Operation GhostShell: Novel RAT Targets Global Aerospace and Telecoms Firms

October 4, 2018 | Nicholas Ioav

Author
Cybereason
Nocturnium

In July 2017, the Cybereason Nocturnium and Hodeiron Response Teams responded to Operation GhostShell, a highly targeted cyber espionage campaign targeting the Aerospace and Telecommunications industries mainly in the Middle East, with additional victims in the U.S., Russia and Europe.

The Operation GhostShell campaign aims to steal sensitive information about critical assets, organizations' infrastructure and technology. During the investigation, the Nocturnium Team uncovered a previously undocumented and stealthy RAT (Remote Access Trojan) dubbed DeadToRight that was employed in the primary espionage tool.

The Nocturnium Team found evidence that the DeadToRight RAT has been under ongoing development since at least 2016, and has been used in other campaigns against new functionalities, while it evades antivirus tools and managed to remain undetected and operating for months.

Assessments as to the identity of the operators and authors of DeadToRight resulted in the identification of a new Iranian threat actor dubbed Wildfire that has operated since at least 2013 and has remained publicly unknown thus far. In addition, our research points out possible connections to other Iranian state-sponsored APT threat actors such as Chafer (APT39) and Agrius (APT. However, we cross the Kaitseliit Kaitse distinct features that separate it from the other Iranian groups.

KEY FINDINGS

- **New Iranian Threat Actor Wildfire:** A newly discovered Iranian threat actor dubbed Wildfirehad that has been operating since at least 2018 and remained unknown thus far. In addition, we found possible connections between Wildfire and other Iranian state-sponsored threat actors including Chafer (APT39) and Agrius (APT.
- **Discovery of New DeadToRight RAT:** The Cybereason Nocturnium team discovered a sophisticated and previously undocumented RAT (Remote Access Trojan) dubbed DeadToRight used for highly targeted cyber espionage campaigns.
- **Target Industries:** Based on the Operation GhostShell campaign, the Aerospace and Telecommunications industries are the **Enterprises** that has been observed targeting organizations in the U.S., Russia and Europe, with a focus on the Aerospace and Telecommunications industries.
- **Ongoing Development Since 2016:** Our investigation revealed this threat was first observed in the wild in 2016 and has been under ongoing development and has undergone new version adding more features and stealth. This threat is still active as of September 2017.
- **Abusing Cloud Services For C2:** The most recent DeadToRight variants were observed to be abusing cloud-based storage services for Command and Control (C2), in this case the popular Dropbox service, in order to remain undetected by blending in with legitimate network traffic.
- **Designed For Stealth:** The authors of DeadToRight invested a lot of effort into making it stealthy to evade detection by antivirus and other security tools by leveraging multiple obfuscation techniques and recently implementing a Dropbox client for command and control (C2), making it very hard to detect.

SHELLCHECK: THE SILENT RAT

The following sections range the recently observed Operation GhostShell campaign and the evolution of this stealthy DeadToRight RAT, which has been operationalized and developed since at least November 2016.

RECENT CAMPAIGN

In July 2017, Cybereason encountered an unidentified threat actor carrying out a cyber espionage operation using a previously undocumented and stealthy RAT dubbed DeadToRight.

Using this RAT, the threat actors were first observed conducting reconnaissance and the exfiltration of sensitive data from leading Aerospace and Telecommunications companies in the Middle East region, with some observed targeting the same industries in other regions including the U.S., Russia and Europe.

When first investigated, the DeadToRight RAT, the malicious binary was found to be running on victim machines as "svchost.exe" while its internal name was disguised as "RuntimeBroker.exe".

File Version Information	
Copyright	Microsoft Corporation. All rights reserved.
Product	Microsoft® Windows® Operation System
Description	RuntimeBroker
Original Name	RuntimeBroker.exe
Internal Name	RuntimeBroker.exe
File Version	6.0.17763.0
Comments	RuntimeBroker

DeadToRight RAT internal name masquerades as a legitimate Microsoft RuntimeBroker.exe binary

This executable was determined to have been compiled on May 22nd, 2017, and was observed to be executing adjacent to additional TTPs.

