新APT组织穆伦鲨(MurenShark) 调查报告：袭向土耳其海军的鱼雷

blog.nsfocus.net/murenshark/

伏影实验室

一、概述

2022年第二季度，绿盟科技伏影实验室监测到了一系列针对土耳其的网络攻击活动。经过分析，研究人员确认本轮攻击活动来自一个由伏影实验室于21年4月确认的新型威胁实体Actor210426。伏影实验室通过行为模式、攻击手法、攻击工具、攻击目标等线索，对该威胁实体进行了深入调查，确认了其独立性与高级威胁性质。

基于该威胁实体的活动区域与近期攻击目标（土耳其海军项目“MÜREN”），伏影实验室将其正式命名为穆伦鲨（MurenShark），对应绿盟科技高级威胁组织标识为APT-N-04。

已监测活动中，穆伦鲨的主要目标区域包括土耳其和北塞浦路斯地区，攻击范围覆盖高校、研究所和军队等领域的多个敏感目标，尤其对军工项目展现明显的兴趣，已经实施了成功的网络间谍活动。

穆伦鲨组织人员具有丰富的对抗经验，擅长反分析和反溯源。调查显示，已暴露的攻击活动只是该组织行动的冰山一角，攻击目标与攻击组件方面不连续的迭代轨迹说明该组织的大量活动仍隐藏在迷雾当中。

本报告将分享该组织的各维度特征，与已知APT组织的关系、以及伏影实验室在调查过程中的其他发现。

二、组织信息

穆伦鲨组织是一个活跃于中东地区的新型威胁实体，主要攻击目标国家为土耳其，已发现的目标包括北塞浦路斯地区高校、土耳其军队和土耳其国家科研机构。

穆伦鲨的主要攻击手法包括投递钓鱼文档与攻击线上服务，直接目的包括扩充攻击资源、渗透目标网络、窃取关键数据。该组织已知的鱼叉式攻击最早出现在2021年4月，对高校网站的入侵行为则早于该日期。

穆伦鲨具有丰富的对抗经验，擅长的手段包括通过跳板节点隐藏攻击者信息、通过组件拆分阻碍流程复现、使用第三方方案减少代码特征等。

穆伦鲨在已实施的活动中较好地隐藏了攻击者信息，目前尚无法确认该组织的地域归属。

三、攻击技术矩阵

下图展示了穆伦鲨的攻击技术矩阵，包含该组织攻击者和开发者掌握的能力以及该组织借助第三方工具实现的能力。

穆伦鲨绿盟科技攻击技术矩阵

四、典型活动

穆伦鲨并不是一个很活跃的攻击者，其攻击活动分布具有明显的聚集性。

穆伦鲨最近的一轮活动集中在今年8月上旬，攻击者投递了多种形式的土耳其语钓鱼文档，对土耳其特定目标进行攻击。

该轮攻击活动中出现的钓鱼文档带有如下文件名：

文件名	机译
Birlestirilmis_GORUSLER.doc	综合意见
MURENPRVZ-KYP-03-EK3-YKS (Yazilim Konfigurasyon Sureci).doc	软件配置流程
MURENPRVZ-KYP-03-EK5-PMF (Platforma Mudahale Formu).doc	平台干预表
MURENPRVZ-STB-XX-XX (Surum Tanimlama Belgesi).doc	版本识别文件
Birlestirilmis_GORUSLER - Tubitak'a Gonderilen2 2022.08.05 14.41.22.doc	综合意见 - 发送至 Tubitak 2022.08.05 14.41.22
KGB Numaralari ve Gecerlilik Tarihleri.xlsx	KGB编号和有效期

穆伦鲨部分钓鱼文档文件名

第一种钓鱼文档显示的标题为“关于 MÜREN 关键设计文档的意见”（MÜREN KRİTİK TASARIM DOKÜMANINA YÖNELİK GÖRÜŞLER），抬头部分显示文档来自“海军司令部第一潜艇舰队TCG萨卡里亚号指挥部”：

T.C.
DENİZ KUVVETLERİ KOMUTANLIĞI
[illegible]
TCG Sakarya Komutanlığı

Sayı : 69405369-540.01.05-361 Haziran 2022

MÜREN KRİTİK TASARIM DOKÜMANINA YÖNELİK GÖRÜŞLER

S.No	Firma (Doküman Adı-Doküman Kodu)	İlgili Bölüm	Mevcut Hali	Öneri
1	MÜREN/PROJE-SSDD-09-2	3.3.1.6.1 IPS Sinyal İşleme Ünitesi	IPS Sinyal İşleme Ünitesi, Şekil 3.18'de verildiği üzere IPS Sinyal İşleme Bilgisayarı ve bu bilgisayar üzerinde çalışan IPS Sinyal İşleme Yazılımı'ndan oluşmaktadır. MÜREN SYS'de 2 (iki) adet IPS Sinyal İşleme Ünitesi bulunacaktır. Bunlardan bir tanesi CHA ve IFNA sinyal işleme işlevlerini, diğeri ise FA ve OA sinyal işleme işlevlerini yerine getirecektir. IPS Sinyal İşleme alt-bileşenleri aracılığıyla bağlantı Şekil 3.19'da verilmiştir.	Seçili paketin, NAS'tan/a cdyn nkendi kayıt yapılabilmesine imkan sağlayacaktır. Bu havuzun kritik tasarım aşamasında ele alınmasının uygun olacağı değerlendirilmektedir.

