New APT group MurenShark investigative report: Torpedoes hit Turkish Navy

Fuying Laboratory ⋮

I. Overview

In the second quarter of 2022 , NSFOCUS's Fuying Lab detected a series of cyberattacks against Turkey. After analysis, researchers confirmed that this round of attacks came from Actor 210426 , a new threat entity identified by Fuying Lab in April 2021 . Fuying Lab conducted an in-depth investigation of the threat entity through clues such as behavior patterns, attack methods, attack tools, and attack targets, and confirmed its independence and advanced threat nature.

Based on the activity area and recent attack target of this threat entity (Turkish Navy project "MÜREN"), Fuying Lab officially named it as MurenShark , which corresponds to the NSFOCUS Advanced Threat Organization as APT-N-04 .

In the monitoring activities, the main target areas of the Mullen shark include Turkey and Northern Cyprus, and the attack range covers many sensitive targets in the fields of universities, research institutes and the army, especially showing obvious interest in military projects, and has implemented successful Cyber espionage.

Mulun Shark organizers have rich experience in confrontation and are good at anti-analysis and anti-source tracing. The investigation revealed that the exposed attack activities are only the tip of the iceberg of the group's actions, and the discontinuous iterative trajectory of attack targets and attack components shows that a lot of the group's activities are still hidden in the mist.

This report will share the various dimensions of the organization, its relationship with known APT organizations, and other findings from Fuying Lab's investigation.

2. Organizational Information

The Mullen Shark Group is a new type of threat entity active in the Middle East. The main target country is Turkey. The discovered targets include universities in Northern Cyprus , the Turkish army and Turkish national scientific research institutions.

The main attack methods of Murren Shark include delivering phishing documents and attacking online services. The direct purpose includes expanding attack resources, infiltrating target networks, and stealing key data. The group's known spear-phishing attacks first appeared in April 2021 , with breaches of university websites earlier than that date.

Mulun Shark has rich experience in confrontation, and its good methods include hiding attacker information through springboard nodes, blocking process recurrence through component splitting, and

using third-party solutions to reduce code features.

Murren Shark has well concealed the attacker's information in the activities that have been implemented, and it is not yet possible to confirm the geographical affiliation of the organization.

3. Attack Technology Matrix

The figure below shows the attacking technology matrix of Murren Shark, including the capabilities mastered by the attackers and developers of the organization and the capabilities the organization has achieved with the help of third-party tools.

入侵	驻留	权限获取	防御突破	信息搜集	横向移动	命令与控制	数据窃取
网络钓鱼	计划任务/作业	提权获得控制机制	提权获得控制机制	用户账户搜集	远程服务	应用层协议	窃取通道
用户执行	BITS任务	操控访问令牌	操控访问令牌	文件和目录搜集	用户认证信息滥用	数据编码	定时窃取
有效帐户	系统服务	创建或修改系统进程	隐藏组件	网络服务扫描搜集		数据混淆	传输协议
第三方受信任权限利用	有效帐户	通过漏洞利用实现权限提升	破坏防御	网络共享搜集		加密通道	
漏洞利用实现客户端执行	Office应用程序启动	计划任务/作业	清除入侵痕迹	权限组搜集		非应用层协议	
	系统功能滥用	有效帐户	修改注册表	进程搜集		协议隧道	
	创建或修改系统进程		混淆文件或信息	注册表搜集		代理	
			进程注入	远程系统搜集		自定义工具传输	
			反射注入	已安装软件搜集			
			破坏信任控件	系统网络配置搜集			
			签名的二进制文件代理执行	系统网络连接搜集			
			有效帐户	浏览器中间人搜集			
			用户认证信息滥用	信息存储库的数据搜集			
			操作系统凭据转储	本地系统的数据搜集			
			虚拟化/沙箱逃逸	键盘输入搜集			
			反调试	屏幕捕获搜集			

Murren Shark Green Alliance Technology Attack Technology Matrix

4. Typical Activities

Mullen shark is not a very active attacker, and its attack activity distribution has obvious aggregation.

The most recent round of Mullen Shark activities focused on the first half of August this year. The attackers delivered various forms of Turkish phishing documents to attack specific targets in Turkey.

Phishing documents appearing in this round of attacks have the following file names:

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

Mullen Shark Partial Fishing Document File Name

The first type of fishing document shows the title "Comments on MÜREN Key Design Documents" (MÜREN KR İTİK TASARIM DOKÜMANINA YÖNELİK GÖRÜŞLER), and the header part shows that the document comes from "The Command of the Naval Command 1st Submarine Fleet TCG Sakarya" :

Phishing Document A

The document, which details the Turkish Navy 's revisions to an in-submarine system called " MÜREN ", is dated June 2022 .