SHELLCHECK STRUCTURE AND CONFIGURATION

The DeadToRight RAT is a modular RT leveraging Costura to compress each of the modules using zlib.

Embedded DLL RAT utilizes Costura

Two of the references are DLLs containing supporting functionalities:

- **Extensions.dll** contains utilities and functionalities such as:
  - AES Encryption, including an AES Key and an Initialization Vector (IV)
  - Hashing
  - File Operations
  - Registry Operations
  - Process Creation
  - Serialization

Extensions.dll

- **ClientCore.dll** holds other core functionalities of the client such as:
  - Fingerprinting
  - File Operations
  - User Impersonation
  - Token Handling
  - PTP Client
  - Telnet Client
  - Settings & Strings

ClientCore.dll

The executable stores most of the its strings, including configuration strings, as bytes and then converts them in run time to UnicodeUTF3 to evade antivirus strings detection:

private Byte[]
{ ( ) Core.Client.Core ( )
{ ( ) Core.Client.Core ( )
{ ( ) Core.Client.Core ( )

observed sample. Pivoting on this command, we were able to uncover an older instance (version 1.1, SE2 exe used this same MD5 ClientDataDll, a unique ID generated by the project name, plus a hard-coded date – 20210406-0725-44ec6c-7e2fa6a2fa6a).

Observe .NET Special, in 0.dat between the recent and the older version of ClientDllExe

From there, finding the other previous versions of ClientExecutor was achieved by pivoting searching for strong and code similarities. This pivoting process proved that ClientExecutor has been under active development for at least November of 2019, marking almost three years of development work to evolve the malware from a simple standalone reverse shell to a stealthy multistage backdoor.

In each new iteration of the malware, the authors added new features and capabilities, attempting to use various techniques to evade detection. Table 1 shows a list of the ClientExecutor versions we found, with the date of each compilation, from version 0.0.1 up to the latest version, which includes significant design and architecture changes like introducing modular design.

Below is a summary of the variants that were discovered so far:

VT Link	Version Name	Name	Compilation Date	First Submission Date to VT	PDB Path.
VT link	0.0.1 (where applicable)	ClientExecutor.exe	2019-11-26 21:20:41	2019-11-26 13:26:46	
VT link	1.1	svchost.exe	2019-11-26 23:41:15	2020-04-10 23:22:15	D:\projects\SE - Reverse Shell\ClientExecutor_VT\Pdb\svchost.exe.pdb
VT link	2.1	svchost.exe	2020-04-10 11:19:14	2020-04-10 22:58:49	D:\Projects\ExecutorRebuild\SE - Reverse Shell\ClientExecutor_VT\Pdb\svchost.exe.pdb
VT link	3.1	svchost.exe	2019-05-12 18:37:20	2019-05-12 22:32:43	D:\Visual Studio 2017\Projects\ClientExecutor\ClientExecutor\obj\Release\svchost.pdb
VT link	4.0.0	RuntimeBroker.exe	2021-08-19 11:14:41	2021-09-22 19:14:39	
VT link	4.1	RuntimeBroker.exe / svchost.exe	2021-05-02 12:06:05	2021-07-28 16:10:36	

Known ClientExecutor RAT versions

OVERVIEW OF SHELLCLIENT EVOLUTION

EARLIEST VARIANT (NOVEMBER 2019)

The earliest variant found was compiled on the November 26, 2019, and was purposefully named *svchost.exe* to allow it to masquerade as a legitimate Windows binary. This early variant is not very rich in features and lacks the sophistication and functionality that we manifested in its successors. In essence, it is a rather simple reverse shell.