1 / 1

钓鱼文档A

该文档详细记录了土耳其海军对一种名为“MÜREN ”的潜艇内系统的修改意见，文档日期显示为2022年六月。

另一类钓鱼文档显示的标题为国家生产综合水下作战管理系统预级应用项目MÜREN-PREVEZE（MİLLİ ÜRETİM ENTEGRE SUALTI SAVAŞ YÖNETİM SİSTEMİ PREVEZE SINIFI UYGULAMASI (MÜREN-PREVEZE) PROJESİ），显示该文档来自土耳其科技研究院信息学与信息安全先进技术研究中心（TÜBİTAK BİLGEM）：

钓鱼文档B

该钓鱼文档对应一种名为“MÜREN-PREVEZE”的软件系统的说明文件。

查询相关关键词后，伏影实验室确定上述两种文档来自土耳其军方项目“MÜREN”。这是一种在潜艇上搭载的水下作战管理系统（CMS），由土耳其科技研究院TÜBİTAK设计（https://bilgem.tubitak.gov.tr/tr/haber/akya-torpidosu-muren-prevezeye-entegre-ediliyor），并已在21年测试完成，在22年提供给土耳其海军司令部（https://raillynews.com/2021/11/denizaltilari-muren-yonetecek/）。土耳其海军对MÜREN项目给予很大期望，认为该项目能够推动土耳其海军系统国产化，并成为土耳其国家级潜艇项目“MILDEN”的关键一步（https://www.navalnews.com/naval-news/2021/11/turkeys-new-submarine-cms-muren-to-enter-service-in-2022/）。

由此可以推断，穆伦鲨在8月上旬的活动主要目标为“MÜREN”项目的相关人员，包括土耳其科技研究院的项目设计人员与土耳其海军的项目审核人员。

通过目前已掌握的信息，伏影实验室无法判断本轮攻击是否已达成预定目的，但从诱饵文档的内容可以看出，穆伦鲨已通过其他攻击活动成功入侵土耳其科技研究院内部并已窃取高价值的文档内容。

穆伦鲨在更早的攻击活动中展现了完全不同的攻击倾向。在伏影实验室已报道的一轮攻击活动（http://blog.nsfocus.net/apt-dogecoin/）中，该组织使用一种与多吉币（Dogecoin）相关的报告文档作为诱饵，对虚拟货币的关注者进行了钓鱼攻击：

钓鱼文档C

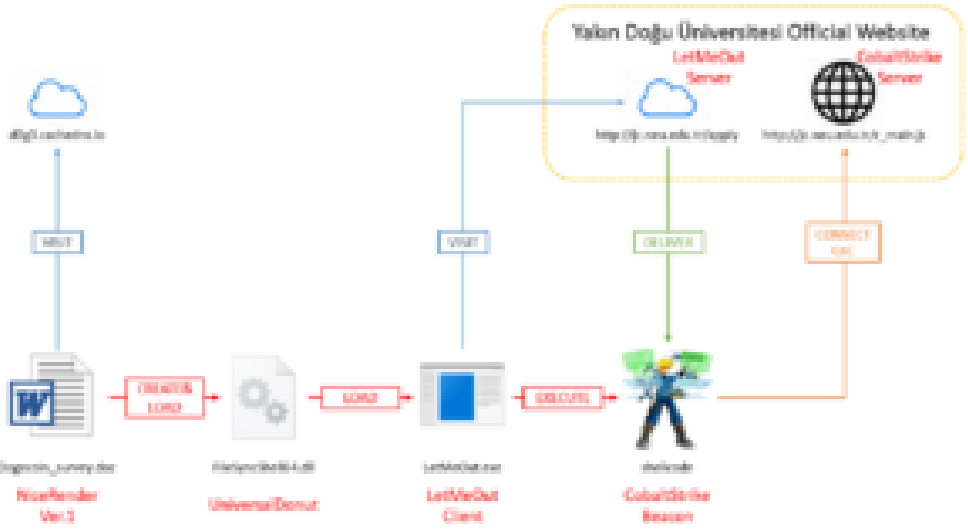
除诱饵文档发现地区为土耳其外，穆伦鲨在该活动中未暴露其他信息。

受国家经济政策影响，加密货币行业在土耳其热度极高。结合组织活动轨迹，伏影实验室推断该类钓鱼攻击是穆伦鲨组织粗精度钓鱼活动的一部分，主要目标同样为土耳其。黑客组织通常会依靠此类具有高话题度的诱饵文档，进行大范围的信息收集活动，再从获取的情报中筛选高价值信息。

