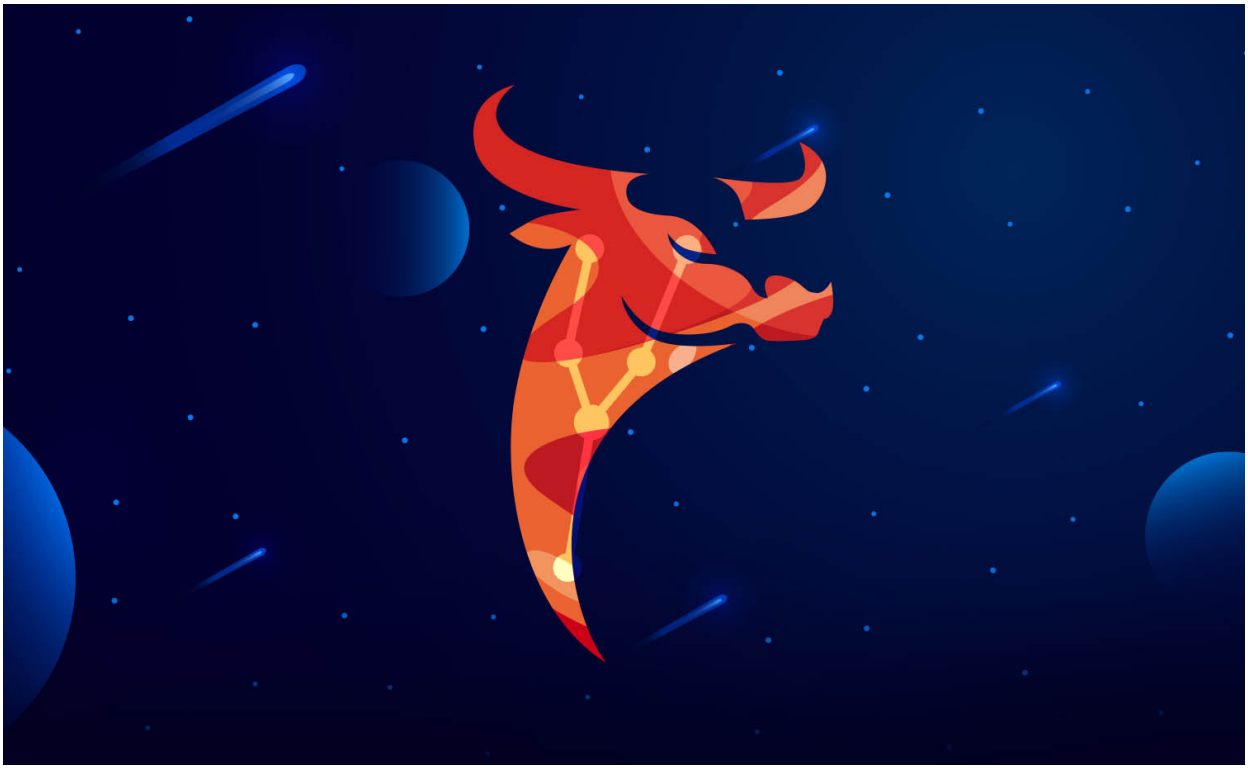
unit42.paloaltonetworks.com /playful-taurus/

Chinese Playful Taurus Activity in Iran

Unit 42 ⋮⋮ 1/18/2023



Executive Summary

Playful Taurus, also known as APT15, BackdoorDiplomacy, Vixen Panda, KeChang and NICKEL, is a Chinese advanced persistent threat group that routinely conducts cyber espionage campaigns. The group has been active since at least 2010 and has historically targeted government and diplomatic entities across North and South America, Africa and the Middle East.

