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.

---

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

OREN J. FALKOWITZ | CO-FOUNDER & CEO

BLAKE DARCHE | CO-FOUNDER & CSO
Campaign Details

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.

In late November 2018, Area 1 Security discovered that this campaign, via phishing, successfully gained access into the computer network of the Ministry of Foreign Affairs of Cyprus, a communications network used by the European Union to facilitate cooperation on foreign policy matters. This network, known as COREU, operates between the 28 EU countries, the Council of the European Union, the European External Action Service, and the European Commission. It is a crucial instrument in the EU system of foreign policymaking.

The campaign was directed by the Chinese government and specifically undertaken by the Strategic Support Force (SSF) of the People’s Liberation Army (PLA). While the targets are disparate, we have identified a consistent set of characteristics and chain of events that tie together a larger campaign that includes targeting the United Nations and the AFL-CIO in addition to accessing diplomatic cables from the COREU network.

\[^{3}\text{PLA was the Signals Intelligence (SI\text{G}INT) agency of the Peoples Republic of China and was reorganized around December 2015 to become part of the Strategic Support Force or SSF (战略支援部队).}\]

\[^{3}\text{https://www.cfr.org/blog/chinas-strategic-support-force-new-home-plas-cyber-operations}\]
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>          .docuvantage
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
03/13/2014  10:49 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
caspilitegent.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.ex 2148 Services                   0     900 K
```
**Campaign Details**

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.

```
vmnet.exe  2180 Services  0   736 K
WMAHost.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
csmmd.exe  3500 Services  0  1,920 K
ccnfAgent.exe  3692 Services  0  5,612 K
cfnetsrvd.exe  3800 Services  0  2,080 K
ccsma.exe  3836 Services  0  4,172 K
rcHost.exe  3956 Services  0  2,804 K
amswsagt.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
hcmd.exe  4344 Console  1  996 K
igfxw.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]
spiwow64.exe  5656 Console  1  3,536 K
eudlg.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
```

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

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

Windows IP Configuration

Host Name . . . . . . . . . . . . : WIN7ENT-T09HKG
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:**

- 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.aflcio.org [10.140.2.12] with 32 bytes of data:
Reply from 10.140.2.12: bytes=32 time=1ms TTL=127
```

**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.aflcio.org.

- User name: [REDACTED]
- Full Name: [REDACTED]
- Comment: [REDACTED]
- User's comment: [REDACTED]
- 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*
  - *Impromtptu XP-SG*
  - *Domain Users*

