Honeynet Weekly Report
Canadian Institute for Cybersecurity (CIC)

Report (11) Captured from 04-05-2018 to 18-05-2018

1-Introduction

The first honeypot studies released by Clifford Stoll in 1990, and from April 2008 the Canadian Honeynet chapter was founded at the University of New Brunswick, NB, Canada.

In computer terminology, a honeypot is a trap set to detect, deflect or in some manner counteract attempts at unauthorized use of information systems. Generally, honeypots essentially turn the tables for Hackers and Computer Security Experts. They consist of a computer, data or a network site that appears to be part of a network, but is isolated, and seems to contain information or a resource that would be of value to attackers.

There are some benefits of having a honeypot:

- Observe hackers in action and learn about their behavior
- Gather intelligence on attack vectors, malware, and exploits. Use that intel to train your IT staff
- Create profiles of hackers that are trying to gain access to your systems
- Improve your security posture
- Waste hackers' time and resources
- Reduced False Positive
- Cost Effective

Our primary objectives are to gain insight into the security threats, vulnerabilities and behavior of the attackers, investigate tactics and practices of the hacker community and share learned lessons with the IT community, appropriate forums in academia and law enforcement in Canada. So, CIC decided to use cutting edge technology to collect a dataset for Honeynet which includes honeypots on the inside and outside of our network.

These reports are generated based on the weekly traffic. For more information and requesting the weekly captured data, please contact us at a.habibi.l@unb.ca.

2- Technical Setup

In the CIC-Honeynet project, we have defined a separated network with these services:

- Email Server (SMTP-IMAP) (Mailoney)
- FTP Server (Dianaee)
- SFTP (Cowrie)
- File Server (Dianaee)
- Web Server (Apache: WordPress-MySql)
- SSH (Kippo, Cowrie)
- Http (Dianaee)
- RDP (Rdpy)
- VNC (Vnclowpot)

Inside the network there are 'like' real users. Each user has real behaviors and surfs the Internet based on the above protocols. The web server is accessible to the public and anyone can see the website. Inside the network, we put **shorewall** firewall at the edge of the network and NAT different services for public users. In the firewall, some ports such as 20, 21, 22, 53, 80, 143, 443 are opened intentionally to capture and absorb attackers' behaviors. Also, there are some weak policies for PCs such as setting common passwords. The real generated data on PCs is mirrored through TAPs for capturing and monitoring by TCPDump and Security Onion.

Furthermore, we add WordPress 4.9.4 and MySQL as database to publish some content on the website. The content of the website is news; and we have formed a kind of honeypot inside of the contact form. So, when the bots want to produce spams, we can grab these spams through "Contact Form 7 Honeypot" (Figure 1).

Figure1: Contact Form 7 Honeypot

CIC-Honeynet uses T-POT tool outside the firewall which is equipped with several tools. T-Pot is based on well-established honeypot daemons which includes IDS and other tools for attack submission.

The idea behind T-Pot is to create a system, which defines the entire TCP network range as well as some important UDP services as a honeypot. It forwards all incoming attack traffic to the best suited honeypot daemons to respond and process it. T-Pot includes docker versions of the following honeypots:

- Conpot,
- Cowrie,
- Dionaea,
- Elasticpot,
- Emobility,
- Glastopf,
- Honeytrap,
- Mailoney,
- Rdpy and
- Vnclowpot

Figure 2 demonstrates the network structure of the CIC - Honeynet and installed security tools. There are two TAPs for capturing, network activities. Outside the firewall, there is T-POT which captures the users' activities through external-TAP. Behind the **shorewall** firewall in the internal network Security

Onion has been used to analyze the captured data through internal-TAP. It is a Linux distro for intrusion detection, network security monitoring, and log management. It's based on Ubuntu and contains Snort, Suricata, Bro, OSSEC, Sguil, Squert, ELSA, Xplico, NetworkMiner, and other security tools.

In the internal network three PCs are running the CIC-Benign behavior generator (an in house developed agent), includes internet surfing, FTP uploading and downloading, and Emailing activities. Also, four servers include Webserver with WordPress, and MySQL, Email Server (Postfix), File Server (Openmediavault) and SSH Server have been installed for different common services. We will change our firewall structure to test different brands every month.

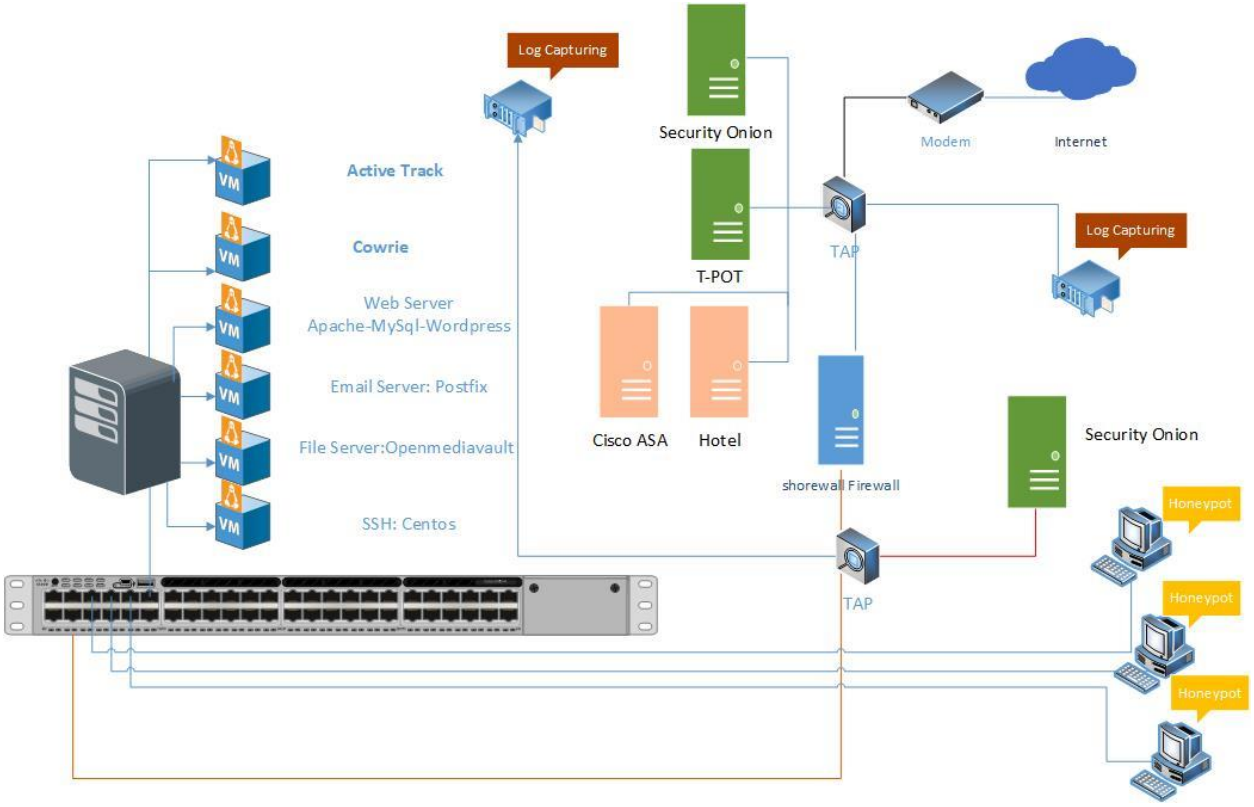

Figure2: Network Diagram

All traffic captured through the internal-TAP and external-TAP and analysis by **CICFlowMeter** which extracts more than 80 traffic features. The source code of CICFlowMeter is available on GitHub.

