

# BackdoorDiplomacy: Upgrading from Quarian to Turian

By Adam Burgher

Archived: 2026-04-02 10:52:13 UTC

## Executive summary

An APT group that we are calling BackdoorDiplomacy, due to the main vertical of its victims, has been targeting Ministries of Foreign Affairs and telecommunication companies in Africa and the Middle East since at least 2017. For initial infection vectors, the group favors exploiting vulnerable internet-exposed devices such as web servers and management interfaces for networking equipment. Once on a system, its operators make use of open-source tools for scanning the environment and lateral movement. Interactive access is achieved in two ways: (1) via a custom backdoor we are calling Turian that is derived from the Quarian backdoor; and (2) in fewer instances, when more direct and interactive access is required, certain open-source remote access tools are deployed. In several instances, the group has been observed targeting removable media for data collection and exfiltration. Finally, both Windows and Linux operating systems have been targeted.

## Links with known groups

BackdoorDiplomacy shares commonalities with several other Asian groups. Most obvious among them is the connection between the Turian backdoor and the Quarian backdoor. Specific observations regarding the Turian-Quarian connection are recorded below in the *Turian* section. We believe this group is also linked with a group Kaspersky referred to as “[CloudComputating](#)” that was also analyzed by [Sophos](#).

Several victims were compromised via mechanisms that closely matched the [Rehashed Rat](#) and a [MirageFox-APT15](#) campaign documented by Fortinet in 2017 and Intezer in 2018, respectively. The BackdoorDiplomacy operators made use of their specific form of DLL Search-Order Hijacking.

Finally, the network encryption method BackdoorDiplomacy uses is quite similar to a backdoor [Dr.Web](#) calls [Backdoor.Whitebird.1](#). Whitebird was used to target government institutions in Kazakhstan and Kyrgyzstan (both neighbors of a BackdoorDiplomacy victim in Uzbekistan) within the same 2017-to-present timeframe in which BackdoorDiplomacy has been active.

## Victimology

Quarian was used to target the [Syrian Ministry of Foreign Affairs in 2012](#), as well as the [US State Department in 2013](#). This trend of targeting Ministries of Foreign Affairs continues with Turian.

Victims have been discovered in the Ministries of Foreign Affairs of several African countries, as well as in Europe, the Middle East, and Asia. Additional targets include telecommunication companies in Africa, and at least one Middle Eastern charity. In each case, operators employed similar tactics, techniques, and procedures (TTPs), but modified the tools used, even within close geographic regions, likely to make tracking the group more difficult. See Figure 1 for a map of victims by country and vertical.

### BackdoorDiplomacy victims, by country and vertical

- ◆ Charitable organizations
- ◆ Diplomatic organizations
- ◆ Telecommunications
- ◆ Unknown

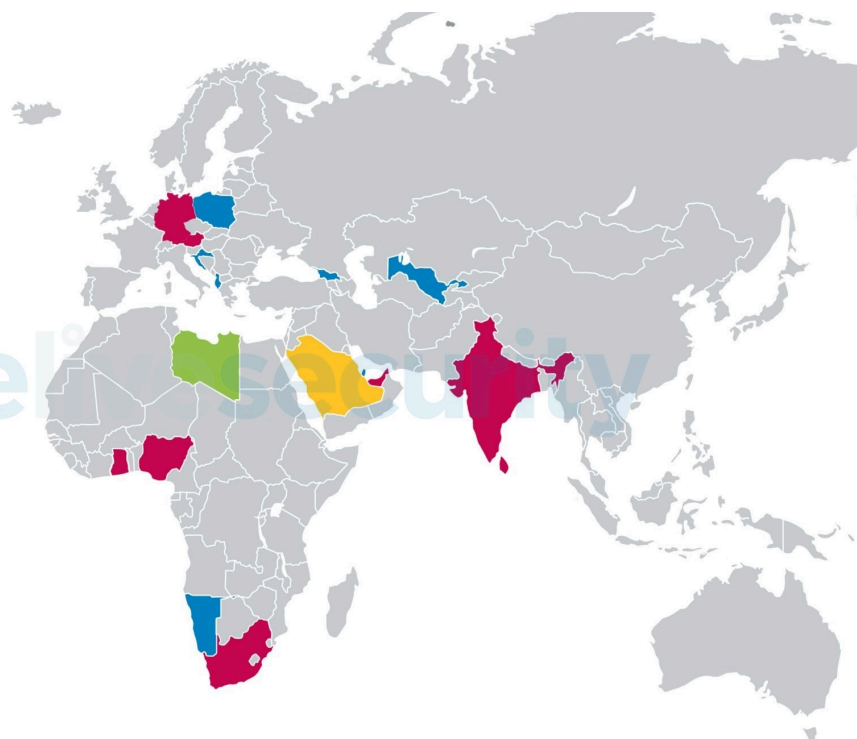


Figure 1. Victims by country and vertical

### Attack vectors

BackdoorDiplomacy targeted servers with internet-exposed ports, likely exploiting unpatched vulnerabilities or poorly enforced file-upload security. In one specific instance, we observed the operators exploit an F5 BIP-IP vulnerability ([CVE-2020-5902](#)) to drop a Linux backdoor. In another, a Microsoft Exchange server was exploited via a PowerShell dropper that installed [China Chopper](#), a well-known webshell in use, by various groups, since 2013. In a third, we observed a [Plesk](#) server with poorly configured file-upload security execute another webshell similar to China Chopper. See Figure 2 for an overview of the exploit chain.

