

The Bitdefender logo is displayed in white text against a dark blue background. The background features a complex network diagram with various nodes and connections, overlaid on a grid pattern. The nodes are represented by small circles in various colors (blue, orange, purple) and some are labeled with alphanumeric codes like '19.78-G', '21.87-A', '39.06-C', '42.49-A', '65.18-B', '73.27-B', '79.81-B', '88.96-B', '94.28-C', and '99.83-C'. Some nodes are highlighted with larger circles or checkmarks.

## Security

# New TrickBot Module Bruteforces RDP Connections, Targets Select Telecommunication Services in US and Hong Kong



# Contents



Executive Summary .....	3	
Key Findings .....	3	
rdpScanDll:.....	3	
TrickBot: .....	3	
Teaching and Old Dog New Tricks .....	3	
New module: rdpScanDll .....	4	
Check Mode.....	4	
TryBute Mode .....	4	
Brute Mode .....	4	
Modules overview .....	6	+
C&C servers .....	8	
Victims .....	9	×
Indicators of Compromise.....	10	
Why Bitdefender .....	16	
Proudly Serving Our Customers .....	16	
Trusted Security Authority .....	16	
Dedicated To Our +20.000 Worldwide Partners .....	16	



## Authors:

Radu Tudorica - Security Researcher, Cyber Threat Intelligence Lab

## Co-authors:

Alexandru Maximciuc - Team Leder, Cyber Threat Intelligence Lab

Cristina Vatamanu - Senior Team Leader, Cyber Threat Intelligence Lab



## Executive Summary

Bitdefender researchers have discovered a new TrickBot module (rdpScanDll) built for RDP bruteforcing operations on select targets. The new module was discovered on January 30 and, based on the IP addresses it targets, victims seem to be US- and Hong Kong-based, predominantly in the telecom industry.

Our researchers have kept a close eye on TrickBot. On January 30, 2020, our monitoring systems reported the delivery of a new module, performing bruteforce operations on a list of targets defined and sent by the attackers.

## Key Findings

### rdpScanDll:

- New module that bruteforces RDP for a specific list of victims
- Still in development, as the module features a broken attack mode
- Targets mostly in telecom, education, and financial services in the United States and Hong Kong

### TrickBot:

- Lateral movement modules receive the most updates
- Dynamic C&C infrastructure, mostly based in Russia.
- Over 100 new C&C IPs added each month, with an average lifetime of about 16 days

## Teaching and Old Dog New Tricks

While TrickBot is a Trojan that has been around since 2016, it turns out that you *can* teach an old dog new tricks. While it started out as a credential-harvesting threat mostly focusing on e-banking, its plugin-based design has made it much more than just a threat focused on financial data theft. Security companies and researchers have previously analyzed a wide range of modules, proving that the Trojan is still under active development and undergoing constant “feature upgrades”.

The flexibility allowed by this modular architecture has turned TrickBot into a very complex and sophisticated malware capable of a wide range of malicious activities, as long as there is a plugin for it.

From “add-ons” for stealing OpenSSH and OpenVPN sensitive data, to modules that perform SIM-swapping attacks to take control of a user’s telephone number, and even disabling Windows built-in security mechanisms before downloading its main modules, TrickBot is a jack-of-all-trades. Another interesting aspect is that, while there are a handful of core modules, each new module is accompanied by a

configuration file, potentially making each functionality fully independent.

TrickBot has been mostly distributed through spam campaigns but it was also seen in cahoots with other threats. Distributed by the Emotet spam-sending botnet to deliver Ryuk ransomware, TrickBot operators have extended its capabilities into one of the most advanced malware delivery vehicles out there.

This combo relied on Emotet for its huge spam campaign and effective social engineering, on TrickBot for its aggressive network spreading capabilities, and on the Ryuk ransomware for the final payload and direct monetization. The spam campaigns have focused on targeting organizations by going after enterprise assets.

## New module: rdpScanDII

The new module was discovered on January 30, and its main functionality is to perform bruteforce operations on a list of targets.

The modus operandi is similar to that of other plugins. The TrickBot executable will download the plugin and its configuration file (from one of the available online C&Cs) containing a list of servers with whom the plugin will communicate to retrieve commands to be executed. TrickBot will load the plugin, executing the “start” and “control” exported functions, passing the configuration file as an argument for the last mention function.

This plugin shares the configuration file with another module, vncDII, but uses different URL endpoints to distinguish itself.

The communication with these new servers has a certain pattern. The structure of the URLs the plugin is using is as follows:

`https://<C&C>/<tag>/<computerID>/<controlEndpoint>`

Where:

- **C&C** – is one of the command and control servers from the configuration file
- **tag** – is the group tag used by the underlying TrickBot sample

- **computerID** – is the computer ID used by the underlying TrickBot sample
- **controlEndpoint** is one of the following:
  - **/rdp/mode** - used to determine what kind of attack the plugin should use
  - **/rdp/freq** - used to determine how frequently to report different statuses back to the server
  - **/rdp/domains** - a list of IP: Port pairs that will be attacked (the targets); note that when the port is missing, the plugin will use the canonical RDP port of 3389
  - **/rdp/over** - a list of IP: Port pairs that will be attacked after the previous list (returned by **/rdp/domains**) is exhausted
  - **/rdp/dict** - a list of passwords to try in the bruteforce process
  - **/rdp/names** - a list of usernames to try in the bruteforce process
  - **/81** - used to report different statuses back to the server (what IP: Port pairs are online or offline and what username - passwords have matched)

The plugin has three attack modes at its disposal: **check**, **trybrute** and **brute**.

