行环境通过沙箱/虚拟机检测，发起一次二阶载荷请求&执行操作，请求地址为 `https[:]//techcross-wne[.]com/include/plugin/snoopy/board/register.php?id={hostname}&sn={请求数}`。

测试发现二阶服务器下发的前几个操作指令如下图所示：

二阶载荷功能较为简单主要包括两个部分，第一个部分是从 `https[:]//techcross-wne[.]com/include/plugin/snoopy/board/libs/ati.dat` 下载程序为 `Autolt3.exe` 解析程序（合法程序），然后 `https[:]//techcross-wne[.]com/include/plugin/snoopy/board/libs/mrd.dat` 下载 `au3` 脚本，解密为 `MiradorShell v2.0` 载荷，第二部分是创建一个名为 `WndowsUpdate_BCF24B33-5871-1795-C09F-F7902903138A` 每隔 5 分钟自动运行一次 `MiradorShell v2.0` 的计划任务。

值得注意的是我们发现一阶恶意载荷所请求的二阶服务器域名 `techcross-wne.com` 应该是韩国公司 `Techcross-WNE (TEHCROSS Water & Energy)` 的官方合法域名。

下图是该网站的CA证书信息：

因此，该服务器可能已被攻陷，同时我们根据请求的二阶服务器的URL路径信息来看 `include/plugin/snoopy/board`，推测该站点可能使用了 `Snoopy` 类库，被攻击者使用相应漏洞攻破。

3. 攻击组件分析

最终的载荷由 `Autolt` 语言编写，为方便后续持续跟踪工作同时根据代码功能和代码中出现的编译和配置信息，我们将其命名为 `MiradorShell` 版本为 `2.0`，后文简称为 `MiradorShell`。

`MiradorShell` 是一个使用 `Autolt` 编写的后门脚本。以下是对 `MiradorShell` 功能的详细技术分析。

3.1) 核心功能概述

`MiradorShell` 是一种基于反向连接的后门脚本，连接到指定的命令控制服务器（`65.21.182[.]178:443`），具备多维度控制能力：首先支持反向 `Shell` 功能，允许攻击者远程执行 `cmd` 命令并实时获取回显；其次提供完整的文件管理功能，包括文件上传下载、目录遍历及文件删除操作；同时具备远程程序执行能力，可在受害者主机上直接运行指定程序；此外还集成指纹识别模块，通过硬件特征生成唯一受害者ID以实现精准控制。

3.2) 功能模块分析

`MiradorShell` 运行后，首先检查是否存在互斥体（`GlobalED74CC72-AA6C-B091-B820-631489DA5F3B`），如果存在则退出，以确保同一时间只有一个木马实例在运行。

接着，使用 `ws2_32.dll` (Winsock) 直接发起 `TCP` 连接，连接成功后，发送数据包（`MSITRUAVDWAX+[受害者ID]+2.0`），其 `MSITRUAVDWAX` 是上线包的标识头，受害者ID是通过计算机名CPU信息硬盘序列号等信息组合拼接而成。

然后，进入命令分发循环，等待服务器发送指令，通过“分割解析命令和参数”，`MiradorShell v2.0` 支持的指令如下所示：

命令关键字	对应功能函数	描述
cmd	REMOTESHELLPROCESS	启动交互式CMD Shell
upload	UPLOADPROCESS	接收服务器发送的文件并保存到本地
download	DOWNLOADPROCESS	读取本地文件并发送给服务器
listdir	LISTDIR	遍历指定目录，返回文件/文件夹列表及大小
delete	DELETEPROCESS	删除指定的文件或文件夹
run	RUNPROCESS	使用ShellExecute运行指定文件

其中反向Shell实现机制是：通过_NAMEDPIPES_CREATEPIPE创建匿名管道重定向标准I/O流，调用CreateProcessA隐藏启动cmd.exe 进程并绑定管道，建立双向数据传输通道——持续读取子进程输出管道（READCHILDOUTPUT）经Socket上传至C2服务器，同时将接收的C2指令写入输入管道（WRITEREMOTESHELL）实现交互式控制，整个过程采用异步通信规避行为检测。其他指令（如文件传输、指令执行等）具体技术细节此处从略。