Another type of fishing document shows the title MÜREN-PREVEZE (M İLLİ ÜRETİM ENTEGRE SUALTI SAVAŞ YÖNETİM SİSTEMİ PREVEZE SINIFI UYGULAMASI (MÜREN-PREVEZE) PROJESİ), which is a national production integrated underwater combat management system pre-level application project, which shows that the document comes from Turkish technology Research Center of Informatics and Information Security Advanced Technology Research Center (TÜBİTAK BİLGEM):

Phishing Document B

This phishing document corresponds to a description file for a software system called " MÜREN-PREVEZE ".

After searching for relevant keywords, Fuying Lab determined that the above two documents were from the Turkish military project " MÜREN ". This is a submarine combat management system (CMS) designed by TÜB İTAK , the Turkish Academy of Science and Technology (https://bilgem.tubitak.gov.tr/tr/haber/akya-torpidosu-muren-prevezeye -entegre-ediliyor), and has been tested in 21 , available to the Turkish Naval Command in 22 (https://raillynews.com/2021/11/denizaltilari-muren-yonetecek/) . The Turkish Navy has high expectations for the MÜREN project, believing that the project can promote the localization of Turkish naval systems and become a key step in the Turkish national-class submarine project "MILDEN" (https://www.navalnews.com/naval-news/2021 /11/turkeys-new-submarine-cms-muren-to-enter-service-in-2022/).

From this, it can be inferred that the main target of Muren Shark’s activities in early August was the relevant personnel of the “ MÜREN ” project, including the project designers of the Turkish Academy of Science and Technology and the project reviewers of the Turkish Navy.

Based on the information currently available, Fuying Lab cannot judge whether this round of attacks has achieved the intended purpose, but from the content of the decoy document, it can be seen that Murren Shark has successfully invaded the interior of the Turkish Institute of Science and Technology through other attack activities and has stolen it. High-value document content.

Mullen sharks showed a completely different tendency to attack in earlier attacks. In a reported attack by Fuying Labs (http://blog.nsfocus.net/apt-dogecoin/), the group used a Dogecoin -related reporting document as bait to target virtual The currency's followers carried out a phishing attack:

Phishing Document C

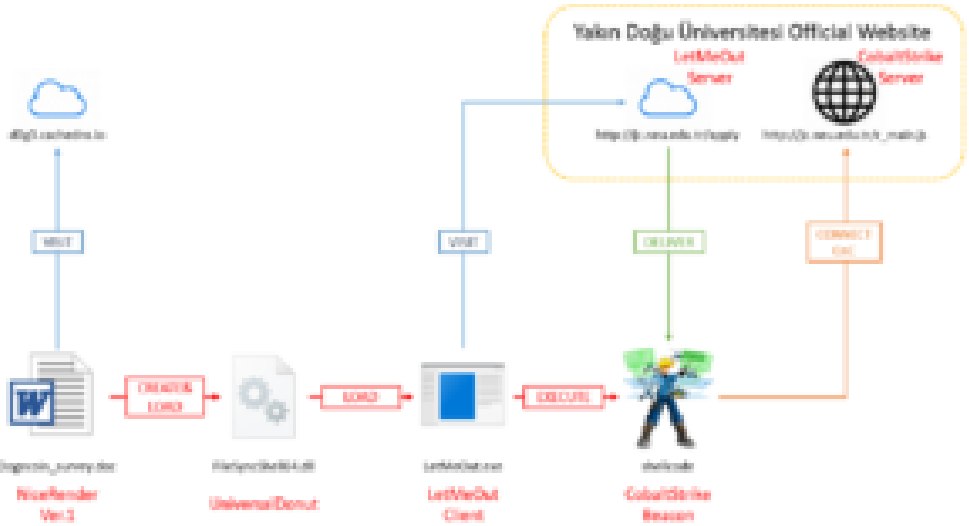
Except that the bait document found that the area is Turkey, no other information was disclosed in the activity of Mullen sharks.

Affected by the national economic policy, the cryptocurrency industry is extremely popular in Turkey. Combined with the organization's activity track, Fuying Lab concluded that this type of phishing attack was part of the coarse-precision fishing activity organized by the Mullen Shark, and the main target was also Turkey. Hacker groups usually rely on such highly topical decoy documents to conduct extensive information collection activities, and then filter high-value information from the obtained intelligence.

5. Typical attack process

Murren Shark frequently uses a representative attack process and continues to improve the process and its components.

