尼日利亚黑客组织SWEED正在散发针对物流行业的钓鱼文档 – 绿盟科技技术博客

By Meet The Author

Published: 2021-06-11 · Archived: 2026-04-05 22:55:58 UTC

一、概要

6月11日，绿盟科技捕获到两封携带cve-2017-11882漏洞利用载荷的钓鱼文档。两封文档分别伪装成土耳其货运公司ALATLI的海关报表以及土耳其制造商mgt air filters物流部门相关工作人员的参会表。两封文档使用了类似形式的漏洞利用，会从同一个网络地址下载封装后的AgentTesla间谍木马并运行。

通过分析漏洞利用载荷形式和AgentTesla木马的封装形式，我们确认这两封文档的制作者为黑客组织Sweed。

二、组织信息

Sweed组织是一个至少从 2017 年就开始运营的从事间谍活动的黑客组织，最早由Cisco Talos发现[1]。

Sweed组织主要使用带有恶意附件的鱼叉式网络钓鱼电子邮件进行攻击，常用的攻击工具包括疑似自主开发的office文档公式编辑器漏洞利用工具、恶意office宏制作工具、AgentTesla木马、Formbook木马、Lokibot木马。 Sweed组织的主要攻击目标包括波黑、加拿大、中国、吉布提、法国、德国、香港、印度、意大利、摩纳哥、俄罗斯、卡塔尔、新加坡、南非、韩国、瑞士、台湾、土耳其、阿联酋、英国、美国等[2]。