We used **Cowrie tools** to mimic the SSH command inside the firewall and captures the user commands. Some easy password such as 1234, 123… are entered in cowrie database to make it vulnerable to attackers.

Also, we use two new tools as it is demonstrated in figure 2. Cisco ASA and Hontel are used for specific attacks. Cisco ASA is specifically simulating Cisco ASA, which is capable of detecting CVE-2018-0101, a DoS and remote code execution vulnerability. Hontel is a Honeypot for Telnet service.

We put ActiveTrack to monitor user's activity in the internal network in the hopes of grabing some screenshots from real attackers and the tools they are using in the system.

3- T-POT Report (External-TAP)
3.1 login attempts

We analyzed the IP addresses that made login attempts using the T-POT. The top ten countries that we recieved login attempts from are listed in Table 1.

Table 1: IP breakdown by country

Country	Number of Attack
United States	187288
Mexico	141749
China	41496
Russia	32843
Netherlands	29122
Brazil	18410
Canada	11321
Japan	7725
Germany	7313
Republic of Korea	5494

In Table2, top 10 of source IP address and the number of attacks are showcased.

Table 2: Top 10 Source IP

Source IP	Number of Attack
35.231.248.54	103368
46.21.154.66	29228
23.247.87.22	20838
31.204.150.58	18810
136.159.181.64	9390
222.173.83.218	8744
185.222.209.151	5714
5.62.63.181	5354
5.62.63.223	5217

In figure3, top 5 of countries are demonstrated by related ports. For example, the attacks from the United States have been 30.42% through port 5900, 21.05% through port 5038, 21 % through port 2222, 19.99% through port 7000 and 7.54% through port 5060.

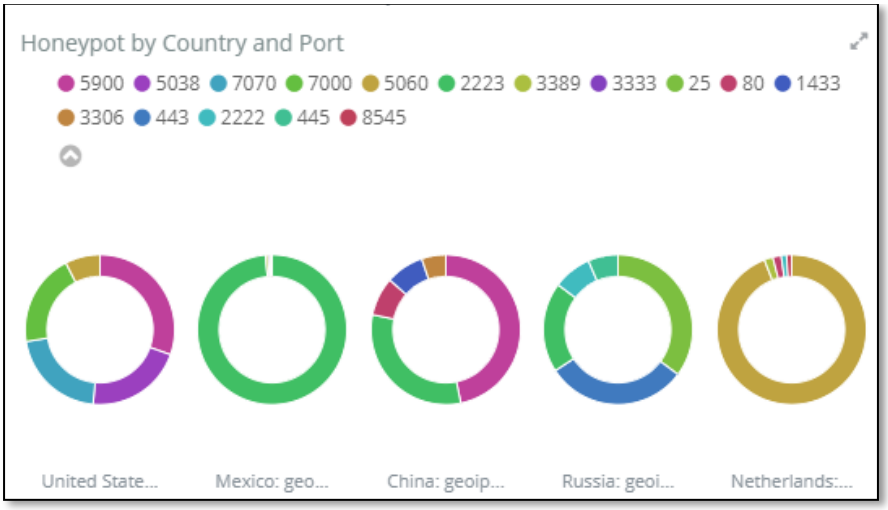

Figure 3: Honeypot by country and port

3.1 Webserver and VNC attacks with related CVEs

During this week, we had CVE-2017-0143 which the number of attacks for each CVE is demonstrated in Table3.

Table 3: Top 10 Source IP

CVE-ID	Numbers
CVE-2017-0143	41

The location of attackers based on the IPs presented in Figure 4.

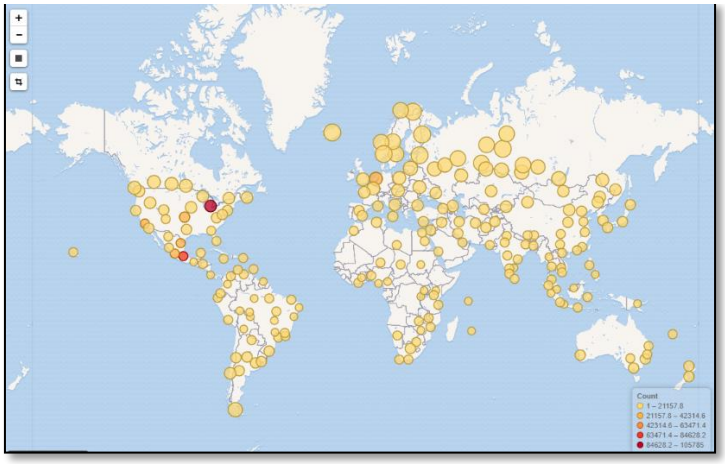

Figure 4: The approximate locations of the IP addresses

Based on T-POT, 51.65% of attacks are from known attackers, while only 47.18% are from addresses with a bad reputation (figure5).

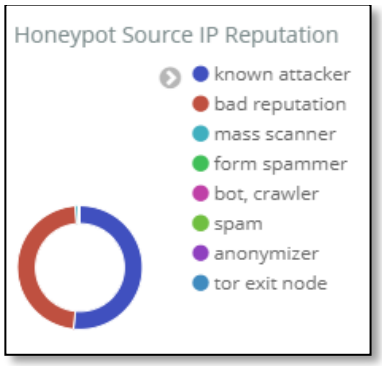

Figure 5: External Honeypot source IP Reputation

In Figure 6, some attacks on NGINX webserver have been presented.

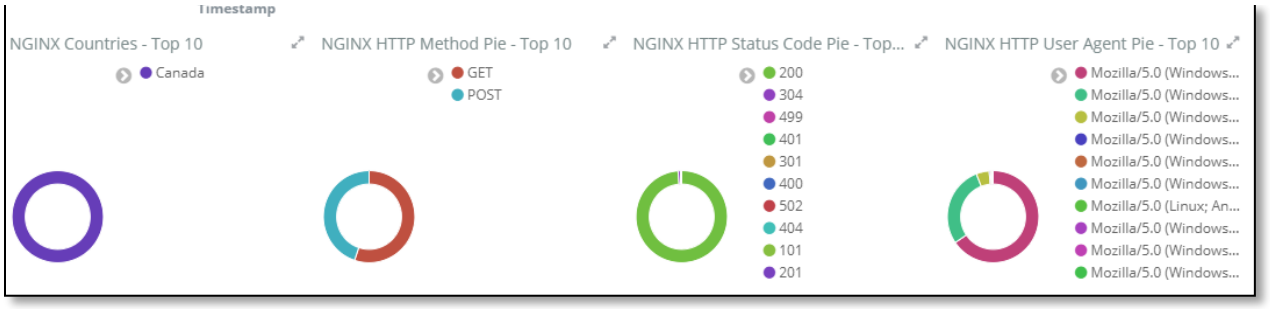

Figure 6: attacks on NGINX

The VNC attacks listed in T-POT have been shown in Table 4 which around 29741 of them are from Swiftway Sp. z o.o.