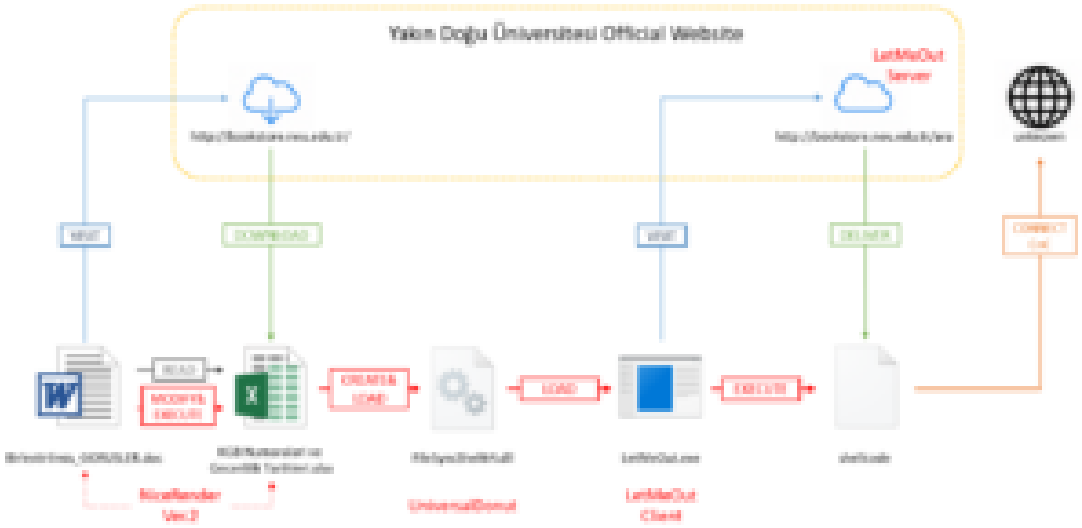
The diagram below shows a typical process used by the organization across its 21-year campaign:



Attack Process A

The attack process consists of three main attack components of Murren Shark, NiceRender, UniversalDonut, LetMeOut, the lost site neu.edu.tr, and the third-party attack tool CobaltStrike, which finally steals the data in the victim's host and stores it on the victim's host. The purpose of lateral movement within the domain.

The following diagram shows the improved process used by the group in recent attacks against Turkish navy and scientific institutions:



Attack Process B

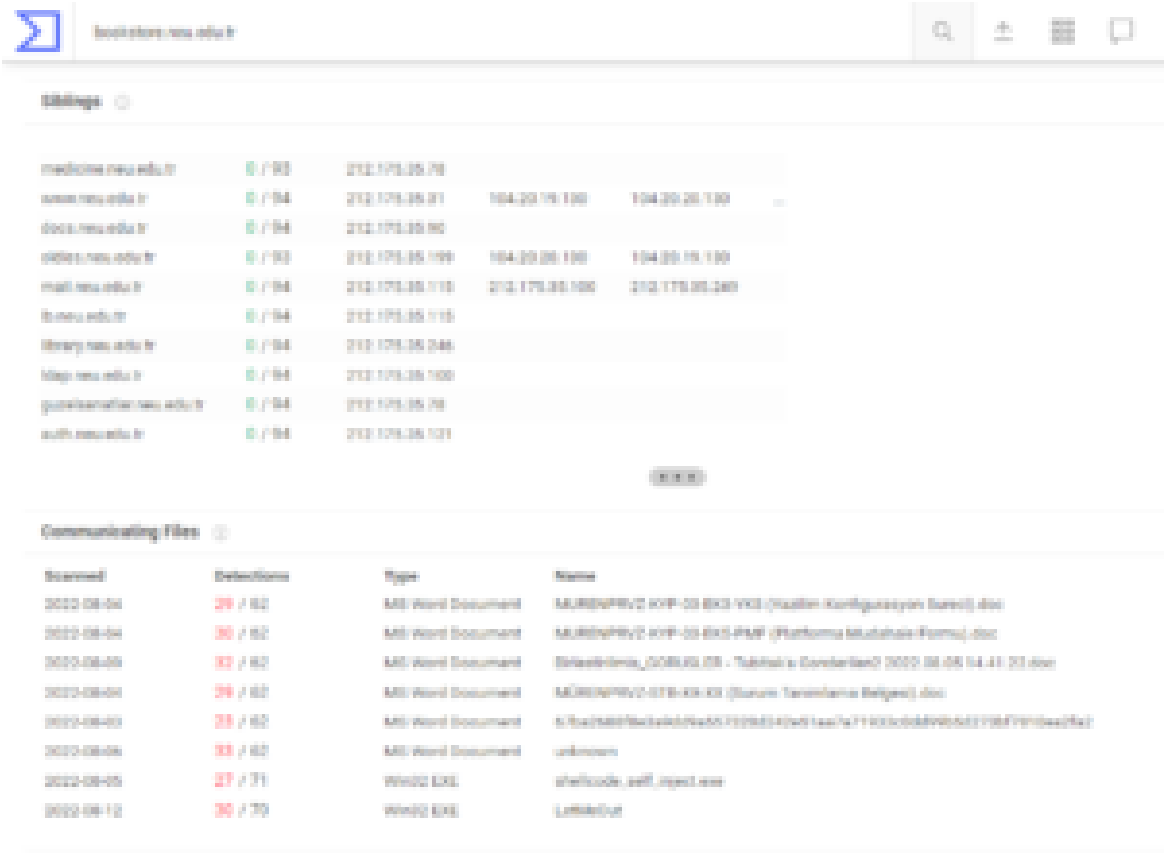
The process also consists of three main components and the same lost site. The difference is that the Mullenshark attackers used a new NiceRender file in the process, while further shortening the process life cycle, which makes it difficult for sandbox-type security products to reproduce the full execution process.