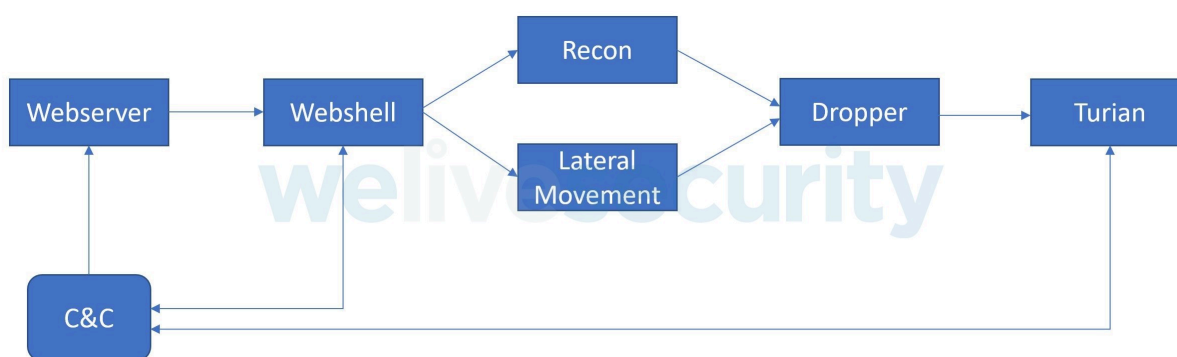


Figure 2. Exploit chain from initial compromise to backdoor with C&C communications

### Reconnaissance and lateral movement

Following the initial compromise, in many instances the BackdoorDiplomacy group employed open-source reconnaissance and red-team tools to evaluate the environment for additional targets of opportunity and lateral movement. Among the tools documented are:

- [EarthWorm](#), a simple network tunnel with SOCKS v5 server and port transfer functionalities

- [Mimikatz](#), and various versions including [SafetyKatz](#)
- [Nbtscan](#), a command line NetBIOS scanner for Windows
- [NetCat](#), a networking utility that reads and writes data across network connections
- [PortQry](#), a tool to display the status of TCP and UDP ports on remote systems
- [SMBTouch](#), used to determine whether a target is vulnerable to EternalBlue
- Various tools from the ShadowBrokers dump of NSA tools including, but not limited to:
  - DoublePulsar
  - EternalBlue
  - EternalRocks
  - EternalSynergy

Commonly used directories for staging recon and lateral movement tools include:

- C:\Program Files\Windows Mail\en-US\
- %LOCALAPPDATA%\Microsoft\InstallAgent\Checkpoints\
- C:\ProgramData\ESET\ESET Security\Logs\eScan\
- %USERPROFILE%\ESET\ESET Security\Logs\eScan\
- C:\Program Files\hp\hponcfg\
- C:\Program Files\hp\hpssa\
- C:\hp\hpsmh\
- C:\ProgramData\Mozilla\updates\

Of the tools listed above, many were obfuscated with VMProtect (v1.60-2.05), a recurring theme with BackdoorDiplomacy tools.

## Windows

### Backdoor droppers

In some instances, operators were observed uploading backdoor droppers. Operators attempted to disguise their backdoor droppers and evade detection in various ways.

- Naming conventions designed to blend into normal operations (e.g. amsc.exe, msvsvr.dll, alg.exe)
- Dropping implants in folders named for legitimate software (e.g., C:\Program Files\hp, C:\ProgramData\ESET, C:\ProgramData\Mozilla)
- [DLL search order hijacking](#)

In one such instance, the operators uploaded, via a webshell, both ScnCf.exe (SHA-1: 573C35AB1F243D6806DEDBDD7E3265BC5CBD5B9A), a legitimate McAfee executable, and vsodscpl.dll, a malicious DLL named after a legitimate McAfee DLL that is called by ScnCf.exe. The version of vsodscpl.dll (SHA-1: FCD8129EA56C8C406D1461CE9DB3E02E616D2AA9) deployed was called by ScnCf.exe, at which point vsodscpl.dll extracted Turian embedded within its code, wrote it to memory, and executed it.

On a different system, operators dropped a legitimate copy of credwize.exe, the Microsoft Credential Backup and Restore Wizard, on disk and used it to execute the malicious library New.dll, another Turian variant.

## Turian

About half of the samples we collected were obfuscated with VMProtect. A compilation of observed operator commands is included in the *Operator commands* section. Unique network encryption schemes are individually discussed below as well.

### Similarities with Quarian

The initial reporting by Kaspersky notes that the victims of Quarian were at the Syrian Ministry of Foreign Affairs, a similar target-set of Turian.