3.3) 逃避与混淆技术

内联库文件

为避免依赖标准库并干扰分析，作者未使用AutoIt的常规[#include指令](#)，而是将所有必需的UDF（如WinAPI、Security、NamedPipes等）的源代码直接嵌入脚本中。这一策略显著增加了脚本体积（从几十行扩展至近12000行），迫使分析人员需要耗费更多时间梳理冗余代码以定位核心功能模块。

直接API调用

为实现更底层的操作并规避简单行为检测，脚本通过DllCall直接调用系统DLL（如kernel32.dll、user32.dll、ws2_32.dll）中的原生函数，而非依赖AutoIt封装的高级API。

原始套接字

脚本未采用AutoIt内置的TCPConnect等网络函数，而是通过手动调用Winsock API（如WSASocket、connect）实现套接字通信。这种设计可能旨在精确控制连接参数（如KeepAlive超时）或绕过针对脚本语言网络行为的特定监控机制，进一步隐蔽恶意流量特征。

三、归属研判

经分析，本次攻击活动中使用的恶意代码及C2基础设施与Konni组织历史攻击样本存在显著关联，具体体现在以下方面：

1. 本次攻击Konni组织仍采用LNK文件作为初始入口，诱骗用户点击后下载加密的后续载荷及诱饵文档，只是本次样本对LNK样本执行命令进行了加密处理，增加分析难度。此外，样本后续会通过Autolt3.exe加载恶意AU3脚本，整体攻击流程与历史样本高度一致。
2. 样本运行后创建的互斥体（GlobalED74CC72-AA6C-B091-B820-631489DA5F3B）在命名风格和结构上，与此前Konni组织样本中的互斥体（如GlobalIRT3AN7C9QS-7UYE-9K6G-A8F1-HY8IT3CNMEQP）高度相似。同时，计划任务的创建逻辑和代码实现也呈现一致性。
3. 本次攻击活动在C2通信环节呈现与Konni组织高度关联的技术特征：攻击样本采用固定格式的URL（https[:]//techcross-wne[.]com/include/plugin/snoopy/board/register.php?id={hostname}&sn={请求数}）获取命令，其参数结构（id={hostname}标识受害主机，sn={请求数}作为序列计数器）与该组织历史攻击中使用的URL设计范式相似；同时，攻击者延续了Konni组织惯用的失陷站点托管策略，通过入侵韩国技术类网站techcross-wne[.]com伪装恶意流量，将载荷隐藏在/include/plugin/snoopy/board/路径下模拟正常插件目录，这种结合动态参数模板与可信域名滥用的手法，既强化了攻击归因依据，也凸显该组织在规避检测方面的成熟度。

结合攻击目标（针对韩国地区）及上述技术特征，本次攻击活动可明确归属于APT-C-28（ScarCruft）组织，符合其长期攻击策略和工具链特点。

附录 IOC

MD5

4692034cd157c417c3868b5033d0e0d7
ca1237bd33f61f77990d76a3df130ef5
e4e7351cf3fc80e6f65c2226d1cafdb2
f9945ddbfc05ee49ba21d49e8087a18

C&C

https[:]//techcross-wne[.]com/include/plugin/snoopy/board/register.php
https[:]//techcross-wne[.]com/include/plugin/snoopy/board/libs/mrd.dat
65.21.182[.]178:443

团队介绍

TEAM INTRODUCTION

360高级威胁研究院

360高级威胁研究院是360数字安全集团的核心能力支持部门，由360资深安全专家组成，专注于高级威胁的发现、防御、处置和研究，曾在全球范围内率先捕获双杀、双星、噩梦公式等多起业界知名的Oday在野攻击，独家披露多个国家级APT组织的高级行动，赢得业内的广泛认可，为360保障国家网络安全提供有力支撑。

| 本篇文章来源于微信公众号: 360威胁情报中心