### Check Mode

The **check** mode should check for RDP connection on the list of targets (both **/rdp/domains** and **/rdp/over**). To do that, it first retrieves the frequency, then it retrieves and checks the list of targeted IPs from **/rdp/domains**, and finally it retrieves and checks the list of targeted IPs from **/rdp/over**. During testing, we found the plugin retrieves and checks the IP list from **/rdp/over** repeatedly. If the plugin is deployed on a larger number of victims, these collective repeated checks could flood the C&C server with requests.

### TryBute Mode

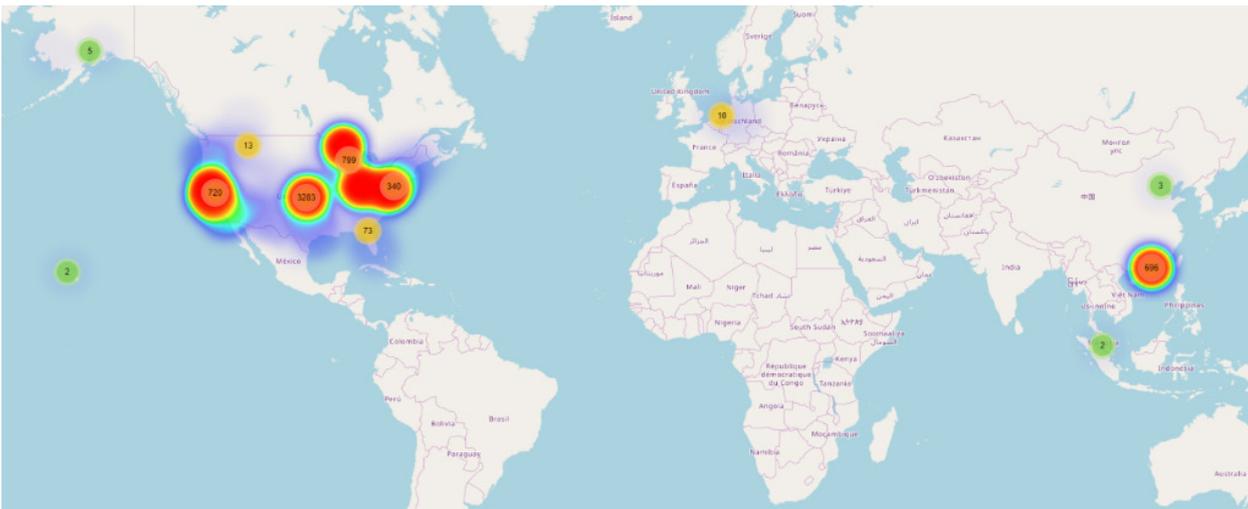
The **trybrute** mode will perform a bruteforce operation on the list of targeted IPs returned by **/rdp/domains**, and later on the one returned by **/rdp/over**, using the usernames from **/rdp/names** and the passwords from **/rdp/dict**.

### Brute Mode

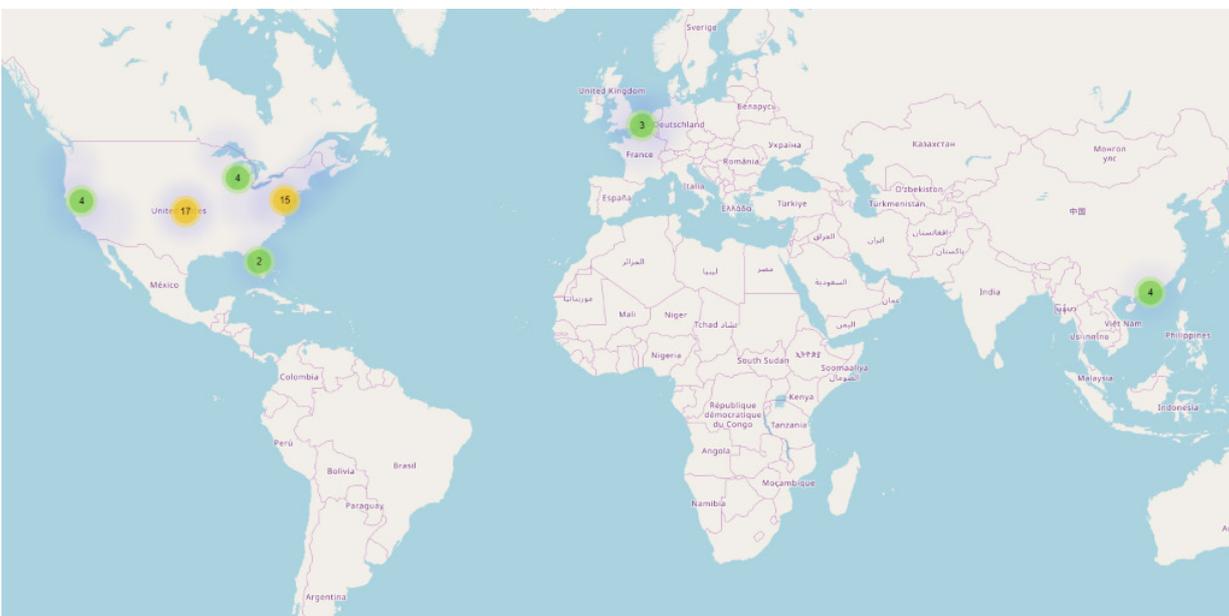
The plugin looks like it's still in development, besides the inclusion in the executable of a set of functions that aren't called, the attack mode **brute** seems broken. The brute attack mode doesn't fetch the username list, causing the plugin to use null passwords and usernames to authenticate on the targets list.