In many of the Turian samples we collected, there are obvious similarities with Quarian. Mutexes are used by both to verify that only one instance is running, although the mutexes used are dissimilarly named. We observed the following mutexes used by Turian:

- winsupdatetw
- clientsix
- client
- updatethres
- Others: dynamically generated based on the system's hostname, limited to eight hex characters, lower-case, and prefaced with a leading zero

C&C server domains and IP addresses are extracted with similar XOR routines; where Quarian uses a decryption key of 0x44, Turian uses 0xA9.

Turian and Quarian both read the first four bytes from the file cf in the same directory as the malware's executable, which are then used as the sleep length as part of the C&C beacon routine.

The Turian network connection process follows a similar pattern to Quarian, attempting to make a direct connection. If that fails due to a local proxy with a response of 407 (Authorization Required), both try to use locally cached credentials.

However, the request sent to the proxy by Turian does not contain any of the grammatical mistakes that Quarian sent. See Figure 3 for a comparison of proxy connection attempts.

```
1 CONNECT %s:%u HTTP/1.1
2 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
3 Host: %s
4 Content-Length: 0
5 Proxy-Connection: Keep-Alive
6 Pragma: no-cache

1 CONNECT %s:%d HTTP/1.0
2 User-Agent: Mozilla/4.0
3 Host: %s
4 Content length: 0
5 Proxy-Connetion: Keep-Alive
6 Pragma: no-cache
```

Figure 3. Comparison of proxy connection attempts, Turian (left) and Quarian (right)

Finally, both Turian and Quarian create a remote shell by copying cmd.exe to alg.exe.

### Persistence

After initial execution, Turian establishes persistence by creating the file tmp.bat in the current working directory, writing the following lines to the file, then running the file:

```
ReG aDd HKEY_CURRENT_USER\SOftWARe\MICrOsOfT\WindOwS\CurRentVeRsiOn\RuN /v Turian_filename> /t
REG_SZ /d "<location_of_Turian_on_disk>\<Turian_filename>" /f
```

```
ReG aDd HKEY_LOCAL_MACHINE\SOftWARe\MICrOsOfT\WindOwS\CurRentVeRsiOn\RuN /v <Turian_filename> /t
REG_SZ /d "<location_of_Turian_on_disk>\<Turian_filename>" /f
```

```
del %0
```

Turian then checks for the presence of the file Sharedaccess.ini in its working directory. If that file is present, Turian attempts to load the C&C IP or domain from there, if present. We did not observe Turian pass IPs or domains in this manner but testing confirmed Turian looks to load the C&C address from here first. After checking Sharedaccess.ini, Turian attempts to connect with a hardcoded IP or domain and sets up its network encryption protocol.

### Network encryption

Quarian is known to have used both an eight-byte XOR key (see Talos on [Quarian: Reversing the C&C Protocol](#)) and an eight-byte nonce to create a session key (see ThreatConnect on Quarian Network Protocol Analysis in [Divide and Conquer: Unmasking China's 'Quarian' Campaigns Through Community](#)). Turian has a distinct method for exchanging network encryption keys. See Figure 4 for a breakdown of the Turian network encryption setup.