绿盟科技曾经报道过Sweed组织对常用的漏洞利用工具的升级过程[3]。

三、攻击过程分析

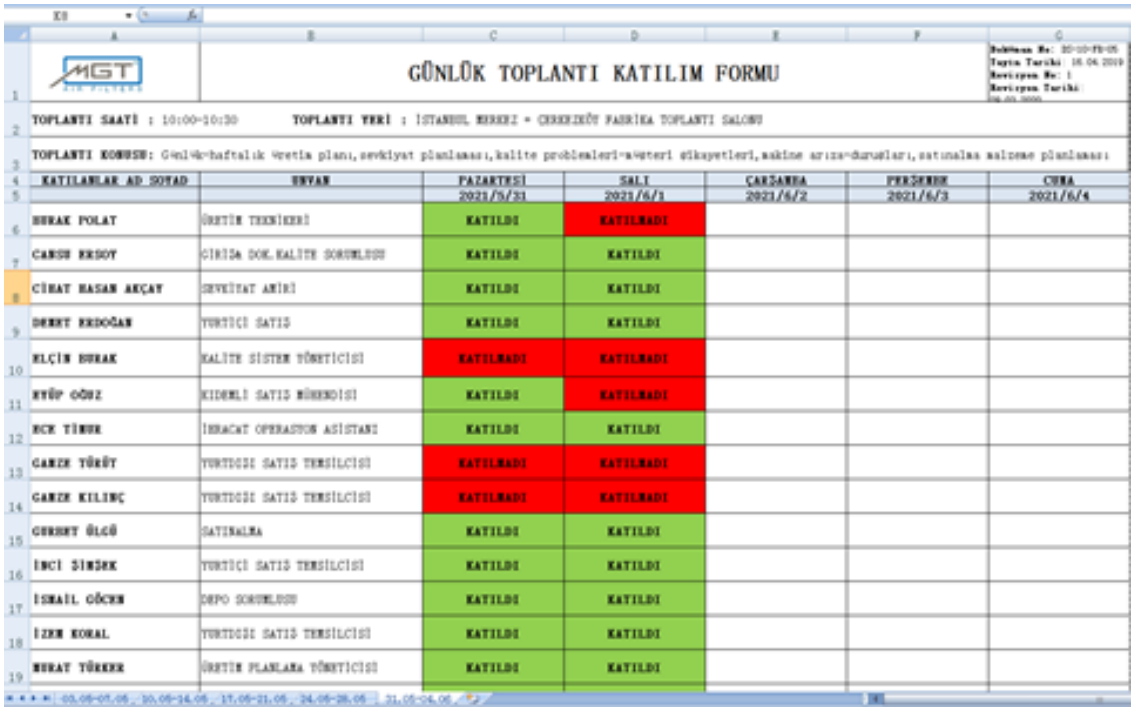
钓鱼文档

如下图所示，两封钓鱼文档在打开后分别显示：

土耳其货运公司ALATLI的海关报表：

ALATLI	REZERVASYON FORMU		Doküman No:	KY.SRC.02/F02
			Yayınlanma Tarihi	2017/11/15
			Revize Tarihi	2021/6/9
FORM NO:		REV. NO:		
REZERVASYON TARİHİ				
ÖNEM DERECESİ	☐ ÇOK ÖNEMLİ	☑ ÖNEMLİ	☐ STANDART	
MÜŞTERİ TEMSİLCİSİ	☑ ANNA G.	☐ TONI D.	☐ ONUR E.	☐
İHRACATÇI FİRMA BİLGİLERİ	STARTIP TIBBI MALZEMELER Atasehir , Istanbul 0090 533 163 76 86 OZLEM TANRIVERDI 0090 216 661 48 48 (EXT.No:4)			
İTHALATÇI FİRMA BİLGİLERİ	VEGA MEDIKAL (FLEXCARGO) Rosen Krastev <rosen.krastev@flexcargo-bg.com>			
GÜMRÜKCÜ VE İRTİBAT BİLGİLERİ	35988804388			
☐ İHRACAT ☑ İTHALAT GÜMRÜK İDARESİ	SOFIA AEROGARA			
T.C. ANTREPO BİLGİSİ				