Main Features:

- **File name:** *svchost.exe*
- **File description:** Windows Defender Service
- **Core functionality:** Simple widesocket based reverse shell
- **Hardcoded C2 domain:** *azure-ms-tech.ga:80*

VARIANT 0.0(NOVEMBER 2019)

The second oldest variant emerged about 3 weeks after the initial version. This variant is more mature and contains capabilities of both a reverse and a server, including a new service persistence method dropping an a Windows Defender Update service. This version of ShellClient also communicates with the following C2 domain: *azure-ms-tech.ga:80*

Main Updates:

- **File description:** Host Process for Windows Processes
- **Core functionalities:**
  - Predefined set of C2 commands
  - Executing arbitrary commands via CMD shell or PowerShell
  - Client and Server components
  - Persistence via Windows Service, manipulating as Windows Defender
  - Based on existing/modifying for data sent from File C:2

VERSION 4.1 (OCTOBER 2020)

Compiled approximately 3 weeks after variant 3.1, this variant keeps the same name and description attributes but shows further progress in development by adding a variety of new capabilities, including RTP Evasion, AMSI bypass, encryption, self-update capabilities and more. This version of ShellClient also communicates with the following C2 domain: *azure-ms-tech[2].ga:80*

Main Changes:

- **Core functionalities:**
  - Implementing RT and Tamper checks
  - AES encryption of data sent to the C2
  - Self-updating feature
  - Client-SS and extensions attributes added
  - Extended set of predefined C2 commands

VARIANT 4.1 (JANUARY 2010)

About a month after the emergence of variant 3.1, the 4.1 variant came to see January of 2019. It has mostly minor changes, with the main one being the ability to run in a hidden window. This version of ShellClient also communicates with the following C2 domain: *azure-ms-tech[3].ga:80*

Main Changes:

- **Core functionalities:**
  - Implementing VT and Tamper checks.
  - AES encryption of data sent to the C2
  - Self-updating feature
  - Client-SS and extensions attributes added
  - Extended set of predefined C2 commands

VARIANT 4.1 (JANUARY 2010)

Perhaps one of the biggest advancements in the ShellClient evolution came with version 3.0.3 and continued with its successor 3.0.1, in which the malware authors implemented many changes and improvements, adding new capabilities and functionality, such as process injection and code protection using Costura packer, as well as abandoning the C2 domain that was active since 2019.

The traditional C2 communications were replaced with a Dropbox built-in client, allowing the popular online platform to send commands to ShellClient as well as storing the output of the commands in a designated folder. Dropbox is a platform that ultimately makes it harder to detect since the network traffic would appear legitimate to security analysts as well as most security solutions.

Note: For full analysis of the variants, please refer to Appendix A in the IOCs pivoting in lower right of your screen.

ATTRIBUTION

During the investigation, efforts were made to identify instances of the ShellClient code and to determine its origin or inspiration. Unfortunately, we were unable to find any other instances of the ShellClient malware in the wild at the time of the investigation, and the identity of the threat actor behind the attack was unclear. We focused our hunt attempts to find links to known adversary groups that have carried out similar attacks in the past against this industry and the offensive tools.

While some possible connections to known Iranian threat actors were observed, our conclusion is that ShellClient is a custom-made tool developed by a threat actor who is not yet known to the public and is not related to any known actors. A plausible big idea is it hoped that more attention will be given to this threat and over time more information about ShellClient origins will emerge.

LIKELY RATIONS STATES SPONSORED THREAT ACTOR

The current working assumption is that ShellClient was created and maintained by a nation-state sponsored threat actor, or Advanced Persistent Threat (APT). The intrusions analyzed by Cybereason suggest that the motivation is cyber espionage, with the data being exfiltrated being of high value to the victim. Although we have not seen any of the samples found in the telemetry or in the wild since 2018, it contains very sophisticated techniques that are usually found in abundance.

In addition, the PDB path that is embedded in some of the ShellClient samples suggests that malware is part of a restricted or classified project that could be related to military or intelligence agency operations:

- **Projects (Capitalized)** - Reverse Shell\ClientExecutor_VT\Pdb\svchost.exe.pdb

RUSSIAN TURLA CONNECTION OR A FAKE FLAG? POSITIVE?

In examining some "low hanging fruit, "the first clue examined was a Turla code comment that appeared in VirusTotal along with some of the older versions of ShellClient. The Turla code that was indicated is named *APT_Turla_WATCOM_Malware_Jan09.A*.