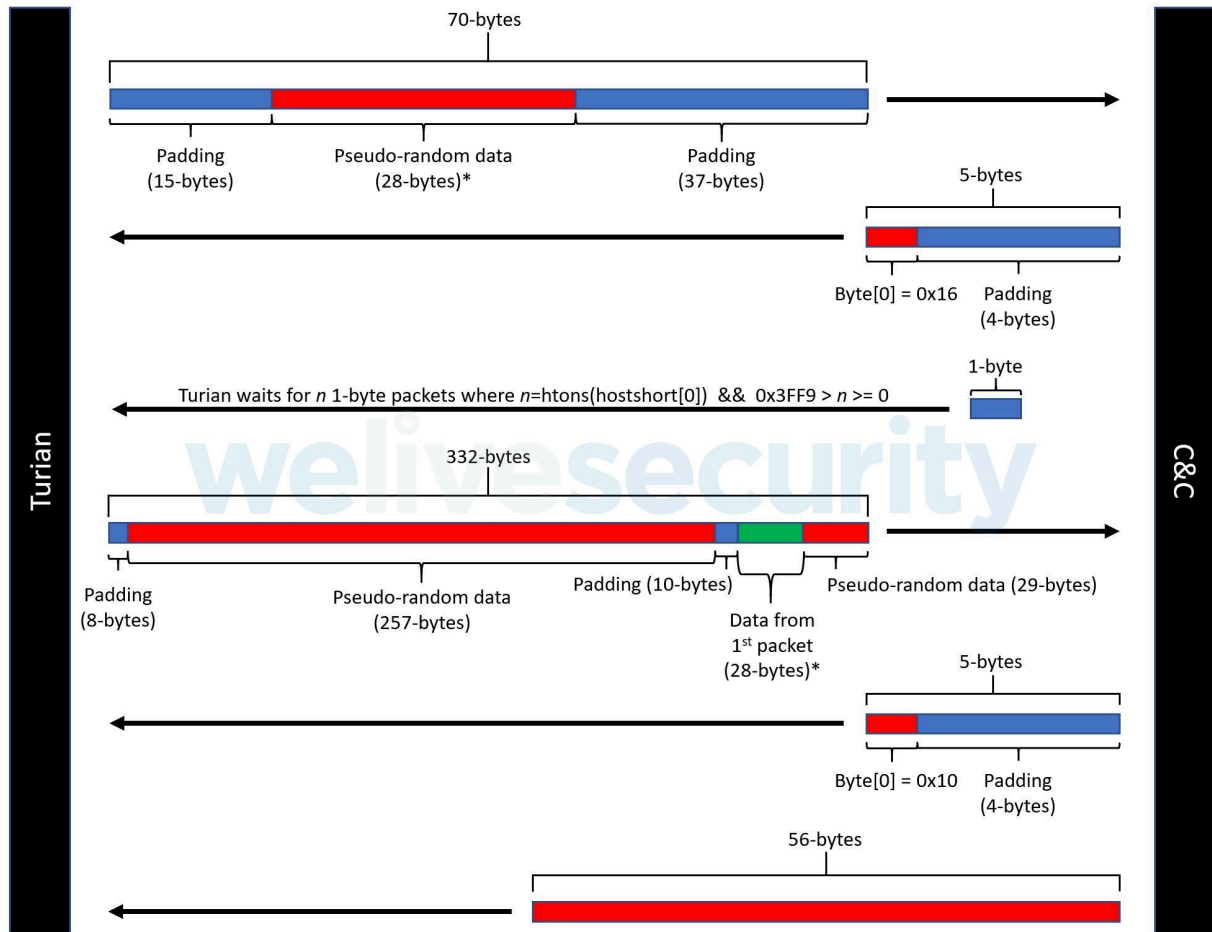


Figure 4. Turian network encryption setup

After receiving the last 56-byte packet, Turian calls the network encryption initialization function in Figure 5, and accepts the 56 bytes of data in the last C&C packet as the only argument.

```
1  encryption_key_initialization(last_56b_pkt)
2  {
3      int v1; // ecx
4      _BYTE *j;
5      int i; // ebx
6      int v4; // esi
7      char result; // al
8
9      v2 = v1 + 4;
10     i = 0;
11     v4 = last_56b_pkt - (_DWORD)v2;
12
13     do
14     {
15         result = ~(_BYTE)i ^ *j ^ j[v4];
16         *j = result;
17         if ( !result )
18             *j = ~(_BYTE)i;
19         ++i;
20         ++j;
21     }
22     while ( i < 28 );
23
24     return result;
25 }
```

Figure 5. Hex-Rays decompiled view of the encryption key initialization function

A second network encryption setup was also observed, as depicted in Figure 6.