五、典型攻击流程

穆伦鲨频繁使用一种具有代表性的攻击流程，并持续对该流程和其中的组件进行改良。

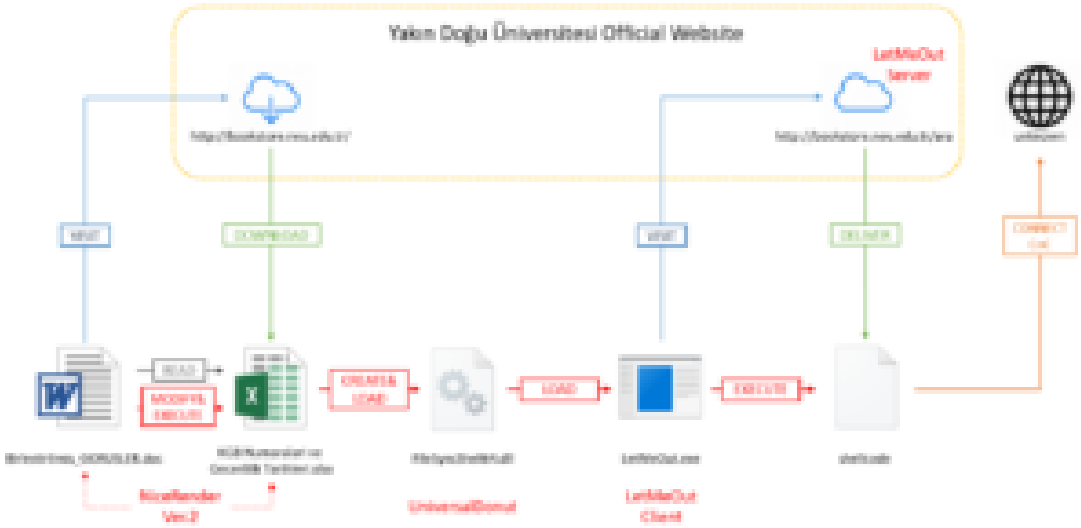
下图展示了该组织在21年的活动中使用的典型流程：



攻击流程A

该攻击流程由穆伦鲨的三种主要攻击组件NiceRender、UniversalDonut、LetMeOut、失陷站点neu.edu.tr、以及第三方攻击工具CobaltStrike组成，最终实现窃取受害者主机中的数据、以及在受害者主机所在域内进行横向移动的目的。

下图展示该组织在近期针对土耳其海军与科研机构的攻击活动中使用的改进型流程：



攻击流程B

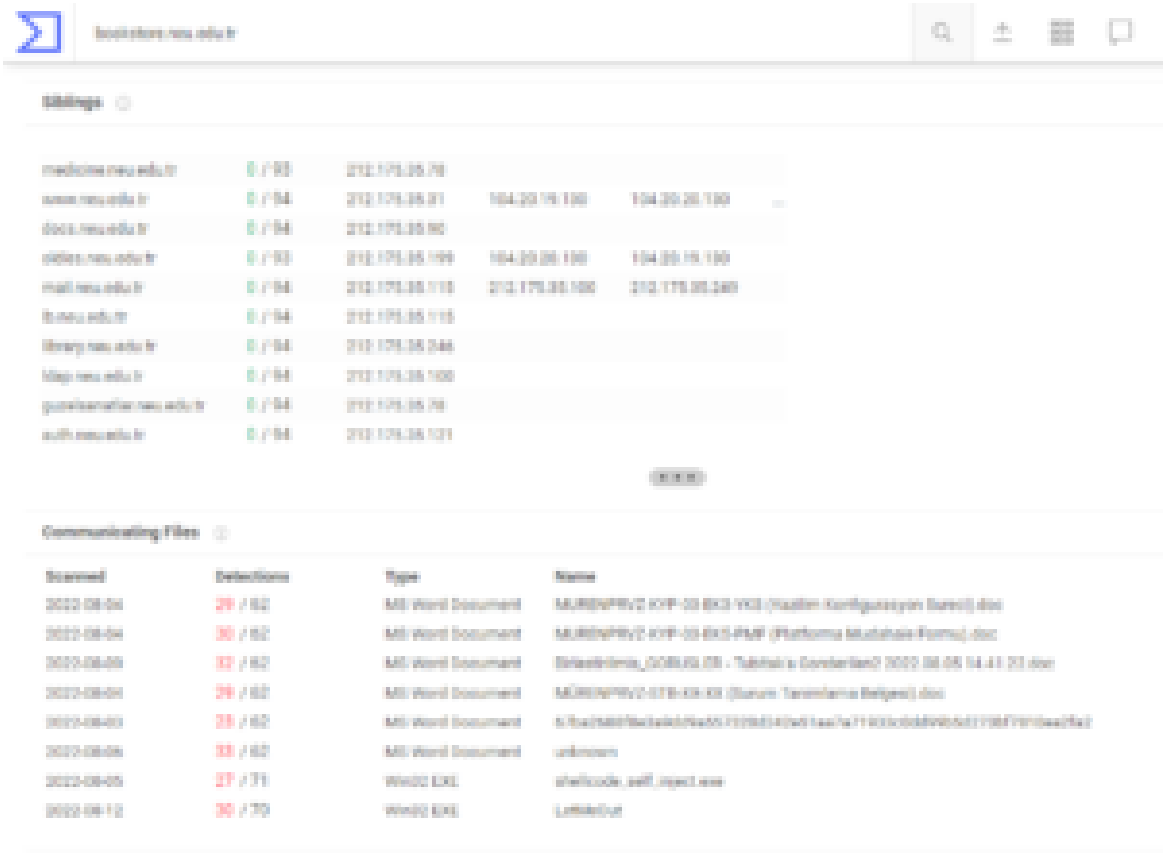
该流程同样由三种主要组件以及相同的失陷站点组成。区别在于穆伦鲨攻击者在该流程中使用了新型NiceRender文件，同时进一步缩短了流程的生命周期，这些操作使沙箱类安全产品难以复现完整执行过程。