In June 2021, ESET reported that this group had upgraded their tool kit to include a new backdoor called Turian. This backdoor remains under active development and we assess that it is used exclusively by Playful Taurus actors. Following the evolution of this capability, we recently identified new variants of this backdoor as well as new command and control infrastructure. Analysis of both the samples and connections to the malicious infrastructure suggests that several Iranian government networks have likely been compromised by Playful Taurus.

Palo Alto Networks customers receive protections from the threats described in this blog through Advanced URL Filtering, DNS Security, Cortex XDR and WildFire malware analysis.

Names for Threat Actor Group Discussed	Playful Taurus, APT15, BackdoorDiplomacy, Vixen Panda, NICKEL

Table of Contents

Playful Taurus Infrastructure

In 2021, the domain vpnkerio[.]com was identified as part of a Playful Taurus campaign targeting diplomatic entities and telecommunications companies across Africa and the Middle East. Since then, this domain and its associated subdomains have shifted hosting to several new IP addresses. Notably, several of the subdomains currently resolve to 152.32.181[.]16.

Analyzing this IP, we identified an expired X.509 certificate that appeared to be associated with Senegal's Ministry of Foreign Affairs (MFA), CN=diplosen.gouv[.]sn.

Suspected Playful Taurus X509 Certificate	
SHA-1	cfd9884511f2b5171c00570da837c31094e2ec72
Issued	2020-04-23
Expires	2021-04-29
Common Name	diplosen.gouv[.]sn
Organization Name	DigiCert, Inc.
SSL Version	3
Locality	Dakar
Country	SN

Table 1. Suspected Playful Taurus certificate.

Despite expiring in April 2021, this certificate continued to be associated with recent infrastructure. For example, this certificate was first observed on 152.32.181[.]16 in April 2022, a full year after it had expired. Coincidentally, that same month, subdomains for vpnkerio[.]com began resolving to this IP.

Exploring all IP associations with this certificate, we found that this certificate was initially associated with what we assess is likely legitimate Senegal government infrastructure. This association remained consistent until the expiration of the certificate in April 2021. Following its expiration, this certificate has been associated with nine different IP addresses. Eight of those nine IPs have hosted Playful Taurus domains.

Observed Activity

Monitoring connections to the malicious infrastructure, we observed the following four Iranian organizations attempting to connect to 152.32.181[.]16 between July and late December 2022.

Iranian Connections to Playful Taurus Infrastructure

IP Address	Organization
109.201.27[.]66	Iranian Government Infrastructure
185.4.17[.]10	Foreign Ministry of Iran Infrastructure
37.156.28[.]101 37.156.29[.]172	Suspected Iranian Government Infrastructure
31.47.62[.]201	Iranian Natural Resource Organization

Table 2. Iranian connections to Playful Taurus infrastructure.

The sustained daily nature of these connections to Playful Taurus controlled infrastructure suggests a likely compromise of these networks. Moreover, these targets also fit historical targeting patterns by the group.

Inside the Wire

While researching the Iranian infrastructure in Table 2, we found that the first IP (109.201.27[.]66) hosted what appears to be a legitimate Foreign Ministry of Iran domain (pro.mfa[.]ir) between May and November 2019. This IP also resides on a netblock that hosts other Iranian government domains.

However, since September 2021, this IP has hosted the domain mfaantivirus[.]xyz. The use of the .xyz top level domain (TLD) seems odd for an IP and netblock that hosts legitimate Iranian government domains.

The registration record for mfaantivirus[.]xyz shows that it was registered by an organization that has only registered eight other domains. Three of those domains, including mfaantivirus[.]xyz, stand out for being hosted on Iranian government netblocks. The two additional domains hosted on Iranian government infrastructure are as follows.

Registration Organization Overlap

IP	Domain	Owner
109.201.27[.]67	pfs1010[.]xyz	Foreign Ministry of Iran *Reverse PTR: cp.econsular[.]ir*
109.201.19[.]184	pfs1010[.]com	Foreign Ministry of Iran

Table 3. Domains sharing a registering organization with mfaantivirus[.]xyz.