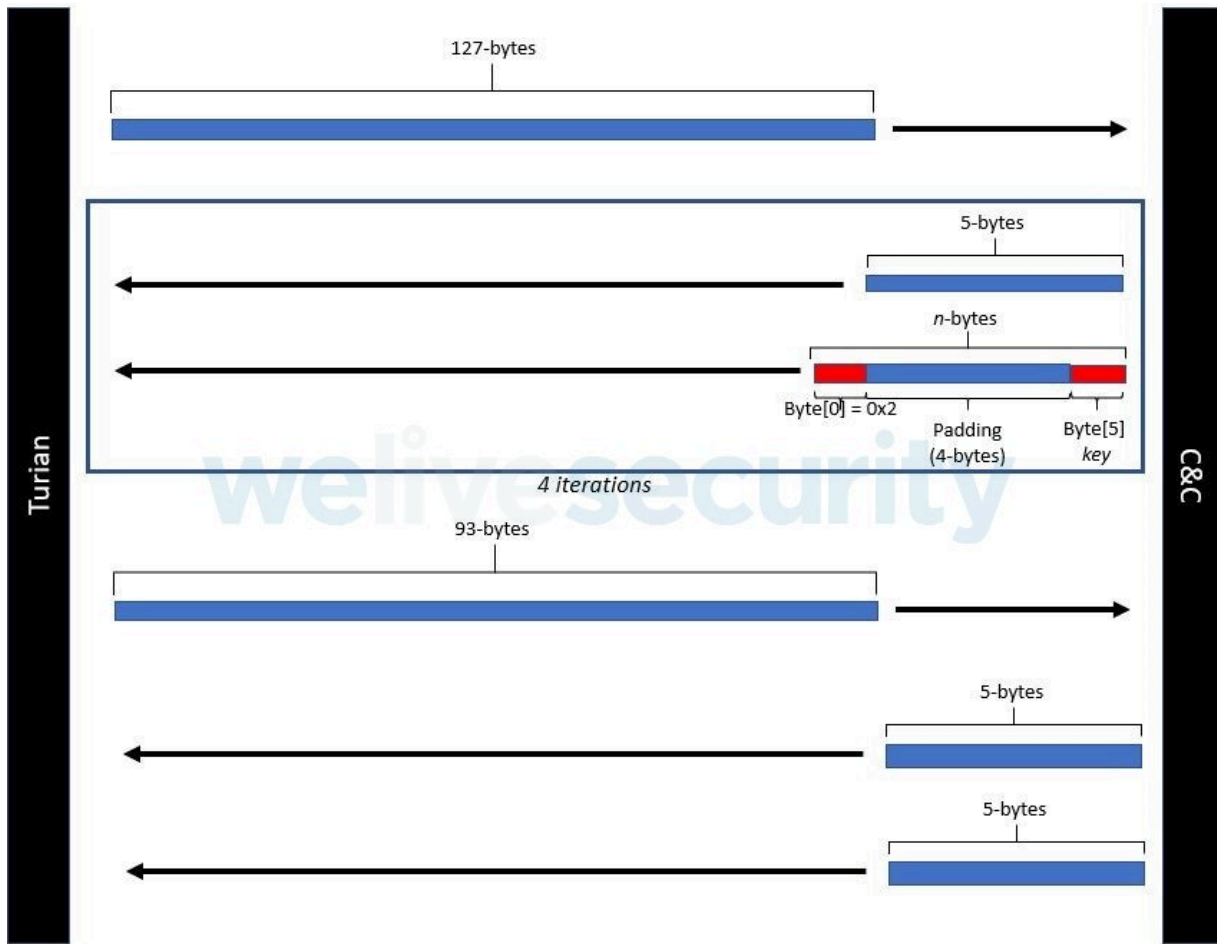


Figure 6. Second Turian network encryption set up protocol

The last iteration of the four-iteration loop (QWORD byte[5]) is used as the seed for the key initialization function, as shown below in Figure 7.

```
1  2nd_encryption_key_initialization(last_5b_pkt)
2  {
3      _BYTE *result; // eax
4      DWORD v2 // [ecx + 4]
5      int i; // edx
6      int v4; // esi
7      bool v5; // zf
8
9      result = v2;
10     i = 0;
11     v4 = last_5b_pkt - v2;
12
13     do
14     {
15         v5 = result[v4] == *result;
16         if ( v5 )
17             *result = ~(_BYTE)i;
18             i++;
19             result++;
20     }
21     while ( i < 8 );
22
23     return result;
24 }
```

Figure 7. Second key initialization function

### Operator commands

The full list of Turian operator commands is shown in Table 1.

Table 1. Turian C&C commands

ID	Description
0x01	Get system information including OS version, memory usage, local hostname, system adapter info, internal IP, current username, state of the directory service installation and domain data.
0x02	Interactive shell – copy %WINDIR%\system32\cmd.exe to %WINDIR%\alg.exe and spawn alg.exe in a new thread.
0x03	Spawn a new thread, acknowledge the command and wait for one of the three-digit commands below.
0x04	Take screenshot.
0x103/203	Write file.
0x403	List directory.
0x503	Move file.
0x603	Delete file.
0x703	Get startup info.

A subset of victims was targeted with data collection executables that were designed to look for removable media (most likely USB flash drives). The implant routinely scans for such drives, specifically targeting removable media (return value of GetDriveType is 2). If found, the implant uses an embedded version of WinRAR to execute these hardcoded commands:

- CMD.exe /C %s a -m5 -hp1qaz@WSX3edc -r %s %s\\*.\*
- CMD.exe /C %s a -m5 -hpMyHost-1 -r %s %s\\*.\*
- CMD.exe /C rd /s /q \"%s\"

The parameters in the command break out to:

- a == add files to archive
- -m[0:5] == compression level
- -hp<password>
- -r == recurse subdirectories
- rd == remove directory
- /s == delete a directory tree
- /q == quiet mode
- \"%s\" == directory to act on

The implant, upon detecting a removable media being inserted, attempts to copy all the files on the drive to a password-protected archive and puts the archive in the following directory, which is hardcoded and so the same for every victim:

- C:\RECYCLER\S-1-3-33-854245398-2067806209-0000980848-2003\

The implant also has the capability to delete files, based on the third command listed above.

## Remote access tools

Occasionally, BackdoorDiplomacy’s operators require a greater degree of access or more interactivity than that provided by Turian. On those occasions, they employ open-source remote access tools such as [Quasar](#), which offers a wide variety of capabilities and runs on virtually all versions of Windows.

## Linux

We discovered, via a shared C&C server domain, a [Linux backdoor](#) using similar network infrastructure and that was deployed after exploiting a known vulnerability in F5 BIG-IP load balancers' traffic management user interface (TMUI), which permits remote code execution (RCE). The Linux variant attempts to persist by writing itself to [/etc/init.d/rc.local](#)

Next, it runs through a loop to extract strings from memory:

- bash -version
- echo \$PWD
- /bin/sh
- /tmp/AntiVirtmp
- eth0
- /proc/%d/exe

Then, it calls its daemon function and forks off a child process which then begins the work of decrypting the C&C IP address and/or domain name then initiates a loop that reaches out to the C&C using Mozilla/5.0 (X11; Linux i686; rv:22.0) Firefox/22.0 as its user-agent. This C&C loop continues until a successful connection is made. Once a connection is established, the Linux agent goes through a similar network encryption setup to what the Windows version of Turian carries out. See Figure 8 for the network encryption protocol used by the Linux variant of Turian.