六、攻击手法特征

利用失陷站点

穆伦鲨在攻击流程中倾向于使用失陷站点作为文件服务器与CnC服务器。如典型攻击流程章节所示，该组织在各时期的活动中都使用了近东大学（Yakın Doğu Üniversitesi）的官网（https://neu.edu.tr/）作为远程服务器。

近东大学是一所私立高校，位于北塞浦路斯地区。已知的攻击流程表明，穆伦鲨已经控制近东大学官方网站服务器超过一年，在网站多个位置寄放了木马程序、运行了LetMeOut木马服务端程序，甚至还部署了CobaltStrike渗透平台的服务器用于对受害者进行持续控制。



被控制的近东大学网站

虽然拥有此类攻击资源，但穆伦鲨对失陷站点的使用整体比较克制，这些站点在绝大多数时间内处于静默状态，并未被交易或被滥用。穆伦鲨对失陷站点的这种利用方式，有效地隐藏了组织痕迹，并延长了资源的可用周期。

组件行为细分

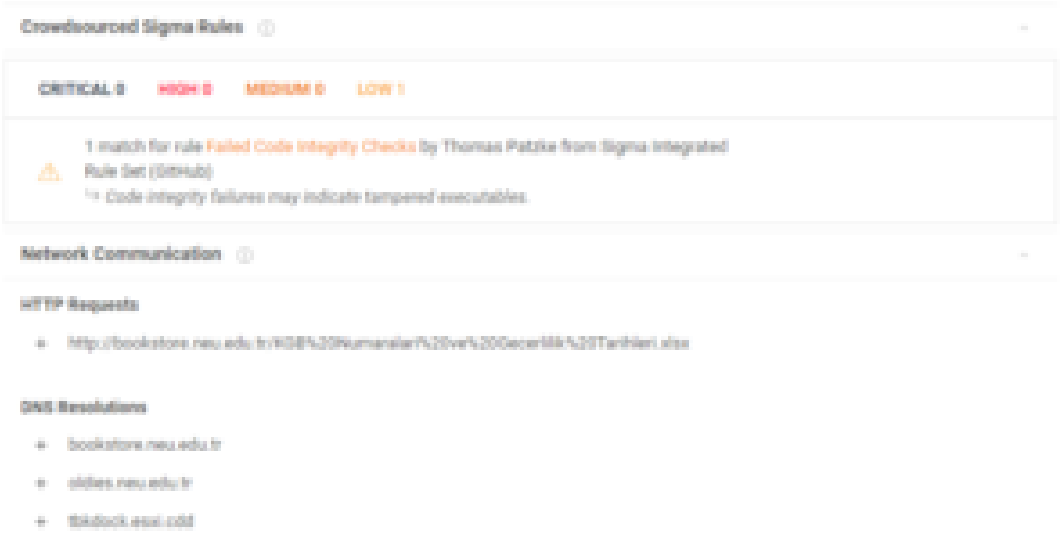
穆伦鲨在设计流程时，遵循一种特别的行为拆分思路。

例如，该组织近期使用的NiceRender新版本攻击组件，将恶意文档的常规功能拆分成了两部分，A部分被设计成一种宏代码读取器和注入器，B部分则被设计成宏代码载体和注入载体，A需要通过网络连接获取B，从而运行完整组件行为。

再如，该组织常用的LetMeOut木马程序也会将其下载功能拆分成两部分。木马首先向CnC上传木马信息与受害者主机信息，收到服务器确认信息后再通过计算获得后续载荷的下载路径。

这种设计思路的优点显而易见。配合上文所述的失陷站点，这些组件在远端地址失效或停止服务时，在网络侧和进程侧不会产生任何恶意行为特征，甚至没有受过训练的人员在打开对应文件时也无法察觉到异常。这些细分的组件行为也对取证分析、攻击过程还原等工作造成了干扰，大量的交互机制有效保护了流程中的网络资源与攻击组件，降低了暴露几率。

CnC失联状态下，新版本NiceRender的行为表现与常规文档相似：



NiceRender在失联状态下的行为

七、已知攻击工具

NiceRender

该工具是一种具有特定执行模式的恶意宏类型文档，穆伦鲨攻击者使用该工具制作各种钓鱼文档，用作攻击活动的初始载荷。该工具目前出现了两个版本。

NiceRender Ver.1

早期版本的NiceRender包括三个功能部分，分别为诱饵解码、上线通知与载荷释放。

1. 诱饵解码

NiceRender与其他常见钓鱼文档的最大区别在于，该组件会使用一种独特的逻辑将文档内文字内容转码成乱码字符，并在执行上述阶段后对这些乱码文字进行解码，给受害者传递一种加密文档确实进行了解密的错觉，从而增加此类钓鱼文档的可信度。