The first IP in Table 3 contains a reverse DNS pointer to cp.econsular[.]ir, and the second IP's netname is "Foreign Ministry of Iran." This suggests that both are affiliated with the Iranian government.

That said, further analysis of these IPs revealed associations with two X.509 certificates. The earliest certificate appears to be related to pfSense and was only associated with these IPs for a single day in

August 2019. This leads us to believe that the two pfs1010.* domains are made to resemble pfSense firewalls. The use of the domain name mfaantivirus[.]xyz loosely fits the security theme as well.

The second certificate associated with the IPs in Table 3 is a self-signed certificate with a common name of www.netgate[.]com. Netgate is the doing business as (DBA) name for Rubicon Communications, who developed pfSense – again sticking with the pfSense theme. Below is the information associated with that certificate.

Netgate X.509 Certificate	
SHA-1	1cf1985aec3dd1f7040d8e9913d9286a52243aca
Issued	2022-04-21
Expires	2032-04-18
Common Name	www.netgate[.]com
Organization Name	netgate
SSL Version	1
Locality	New York
State/Province	New York
Country	United States

Table 4. Second suspected Playful Taurus certificate.

There are five additional malicious IPs associated with this certificate, but the two we wish to highlight are the following.

X509 Certificate Two - IP Associations	
IP	**Owner**
151.248.24[.]251	NYNEX satellite OHG Previous Cert: portal-Share.mfa[.]new
158.247.222[.]6	Constant Company VPS

Table 5. X509 certificate two – IP associations.

The first IP contains a historical certificate reference to portal-Share.mfa[.]new, which suggests an ambiguous “Ministry of Foreign Affairs (MFA)” nexus. The second is a virtual private server (VPS) owned by The Constant Company. This second IP (158.247.222[.]6) hosted the domain www[.]delldrivers[.]in from July 7, 2022 to Oct. 11, 2022. This domain is associated with a Turian backdoor sample.

Tying this all together, we identified Iranian government infrastructure establishing connections with a known Playful Taurus command and control (C2) server. Pivoting on one of the Iranian government IPs, we then identified additional infrastructure hosting certificates that overlap with a second Playful Taurus C2 server.

Turian Backdoor

Analyzing the domain *.delldrivers[.]in resulted in the identification of the following sample of malware.

File Details

File Details	
Filename	dellux[.]exe
Creation Time	2022-06-27 01:25:26 UTC
SHA256	67c911510e257b341be77bc2a88cedc99ace2af852f7825d9710016619875e80
Connections	update.delldrivers[.]in

File Details	
Filename	dellux[.]exe
Creation Time	2022-06-27 01:25:26 UTC
SHA256	67c911510e257b341be77bc2a88cedc99ace2af852f7825d9710016619875e80
Connections	update.delldrivers[.]in

Table 1. Details for Trojan samples

This sample was uploaded to VirusTotal from submitters in Iran on Nov. 12 and 13, 2022. We further observed that these same submitters uploaded files and URLs that suggest a likely affiliation with Iran's Ministry of Foreign Affairs.

Technical Analysis

We found that this sample is packed with VMProtect. However, the final payload is not virtualized and is ultimately unpacked into the .text, .data and .rdata sections of the payload. Unfortunately, VMProtect obfuscates all API calls within the sample. So whenever an API call is made, execution jumps to the .vmp0 section to resolve the import and execute it.

While the functionality of the sample becomes increasingly difficult to analyze due to the API obfuscation, the strings within the unpacked .data section provide a useful pivot point for identifying additional samples that contain the same functionality but are not packed with VMProtect.

Alongside the strings, the sample also contains a fairly unique XOR decryption function (shown in Figure 1). This is used to decrypt the embedded C2 server, update.delldrivers[.]in.

```
result = 0;
v2 = strlen(a1) + 1;
v3 = v2 - 1;
if ( v2 != 1 )
{
  do
  {
    v3 = 134775813 * v3 + 1;
    a1[result++] ^= v3;
  }
  while ( result < v2 - 1 );
}
return result;
}
```

Figure 1. Fairly unique decryption algorithm.