土耳其制造商mgt air filters物流部门相关工作人员的参会表：



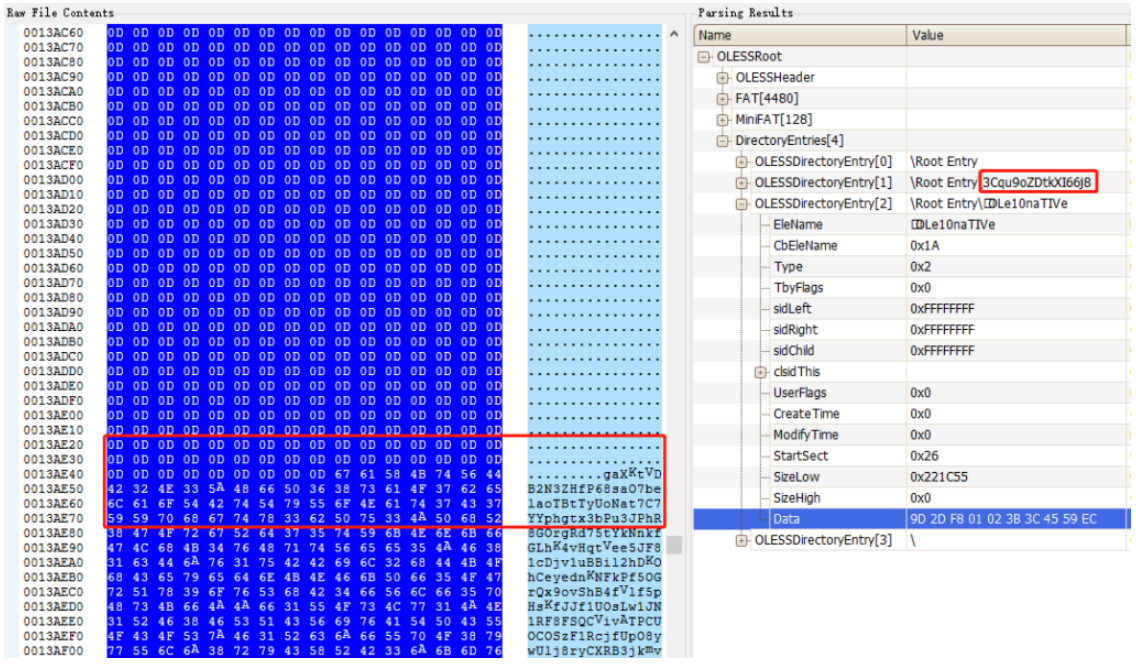
GÜNLÜK TOPLANTI KATILIM FORMU

TOPLANTI SAATİ : 10:00-10:30 TOPLANTI YERİ : İSTANBUL MERKEZ - ÇERKEZKÖY FABRİKA TOPLANTI SALONU

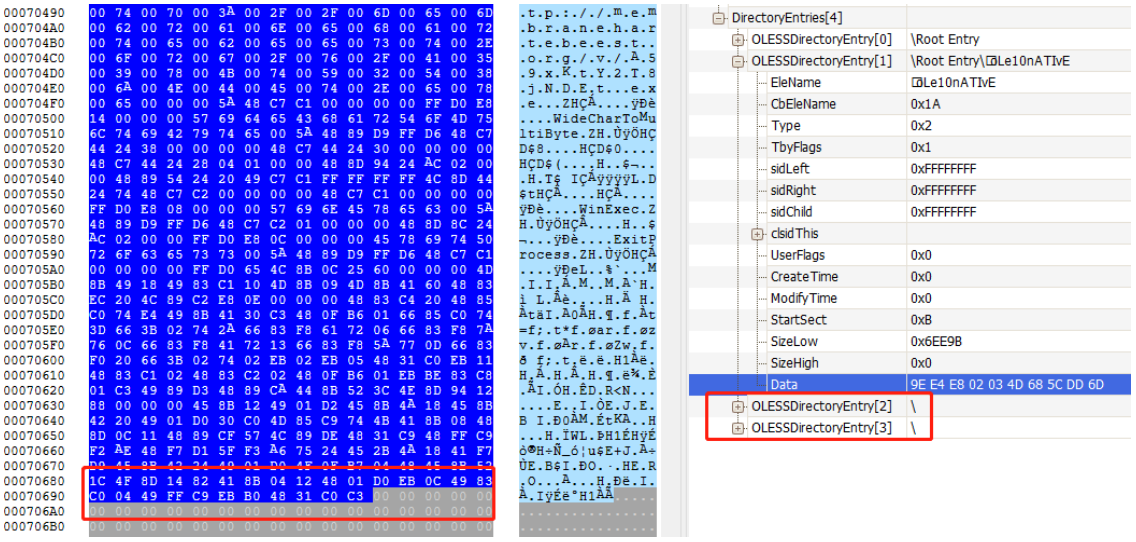
TOPLANTI KONUSU: Günlük-haftalık üretim planı, sevkiyat planlaması, kalite problemleri-müşteri şikayetleri, makine arıza-durusları, satınalma malzeme planlaması

KATILANLAR AD SOYAD	UNVAN	PAZARTESİ 2021/5/31	SALI 2021/6/1	ÇARŞAMBA 2021/6/2	PERŞEMBE 2021/6/3	CUMA 2021/6/4
MURAT POLAT	ÜRETİM TEKNİKERİ	KATILDI	KATILMADI			
CANSU ERSOY	GİRİŞİm DOK.KALİTE SORUMLUSU	KATILDI	KATILDI			
CİHAT HASAN AKÇAY	SEVKİYAT AMİRİ	KATILDI	KATILDI			
DERYA ERDOĞAN	YURTİÇİ SATIŞ	KATILDI	KATILDI			
KILÇİN MURAT	KALİTE SİSTEM YÖNETİCİSİ	KATILMADI	KATILMADI			
KÜÇÜK OĞUZ	KIDEMLİ SATIŞ MÜHENDİSİ	KATILDI	KATILMADI			
ECE TİMUR	İHRACAT OPERASYON ASİSTANI	KATILDI	KATILDI			
CANAN TÜRÜT	YURTİÇİ SATIŞ TEMSİLCİSİ	KATILMADI	KATILMADI			
CANAN KILINÇ	YURTİÇİ SATIŞ TEMSİLCİSİ	KATILMADI	KATILMADI			
CUNEYT ÜLGÜ	SATINALMA	KATILDI	KATILDI			
İNCİ SİNİRK	YURTİÇİ SATIŞ TEMSİLCİSİ	KATILDI	KATILDI			
İSMAİL GÖCEN	DEPO SORUMLUSU	KATILDI	KATILDI			
İZEN KORAL	YURTİÇİ SATIŞ TEMSİLCİSİ	KATILDI	KATILDI			
MURAT TÜRKER	ÜRETİM PLANLAMA YÖNETİCİSİ	KATILDI	KATILDI			