NiceRender的字符转码逻辑为，搜索特定宽字节字符并将其转为对应的ASCII字符。

待转换的宽字符对应的十进制值序列为：

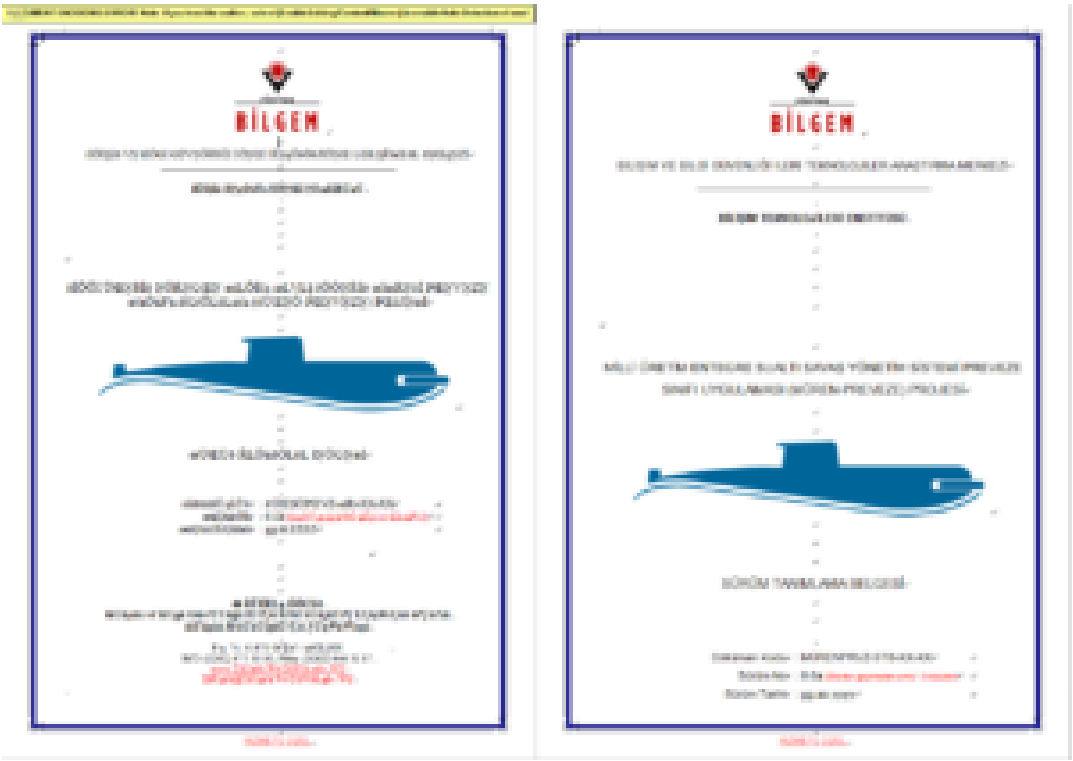
[321, 325, 338, 334, 332, 331, 324, 329, 335, 333, 341, 340, 339, 322, 345, 353, 357, 361, 370, 366, 364, 363, 356, 367, 365, 373, 372, 371, 354, 377]

对应的ASCII字符序列为：

[A, E, R, N, L, K, D, I, O, M, U, T, S, B, Y, a, e, i, r, n, l, k, d, o, m, u, t, s, b, y]