The command completed successfully.
PHISHING DIPLOMACY

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
```

<table>
<thead>
<tr>
<th>Share name</th>
<th>Type</th>
<th>Used as</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>5thComm_Common</td>
<td>Disk</td>
<td>DM/EO/5thCommittee CPC Data</td>
<td>5th Committee Common Files</td>
</tr>
<tr>
<td>CSS_Common</td>
<td>Disk</td>
<td>DM/CSS Common Files</td>
<td>CSS_Common</td>
</tr>
<tr>
<td>CSS_CPC</td>
<td>Disk</td>
<td>DM/CSS CPC Data</td>
<td>CSS_CPC</td>
</tr>
<tr>
<td>CSS_HCC</td>
<td>Disk</td>
<td>DM/CSS HCC Files</td>
<td>CSS_HCC</td>
</tr>
<tr>
<td>CSS_OCSS</td>
<td>Disk</td>
<td>DM/EO</td>
<td>CSS_OCSS</td>
</tr>
<tr>
<td>CSS_Studies</td>
<td>Disk</td>
<td>DM/CSS Studies</td>
<td>CSS_Studies</td>
</tr>
<tr>
<td>DMEO_Common</td>
<td>Disk</td>
<td>DMEO Common Files</td>
<td>DMEO_Common</td>
</tr>
<tr>
<td>DMEOSG_Common</td>
<td>Disk</td>
<td>DM-EOSG Common Files</td>
<td>DMEOSG_Common</td>
</tr>
<tr>
<td>DMEOSG_Internal</td>
<td>Disk</td>
<td>DM-EOSG Internal Service Files</td>
<td>DMEOSG_Internal</td>
</tr>
<tr>
<td>DPA_Common</td>
<td>Disk</td>
<td>DM/EO</td>
<td>DPA_Common</td>
</tr>
<tr>
<td>FMD_IRU</td>
<td>Disk</td>
<td>DM/CSS/FMD IRU</td>
<td>FMD_IRU</td>
</tr>
<tr>
<td>FMD_OSPU</td>
<td>Disk</td>
<td>DM/CSS/FMD BMScadd OPU</td>
<td>FMD_OSPU</td>
</tr>
<tr>
<td>FMD_Paradox</td>
<td>Disk</td>
<td>DM/CSS/FMD Paradox</td>
<td>FMD_Paradox</td>
</tr>
<tr>
<td>FMD_PMU</td>
<td>Disk</td>
<td>DM/CSS/FMD PMU</td>
<td>FMD_PMU</td>
</tr>
<tr>
<td>ITSD_MAA</td>
<td>Disk</td>
<td>McAfee DAT share</td>
<td>ITSD_MAA</td>
</tr>
<tr>
<td>OUSG_Clearance_Database</td>
<td>Disk</td>
<td>OUSG_Clearance_Database</td>
<td>OUSG_Clearance_Database</td>
</tr>
<tr>
<td>Treasury_Frustram</td>
<td>Disk</td>
<td>DM/OUSG/Treasury Frustram Application</td>
<td>Treasury_Frustram</td>
</tr>
<tr>
<td>Treasury_Lotus</td>
<td>Disk</td>
<td>DM/OUSG/Treasury Lotus Calendar</td>
<td>Treasury_Lotus</td>
</tr>
<tr>
<td>Treasury_Off</td>
<td>Disk</td>
<td>DM/OUSG/Treasury Off Directory</td>
<td>Treasury_Off</td>
</tr>
<tr>
<td>Treasury_Shared</td>
<td>Disk</td>
<td>DM/OUSG/Treasury Shared Files</td>
<td>Treasury_Shared</td>
</tr>
<tr>
<td>Treasury_Treasury</td>
<td>Disk</td>
<td>DM/OUSG/Treasury Files</td>
<td>Treasury_Treasury</td>
</tr>
<tr>
<td>Treasury_TRSCV</td>
<td>Disk</td>
<td>DM/OUSG/Treasury TRSCV Directory</td>
<td>Treasury_TRSCV</td>
</tr>
<tr>
<td>UNDSS_Admin</td>
<td>Disk</td>
<td>DM/OUSG/Treasury TRSCV Directory</td>
<td>UNDSS_Admin</td>
</tr>
<tr>
<td>UNDSS_Common</td>
<td>Disk</td>
<td>DM/OUSG/Treasury TRSCV Directory</td>
<td>UNDSS_Common</td>
</tr>
<tr>
<td>undss_data</td>
<td>Disk</td>
<td>DM/OUSG/Treasury TRSCV Directory</td>
<td>undss_data</td>
</tr>
<tr>
<td>UNRWA_Common</td>
<td>Disk</td>
<td>DM/OUSG/Treasury TRSCV Directory</td>
<td>UNRWA_Common</td>
</tr>
</tbody>
</table>

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\[REDACTED]\AppData\Roaming\sysinfo>net use \MFACENTRALREGIS\ipc$ [REDACTED] /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.

<table>
<thead>
<tr>
<th>Status</th>
<th>Local</th>
<th>Remote</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>H:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>\SECF09\Home</td>
<td>Microsoft Windows Network</td>
<td></td>
</tr>
<tr>
<td>OK</td>
<td>K:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>\secf04\batch_dpko</td>
<td>Microsoft Windows Network</td>
<td></td>
</tr>
<tr>
<td>OK</td>
<td>O:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>\SECF05\WIN7PROD</td>
<td>Microsoft Windows Network</td>
<td></td>
</tr>
<tr>
<td>OK</td>
<td>T:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>\unhq.un.org\Shared\dpko_o0\aasg-oo files</td>
<td>Microsoft Windows Network</td>
<td></td>
</tr>
</tbody>
</table>

The command completed successfully.

at \10.130.133.18

<table>
<thead>
<tr>
<th>Status ID</th>
<th>Day</th>
<th>Time</th>
<th>Command Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tomorrow</td>
<td>4:39 PM</td>
<td>c:\intel\windowsupdate.exe</td>
</tr>
</tbody>
</table>

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

net use \815-san-31\ipc$ [REDACTED] /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.