A similar algorithm has been seen within the Neshta file infector, back in 2014. Data encrypted with this algorithm can be decrypted with the Python snippet shown in Figure 2.

```
enc = b"encrypted_data"
dec = b""
counter = 0
key = len(enc) - 1

while counter < (len(enc) - 1):
  key = (134775813 * key + 1) & 0xFF
  dec += bytes([(enc[counter] ^ key)])
  counter += 1
```

Figure 2. Python data decryptor.

Pivoting on the algorithm's byte pattern {69 D2 05 84 08 08 8A 1C 30 42 32 DA 88 1C 30} allows us to identify two additional malware samples.

File Details	
Filename	scm[.]exe
Type	EXE
Creation Time	2022-04-28 02:56:26 UTC
SHA256	8549c5bafbfad6c7127f9954d0e954f9550d9730ec2e06d6918c050bf3cb19c3
Connections	scm.oracleapps[.]org

Table 7. File details of the first sample located via pivoting on algorithm byte pattern.

File Details	
Type	DLL
Creation Time	2022-06-18 14:43:13 UTC
SHA256	ad22f4731ab228a8b63510a3ab6c1de5760182a7fe9ff98a8e9919b0cf100c58
Connections	update.adboeonline[.]net

Table 8. File details of the second sample located via pivoting on algorithm byte pattern.

The Turian Link

Aside from the C2 infrastructure being very similar in naming convention, comparing the code bases of these samples to the unpacked VMProtect sample indicates clear overlap between the functionality.

Due to the almost identical code base, we opted to focus our analysis on the executable, rather than the DLL. Before doing so, we had a look at the DLL and noticed several cleartext strings.

```
ReG aDd %s%S /v ImagePath /t REG_EXPAND_SZ /d "%S" /f
ReG dELete %s%S\pARamEteRs /v ServiceDllUnloadOnStop /f
ReG aDd %s%S /v Start /t REG_DWORD /d 2 /f
ReG aDd %s%S\pARamEteRs /v ServiceDll /t REG_EXPAND_SZ /d "%S"
/f
hKEy_LOcAl_MaChiNE\SYsTEm\CuRRenTCoNTRolSeT\SeRViCeS\
```

Searching for samples with similar strings, we identified two additional samples.

File Details	
Type	DLL

File Details	
Type	DLL
Creation Time	2022-04-28 02:56:26 UTC
SHA256	5bb99755924ccb6882fc0bdedb07a482313daeaaa449272dc291566cd1208ed5
Connections	127.0.0.1

Table 9. File details of the first sample located via pivoting on registry strings.

File Details	
Type	x64 DLL
Creation Time	2022-06-18 14:43:13 UTC
SHA256	6828b5ec8111e69a0174ec14a2563df151559c3e9247ef55aeaaf8c11ef88bfa
Connections	mail.indiarailways[.]net

Table 10. File details of the second sample located via pivoting on registry strings.

These samples have been tagged in VirusTotal as being APT_MAL_LNX_Turian_Jun21_1, which is a Linux version of the Turian backdoor. However, these samples are clearly not for Linux systems. This tag did point us toward previous reporting on the Turian/Quarian backdoors, which established a link between our dellux.exe sample and Turian.

An Updated Variant

Key differences between our samples and the previously documented Turian samples indicated that we were likely looking at a newer version, with some additional obfuscation and a modified network protocol.

The first key difference was the C2 decryption algorithm. In prior Turian samples, the C2s were decrypted with an XOR against a hard coded byte, such as 0xA9.

```
dec = b""
counter = 0
while counter < (len(enc)):
  dec += bytes([enc[counter] ^ (counter ^ 0xA9)])
  counter += 1
```

Whereas in the dellux.exe sample, the algorithm has clearly been updated.