转换完成后，NiceRender会隐藏原始内容顶部的启用编辑功能提示，进一步提高文档可信度。

下图为典型NiceRender诱饵原始内容与转码后效果的对比。

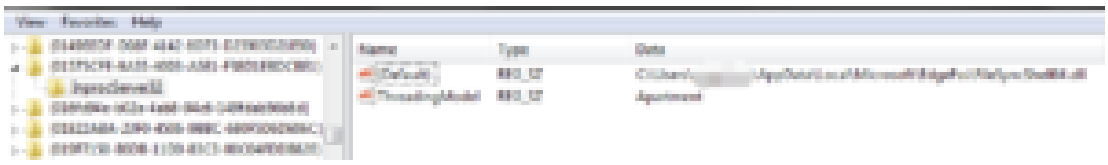


NiceRender诱饵解码前后对比

2. 上线通知

该版本的NiceRender带有一种特殊的操作，会在宏代码运行时通过网络对攻击者进行通知。

这种通知操作通过DNS解析机制实现。NiceRender制作者首先注册名为”cachedns.io”的域名，并且将该域的解析服务器绑定至自身：



cachedns.io域名WHOIS信息

该NiceRender文档的宏代码运行时，会获取当前时间戳组合成一个如下格式的域名：

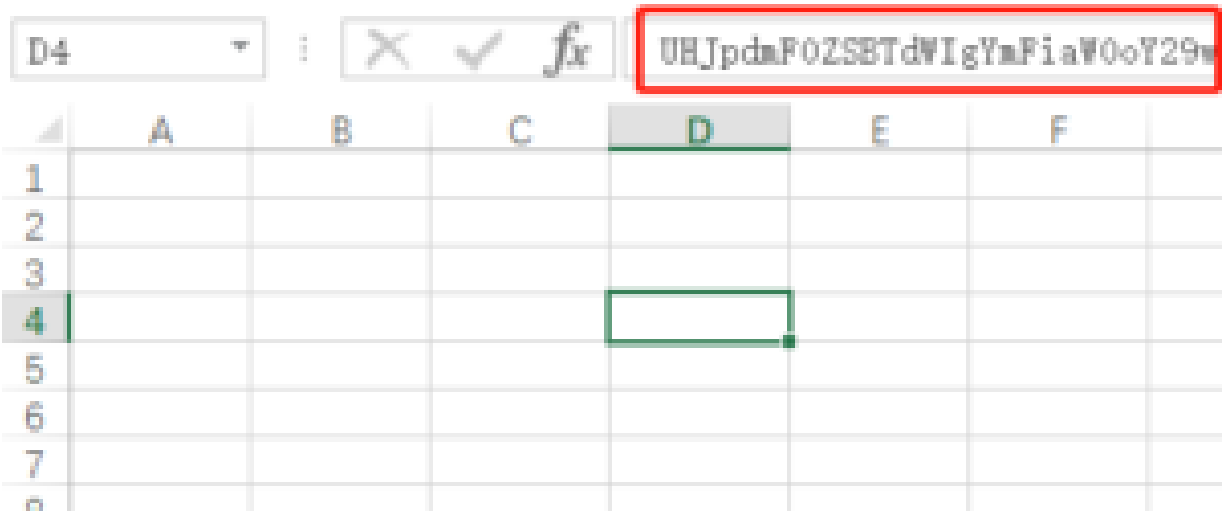
[时间戳].d0g3.cachedns.io

木马随后对该域名进行DNS查询。由于攻击者对该主域进行了如上所述的设置，DNS的相关查询请求会直接发送至攻击者部署的域名服务器当中。攻击者可以读取该域名，获取对应NiceRender组件的标记（d0g3）和运行时间（时间戳）信息，从而掌控该组件的运行状态和攻击规模。

3.载荷释放

NiceRender随后读取文档内特定对象中的文字信息，获取一个PE文件并保存至%LOCALAPPDATA%\Microsoft\EdgeFss\FileSyncShell64.dll。该PE文件即UniversalDonut木马程序。

需要注意的是，NiceRender使用了一种COM组件劫持的策略加载该dll文件。该工具通过修改注册表项，给windows计划任务MsCtfMonitor增加了一个运行项，该项指向上述dll文件路径，从而实现运行恶意程序。



NiceRender写入的注册表项

该劫持逻辑的具体实现可参考
https://github.com/S3cur3Th1sSh1t/OffensiveVBA/blob/main/src/COMHijack_DLL_Load.vba

UniversalDonut

穆伦鲨攻击者频繁使用一种dll形式的木马程序作为其攻击过程中的过渡组件，伏影实验室根据该组件的关键信息将其命名为UniversalDonut。

UniversalDonut是一种shellcode加载器类型的木马程序。木马执行后首先检测以下项目：

1. 检测父进程名称是否为c:\windows\system32\taskhost.exe；
2. 检测自身是否为高权限进程

检测通过后，木马使用多字节异或算法解密资源段中包含的一段shellcode并运行。

UniversalDonut搭载的shellcode是由开源框架Donut（https://github.com/TheWover/donut）生成的完整载荷。借助该框架，UniversalDonut可以在shellcode执行阶段实现大量对抗功能，包括Chaskey算法加密、AMSI/WDLP绕过、连通性检测等。最重要的是，Donut提供的.Net支持使穆伦鲨攻击者可以使用该shellcode加载后续阶段主要木马LetMeOut。

LetMeOut

LetMeOut是一种.Net下载者木马程序，搭载了独特的保险机制。穆伦鲨在入侵流程中多次了使用该木马。

LetMeOut木马的主要代码逻辑分为两部分：

程序首先确认目录%LOCALAPPDATA%\Microsoft\EdgeFss\下是否存在名为FileSyncShell64.dat的二进制文件，如果发现该文件，则使用多字节异或算法和gzip压缩算法对文件进行解密和解压缩，随后载入内存中运行。

通过行为判断，该FileSyncShell64.dat是木马程序经过CnC通信后缓存在本地的加密木马文件。

如果指定目录下未发现名为FileSyncShell64.dat的文件，木马会指定CnC地址进行http通信，并在http参数部分附加三段信息，对应如下：

LetMeOut通信中传递的参数

参数名	参数内容
P1	base64转码，当前代理内容
P2	base64转码，http User-Agent内容
P3	布尔值，是否为64位进程

随后，程序进行第二次http请求，获取一个通过计算得到的hash路径中的内容。该hash路径通过以下参数计算而成：

LetMeOut计算hash路径时使用的参数

回复包中所含加密内容的解密方式与前述对FileSyncShell64.dat文件的处理方式相同，LetMeOut木马将把解密后的内容以shellcode形式运行。