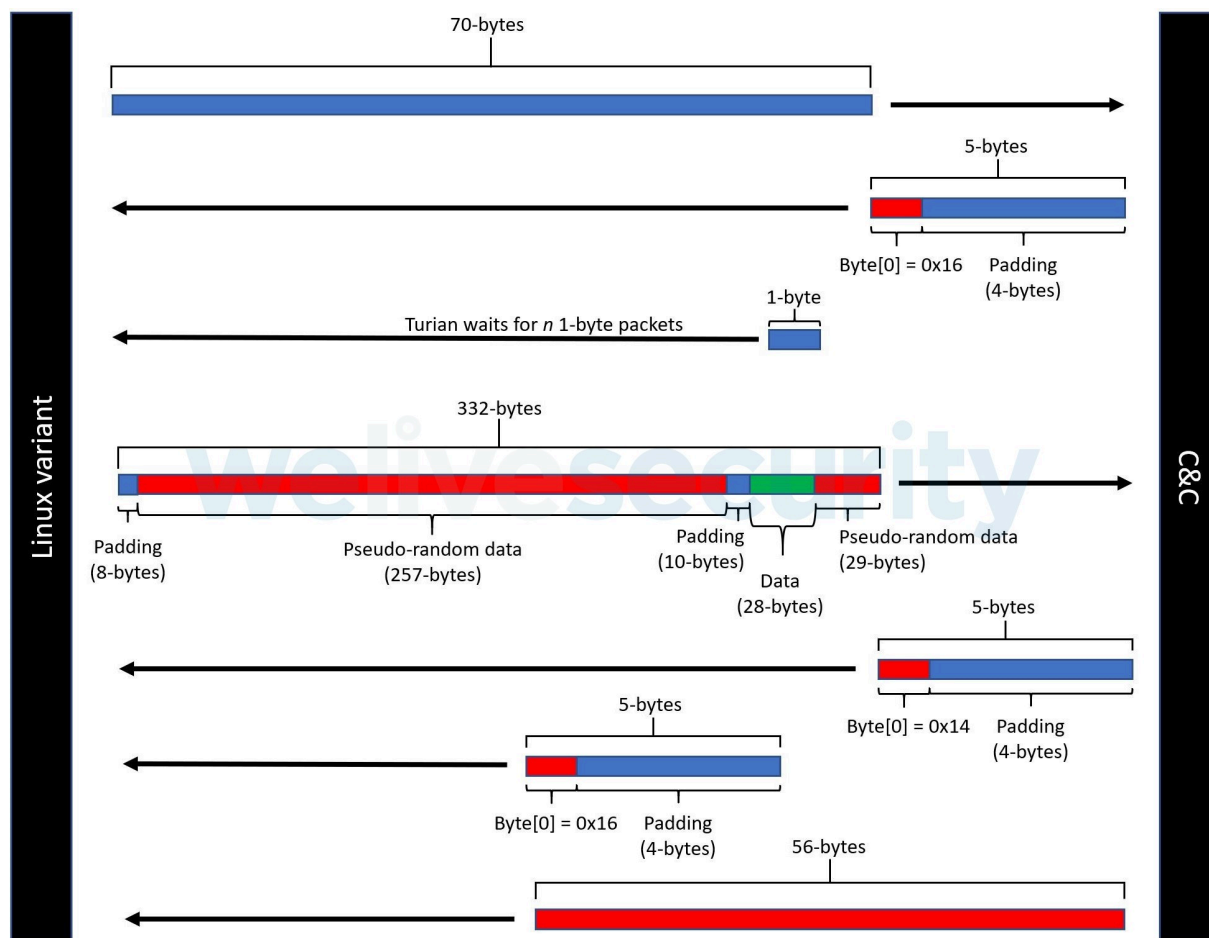


Figure 8. Linux Turian variant - network encryption protocol setup routine

After receiving the last 56-byte packet, the Linux agent calls the network encryption key initialization function depicted in Figure 9.

```
1  int64 __fastcall sub_401F00(_BYTE *recv_buf, _BYTE *a2)
2  {
3      __int64 result; // rax
4      char v3; // dl
5
6      LODWORD(result) = -1;
7      do
8      {
9          v3 = result ^ *a2 ^ *recv_buf;
10         if ( !v3 )
11             v3 = result;
12         result = (unsigned int)(result - 1);
13         ++recv_buf;
14         *a2++ = v3;
15     }
16     while ( (_BYTE)result != 0xE3 );
17     return result;
18 }
```

Figure 9. Hex-Rays decompiled network encryption key initialization function

Upon successful completion of the network protocol setup, it forks off another child process and attempts to spawn a TTY reverse shell :

- python -c 'import pty; pty.spawn("/bin/sh")'

## Conclusion

BackdoorDiplomacy is a group that primarily targets diplomatic organizations in the Middle East and Africa, and less frequently, telecommunication companies. Their initial attack methodology is focused on exploiting vulnerable internet-exposed applications on web servers, in order to drop and execute a webshell. Post compromise, via the webshell, BackdoorDiplomacy deploys open-source software for reconnaissance and information gathering, and favors the use of DLL search order hijacking to install its backdoor, Turian. Finally, BackdoorDiplomacy employs a separate executable to detect removable media, likely USB flash drives, and copy their contents to the main drive's recycle bin.