```cmd
xcopy \MFA\[REDACTED]\c$\[REDACTED]\[REDACTED]\COREU\201807\*.txt /s /d:07/23/2018
```

[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

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.

Example: XCOPY of File Server from within the United Nations

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.
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.

Example: COREU RAR from within the Ministry of Foreign Affairs of Cyprus
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 c1c80e237f6feb2c61b82c3325dd836f3849ca036a28007617e4e27ba2f16c4b 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

```pascal
procedure TMainForm.FormCreate(Sender: TObject);
begin
  GoogleDrive := TGoogleDrive.Create;
  GoogleDrive.OnUploadProgress := OnPropertyChanged;
  GoogleDrive.OnDownloadProgress := OnProgress;
  GoogleDrive.LogFileName := 'GoogleDrive.log';
  ClientIDEd.Text := IniFile.ReadString('General', 'ClientID', 'Enter your client ID here');
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.

https://www.sync-components.com/google-delphi-components/google-drive

```
GoogleDriveDemo.pas

push offset a65149531452_ap : "93149531452.apps.googleusercontent.com"
lea eax, [ebp+var_6]
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, [esi+3bh] : this
call sub_53B6E8
push offset a2b3q12teh1ytjkn : "u2Xq12tEH1yjKJPEFOUIOL.Cp"
lea eax, [ebp+var_8]
push eax
mov eax, [esi+458h]
mov ecx, offset aClientSecret : "ClientSecret"
mov edx, offset aGeneral : "General"
```

```
send.exe

push offset aEnterYourClient : "Enter your client ID here"
lea eax, [ebp+var_10]
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_10]
mov eax, ds:dword_55E444
add eax, 14h
call sub_6873C8
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-eg0r569euk8qef5kab52b01c1513nn5.apps.googleusercontent.com
ClientSecret=**d6e884fb2021f7852a68b84ddedd7e3764f4f1d7**
RefreshToken=**46836a597b3213683986d5b27f4e1f1**
# Tactics, Techniques, and Procedures (TTPs)

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

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

plugx.dll

```plaintext
rule Area1_SSF_PlugX {
    strings:
        $feature_call = { 8b 0? 56 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 10 66 8b 46 10 66 8b 4e 1a 57 f4 52 c7 45 f4
            01 00 00 06 00 c7 45 f8 6a 07 6a ff ff d0 8b f0 85 f6 74 14 }
        $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 6b c8 0f af ca
            b8 1f 85 eb 51 ff ff 0f b7 56 14 6b c8 0f af ca b8 1f 85 eb 51 }
    condition:
        3 of them
}
```

send.exe

```plaintext
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 0e 6b ?? ?? ?? ?? ?? 5a 59 b8 00 0e 00 00 f0 0f b0 23 0f ?? ?? ?? ?? 51 52
            6a 0e 6b ?? ?? ?? ?? ?? 5a 59 eb c3 }
    condition:
        uint16(0) == 0x05a4d and all of them
}
```
Indicators

**NVSMARTMAX.DLL (PLUGX LOADER)**

SHA-256 Hashes: f6c42bc2220fd864ed475b712d2d239ef133a2960f84edcb419aceac4ebe3
SHA-1 Hashes: dce0f3d5a537b722efa0f4f6f817e1b5b97248b
MD5 Hashes: 1d8f21039c629d08c65e9766691483fd | Nv.mp3 (PlugX Encrypted Payload)
SHA-256 Hashes: 73d016ca6988bb85bf294adb1f11e3fb7bc90222085fbd95fe0723aa4428
SHA-1 Hashes: ed88b9b951b6b2a488991f763894199e7a1447d7
MD5 Hashes: 73d016ca6988bb85bf294adb1f11e3fb7bc90222085fbd95fe0723aa4428

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

**PLUGX PAYLOAD**

SHA-256 Hashes: c1c80e237f6fbc2c61b82c3325dd836f3849ca036a28007617e4e27ba2f16c4b
SHA-1 Hashes: 88222c4fe9b9af8300b135229ad7b3303c299aab
MD5 Hashes: c1c80e237f6fbc2c61b82c3325dd836f3849ca036a28007617e4e27ba2f16c4b

**SEND.EXE**

SHA-256 Hashes: b65c57a380a1df69e61462e8a14575bf93a8ea5772621c1f19ccff5bdd6a3e8f
SHA-1 Hashes: c1c80e237f6fbc2c61b82c3325dd836f3849ca036a28007617e4e27ba2f16c4b
MD5 Hashes: 232c85f65de1ef2cab812f01f3761d49
Exfiltration Address: 205408245657-eg0r569eukqef5nkab52b01cl5i3nn5.apps.googleusercontent.com

**Exfiltration Address:**

205408245657-eg0r569eukqef5nkab52b01cl5i3nn5.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.

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