If a host is found online, the plugin reports to the C&C through a POST multipart request to the /81 endpoint with the list of online IPs. The same happens if the plugin finds the credentials to a certain target. The plugin also reports to the /81 endpoint on a regular basis, with information about its state. At the same time, it will report to the main TrickBot executable statistics about the state of the execution and, when it finds working credentials, the username and password it found for a particular target.

During the analysis of pScanDll module, we were able to retrieve several updates for the lists of targeted IPs (both /rdp/domains and /rdp/over). At the time of writing, the lists contained 49 IP addresses (/rdp/domains) and 5,964 IP addresses (/rdp/over). Most of these targets are located in Unites States and Hong Kong. The geographical distribution of these lists is illustrated below.

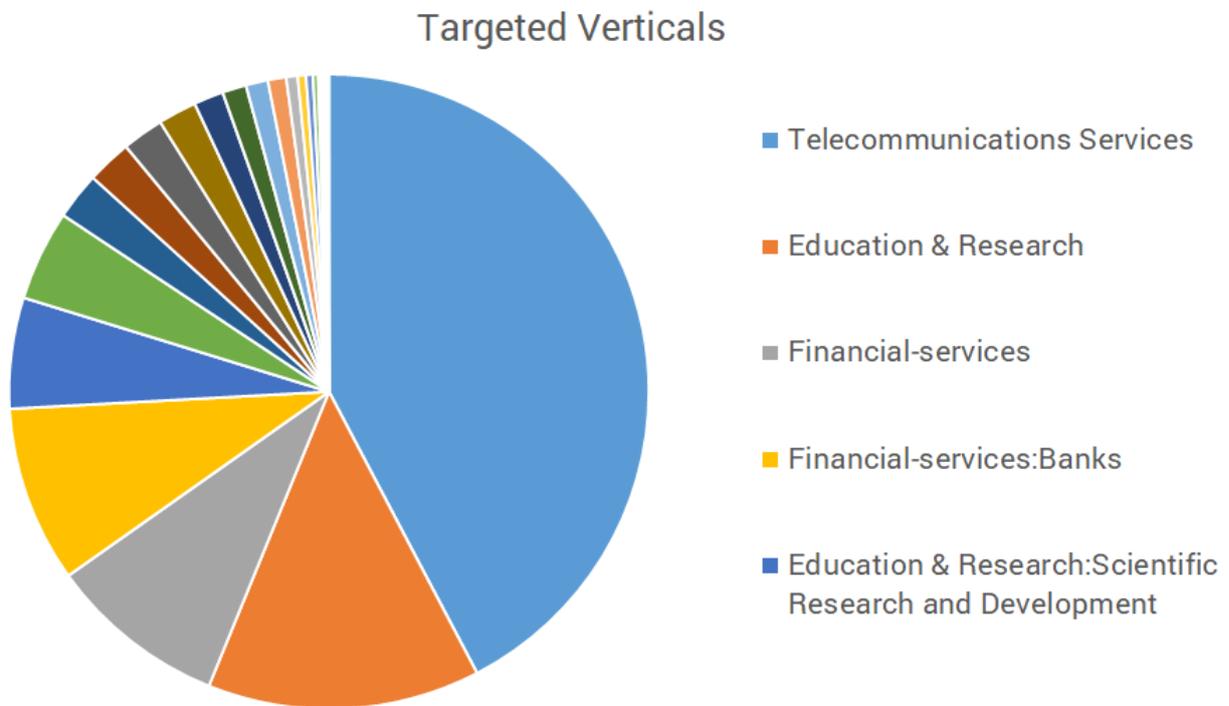


**Fig. 1 - Geographical distribution of /rdp/over IP addresses**



**Fig. 2 - Geographical distribution of /rdp/domains IP addresses**

When performing a screen on these targets, we found that they fall on different verticals, as observed in the chart below:



**Fig. 3 - Most affected verticals**

## Modules overview

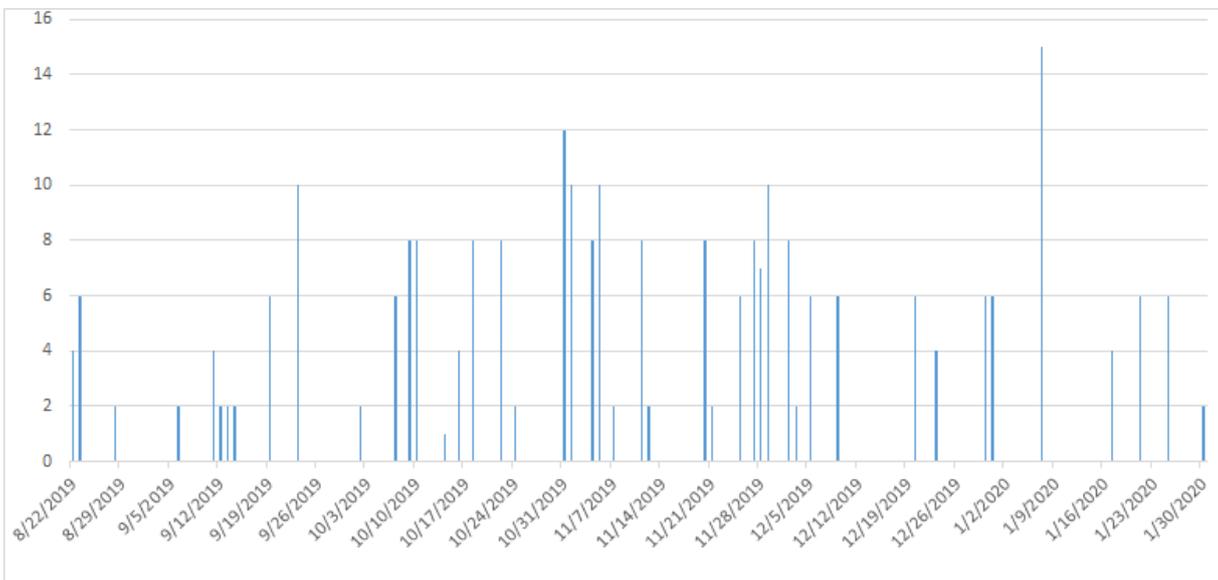
TrickBot has an embedded list of command and control servers and a list of “must-have” plugins. First, it contacts the servers to retrieve these plugins, as well as an updated list of command and control servers and an additional list of servers, used only for downloading purposes. After these initial actions, it awaits further instructions. One command is to start a certain plugin. If that plugin does not exist, it uses the list of download servers to retrieve it first, then it loads the plugin and executes the indicated exported function (from the command). As a persistence mechanism, some of the plugins are loaded automatically when TrickBot malware is started, without waiting for a command from the C&C servers.

During the last 6 months of close monitoring and gathering statistics about this threat, our systems were able to retrieve updates for several different active plugins, gathered around different functionalities, proving to have all the right tools to perform an end-to-end attack:

- **Lateral Movement**
  - *WormDII/mWormDII/tWormDII* - a worm component responsible for spreading into the local network via SMB by exploiting through EternalBlue
  - *TabDII* - uses EternalRomance to spread into the network via SMB
  - *ShareDII/mShareDII/tShareDLL* - remote service manager using stolen credentials to install remote services on other computers from the network
- **Reconnaissance**
  - *SystemInfo* - collects information about the affected system
  - *NetworkDII* - performs network mapping

- *PsfIn* - meant to identify POS-related terminals inside the compromised domain
- **Collection**
  - *ImportDll* - collects varying browser information such as cookies or browser configuration
  - *Pwgrab* - steals credentials from various applications
  - *aDll* - steals active directory credentials
- **Setting Foothold**
  - *NewBCtestnDll* - performs reverse proxy and executes commands
  - *VncDll* - used by the attacker as RAT, giving the option to remotely view and control the victim's computer
- **Exfiltration**
  - *Mailsearcher* - searches for files with certain extensions (usually document files)
- **Financial data theft**
  - *InjectDll* - used to steal financial information through webinjects by monitoring various banking websites
- **Credential Access**
  - *RdpScanDLL* - performs bruteforce attack on a certain list of targets (indicated by the attacker)

While monitoring the updates of malicious plugins, we observed that the most frequently updated ones were those performing lateral movement: 32.07% of them were wormDll, 31.44% were shareDll and 16.35% were tabDll. The rest of the plugins had fewer than 5% occurrences.



**Fig. 4 - Timeline for plugin update**

Some of these plugins can have configuration files, which serve varying purposes. If needed, they will be retrieved from the command and control servers. Some of those retrieved by our researchers are described below:

- *dinj* - configuration file for injectDLL plugin, containing information about targeted financial institutions; the attack uses server-side injections
- *sinj* - configuration file for injectDLL plugin, containing information about targeted financial institutions; the attack uses redirections (also known as web fake injections).
- *dpost* - also used by the injectDLL module, containing a list of servers; the stolen financial information is sent to one of the servers from this list

- *mailconf* - used by mailsearcher for exfiltration
- *srv* - used by rdpScanDLL as a list of C&C servers
- *vnccconf* - used by vncDLL and rdpScanDll for as a list of C&C servers

## C&C servers

Our monitoring systems focused on collecting new command and control servers, both from embedded lists inside the samples and by constantly checking for C&C updates. We were able to retrieve 3,460 IP addresses, divided into 2,926 command and control servers and 556 servers dedicated to downloading new plugins, and 22 IPs serving both roles. The dynamics of the infrastructure can be defined by a rough statistic of around 100 new IPs added each month with each IP having an average lifetime of about 16 days.

Illustrated below is the geographical distribution of these servers. As can be observed, the threat actor prefers infrastructure from Russia.



**Fig. 5 - Geographical distribution of Command and Control servers**



**Fig. 6 - Geographical distribution of Servers used for download purposes**

# Victims

Since TrickBot is a mass attack threat, spreading mostly through spam e-mails, victims fall into multiple verticals and are spread all over the globe. Telemetry from our Network Attack Defense technology for the last month shows that most victims attempting to connect to a command and control server are based in the US, followed by Spain. This kind of distribution usually can be observed when massive spam campaigns are focused on particular geographical areas.