BackdoorDiplomacy shares tactics, techniques, and procedures with other Asian groups. Turian likely represents a next stage evolution of Quarian, the backdoor last observed in use in 2013 against diplomatic targets in Syria and the United States. Turian's network encryption protocol is nearly identical to the network encryption protocol used by Whitebird, a backdoor operated by Calypso, another Asian group. Whitebird was deployed within diplomatic organizations in Kazakhstan and Kyrgyzstan during the same timeframe as BackdoorDiplomacy (2017-2020). Additionally, BackdoorDiplomacy and APT15 use the same techniques and tactics to drop their backdoors on systems, namely the aforementioned DLL search order hijacking.

BackdoorDiplomacy is also cross-platform group targeting both Windows and Linux systems. The Linux variant of Turian shares the same network encryption protocol characteristics and attempts to return a TTY reverse shell to the operator.

## IoCs

## Samples

SHA-1	Filename	ESET Detection Name	Description
3C0DB3A5194E1568E8E2164149F30763B7F3043D	logout.aspx	ASP/Webshell.H	BackdoorDiploma webshell – variant N2
32EF3F67E06C43C18E34FB56E6E62A6534D1D694	current.aspx	ASP/Webshell.O	BackdoorDiploma webshell – variant S1
8C4D2ED23958919FE10334CCFBE8D78CD0D991A8	errorEE.aspx	ASP/Webshell.J	BackdoorDiploma webshell – variant N1
C0A3F78CF7F0B592EF813B15FC0F1D28D94C9604	App_Web_xcg2dubs.dll	MSIL/Webshell.C	BackdoorDiploma webshell – variant N3
CDD583BB6333644472733617B6DCCEE2681238A11	N/A	Linux/Agent.KD	Linux Turian backdoor
FA6C20F00F3C57643F312E84CC7E46A0C7BABE75	N/A	Linux/Agent.KD	Linux Turian backdoor
5F87FBFE30CA5D6347F4462D02685B6E1E90E464	ScnCfg.exe	Win32/Agent.TGO	Windows Turian backdoor
B6936BD6F36A48DD1460EEB4AB8473C7626142AC	VMSvc.exe	Win32/Agent.QKK	Windows Turian backdoor
B16393DFFB130304AD627E6872403C67DD4C0AF3	svchost.exe	Win32/Agent.TZI	Windows Turian backdoor
9DBBEBEBBA20B1014830B9DE4EC9331E66A159DF	nvsvc.exe	Win32/Agent.UJH	Windows Turian backdoor
564F1C32F2A2501C3C7B51A13A08969CDC3B0390	AppleVersions.dll	Win64/Agent.HA	Windows Turian backdoor
6E1BB476EE964FFF26A86E4966D7B82E7BACBF47	MozillaUpdate.exe	Win32/Agent.UJH	Windows Turian backdoor
FBB0A4F4C90B513C4E51F0D0903C525360FAF3B7	nvsvc.exe	Win32/Agent.QAY	Windows Turian backdoor
2183AE45ADEF97500A26DBBF69D910B82BFE721A	nvsvcv.exe	Win32/Agent.UFX	Windows Turian backdoor
849B970652678748CEBF3C4D90F435AE1680601F	efsw.exe	Win32/Agent.UFX	Windows Turian backdoor
C176F36A7FC273C9C98EA74A34B8BAB0F490E19E	iexplore32.exe	Win32/Agent.QAY	Windows Turian backdoor

SHA-1	Filename	ESET Detection Name	Description
626EFB29B0C58461D831858825765C05E1098786	iexplore32.exe	Win32/Agent.UFX	Windows Turian backdoor
40E73BF21E31EE99B910809B3B4715AF017DB061	explorer32.exe	Win32/Agent.QAY	Windows Turian backdoor
255F54DE241A3D12DEBAD2DF47BAC5601895E458	Duser.dll	Win32/Agent.URH	Windows Turian backdoor
A99CF07FBA62A63A44C6D5EF6B780411CF1B1073	Duser.dll	Win64/Agent.HA	Windows Turian backdoor
934B3934FDB4CD55DC4EA1577F9A394E9D74D660	Duser.dll	Win32/Agent.TQI	Windows Turian backdoor
EF4DF176916CE5882F88059011072755E1ECC482	iexplore32.exe	Win32/Agent.QAY	Windows Turian backdoor