Table 4: Top 10 Source IP of VNC attack

Username	Number of occurrences
46.21.154.66	29741
23.247.87.22	20834
222.186.138.19	2425
221.229.204.12	2021
222.186.138.7	1954
123.249.79.177	1457
176.31.90.139	217

3.3 TOP Username and password for brute force attack

For brute force attacks, attackers most frequently used the usernames and passwords which are listed in table 5 and 6:

Table 5: common username used by attackers

Username	Number of occurrences
root	45035
admin	25948
shell	11582
enable	9409
guest	5051
default	4401
user	3169
support	2684
telecomadmin	2452
telnetadmin	2327

Table 6: common password used by attackers

password	Number of occurrences
system	11636
sh	8603
admin	4778
12345	4708
123456	3694
7ujMko0admin	3301
5up	3256
support	3222
vizxv	2930
xc3511	2749

3.4 TOP Commands

Table 7 and 8, show the most common commands used by attackers in the Cowrie and Mailoney external honeypots. (All commands are available in capturing data)

Table 7: common command used by attackers grabbed by Cowrie

	command	Number of occurrences
1	mkdir /tmp/.xs/	970
2	/tmp/.xs/daemon.armv4l.mod	194
3	/tmp/.xs/daemon.i686.mod	194
4	/tmp/.xs/daemon.mips.mod	194
5	/tmp/.xs/daemon.mipsel.mod	194
6	/tmp/.xs/test.mod	194
7	chmod 777 /tmp/.xs/daemon.armv4l.mod	194
8	chmod 777 /tmp/.xs/daemon.i686.mod	194

Table 8: common command used by attackers grabbed by Mailoney

	command	Number of occurrences
1	QUIT	1157
2	AUTH LOGIN	1148
3	HELO mailserver	1135
4	HELO *.*	28
5	STARTTLS	7
6	Accept: */*	3
7	EHLO masscan	3
8	Host: 205.174.165.85:25	3
9	Accept-Encoding: gzip	2
10	Data	2

3.5 Cisco ASA

A low interaction honeypot for the Cisco ASA component capable of detecting CVE-2018-0101, a DoS and remote code execution vulnerability. The honeypot run with http on port 8443 and IKE on port 5000. It is tested on our network, but we haven't received CVE-2018-0101 this week.

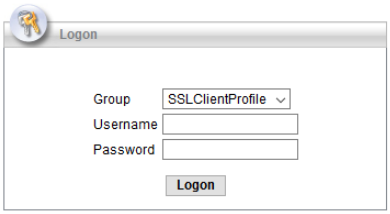

Figure7: Cisco ASA honeypot (First Page)

3.6 Hontel

Hontel is a Honeypot for Telnet service. Basically, it is a Python v2.x application emulating the service inside the chroot environment. Originally it has been designed to be run in the Ubuntu environment, though it could be easily adapted to run in any Linux environment.

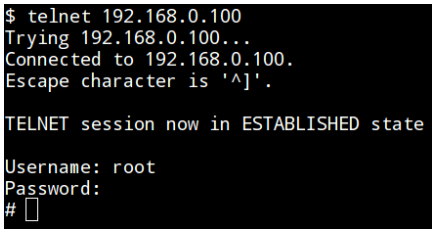

Figure 8: attacks on NGINX

We have received a lot of attacks through Telnet from different IP address.

4. Internal Honeypot (Internal-TAP)

As we talked in section 2, inside of our network, **Security Onion** is capturing the number of attacks, which is demonstrated in Figure 7. Also, we can prove it in Squert and SGUIL which are Security Onion tools to exactly detect attackers (figure 9, 10, 11, 12). The only difference here is that we intentionally opened some ports on the firewall and when attackers pass the firewall, they face the real network. Inside the firewall, as we mentioned in section 2, we have 3 PCs and 4 servers for different services. By analyzing the captured data through Security Onion, we get different results than from section 3.

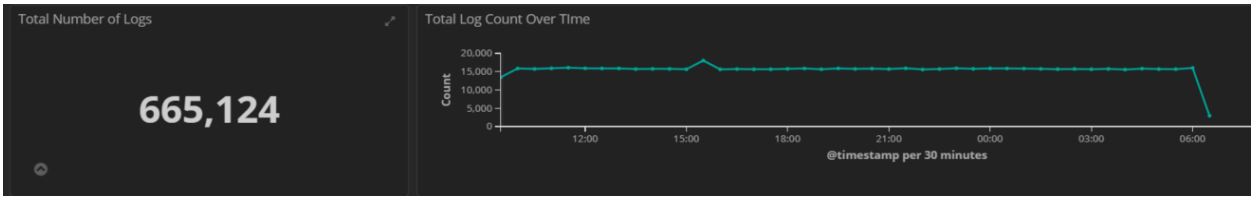

Figure 9: Traffic requested by users

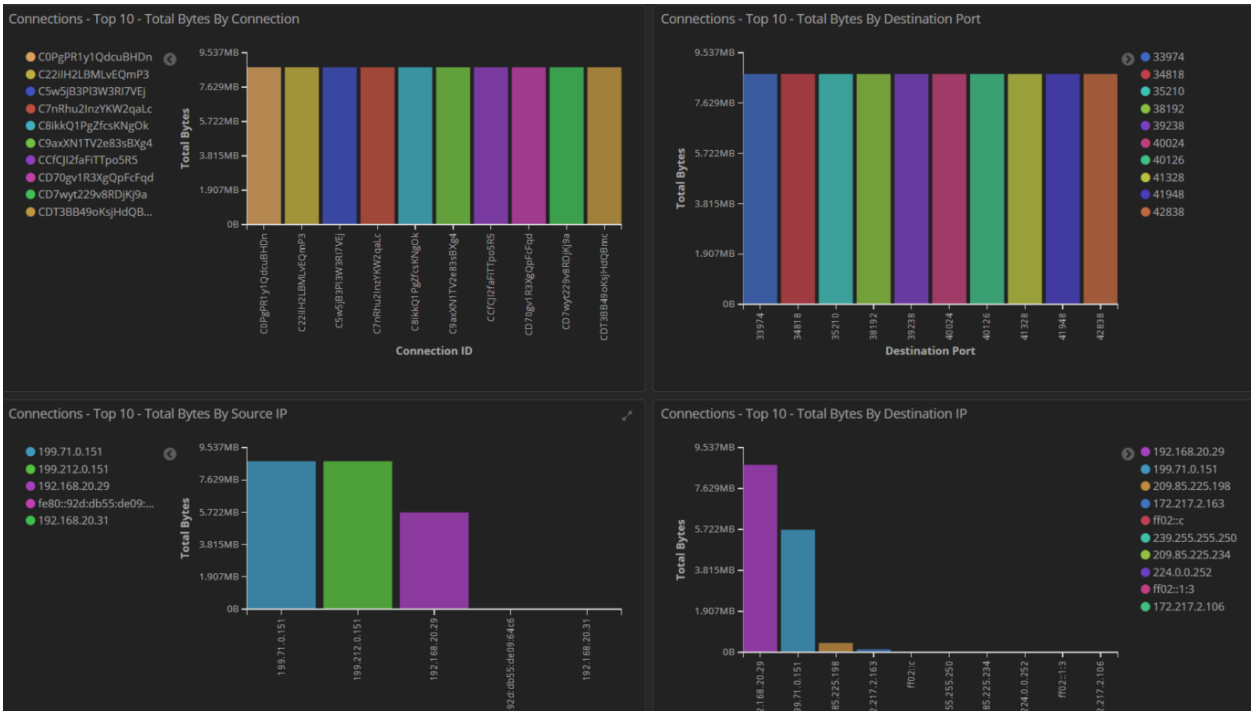

Figure 10: users' traffic inside network

As it is mentioned, we have seen 43.77% is SSH Scan, 1.89% MySQL, 3.77% VNC.