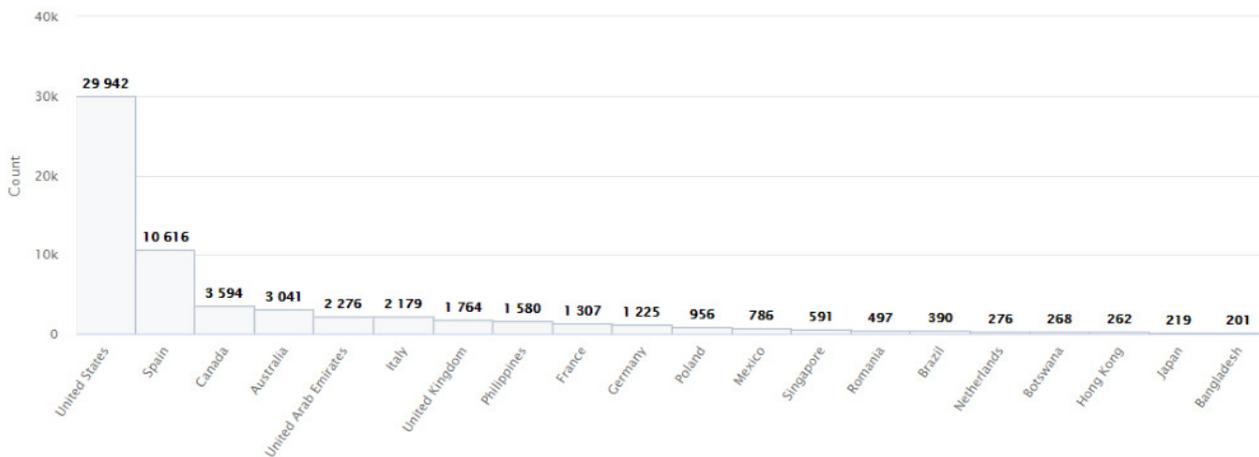


Fig 7 - Geographical distribution of victims contacting command and control server over the last month

# Conclusions

The new rdpScanDll module may be the latest in a long line of modules that have been used by the TrickBot Trojan, but it's one that stands out because of its use of a highly specific list of IP addresses. While the module seems to be under development, as one attack mode seems broken, newer versions of rdpScanDll will likely fix this and potentially add new ones.

The new module also offers a glimpse into how TrickBot operators act. Using an existing infrastructure of TrickBot victims, the new module suggests attackers may also be focusing on verticals other than financial, such as telecommunications services and education & research.

# Indicators of Compromise

An up-to-date list of indicators of compromise is available to Bitdefender Advanced Threat Intelligence users. More information about the program is available at <https://www.bitdefender.com/oem/advanced-threat-intelligence.html>.

## Plugin samples

### **NewBCtestnD1132**

```
6e61106594e106fc2192fdf341b63732d7cc2d13ee50dbb07234de416b851905
042774b7335f33a0813862b366c5fc2e70768f63b4cb0b98d53523a9636482b4
99f2d1f09246f6903a72d1056b96782a0242f1862d38d51e083e453acf1cde67
0cbca659207cc738798475355307ac580a75e5d3ac366ae377e622bb718ac723
```

### **NewBCtestnD1164**

```
de7273f2d4a9f34523e4bb51cb867f91aafeccldfbce8df93299bd4038b1af69
cc9afe85292904747cac2ab4f13d9e02414ec561315f186b844b135a9cfa45aa
3c665472455558ea2ce7a7de637d53dd1868baaa6eff77538d31303424a86fdd
8f2ff42df687d6e2ed6df2c3c45092be7a07347b9819c5cd7589c64c3b4dee60
```

### **importD1132**

```
cd79145f9eff2131d015fb729b32d79270a1690d2955b0945d6b8451bafebb99
5a5ed23fafa8038a44213cefab6fbd392ff672e27025e4185f94c68fe6590e91
4eb803eb95eb8b9533e957706e1861932036beb5eef019bf77aaeba7202fa303
```

### **importD1164**

```
03e19745382c0f0a94a098a6d58630ba2af2b6bf65e21a230084e8cadcbef368
709a62ed92806ee68cd062966102354cae371d0f9f7a9cd17edf31e4c8dcb663
e557d2018fae0621065c0d93836d09848d84f92e8188f947b8c8a1fa436f5632
```

### **injectD1132**

```
a58f21fd1cf462ce8b3259aff19e03709a416b872ada566e8f11afcba2f20aeb
5bc9740e7f5b26d0d5522e2f6eb612908ea298c8f83476b3c455106342579a5c
```

### **injectD1164**

```
fd8fb7d97a9f5f00c0a7306baafb54667ba0d34bd2bbd253554c3a036a8c7b24
26d1ecab7e74a7bd1ecc84ef047a4908cb22d2ef47da191c7163bc7749e035ff
```

### **mailsearcher32**

```
a4f94ae7bd9ead9d4cb9f7510bd7af861767f1a1aa57e1c40c334e559b882cc7
79ff0c8a3338b7e97b3bd454373e163e8156ab8097229083eb1285940974f9d8
```