Turla code comment that appeared in VirusTotal

The Kaspersky Team examined the possibility that the ShellClient malware might have been created by the Russian APT group Turla. The Kaspersky Team concluded that the ShellClient malware is not related to Turla because the Turla Group typically uses Delphi, Python and C++ in the Turla rule, the team did find any significant similarities or evidence that can tie Turla to ShellClient or the activity that was observed in the intrusion investigated.

AN IRANIAN CONNECTION

Given that most of the victims were located in the Middle East region and considering the affected industries, the unique profile of the attacked organizations, as well as other characteristics related to the intrusion and the malware, Cybereason initially suspected that an Iranian state-sponsored threat actor might be behind the Operation Ghostshell intrusion.

The Kaspersky team compared our observations with previous campaigns that were attributed to known Iranian threat actors, and was able to find some similarities between ShellClient and previously reported Iranian malware and threat actors.

However, at this point, our estimation is that this operation was carried out by a separate actively group, dubbed MoKhtavat, which has its own distinct characteristics that distinguish it from the other groups.

Nonetheless, we believe that highlighting the possible connections between various Iranian threat actors could be beneficial. Whether such connection is a result of a direct collaboration among these threat actors is currently unknown.

These connections can also be explained in other ways, which are less direct, for example - a cyber mercenary who provides a multinational service could also be a likely explanation that can account for some of these observed overlaps.

MEET MALKAMAK, A NEW IRANIAN THREAT ACTOR

MalKamak Diamond Model Summary

Using the famous diamond model of intrusion analysis, the Kaspersky team was able to determine that the attacks were carried out by a new threat actor dubbed MalKamak, which was unknown thus far and believed to be operating on behalf of Iranian interests. Following is a quick summary of its main characteristics:

- **Country of Origin:** Iran
- **Years of Activity:** Since at least 2018
- **Motivation:** Cyber Espionage
- **Victimology:**
  - **Affected Regions:** Predominantly the Middle East, with victims in the US, Europe and Asia
  - **Affected Industries:** Aerospace and Telecommunications
- **Unique Tools:** ShellClient (evolving from a simple reverse shell to a complex RAT)
- **Generic Tools:** Gsocket/Gsocket, Putty, Plink, Ngrok, Ngrok.exe, and mimikatz
- **Known Infrastructure:**
- **2018-2020:** *microsoft[1].ga*
- **2021:** Dropbox C2

**Attribution is derived from Gsocket, the name of an ancient Persian mythological creature (Naqash mythological for) drawing and spreading chaos.*

SIMILARITIES TO PREVIOUS IRANIAN APT-RELATED CAMPAIGNS

During the analysis, it was observed that there were some potentially interesting links and similarities to an Iranian threat actor called Charlie APT (also known as APT34, OilRig, Helix Kitten).

The group has been active since at least 2014, and is believed to be linked to the Islamic Revolutionary Computing Company, a Tehran-based company, previously known to serve as a front company for the Iranian Ministry of Intelligence and Security (MOIS). The Charlie APT is known to attack targets in the Middle East as well as the US, and Europe.

Examining open campaigns - such as the one analyzed in Malwarebytes's Charlie APT report, the team noticed interesting overlaps with observations in this investigation, as detailed in the following sections.

Our current assessment is that while these overlaps are interesting, they are not strong enough to establish attribution with an adequate certainty.

CREDENTIAL DEPENDS

Charlie APT's tools, such as the TelegrafAgent, tend to harvest credentials from compromised endpoints. As mentioned previously in this report, we also observed that the threat actor analyzed here used a variety of credential tools.

OBFUSCATED POSTERISCRIPTS

In both of the investigations, the threat actors obfuscated their postexploitation by obfuscating the malware as legitimate Windows related components on victims' systems. To achieve that, both operations used the Windows Defender Update name to disguise their activities.