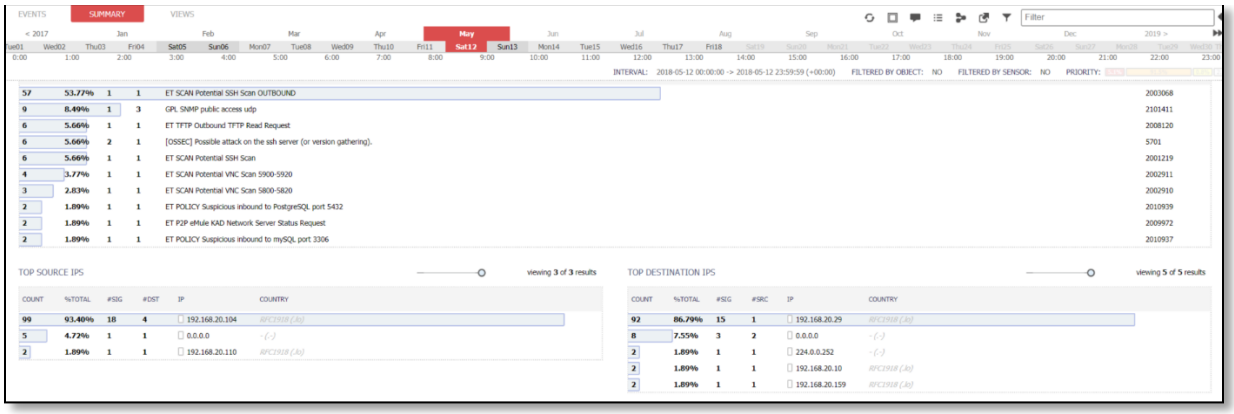

Figure11: Squert summary for attacks

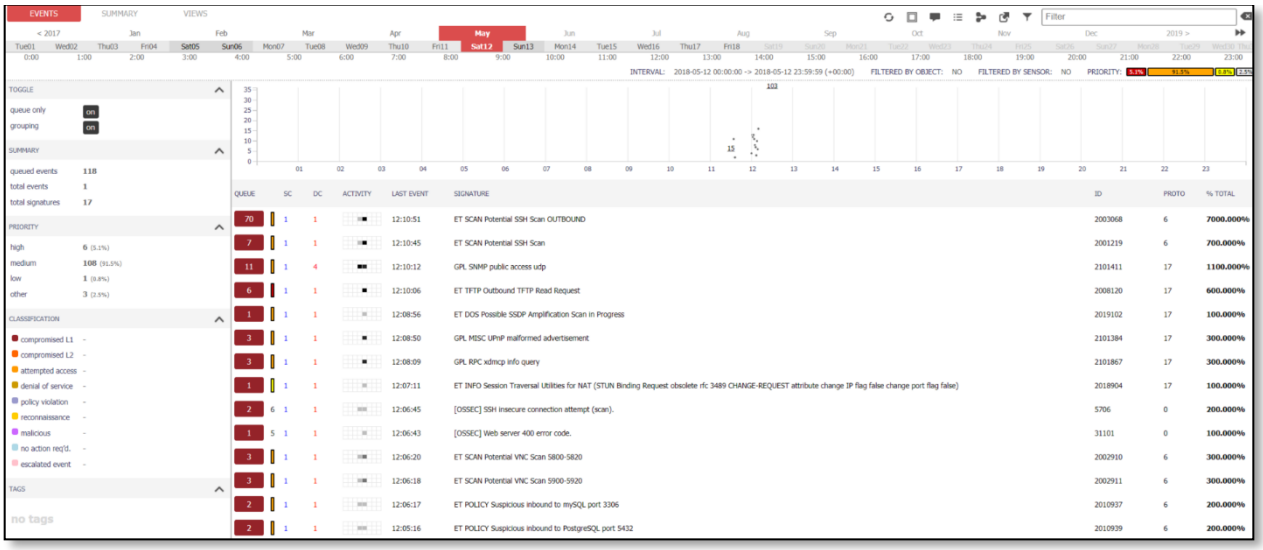

Figure12: Squert shows different attacks on Saturday 12th of May

4.1 Attacker activities' screenshot

Figures 13-20 shows a real attacker screenshot which is installing some software such are Advance Port Scanner, Friends and RDP Recognizer to attack other machines.