### **mailsearcher64**

```
8e9623a5210e0e99e519f48abd5ff90601d8858d53613e0045c88b94113c560f
c668899703e90877ea5498391b377ae58504768b050595266ea82434a82e68e5
```



**mshareD1132**

adb0a247879d65f56eb4d2409dcad6bf4feeb3cb9ee81278afba568c9bfcffd7  
ac1199d506c66802d5bb10eb77de437fc29dd7b5d2798ab2aa7c1031725a0f67  
5e3bff42eccdf5a3f06bf6fa3eb5a016c19f75a805208e16a25d92002f1760c7  
2b8e4c4f89209a45a96b9a0975d290426c8481211ebb62d2cd43b8f0cec490a7  
3f3de77ef281e8a2368519411970663da8dac57c58fe937bd7f9d9b7e01fd58f  
4f8bf23b354a3ae6aa1dd39808d8abdbel1a1628478f75d74799fca442eae376a  
6cd0d4666553fd7184895502d48c960294307d57be722ebb2188b004fc1a8066  
a575cc45be5459d28b966b4e5fc03099ba929cb77a899834a96163ffde1dc4a5  
f626b2a68e1307b407ad81707a42f165e4167be2f409dfa82c0ff98022d39da2  
1d63030e9e254bd2b6a358b4d0bf980a9adb4f9d57f1740adb16d95452bc35  
f6053b093374191c8f8fb2ab2cd474be0d9b843c13074f7956bf242d1f2ebc41

**mshareD1164**

814ebcc9099c4990cdf83ed7c1b58b1d2bf2f504d3cfe68d1e7ff5cff4f16580  
37977d9b815cff6e0dd3520442e6c4a5e84e818ffaff15dc4c1a4f84e17eeb0  
a6553de8d4fd0aa26aac62cf125406bd44058b2146b9ef984b9713467968b475  
228e9ade65bb48307a04b41925d9119de10a59e0a9804a9fed90f1a8e9e1e823  
77b23c2f76b57ab07b3d31d4ef920a2fa8172bd736efb16463d34270702a27fa  
45e5fbff482f532a35acd5549088cb3196175881db633f21c9a5a66bc215ed3e  
c71c63aa51d1109bebb5252eb4e69180cd0393bbaba715bf416998a0d699069d  
72ba7b2ab86a5d0325a6470c64c973e74ac60bb36c6783ea3a0972db3ae5e211  
255cfbd4ba7a83cf0b992b086aec8ded98351ce7483f3a156fbcdd0eb0405603  
3416b411b362bd1114975f0197f8d27a77f72d47fcc47acceae71a8b4bd333

**mwormD1132**

7af8aa870398f4687cd4cadef4bc5aead9c36c54878e027d5d227e61bac7d06d  
4a0968256093530e606d8ced6fbdc77da7b10170aad9a8e91cfb67e6bf92e37b  
d2bd6b842cbeb80f08403bf9fb694b47c7214d8634b3173ea8d87a4c1af8dedf  
8429b23b05cc45f17da5f146039af9ff38b26f090e90337fc5125b9e9f98ebcb  
de22e8b47a5e172303a5d8928eb4a03dbb728eb1026941d13bfe1467f97fe170  
05504a56f9137c1b65490c18a50c9c6550473abfcc89ed08ce61eb0160ad6a11  
c0560cbd24c4862341c646705424ed58cd800c1c78f82cdce01c09d622331bf8  
dead3e2f4b66b60898868128363b68ebacea030954fa8b45ff70cc0abaaaf6df  
4a3fe44f60d7f82370e13c25d77f500ff0a45f21645dc189c0c27cf71fc30828  
b43881e63ef433624f3d29b09f48f4057ef22e2ca6624baa1fdc41e55083a496

**mwormD1164**

2b0c29f925d3d806623bd880fc1b3e6bc54d01014a8187fec010cb441d627c41  
700d92359c78800590469c0ab4f5ea4b9deb76de812820ac059f7937e7e529c6  
80f7f8d43e02da5e346bb930d29befd96028004f6549bc4dcabb10aa0d6d31e6  
1f4ab725bb2137c82f2c84e7979322245fe2ac57725fc3d7e625e0f4bd5d8aa6  
6037572cb4074aebad9e6ef0257b87d64ca1b6403969defce3573fc2e5f63306  
0468dca9810c84d7f01dc48f089d555594ddeaa691b213c993bc8372eca85abc  
272d921f8f75b3ed63fe15d5c15b134a4a8c3e5af7b94b8e634aedba8deb258e



7e648ee08c0e23439cdd5e6734a1efec680c06fe7e1bc07ed158a4ac1f249b0c  
7209d656d9b8b15135ef6e4e56fff3af530c10b6b6859282c4285cad412cd36b  
0557632c74a86fc612d9f428425b19615a525a279d8aad1df025ce7d389fe373

**networkD1132**

c8c789296cc8219d27b32c78e595d3ad6ee1467d2f451f627ce96782a9ff0c5f  
e8112e2293775325e623f347623553514b7ac3111856e594c21870a327a702ab  
ec26875adfa3922e048f1b1406f9b2ded1c4dd77fbad342ef78d9a9f0c09e2cb

**networkD1164**

99b51e28c9e57f3aff2e5753298e676fc6bbec8bef2b23c299a75ccfdcbd9ab3  
85357172baec996f8b27c13ba5e71f76f6897005773580c914e2d0ef0c8529cd  
7b85b56eef3ab1c1bd2cba1a0e215e37c4e087d6d0d40142edee8821c3377fdc