six,Attack method characteristics

- **Take advantage of the lost site**

Murren Shark tends to use the compromised site as a file server and CnC server in the attack process. As shown in the chapter on the typical attack flow, the group used the official website of the Near East University (Yakın Doğu Üniversitesi) (https://neu.edu.tr/) as a remote server for its activities in each period.

Near East University is a private university located in the Northern Cyprus region. The known attack process shows that Murren Shark has controlled the server of the official website of Near East University for more than a year, and has deposited Trojans in multiple locations on the website, ran the LetMeOut Trojan server, and even deployed the server of the CobaltStrike penetration platform for Sustained control over the victim.



Controlled Near East University website

Despite possessing such attack resources, Murren Shark's use of lost sites is generally restrained, and these sites are silent for the vast majority of the time and have not been traded or abused. This use of the lost site by the Mullen shark effectively hides traces of the organization and prolongs the availability of resources.

- **Component behavior breakdown**

When designing the process, Murren Shark follows a special behavioral splitting idea.

For example, the new version of the NiceRender attack component recently used by the group splits the regular functions of malicious documents into two parts. Part A is designed as a macro code reader and injector, and part B is designed as a macro code carrier and an injector. Injecting a vector, A needs to get B over a network connection to run the full component behavior.

For another example, the LetMeOut Trojan program commonly used by the organization will also split its download function into two parts. The Trojan first uploads the Trojan information and the victim's host information to CnC, and then obtains the download path of the subsequent load through calculation after receiving the confirmation information from the server.

The advantages of this design idea are obvious. In conjunction with the compromised sites described above, these components will not produce any malicious behavior on the network side and process side when the remote address fails or stops serving, and even untrained personnel cannot detect it when opening the corresponding file. abnormal. These subdivided component behaviors also interfere with forensic analysis and attack process restoration. A large number of interaction mechanisms effectively protect network resources and attack components in the process, reducing the exposure probability.

When CnC is disconnected, the behavior of the new version of NiceRender is similar to that of regular documents:

NiceRender behavior in disconnected state

7. Known attack tools

- **NiceRender**

The tool is a malicious macro-type document with a specific execution mode, which is used by the Mullenshark attackers to craft various phishing documents, which are used as initial payloads for their attack campaigns. There are currently two versions of the tool.

- **NiceRender Ver.1**

The early version of NiceRender includes three functional parts, namely decoy decoding, online notification and payload release.

1. Decoy decoding

The biggest difference between NiceRender and other common phishing documents is that this component will use a unique logic to transcode the text content in the document into garbled characters, and after performing the above stages, decode these garbled characters, and deliver a message to the victim. The illusion that encrypted documents are indeed decrypted, increasing the credibility of such phishing documents.

NiceRender's character conversion logic is to search for a specific wide-byte character and convert it to the corresponding ASCII character.

The sequence of decimal values corresponding to the wide character to be converted is:

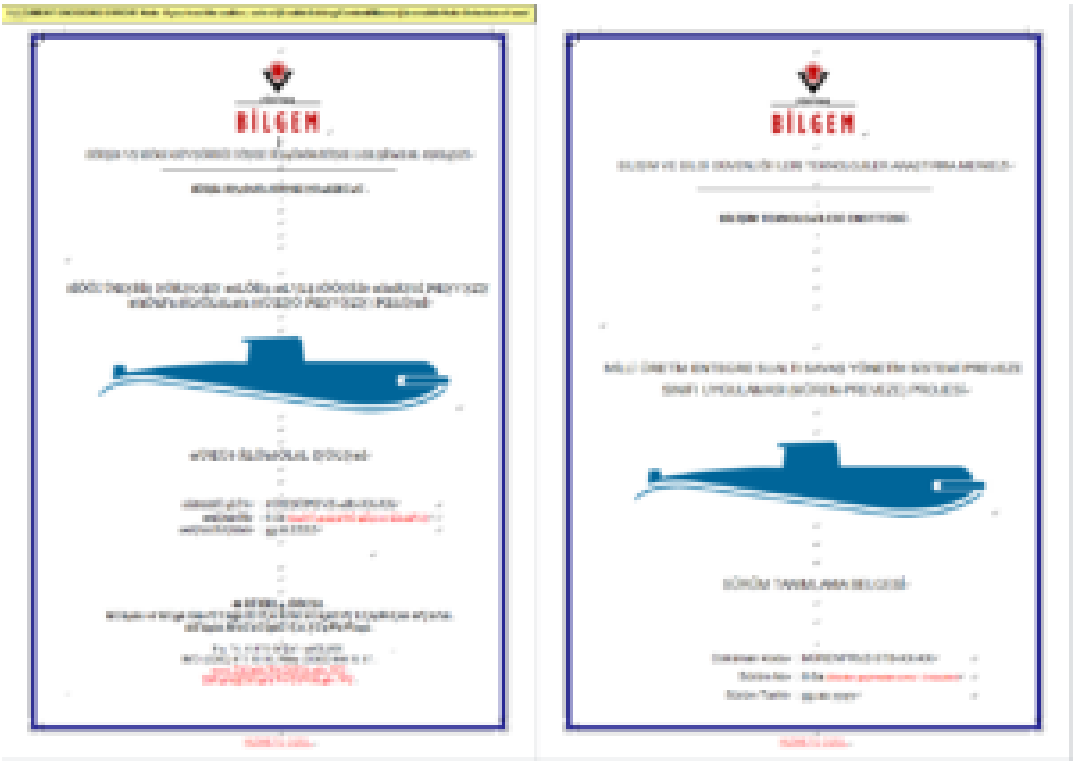
[321, 325, 338, 334, 332, 331, 324, 329, 335, 333, 341, 340, 339, 322, 345, 353, 357, 361, 370, 366, 364, 363, 356, 367, 365 , 373, 372, 371, 354, 377]

The corresponding ASCII character sequence is:

[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]

Once the conversion is complete, NiceRender hides the Enable Editing feature at the top of the original content, further enhancing document credibility.

The image below shows a comparison of the original content of a typical NiceRender decoy with the transcoded effect.

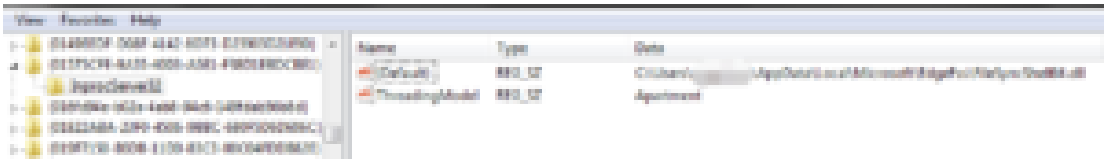


NiceRender decoy decoding before and after comparison

2. Online notification

This version of NiceRender comes with a special action that notifies the attacker over the network when the macro code is running.

This notification operation is implemented through the DNS resolution mechanism. The NiceRender creator first registers a domain name called "cachedns.io" and binds the resolver server for that domain to itself:



cachedns.io domain WHOIS information

When the macro code of the NiceRender document runs, it will obtain the current timestamp and combine it into a domain name in the following format:

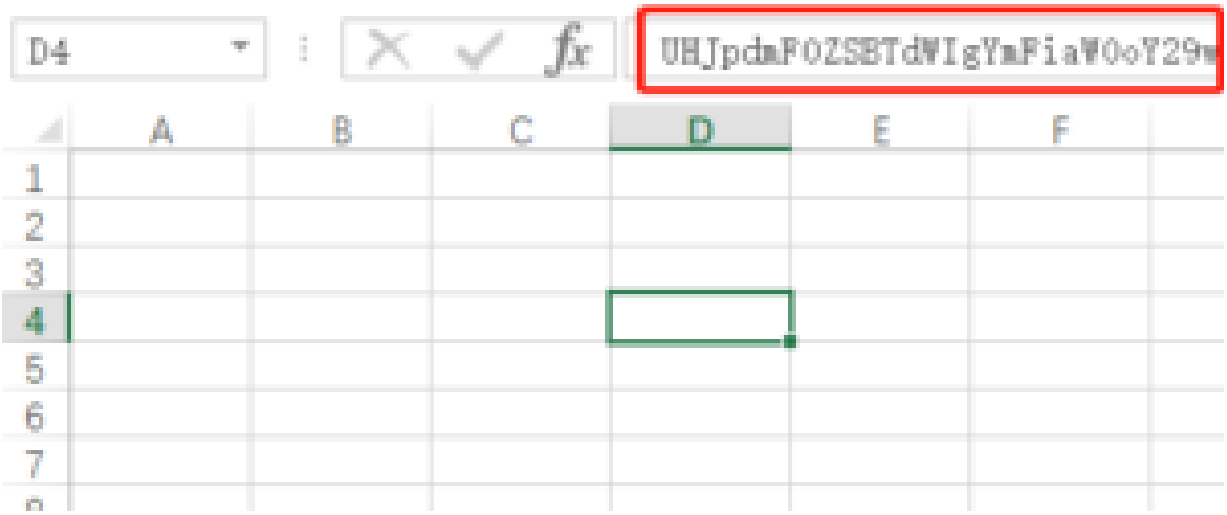
[timestamp].d0g3.cachedns.io

The Trojan then performs a DNS query for the domain name. Since the attacker has set the primary domain as described above, the related DNS query request will be sent directly to the domain name server deployed by the attacker. An attacker can read the domain name to obtain the tag (d0g3) and running time (timestamp) information of the corresponding NiceRender component , so as to control the running status of the component and the scale of the attack.

3. Load release

NiceRender then reads the text information in the specific object in the document, obtains a PE file and saves it to %LOCALAPPDATA%\Microsoft\EdgeFss\FileSyncShell64.dll . The PE file is the UniversalDonut Trojan.

It should be noted that NiceRender uses a COM component hijacking strategy to load the dll file. By modifying the registry key, the tool adds a run item to the Windows scheduled task MsCtfMonitor , which points to the above-mentioned dll file path, so as to run malicious programs.



Registry key written by NiceRender

For the specific implementation of the hijacking logic, please refer to https://github.com/S3cur3Th1sSh1t/OffensiveVBA/blob/main/src/COMHijack_DLL_Load.vba

- **UniversalDonut**

Mullenshark attackers frequently use a Trojan in the form of dll as a transitional component in their attack process, and Fuying Lab named it UniversalDonut based on the key information of this component.

UniversalDonut is a shellcode loader type Trojan. After the Trojan is executed, it first detects the following items:

1. Check if the parent process name is c:\windows\system32\taskhost.exe;
2. Check if it is a high-privileged process

After the detection is passed, the Trojan uses the multi-byte XOR algorithm to decrypt a piece of shellcode contained in the resource segment and run it.

The shellcode carried by UniversalDonut is a complete payload generated by the open source framework Donut (https://github.com/TheWover/donut). With this framework, UniversalDonut can implement a large number of countermeasures in the shellcode execution stage, including Chaskey algorithm encryption, AMSI/WDLP bypass, connectivity detection, etc. Most importantly, the .Net support provided by Donut allows Murrenshark attackers to use this shellcode to load the main trojan LetMeOut in subsequent stages.

- **LetMeOut**

LetMeOut is a .Net downloader Trojan with a unique insurance mechanism. Murren Shark used this Trojan several times during the intrusion process.

The main code logic of the LetMeOut Trojan is divided into two parts:

The program first confirms whether there is a binary file named FileSyncShell64.dat in the directory %LOCALAPPDATA%\Microsoft\EdgeFss\. If the file is found, it uses the multi-byte XOR algorithm and the gzip compression algorithm to decrypt and decompress the file, and then download the file. run in memory.

Judging by the behavior, the FileSyncShell64.dat is an encrypted Trojan file cached locally after the Trojan program communicates with CnC.

If the file named FileSyncShell64.dat is not found in the specified directory, the Trojan will specify the CnC address for http communication, and append three pieces of information to the http parameter part, corresponding to the following:

Parameters passed in LetMeOut communication

parameter name	Parameter content
P1	base64 transcoding, current proxy content
P2	base64 transcoding, http User-Agent content
P3	boolean, whether it is a 64-bit process

Subsequently, the program makes a second http request to obtain the content in a hash path obtained by calculation. The hash path is calculated with the following parameters:

Parameters used by LetMeOut to calculate the hash path

The decryption method of the encrypted content contained in the reply packet is the same as the above-mentioned processing method for the FileSyncShell64.dat file, and the LetMeOut Trojan will run the decrypted content in the form of shellcode.