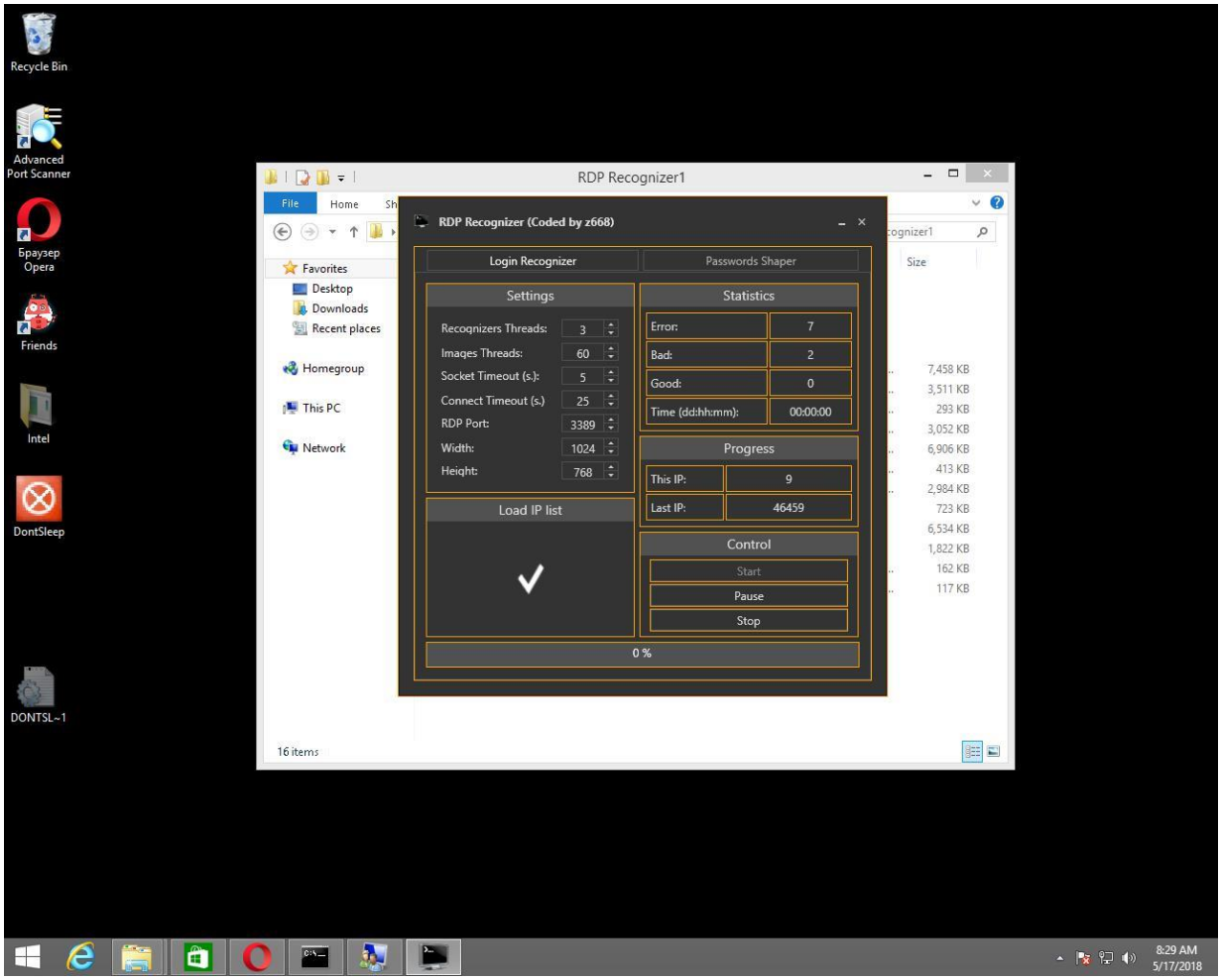

Figure13: screenshot of real attacker

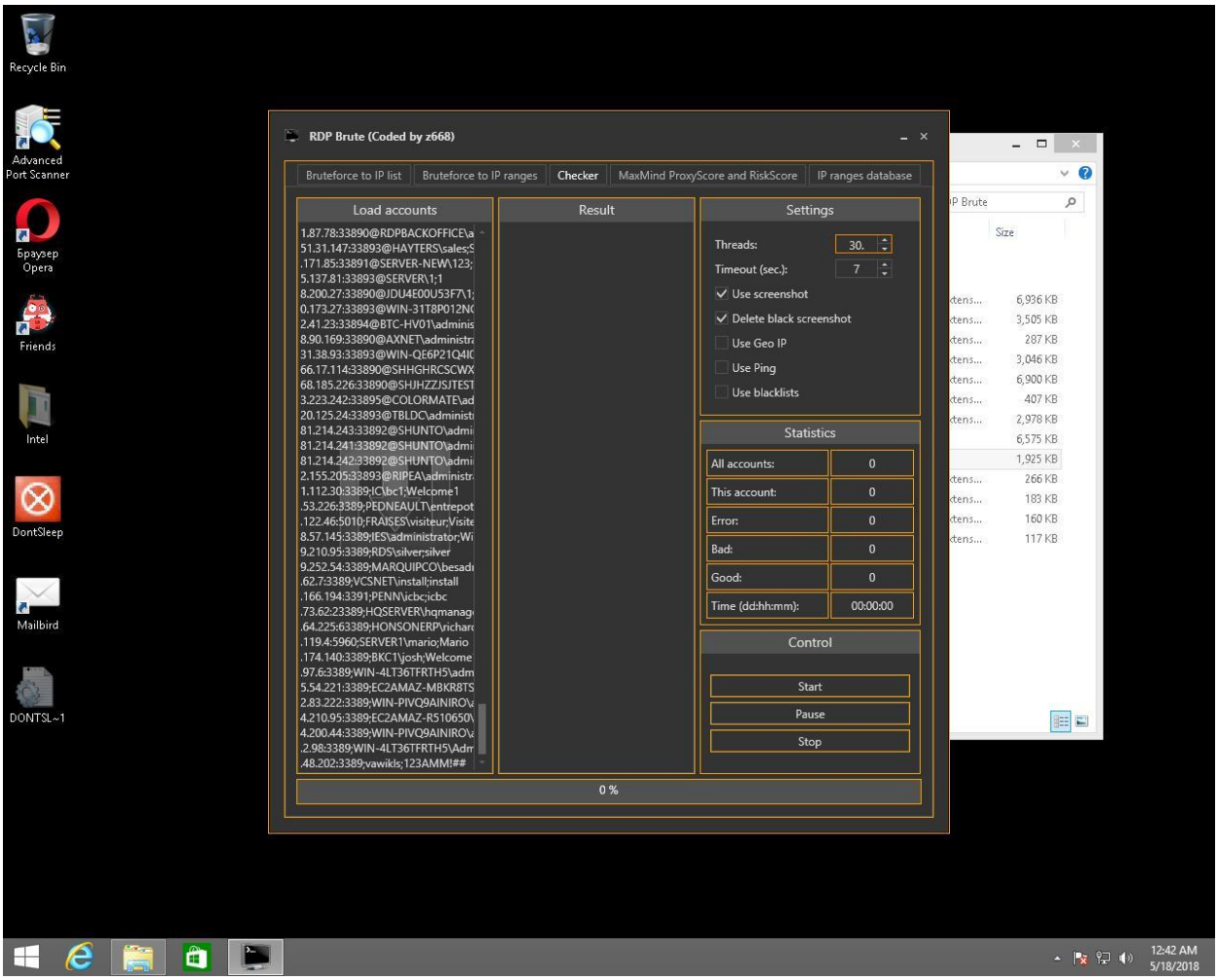

Figure14: the attacker using an RDB brute force tool