**psfin32**

accb0a583c2a361599460880f2ab31de768bd95cd3a06a4948a52addc555ca2c

**psfin64**

6c0b2d61b8b0f220b8ad59d98920af77d01b7eff84edcf582bcd3403817d9c1b

**pwgrab32**

f8a2bb30bea60dae8f7d15638350c79962669cc2a45912f0d52a4e0f209d0967  
a46839052ed12db3687196dac249a651c7a58793552d191c83f35ce47d19abea  
52f3d9a9e6a8e06e86acf5add134d3e77a80cf954584abd469e040879f80ec9a

**pwgrab64**

7c457d326b3fb97d3a48047d92e9a2a6968968cdbc4aa975539521a12f1952f9  
9e5ed19e851e1decafa71a0cd24a16c4eb7cd2569f4d238726113ace04bcc5fe  
ca676483d55cbf63256fdf5828ada78d3fbb440aec391c03eef07744a31fbcfd

**rdpscanD1132**

f0638d630e847f421656de482b0503e468f34ea13e913ee89b30acafcc05940e

**rdpscanD1164**

b85284564923d39aaa0e64ccf1627e21a76188dbcefbal275bbe4bd3deeb9430

**shareD1132**

0c3042cf12dc545125f58a057570e0519fb03ee02464c61f7502ca16a759fd89  
643f4afcf9a5b1045cb0f9bdef6850546817db09671b05865670a02a9a59126d  
555f281cee6970b19879d8f7856954b84497740ad7f2ec74588ec452104b10d8  
873bdf9ccff49dbb8a03a800195112743eed8001ec54f47941c818a0d2cadf29  
2d334c2ed20419331ded6d388befc5e882fbd6e6af0b85b7b2acba226fde6b89  
22a79157bae384587f714c360613bb24f3970bd48d362c15eb1d4bf9c4a50fe5  
38a203e6573683cf8a495ebab078ab9c0db90b34977e5414e901c4f22e140480  
7e1a2443c20f7d142b6b5ae170b726d28e459fdb9ca033a0944eed9905c3fe8a  
17af9ac2da4bd5a180f39ece942dd454eaca1135cb4b4f6aaa9955564ed61c76  
783e8393343ef26a8dfd865660e15cfcad702979c4e5fc44487645de11ebed28

**shareD1164**

786719da4638be77328ad3fd84763d6180da94801e5e968f0a98d85f9e4b43a6



14929993acedf51302fdd15d774e98e43b859d1f7af865a33d6fd8970149d900  
c94d962c1eb72b27334a8fe09be727b8d5afd964bba76862f7ff8c67bc56534c  
acabcb79f0ba5acc60572953e7d642aea4549026efb807d588b8240513f53917  
a557d251f790cf9030b34d462079668f2475d20b135fc9c444edd41258d00a8c  
2fa917796b7bf2167e3152eb368b8c804f077ce202607c90c9c9bd611fa6dd71  
359881db691dc8ef48cef5f2a8042655c71ee707989a512c178bf097417cf545  
3827028486903803610cfd769a65bcc34400ad5e0914ef9c148c24c9ff89c11b  
358b682614fdff5b53ecf00a89e55ba693b029748a21b2454e54518b921fe96  
049549d9db41999958fa33d12b781d6b104eae40fe77c9dae2f09ea70553a556

**systeminfo32**

76db54ae9f221072fd63c2909ad2a3f2c7cf161ae198b58096545f4df00c024f  
bc071fd542a7fa17791fa2f876bce4e2981d2ba6a4116f533685864469e915dc  
19de921e3e862b5cf87dc5d378749e0752bad54bb6f432474668942bf7dce2e1

**systeminfo64**

55df055d4e9087e7692b439194300e90b286032928fbbb87508354ec6b71fc64  
974dbc8132488c0022b4dd865b1607e8faa7dd6fccebd7112a3ae4492d1112ea

**tabD1132**

a559228b92b0377e281801f502ea65de1e2b3d42cfa24986578fb997d1d7989a  
ce3a6d8cbc4d22abc8154bf913508716c8c5ee5f8bc80e6cd876a59c2b747c60  
55f65f4c56f409ec4161d366d9c858430f781cb8975207256ac208d11699859f  
724a2789ef56847fe5ece5e2339bd51e62bbc1181663e494502442dd86325b75  
deabceac416c95f7eb58eed2d1f5082124201637341249b806fa9cddb2c794a  
b46178d93a007999aa0d3396dce329706bb52999cb76f67dbda4edd32eb52966  
e6056f63663e6cdc2958d6c244511a3808943ca81d3d53fc61cae6514bc6213  
461c169f4d99096360b39839b563599d91f1ed537cc829fd43b3617fb7b41c0a  
0d7aef995678ed51ac9349e3a6b22db024a79b00c9228ddf8abb88e87938cd1c  
157c4de12d4f746dc075545cd1cb6c9dabcbaf6f15502abecb5a86fb5a6d4d28