Additionally, the network protocol in use by Turian and Quarian backdoors has historically been very distinct, especially during the initial key exchange. In this variant, the network protocol has been altered to instead make use of the Security Support Provider Interface (SSPI).

On startup, Turian will retrieve a pointer to the SSPI Dispatch Table via a call to InitSecurityInterfaceA(), before calling AcquireCredentialsHandleA(). A socket is then opened to the remote C2, using standard Winsock API, with connect() being called to establish a connection.

Once a connection has been made, Turian then performs an SSL handshake with the C2. This is done through a call to InitializeSecurityContextA(), which will return a token to send to the C2 server.

Once sent, Turian waits for a 5 byte response (the SSL/TLS record header). This response contains the length of data also to be received from the C2 server, after the initial header. The remaining data is then

passed into another call to InitializeSecurityContextA(), before returning. At this point, the handshake has been successful and secure communications can begin.

All packets sent to the C2 server are encrypted using the EncryptMessage() API, but are also XORed with the key 0x56 beforehand. The same functionality is performed on received packets, with the data being decrypted with DecryptMessage(), followed by XORing with 0x56.

The updated backdoor offers fairly generic functionality, from updating the C2 to communicate with, to executing commands and spawning reverse shells. The main differences with this compared to other variants of Turian are the command IDs. Whereas before, the IDs started at 0x01 and followed an order, the IDs in this variant appear to be randomized.

Commands Table	
0xBC5B	Clean up
0xA8CB	Update C2
0x9D58	Execute Command
0x9A3C	Spawn File Explorer Thread
0x7C0D	(Unknown)
0x6394	Set Flag
0x74D2	(Unknown)
0x53A6	Get System Info
0x26CD	Spawn Reverse Shell Thread

Table 11. Updated Turian commands.

Conclusion

Playful Taurus continues to evolve their tactics and their tooling. Recent upgrades to the Turian backdoor and new C2 infrastructure suggest that these actors continue to see success during their cyber espionage campaigns. Our analysis of the samples and connections to the malicious infrastructure suggest that Iranian government networks have likely been compromised. At the same time, we would also caution that Playful Taurus routinely deploys the same tactics and techniques against other government and diplomatic entities across North and South America, Africa and the Middle East.

Palo Alto Networks has shared these findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Protections and Mitigations

For Palo Alto Networks customers, our products and services provide the following coverage associated with this group:

- WildFire cloud-based threat analysis service accurately identifies the Turian malware described in this blog as malicious.

- Advanced URL Filtering and DNS Security identify domains associated with Playful Taurus as malicious.
- Cortex XDR prevents the execution of known malware samples as malicious. It also prevents the execution of Turian malware using Behavioral Threat Protection and the new in-memory shellcode protection released in Cortex 3.5.

If you think you may have been impacted or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Indicators of Compromise

Infrastructure

152.32.181[.]16
158.247.222[.]6
vpnkerio[.]com
update.delldrivers[.]in
scm.oracleapps[.]org
update.adboeonline[.]net
mail.indiarailways[.]net

Playful Taurus Certificate SHA-1

cfd9884511f2b5171c00570da837c31094e2ec72
1cf1985aec3dd1f7040d8e9913d9286a52243aca

Turian Sample SHA-256

67c911510e257b341be77bc2a88cedc99ace2af852f7825d9710016619875e80
8549c5bafbfad6c7127f9954d0e954f9550d9730ec2e06d6918c050bf3cb19c3
5bb99755924ccb6882fc0bdedb07a482313daeaaa449272dc291566cd1208ed5
ad22f4731ab228a8b63510a3ab6c1de5760182a7fe9ff98a8e9919b0cf100c58
6828b5ec8111e69a0174ec14a2563df151559c3e9247ef55aeaaf8c11ef88bfa