两封文档都携带了cve-2017-11882漏洞利用载荷，其中，ALATLI文档中的载荷形式符合Sweed组织新版本漏洞文档制作工具的特征：



mgt air filters文档中的载荷形式则符合Sweed组织旧版本漏洞文档制作工具的特征：



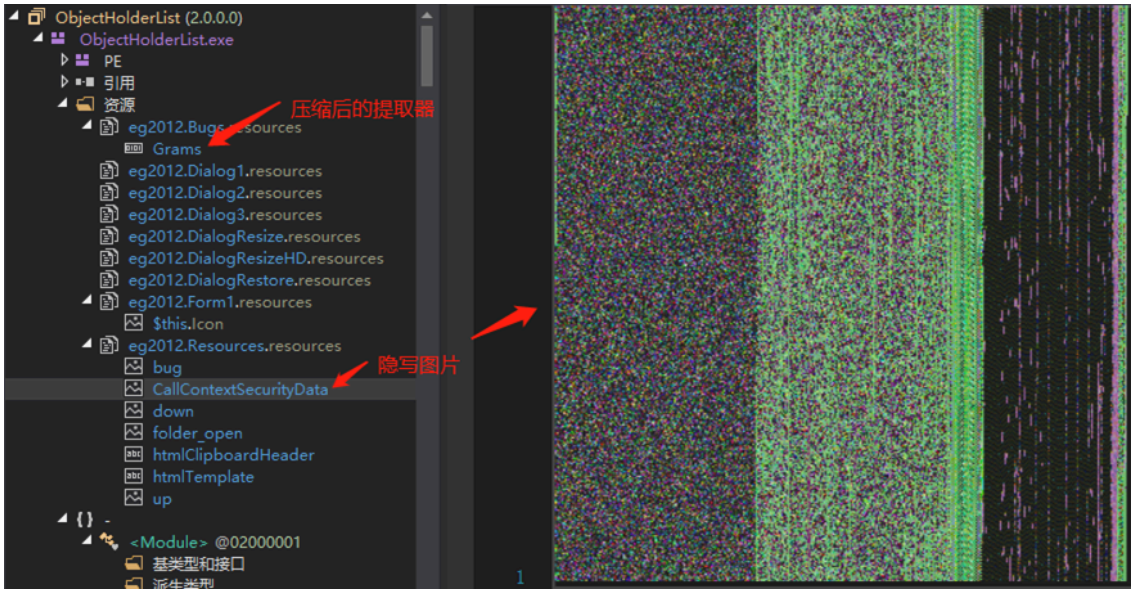
两封文档的漏洞利用部分包含的shellcode代码逻辑大致相同，功能为通过UrlMon提供的API下载指定网络地址的内容。

两封文档中硬编码的网络地址相同，为hxxp://membranehartebeest.org/v/A59xKtY2T8jNDEt.exe：

间谍木马

上述钓鱼文档下载的可执行文件，是带有近期主流封装形式的AgentTesla间谍木马。

带有这种封装形式的Dropper程序，会在C#主程序的资源部分存储一个读取器以及一张隐写图片：



读取器会获取隐写图片的二进制内容，组合为第二阶段的Dropper程序。

第二阶段的Dropper程序是一种带有少量附加功能的进程注入器，主要功能为提取并使用xor_dec逻辑解密一段资源，将其注入至系统进程中。

该注入器最终注入的文件是AgentTesla本体程序。

该AgentTesla程序的CnC地址为ftp.manpowerpooling.ro，当前IP为89.43.19.227。

木马功能

常见的AgentTesla间谍木马会尝试：

a.搜集受害主机以下浏览器中保存的账号密码等用户数据：

Opera Browser
Yandex Browser
Iridium Browser
Chromium
7Star
Torch Browser
Cool Novo
Kometa
Amigo
Brave

CentBrowser
Chedot
Orbitum
Sputnik
Comodo Dragon
Vivaldi
Citrio
360 Browser
Uran
Liebao Browser
Elements Browser
Epic Privacy
Coccoc
Sleipnir 6
QIP Surf
Coowon
Chrome
SRWare Iron
Brave Browser
CoolNovo
Epic Privacy Browser
Fenrir
QQ Browser
UC Browser
uCozMedia

b.搜集以下浏览器的应用数据：

Firefox
IceCat
PaleMoon
SeaMonkey
Flock
K-Meleon
Postbox
Thunderbird
IceDragon
WaterFox
BlackHawk
CyberFox

c.搜集以下FTP相关应用中存储的用户信息：

CoreFTP
FTP Navigator
SmartFTP
WS_FTP
Cftp
FTPCommander
FTPGetter

d.主机基本软硬件信息；

e.屏幕截图；

f.键盘记录；

g.窗口程序文本内容。

AgentTesla会定期将收集到的信息通过SMTP服务上传到攻击者的邮箱中。

五、小结

对事件的分析表明，近期高度活跃的Sweed组织开始对土耳其物流行业进行鱼叉邮件钓鱼攻击。这些攻击活动倾向使用公式编辑器漏洞和内容可信度较高的诱饵，使受攻击目标难以分辨和规避这些攻击。

通过关联分析，绿盟科技确定已有土耳其政府官员收到该次攻击的影响。

参考链接

[1] https://blog.talosintelligence.com/2019/07/sweed-agent-tesla.html

[2] https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Sweed&n=1

[3] https://blog.nsfocus.net/cve-2018-0798/

版权声明