CobaltStrike

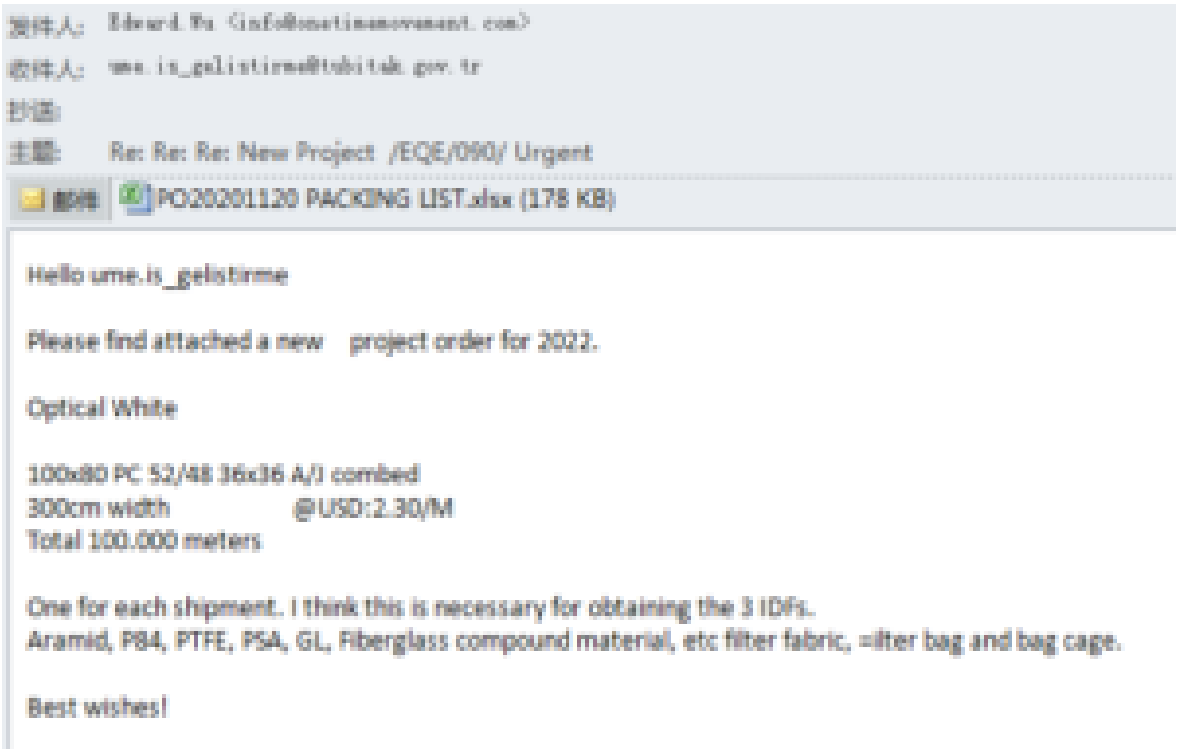
穆伦鲨使用著名的CobaltStrike渗透平台对已入侵成功的主机进行管理，通过CobaltStrike Beacon木马程序完成横向移动与窃密等操作。

八、关联调查

针对土耳其科技研究院的攻击

伏影实验室对调查发现，穆伦鲨的主要目标之一的土耳其科技研究院（TÜBİTAK）并非是第一次受到此类攻击。相反，作为承接了大量土耳其国家项目的顶级科研单位，该科技研究院是各种黑客行为乃至APT活动的重点受害者。

一类多发的针对该机构的攻击以钓鱼邮件的形式发起，攻击者使用压缩包附件、漏洞文档等常见载荷，向tubitak.gov.tr邮箱用户投递AgentTesla等窃密木马，收集受害者主机上的文件、凭证和浏览器缓存数据。


发件人: Edward Wu <is5@austinmovenet.com>
收件人: ume.is_gelistirme@tubitak.gov.tr
抄送:
主题: Re: Re: Re: New Project /EQE/090/ Urgent
邮件 PO20201120 PACKING LIST.xlsx (178 KB)

Hello ume.is_gelistirme

Please find attached a new project order for 2022.

Optical White

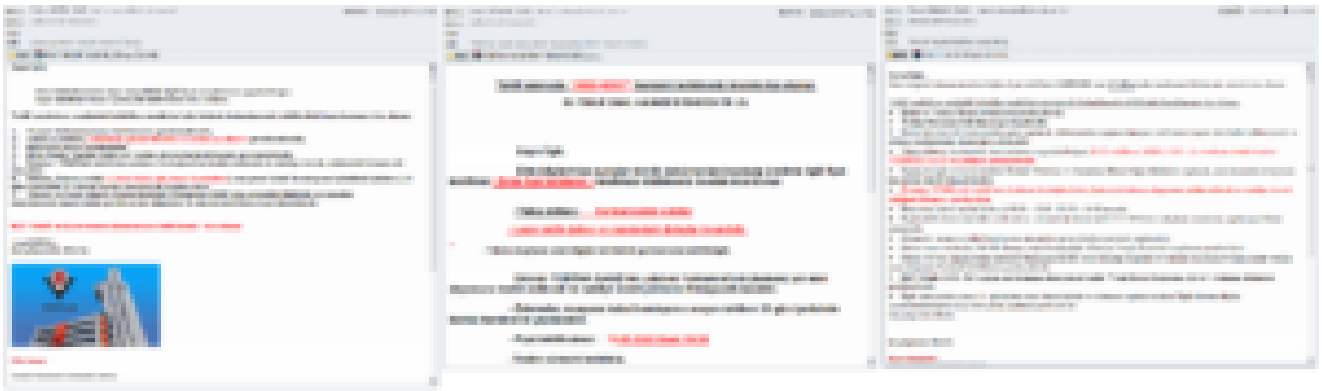
100x80 PC 52/48 36x36 A/J combed
300cm width @USD:2.30/M
Total 100.000 meters

One for each shipment. I think this is necessary for obtaining the 3 IDFs.
Aramid, P84, PTFE, PSA, GL, Fiberglass compound material, etc filter fabric, =ilter bag and bag cage.