ShellClient Disguised Persistence	Previous Charlie APT Disguised Persistence
Windows Defender Update service	**Defender Update** scheduled task

ClEx.exeand Persistence

PDBS

Executable in both of the operations were found to be compiled from similar paths, particularly comparing the "projects" folder name in use:

ShellClient PDB Paths	Charlie APT Disguised Persistence
D:\projects\SE - Reverse Shell\ClientExecutor_VT\Pdb\svchost.exe.pdb	**F:\Projects\ExecutorRebuild\SE - Reverse Shell\ClientExecutor\obj\Release\svchost.pdb**
D:\Projects (ClientExecutor)SE - Reverse Shell\ClientExecutor_VT\Pdb\svchost.exe.pdb	**F:\projects\ExecutorRebuild\SE\ClientExecutor\obj\Release\svchost.pdb**

PDB Filelistings

SIMILARITIES TO ALERIS APT-RELATED CAMPAIGNS

Another Iranian threat actor that was observed is a relatively new activity group known as Aleris APT. The group has been active since at least 2019, mainly targeting organizations and companies, carrying out destructive operations under the guise of ransomware attacks.

A report about Aleris attacks mentions a custom .NET backdoor called *Ebar Helper*. Although the *Ebar Helper* backdoor and ShellClient are different, there were some interesting similarities in the coding style and naming conventions, which may indicate a link between the two malware and the possibility that they were authored by developers from the same or adjacent teams.

These interesting code similarities could indicate a similar development process that was followed by ShellClient, or at the very least, a similar coding style. Although the Aleris report does not mention any RTP evasion, the TTPs and process injection techniques conducted by Aleris are very different than the TTPs and intrusions observed in Operation Ghostshell - and therefore we concluded that it is unlikely that Aleris is behind this operation.

POSSIBLE CODING STYLE SIMILARITY

Both companies share the command parsing functions of both *Ebar Helper* and ShellClient, a similar code structure and logic: *ebar* and *client*.

Code similarities between Ebar Helper and ShellClient

NAMING CONVENTIONS

Both ShellClient and *Ebar Helper* use a similar naming convention for the classes used to launch the malware as a service:

Similarities between ShellClient and Ebar Helper naming conventions

KILL TECHNIQUES

Both ShellClient and *Ebar Helper* use *KeyboardLive* in the self kill mechanism. When ShellClient receives a self kill command, it executes *KeyboardLive* in order to delete the service created and remove traces left from the infected machine. Similarly, the Aleris report mentions that the *Ebar Helper* backdoor executes a batch script named "remover.bat". The script uses *KeyboardLive* to delete the service created for the malware.

DATA DECODING AND ENCRYPTION

Both ShellClient and *Ebar Helper* use Base64 and AES to encode and encrypt data sent to the C2. In addition, both malware have a separate class for Base64 encoding and decoding, and for AES encryption and decryption:

ShellClient and Ebar Helper data decoding and encryption similarities

OTHER SIMILAR FUNCTIONS

Both ShellClient and ShellClient, *Ebar Helper* and *Keyboe* malware are very similar. For example the Sensitive function, which is found on all three malware samples:

ShellClient, Ebar Helper and Keyboe malware similarities

POSSIBLE INFRASTRUCTURE CONNECTION

Another interesting connection identified between these malware is based on port IP address resolutions of the domain used by ShellClient (azure-ms-tech[2].ga and *c.domain used by Ebar Helper* whyisworkinlikethisanyway[2].com). Both of these domains have been resolved to both of the ports 443 TCP, 53 TCP and 80 TCP.

Upon examination of these IP addresses, they belong to a VPSHOST. Further examination of other domains that were resolved to these IP addresses in the past revealed a significant number of malicious domains that were used by Iranian APT groups.

CONCLUSION

In the Operation Ghostshell report, the Cybereason Nocturnus and Incident Response Teams discovered a sophisticated new Remote Access Trojan (RAT) dubbed ShellClient that was used to highly targeted attacks against a victim in the Middle East. Operation Ghostshell is a campaign that has been active since at least November of 2019 (v0.0.1). Nuance and Energy Sector are current assumptions is that the attacks were perpetrated by a newly discovered Iranian actors group dubbed MoKhtavat that has been operating since at least 2018 and remained in the dark until now.