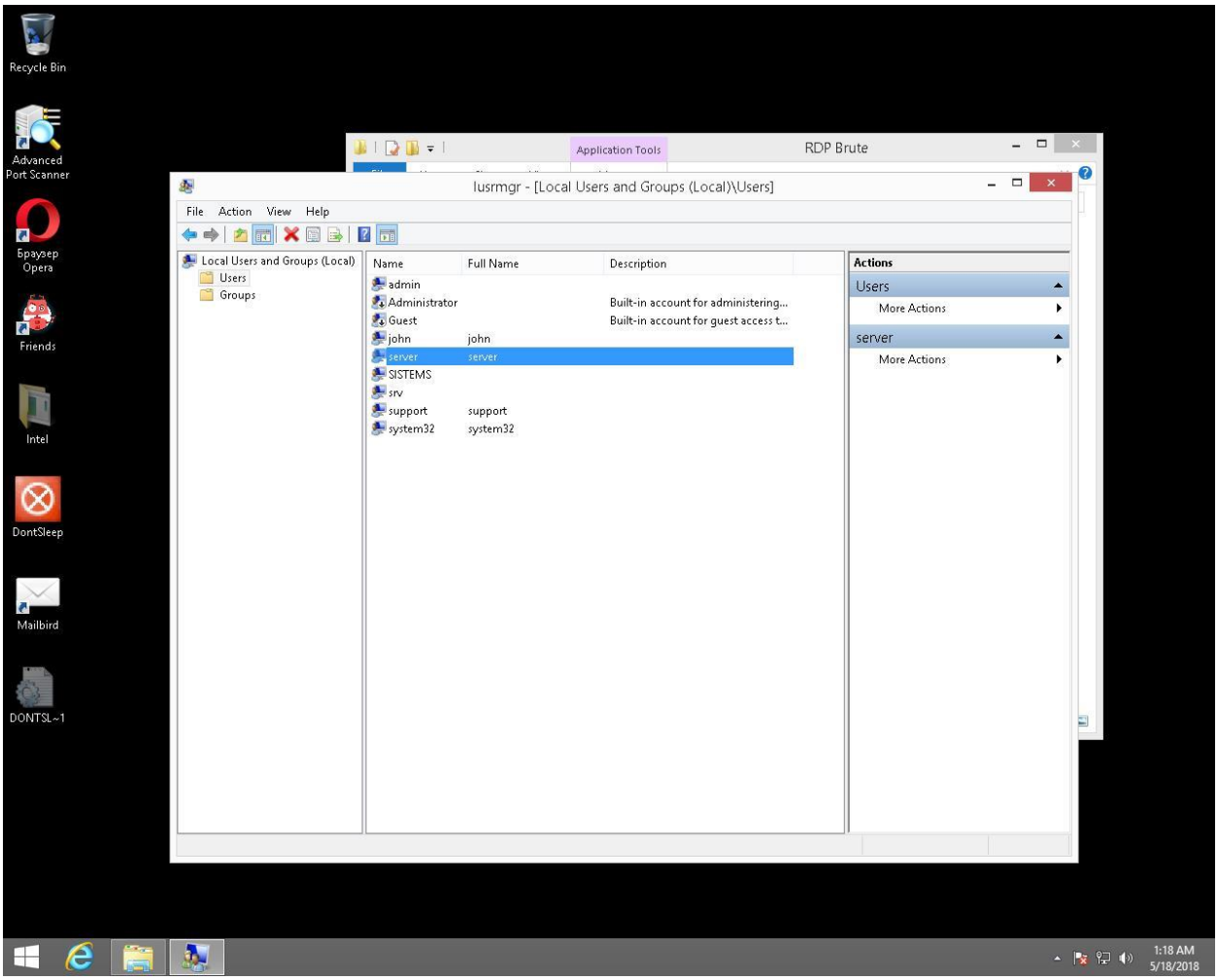

Figure15: the attacker is creating another user

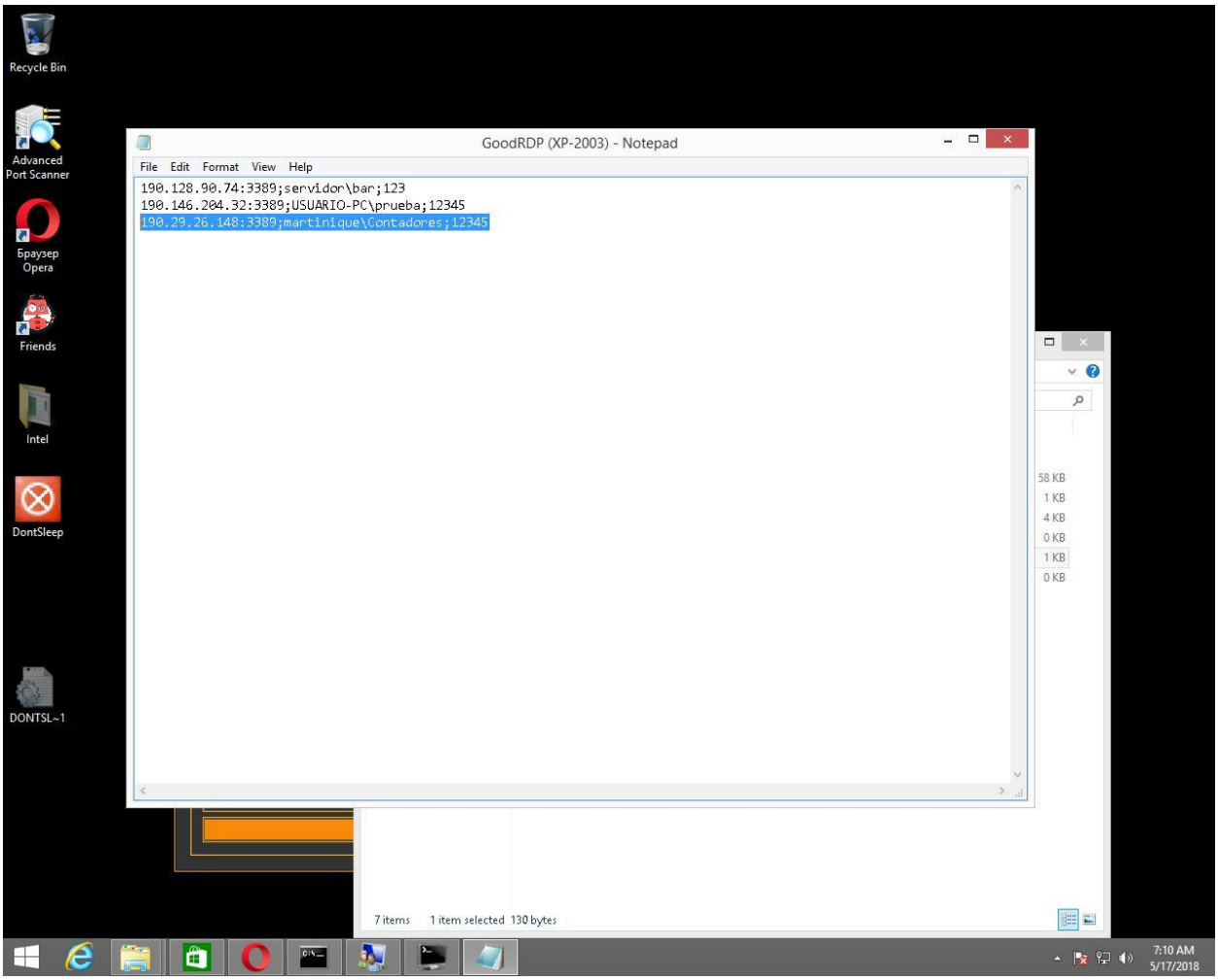

Figure16: the attacker listing goodRDP