Best wishes!

针对土耳其科技研究院的钓鱼邮件A

还有一些邮件正文带有伪造的土耳其科技研究院报价请求与机构图片，邮件的附件部分携带压缩包形式的AgentTesla木马。



针对土耳其科技研究院的钓鱼邮件B

上述几类攻击在近几年的钓鱼邮件类活动中非常典型，邮件黑客组织会使用这种手法窃取受害者主机中的各类文档并在地下平台中出售。这些钓鱼邮件表明，土耳其科技研究院长期处于较高的数据泄露风险中。

另一类攻击则更为严重，直接指向伊朗APT组织MuddyWater。MuddyWater曾在2019年前后对土耳其科技研究院发起了一系列钓鱼攻击，此类攻击的流程比较单一，通过带有TÜBİTAK关键词的诱饵文档投递该组织常用的几类PowerShell木马实现入侵。

针对土耳其科技研究院的钓鱼文档A

针对土耳其科技研究院的钓鱼文档B

发现该线索后，伏影实验室对穆伦鲨和MuddyWater的可能关系展开了调查。

伏影实验室复盘了MuddyWater针对土耳其科技研究院的已知活动和在野样本，在以下维度与穆伦鲨活动进行比对：

相关活动特征对比

	穆伦鲨	**MuddyWater**
直接目标	土耳其科技研究院或土耳其军方	土耳其科技研究院
初始载荷	钓鱼文档	钓鱼文档

诱饵样式	可恢复的文档	不可恢复的文档片段
攻击工具	UniversalDonut，LetMeOut	POWERSTATS或其他PowerShell木马
网络资源	失陷站点	VPS服务器
最终载荷	CobaltStrike Beacon木马	PowerShell后门

通过对比可以看出，穆伦鲨与MuddyWater在特征上的差异大于共性。两者在攻击目标选择、初始阶段组件部分展现出相似性，但后续执行流程则没有重叠。

总体看来，由于MuddyWater的攻击活动比较密集，MuddyWater攻击者在组件设计和资源使用上显得缺乏耐心。该组织在对土耳其科技研究院的活动中照搬了已知攻击手法，组件设计也比较粗糙，伏影实验室在复盘过程中观测到了无法解还原的诱饵内容、复用已暴露的CnC地址等设计缺陷。穆伦鲨则恰恰相反，其开发者在组件和流程设计上更为细致，重点考虑隐藏行为痕迹与个人信息，以减少暴露风险。

MuddyWater是老牌APT组织，其行动代表伊朗国家利益。穆伦鲨在攻击目标方面与MuddyWater的交集，为后续判定组织归属提供了少许线索。

九、总结

穆伦鲨是一个针对土耳其的新型APT组织。伏影实验室通过调查分析，挖掘了该组织的主要活动和主要技术、确定了其独立性和APT属性。调查结果显示，该组织具有明确的攻击目标和丰富的对抗经验，也保留了大量谜团等待解答。

中东地区复杂的国际关系催生了大量APT组织，多个组织具有对土耳其的攻击历史。穆伦鲨究竟是浊浪过后的潺潺细流，还是深埋之下的暗流涌动，目前尚未可知。伏影实验室将持续关注该组织的活动和变化。

十、IoCs

NiceRender ver.1

0a286239b3fe2e44545470e4117f66eb

88bba0077207359cdb9bddb3760f1f32

423cff633679c5dc1bfb27b4499eb171

NiceRender ver.2 partA

3592e56022ce1d87000e36cc0dd37d0e

bb9e1f1e5ef6f3f9f8de6d12d626c435

11a5c681e108cf84a2cc669e8204ac53

0a768a5c9f4714f7ca92545baf9f72c9

a92c6617aa28d4041c44f4b9cc3a5fa3

9a31e7918ae4de42c28d67e711802f58

NiceRender ver.2 partB

07e4844bde106bb6786e9e767d376408

9a0889667c89e592914e74916fd1ec56

468b3eaf031b5aef98b34b5ce39facad

c0f37db18293732872643994e12a4ad2

44da01a0a636a6fa3141c698f3bb2673

UniversalDonut

e6c1685e504fe1d05aa365c79a5e0231

32704a3fb28508e3b15bbbd28716ec76

dc60577efe1d18c05b7c90853bac4c86

349341fe3519a81c0178c5840009cf87

LetMeOut

156e197d7838558f44eed800b3b3ee8a

0f5b520120008ca6969ccad439020f98

d509145bcf4e6af3de1a746609c23564

156e197d7838558f44eed800b3b3ee8a

CobaltStrike Beacon

e4b353f731739487dd48e322bf540405

urls

http[:]//jc.neu.edu[.]tr/apply

http[:]//jc.neu.edu[.]tr/r_main.js

http[:]//bookstore.neu.edu[.]tr/KGB%20Numaralari%20ve%20Gecerlilik%20Tarihleri.xlsx

http[:]//bookstore.neu.edu[.]tr/ara

d0g3.cachedns[.]io

声明