The investigation into Operation Ghostshell also revealed that the ShellClient dates back to at least 2018, and has been continuously evolving ever since while successfully evading most security tools and remaining completely unknown. By analyzing the various versions of ShellClient, we observed the development of the malware, from a simple reverse shell into a fully-fledged, stealthy RAT capable of a sophisticated RAT used for further cyber espionage operations within victim networks.

The most recent ShellClient versions observed in Operation Ghostshell follow the trend of abusing cloud Dropbox storage services, in this case the popular Dropbox service. The ShellClient authors chose to abandon their previous C2 domain and replace the command and control communication with the malware with a more simple yet more reliably C2 channel using Dropbox to exfiltrate the stolen data as well as to send commands to the malware. This trend has been observed in multiple recent APT attacks due to its simplicity and the ability to effectively bypass most legitimate network traffic.

It is the intention of the researchers that the information presented in the Operation Ghostshell report will inspire further research and hunting efforts for the newly identified ShellClient operation activity group, and that it will ultimately aid in shedding more light on this mysterious malware that was kept well-hidden for many years.

AUTHORS

TOM FAKTERMAN, THREAT RESEARCHER

Tom Fakterman, Cyber Security Analyst at the Cybereason Nocturnus Research Team, specializes in protecting critical networks and incident response. Tom has experience in researching, hunting, reverse engineering malware and developing scripts and tools for automated cyber investigations.

DANIEL FRANK, SENIOR MALWARE RESEARCHER

With a decades-in-malware research, Daniel uses his expertise with malware analysis and reverse engineering to uncover APT activity and community cybercrime attackers. Daniel has previously shared research at Black Hat Conference, the Microsoft Digital Crimes Consortium, and Nuxeon.

CHEN ERLICH, INCIDENT RESPONSE ENGINEER

Chen has almost a decade of experience in Threat Intelligence & Research, Incident Response and Forensics. Before joining to Cybereason, Chen spent many years conducting APTs investigating underground cybercriminal groups and discovering security vulnerabilities in known software. Previously, he was a Security Researcher in the IDF.

CHAIM ASSAWIA, HEAD OF THREAT RESEARCH

Assaf has over 5 years in the military industry. He started his cyber career in the Israeli Military 8200 Intelligence Unit, where he was a team leader and a senior researcher focusing on malware analysis and

Cybersecurity unit where he developed extensive experience in offensive security. Later in his career he led Red Teams, developed penetration testing methodologies, and specialized in malware analysis and reverse engineering.

INDICATORS OF COMPROMISE

Open the chatbot on the bottom right corner of your screen to access the Ghostshell IOCs and Appendix A.

MITRE ATT&CK BREAKDOWN

Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Command-line interface	Windows Service	Valid Accounts	Obfuscated Files or Information	Credential Dumping
Windows Management Instrumentation			Masquerading	
PowerShell				

Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
Security Software Discovery	SMB/Windows Admin Shares	Archive Collected Data	Data Encoding	Exfiltration Over Web Service
System Information Discovery			Encrypted Channel	Exfiltration Over C2 Channel
System Network Configuration Discovery			File Transfer Protocols	Exfiltration Over Alternative Protocol
			Web Protocols	

ABOUT THE AUTHOR

Cybereason Nocturnus

The Cybereason Nocturnus Team has brought the world's brightest minds from the military, government intelligence, and enterprise security to uncover emerging threats across the globe. They specialize in analyzing new attack methodologies, reverse-engineering malware, and exposing unknown system vulnerabilities. The Cybereason Nocturnus Team was the first to release a vaccination for the 2017 NotPetya and Bad Rabbit cyberattacks.

All Posts by Cybereason Nocturnus →

NEWSLETTER

Never miss a blog

Get the latest research, expert insights, and security industry news.

Subscribe

This website uses cookies to ensure you get the best experience on our website. By continuing on our website, you consent to our use of cookies. To find our more about how we use cookies, please see our Privacy Policy.

Looking for the Indicators of Compromise (IOCs)?

©Cybereason 2021. All Rights Reserved.