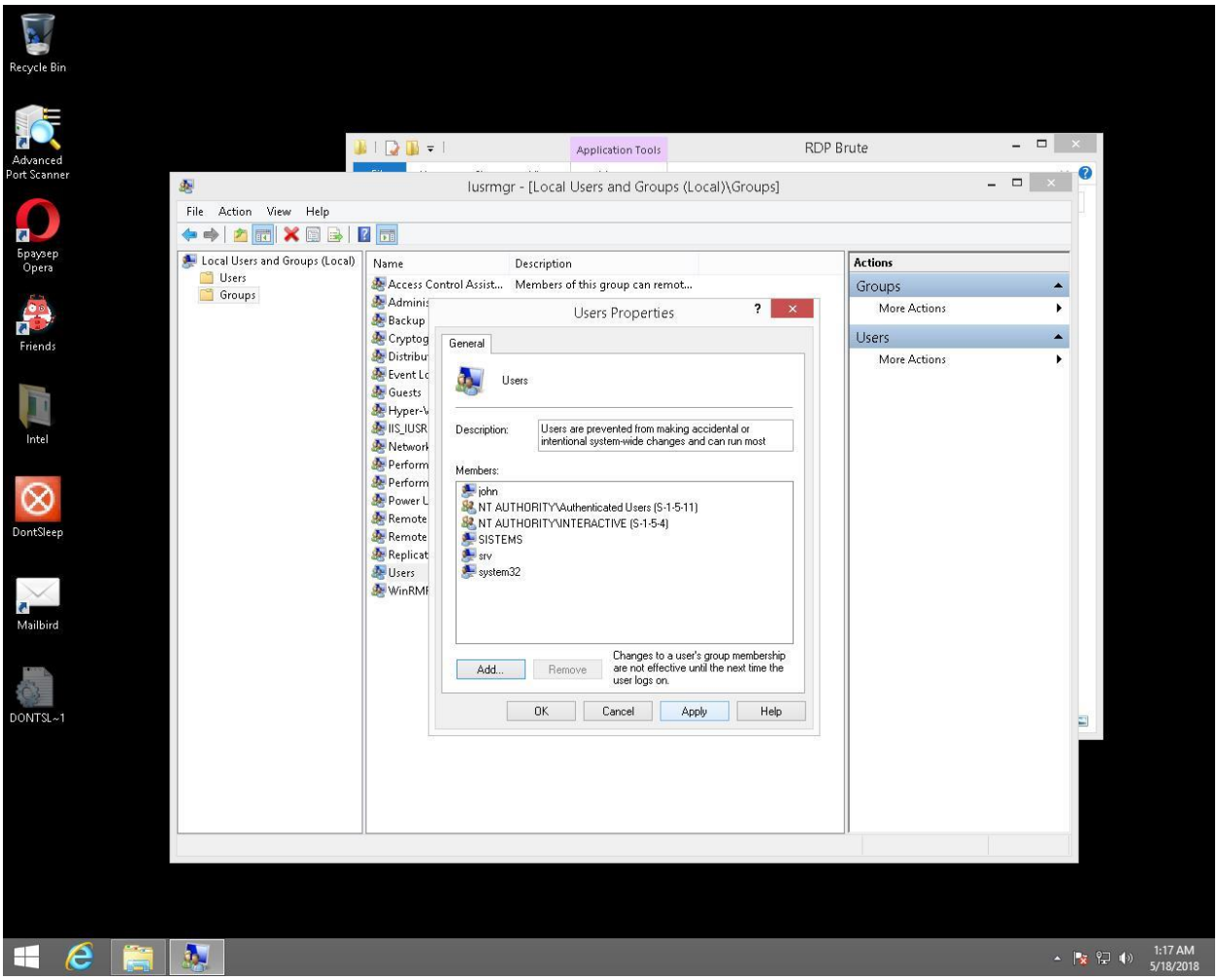

Figure17: the attacker is adding another user

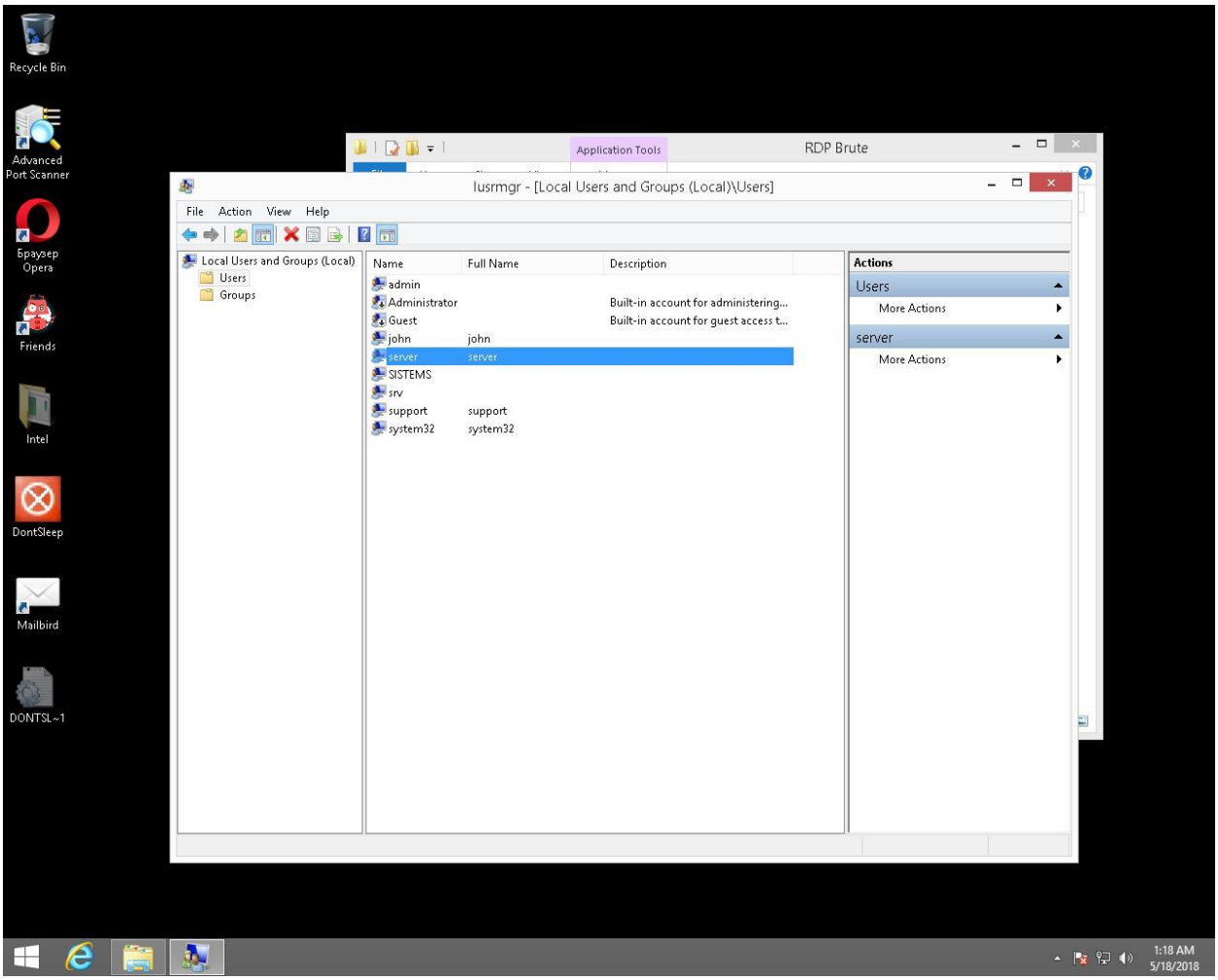

Figure18: the attacker checking users