- **CobaltStrike**

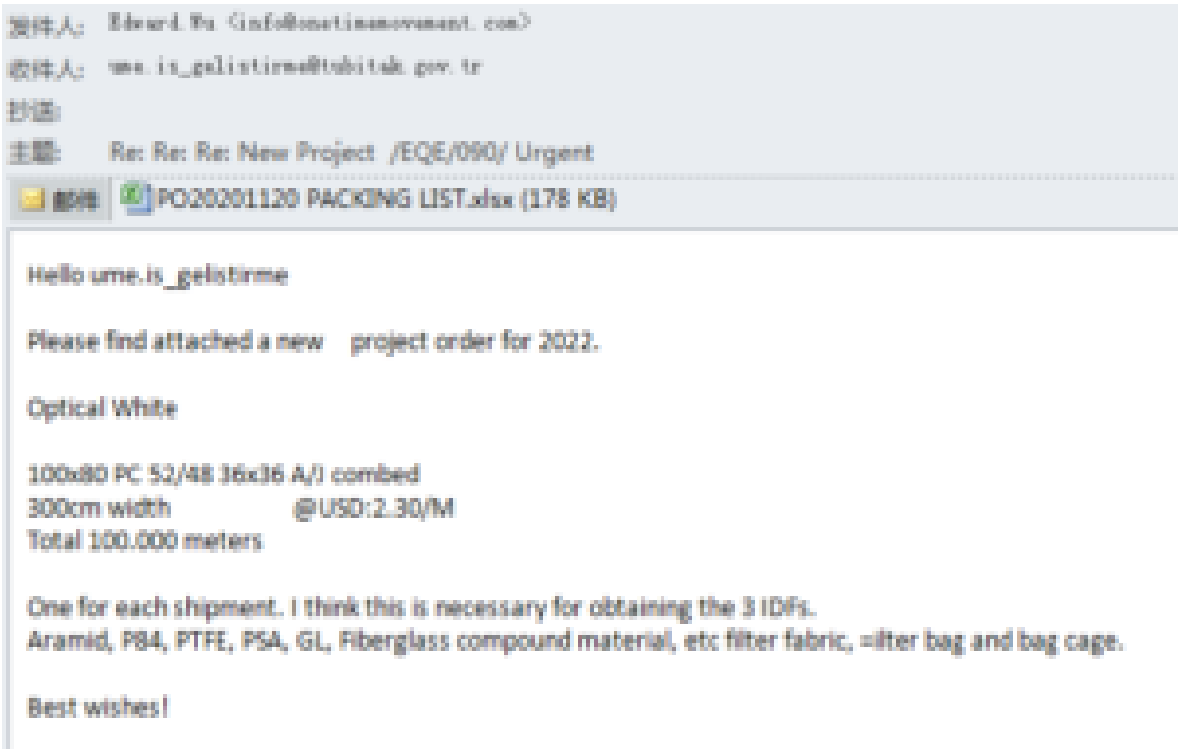
Murren Shark uses the famous CobaltStrike penetration platform to manage the successfully invaded hosts, and uses the CobaltStrike Beacon Trojan to complete operations such as lateral movement and stealing.

Eight,Association investigation

- **Attack on Turkish Institute of Science and Technology**

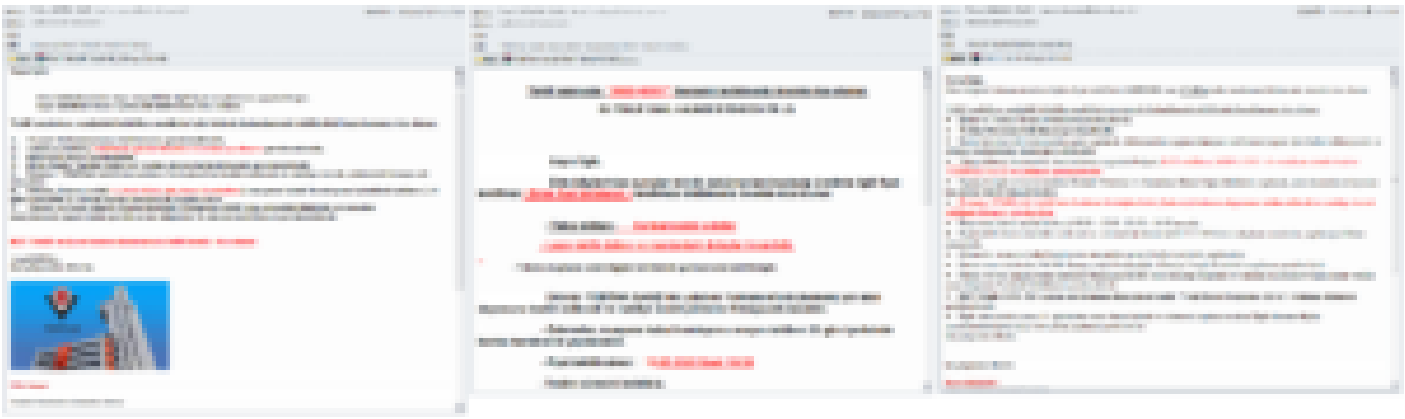
The investigation by Fuying Lab found that it is not the first time that the Turkish Institute of Science and Technology (TÜBİTAK), one of the main targets of the Murren shark, has been attacked. On the contrary, as a top scientific research institution that undertakes a large number of Turkish national projects, the Institute of Science and Technology is a key victim of various hacking and even APT activities.