## Network

### C&Cs

AS	Hoster	IP address	Domain
AS20473	AS-CHOOA	199.247.9[.]67	bill.microsoftbuys[.]com
AS132839	POWER LINE DATACENTER	43.251.105[.]218	dnsupdate.dns2[.]us
	#rowspan#	43.251.105[.]222	#rowspan#
AS40065	Cnservers LLC	162.209.167[.]154	#rowspan#
AS132839	POWER LINE DATACENTER	43.225.126[.]179	www.intelupdate.dns1[.]us
AS46573	LAYER-HOST	23.247.47[.]252	www.intelupdate.dns1[.]us
AS132839	POWER LINE DATACENTER	43.251.105[.]222	winupdate.ns02[.]us
AS40065	Cnservers LLC	162.209.167[.]189	#rowspan#
AS25820	IT7NET	23.83.224[.]178	winupdate.ns02[.]us
	#rowspan#	23.106.140[.]207	#rowspan#
AS132839	POWER LINE DATACENTER	43.251.105[.]218	#rowspan#
AS20473	AS-CHOOA	45.76.120[.]84	icta.worldmessg[.]com
AS20473	AS-CHOOA	78.141.243[.]45	#rowspan#
	#rowspan#	78.141.196[.]159	Infoafrica[.]top
	#rowspan#	45.77.215[.]53	szsz.pmdskm[.]top

AS	Hoster	IP address	Domain
	#rowspan#	207.148.8[.]82	pmdskm[.]top
AS132839	POWER LINE DATACENTER	43.251.105[.]139	www.freedns02.dns2[.]jus
	#rowspan#	43.251.105[.]139	web.vpnkerio[.]com
AS20473	AS-CHOOPA	45.77.215[.]53	
AS135377	UCloud (HK) Holdings Group Limited	152.32.180[.]34	
AS132839	POWER LINE DATACENTER	43.251.105[.]218	officeupdates.cleansite[.]jus
AS25820	IT7NET	23.106.140[.]207	dynsystem.imbbs[.]in
	#rowspan#	#rowspan#	officeupdate.ns01[.]jus
	#rowspan#	#rowspan#	systeminfo.oicp[.]net
AS40676	Psychz Networks	23.228.203[.]130	systeminfo.myftp[.]name
#rowspan#	#rowspan#	systeminfo.cleansite[.]info	
#rowspan#	#rowspan#	updateip.onmypc[.]net	
#rowspan#	#rowspan#	buffetfactory.oicp[.]io	

### Registrars

Registrar	Domain
expdns[.]net	update.officenews365[.]com
ezdnscenter[.]com	bill.microsoftbuys[.]com
changeip[.]org	dnsupdate.dns2[.]jus
	dnsupdate.dns1[.]jus
	www.intelupdate.dns1[.]jus
	winupdate.ns02[.]jus
	www.freedns02.dns2[.]jus
	officeupdates.cleansite[.]jus
	officeupdate.ns01[.]jus
	systeminfo.cleansite[.]info
updateip.onmypc[.]net	
hichina[.]com	Infoafrica[.]top
domaincontrol[.]com	web.vpnkerio[.]com
exhera[.]com	dynsystem.imbbs[.]in

Registrar	Domain
systeminfo.oicp[.]net	

## MITRE ATT&CK techniques

Note: This table was built using [version 9](#) of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Initial Access	<a href="#">T1190</a>	Exploit Public-Facing Application	BackdoorDiplomacy exploits the vulnerability CVE-2020-5902.
Execution	<a href="#">T1059.003</a>	Windows Command Shell	Turian relies on a batch script to create persistence.
	<a href="#">T1203</a>	Exploitation for Client Execution	Turian has exploited client software vulnerabilities for execution, such as CVE-2020-5902.
Persistence	<a href="#">T1547.001</a>	Registry Run Keys / Startup Folder	Turian uses the HKLM and HKCU CurrentVersion Run keys to persist after reboot.
	<a href="#">T1548.002</a>	Bypass User Account Control	Turian uses JuicyPotato to bypass UAC.
Privilege Escalation	<a href="#">T1547.001</a>	Registry Run Keys / Startup Folder	Turian uses the HKLM and HKCU CurrentVersion Run keys to persist after reboot.
	<a href="#">T1548.002</a>	Bypass User Account Control	Turian uses JuicyPotato to bypass UAC.
Defense Evasion	<a href="#">T1140</a>	Deobfuscate/Decode Files or Information	Turian uses VMProtect to obfuscate its code.
	<a href="#">T1550</a>	Use Alternate Authentication Material	Turian uses Mimikatz.
	<a href="#">T1083</a>	File and Directory Discovery	Turian lists drives.
Discovery	<a href="#">T1550</a>	Use Alternate Authentication Material	Turian uses Mimikatz.
Lateral Movement	<a href="#">T1005</a>	Data from Local System	Turian collects files from the victim's machine.
Collection	<a href="#">T1113</a>	Screen Capture	Turian captures screenshots.
	<a href="#">T1071.001</a>	Web Protocols	Turian uses HTTP to communicate with the C&C server.
Command and Control	<a href="#">T1573.001</a>	Symmetric Cryptography	Turian uses XOR routine to encrypt communication with the C&C server.

Tactic	ID	Name	Description
<a href="#">T1095</a>	Non-Application Layer Protocol	Turian uses raw sockets to communicate with the C&C server.	



Source: <https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/>