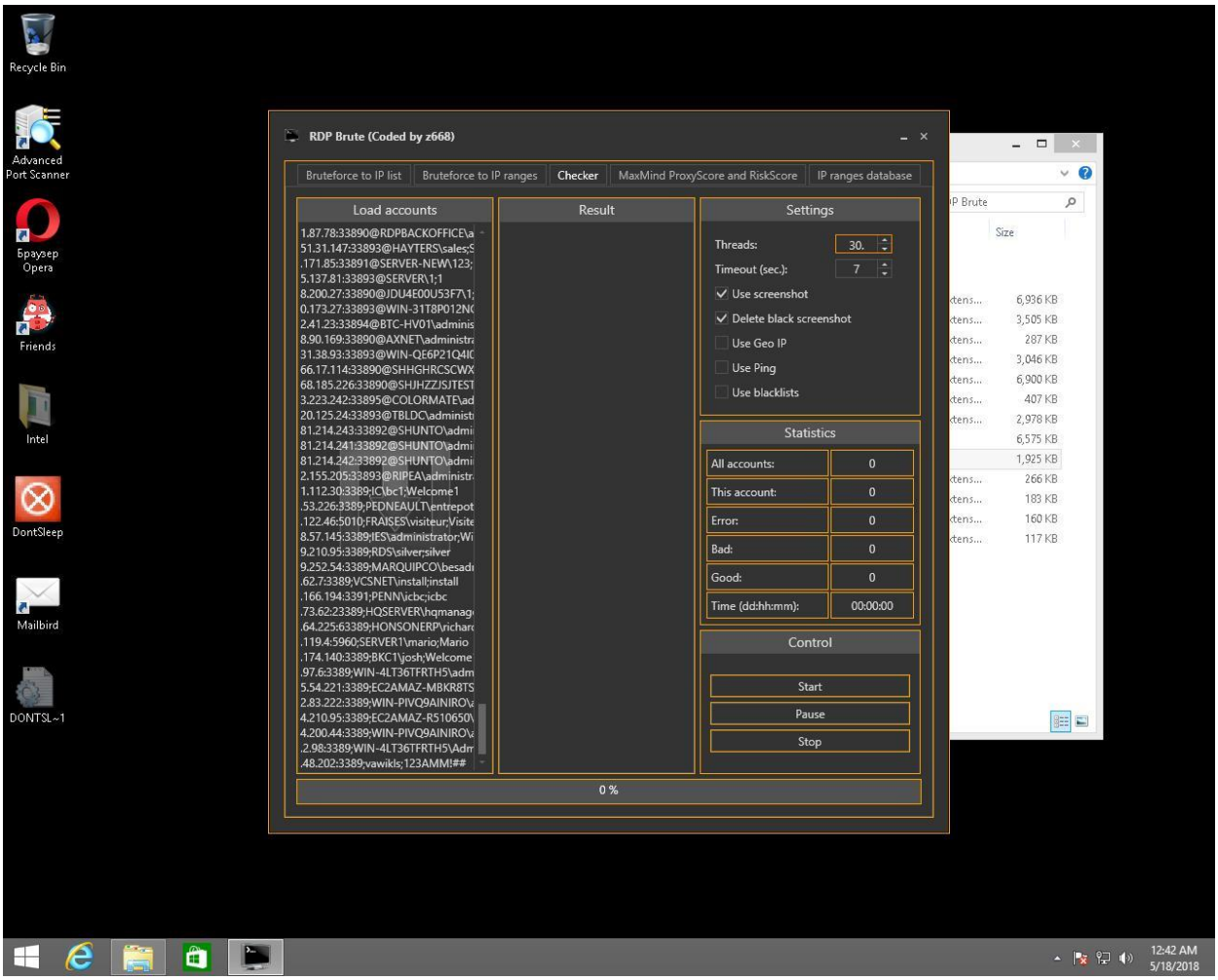

Figure19: the attacker running RDP Brute tool

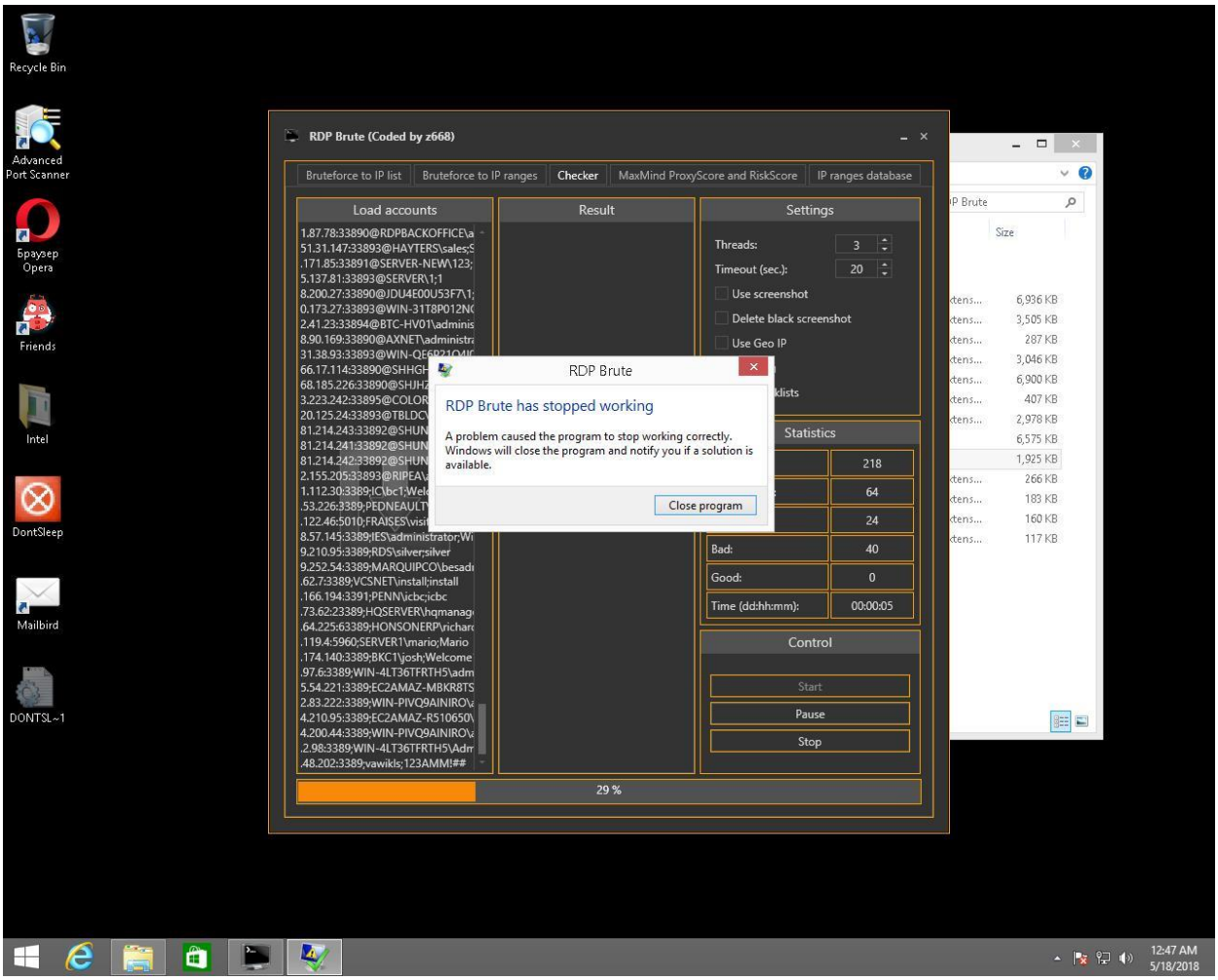

Figure20: the attacker running RDP Brute tool