A type of frequent attacks against the organization are launched in the form of phishing emails. The attackers use common payloads such as compressed package attachments and vulnerability documents to deliver secret-stealing Trojans such as AgentTesla to tubitak.gov.tr mailbox users to collect files on the victim's host. , credentials, and browser cache data.



Phishing email A targeting the Turkish Academy of Science and Technology

There are also some emails with forged quotation requests and institutional pictures from the Turkish Academy of Science and Technology, and the attachments of the emails carry the AgentTesla Trojan in the form of a compressed package.



Phishing Email B targeting Turkish Institute of Science and Technology

The above types of attacks are typical of phishing email campaigns in recent years. Email hacking groups use this method to steal various documents from victims' hosts and sell them on underground platforms. These phishing emails indicate that the Turkish Institute of Science and Technology has long been at a high risk of data breaches.

Another type of attack is more serious, directly targeting the Iranian APT group MuddyWater. MuddyWater launched a series of phishing attacks on the Turkish Academy of Science and Technology around 2019. The process of such attacks is relatively simple. Several types of PowerShell Trojans commonly used by the organization are delivered through decoy documents with TÜBİTAK keywords.

Phishing Document A for Turkish Academy of Science and Technology

Phishing Document B for Turkish Academy of Science and Technology

After discovering this clue, Fuying Lab launched an investigation into the possible relationship between Muren Shark and MuddyWater.

Fuying Lab reviewed the known activities of MuddyWater against the Turkish Institute of Science and Technology and samples in the field, and compared the activities of MuddyWater with the activities of Muren sharks in the following dimensions:

Comparison of related activity characteristics

	Mullen Shark	**MuddyWater**
direct target	Turkish Institute of Science and Technology or Turkish Military	Turkish Institute of Science and Technology
initial load	Phishing Documentation	Phishing Documentation
bait style	recoverable documents	Unrecoverable Document Fragments
attack tool	Universal Donut, LetMeOut	POWERSTATS or other PowerShell Trojans

Internet resources	lost site	VPS server
final load	CobaltStrike Beacon Trojan	PowerShell backdoor

By comparison, it can be seen that the differences in characteristics between Muren sharks and MuddyWater are greater than the commonalities. The two show similarities in attack target selection and components in the initial stage, but there is no overlap in the subsequent execution process.

Overall, MuddyWater attackers are impatient in component design and resource usage due to the intensive attack activities of MuddyWater. The organization copied the known attack methods in the activities of the Turkish Academy of Science and Technology, and the component design was relatively rough. During the review process, Fuying Lab observed unrecoverable bait content, reused exposed CnC addresses, etc. Design flaws. Murren Shark is the opposite. Its developers are more meticulous in the design of components and processes, focusing on hiding behavior traces and personal information to reduce the risk of exposure.

MuddyWater is a veteran APT organization whose actions represent the national interests of Iran. The intersection of Muren Shark and MuddyWater in terms of attack targets provides some clues for the subsequent determination of the organization's ownership.

9. Summary

Murren Shark is a new type of APT group targeting Turkey. Through investigation and analysis, Fuying Lab excavated the main activities and main technologies of the organization, and determined its independence and APT attributes. The survey results show that the organization has a clear attack target and rich experience in confrontation, and also retains a lot of mysteries waiting to be answered.

The complex international relations in the Middle East have spawned a large number of APT organizations, many of which have a history of attacking Turkey. Whether the Mulun shark is a trickle after the turbid waves or a surging undercurrent under the deep burial is still unknown. Fuying Lab will continue to monitor the organization's activities and changes.

ten,loCs

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

statement

This security bulletin is only used to describe possible security issues, and NSFOCUS does not provide any guarantee or commitment to this security bulletin. Any direct or indirect consequences and losses caused by the dissemination and use of the information provided in this security bulletin are the responsibility of the user, and NSFOCUS and the author of the security bulletin do not assume any responsibility for this.

NSFOCUS reserves the right to modify and interpret this security announcement. If you want to reprint or disseminate this security bulletin, you must ensure the integrity of this security bulletin, including the copyright notice and other contents. Without the permission of NSFOCUS, the content of this security bulletin shall not be modified or added arbitrarily, and shall not be used for commercial purposes in any way.