**tabD1164**

fe828ffc5a6c93d63633ba41284483d3885ec706c63792a18caba9b7a0218074  
db93d4abc97a956ad77286dbb48efae64cd02d2f366ab758ed34de6940c570d2  
bb41b7c0a350eac9bd7c44b7d6077ca94dd1f97c63d774207b22ffa1db544261  
48c6297838049e8f5244ea7cae3dd0a678328cf8016e9c9526dcfdb94b8b49be  
997b8be5c594123ed6f4f491c3b0062ec68c44c441aabd74cde53b267c1c7a5c  
3963649ebfabe8f6277190be4300ecdb68d4b497ac5f81f38231d3e6c862a0a8  
43eef20ca805e1501a149185d27c1fcd160a766b14e6c1bf47ba77acc6b9038b  
70aa53c9ac1ff49aa6e0252746a2acefe90b8d912f57a6fa3f60d1bd194971ae  
1bec303a51433cde51b3de640d9b04bcbb9167f15bef25898b88a35bc42243ae  
cf543eb66a29c3bd1d88e685cf7ed9f543e80367f4efa92d8a1f6789e96a249ce

**tshareD1132**

58f77b63494cce44ee6de4f72f9cec544f0aee0451e0b268cff10c97293b11ba



**tshareD1164**

afbec7bec0cd3b29f33b92ed541f26762ad9bb7837859af6ca13b3ed028c19f1

**twormD1132**

264e279e0da3d5820cdd03c39a23ee562e08932ef7e85e9cb8a3e70915db3ecc

**twormD1164**

9c768d72568917461e5fdf1118da126af8a3cb01192f80b47fb3b8fc27ff2581

**wormD1132**

09ce3637f90db2f328902c8ce6add108351556f5f936cf50621a902e484a9d2e  
0c9bd21d85437ef7f3a024d512c70c631c3fbe74cc806d4b608c8aebf4e99526  
7c9043991b864a72bbf41fa55f594ecd3ee76cded430ebb9cc3a1c83b0330957  
588d77956fc66fec8ef8ca71c9166acb743671738bf29964bb29e1c714480e43  
cd6950df48fc051f45652e85041b92aa9abd4ae8f78fde9d0cbc0a160b09f1ee  
2fdc97ec644d31e650ce21dfc8764c3dabb97297ee43749ab0b8bdf83bbf56dd  
ecdfde2f22e75d6455289133f0802f29c430bb481819d91717bf3a403cd1f34  
42ed334fdd47c7632de55a0f1864c4b1ca909893c3b3f5ddc7dc66ba1e6af341  
59f9312174c5daed6b10d3b09d7bc72c50c40438b96935b3276f057584a1232b  
c326e3e4b2cb82e0d1747c881cecbfde36def0e205d0928972e54cd3a00fab43

**wormD1164**

f9b52b0c8fb832ee54d322c4d18b697360b2ae907e26151639235aaebbbbba29b  
1b9540f1c74e0f7fab2b2d60cafb3ab45e62256c64cbcd1125485bb94c9ea6b3  
547f73eaf24fa661370d4058e85e0bd0cb8d301bb181be35ed9805d9b79a4d81  
e103333d4c1e8cb5c7e1d66c0ec55d5ca9e92871939452400b8406182defed0c  
869fcade7e5ed29819fa3ac21a9a3137cb5a92537e297a8dd44aeaf842e17374  
f635e7e7d04064a66def364a469308cd4e490acfa2b841d425c8ad42a9100e8e  
51acaa6487663bafa831f1823b7da54e5e02837bf405cddf76d73d7aa33ab326  
c67547de94ff738e770e9708a6f364f0a084414db4e5a48ebc18362e007f9211  
58c2bbf942d699e6f92702d3a05e500d9290b1fd49af7fd2acd5996121f8946e  
58092c2f4ffa4996597a9602ec9a1125733efff3422d59604dab9886a3ab4072

# TrickBot Samples

b49f9422344bc2c6ce84bc35912f67df81895bcf0c361acdb0a740260a3a6775  
261ba3edfd9dda2b6c0fb7b00a80c7e2df20934ea3d85258ef244b78aa014ea1  
aaf296dc72f8d2fc650684368d3c18bfd7b7ed00a58befa2c6dd1c9859be1420  
d69612656c52e36f52b84607971a9c868a892ae5ae101d71e6b70d957a9b5022  
49e3552bbe7c73284ad2387a85ddcd13c39efb8d21b16eefb42ac4a4ac05bfbf  
3d99c88900c409cb3d9992462e0d60f8868383bc08fcd10b38db4fd2db38f7d4  
73fa67e2370331c0371d8d1b7dc1b269c5e19c934d0e8ee0de32b393f706c045  
bf96e2c4f38391ec0b3fda44675b190d6ae70c74bd91de2917bba662ae339785



10e271a213eff0f1f95cd1f97ebf62cff19a28195cf1f0eb0341a10bd195f561  
2fae13dcd3782c5360de27d6c523092a1c497fa0a0103070ffd76a0197873277

## Command and Controls servers

45.148.120.13:443  
5.2.78.77:443  
107.172.165.149:443  
45.148.120.14:443  
23.95.231.164:447  
51.89.73.154:447  
45.148.120.31:447  
178.156.202.143:447  
198.23.252.136:447  
64.44.133.39:447  
146.185.253.170:447  
185.252.144.64:447

# 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



### TECHNOLOGY ALLIANCES



# Bitdefender

## UNDER THE SIGN OF THE WOLF

**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

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.