*Production Systems and Information Engineering*
Volume 10 (3), pp. 31–39.
https://doi.org/10.32968/psaie.2022.3.3

# PROTECTION AGAINST REMOTE DESKTOP ATTACKS

OLIVÉR HORNYÁK
University of Miskolc
Hungary Institute of Information Technology
oliver.hornyak@uni-miskolc.hu

**Abstract.** This paper overviews the most common malicious software types. The motivation of writing this paper was a real word case study that had to be investigated. A computer was suspected to have had an unwanted remote desktop connection attack. This paper presents how to investigate the event log artifacts. For the unfortunate case when such an attack is proved to have happened, the second part of the article describes a method that allows the system administrator to detect brute force attacks through the remote desktop connection. When such an attack was revealed, the attacker's IP address can be blacklisted.

*Keywords*: computer, security

## 1. An overview of attacks, threats, and vulnerabilities

Malicious software, malware, malicious code, or malcode – these describe a piece of software that is designed for something bad, harmful, and unwanted thing:

- steal,
- damage,
- illegitimate,
- disrupt,
- use resources (memory, processing), etc.

The classification of the malware is as follows: viruses, worms, trojans, and bots.

A computer virus inserts a copy of itself into another program and becomes a part of it. Some of the viruses do something annoying, some damage your data, and some may cause denial-of-service attacks. Generally, a virus exists on the computer as a part of an executable file. The infected host program may continue to work as before. Some viruses however destroy their host program.

The viruses can be transferred to other computers by

- network,
- external memory sticks,
- file sharing,
- email attachments,

- system upgrades,
- disk.

A computer worm can also replicate itself to another computer so that it can spread. A worm is a standalone program, it requires no host file to spread. Worms may exploit a vulnerability to enter the system.

Trojans were named after the Greek wooden horse. Usually, it uses a trick to get into your system. Trojans may damage the host computer by stealing, deleting, encrypting your data, pen a backdoor, and giving access to other malicious code. Trojans have no replication capabilities.

Bots are automated processes, the name stems from the word robot. They are intraduct with other network services. Bots may steal passwords, gather information, log keystrokes, and relay spam messages.

## 2. Malware attack

[4] gives an overview on Malware attacks including average monthly malware attacks count by region, the worldwide rate is reported to be 4%. To properly understand the scope this section overviews the literature on malware.

In the early days, Malware was written for simple purposes, thus, it was easier to detect. Nowadays Malware is more sophisticated, it used hard-to-follow techniques to hide itself. [7]. Once inside, they hide, replicate and disable host protections. After getting installed, they call their command and control servers for further instructions, which could be to steal data, infect other machines, and allow reconnaissance [9].

Typical phases of the malware attack can be described as [2]:


**Figure 1.** Malware attack phases

Probe – identifies targets
Penetrate – transfers malicious code to the target
Persist – malware attempts to remain in the system
Propagate – extend to other systems
Paralyze – malware causes damage

According to the predictions in 2021 the cost of cybercrime will cause USD 6,000,000,000,000 (6 trillion USD) damage, and 12 people will be a victim in every second.

It is interesting to see how malware evolved in recent years [11]:

- The first generation (DOS Viruses) of malware mainly replicate with the assistance of human activity.
- Second generation malware self-replicate without help and share the functionality characteristics of the first generation. They propagate through files and media.
- Third Generation utilise the capabilities if the internet in their propagation vectors leading to big impact viruses.
- Fourth Generation are more organisation specific and use multiple vectors to attack mainly anti-virus software or systems due to the commercialisation of malware. Fifth Generation is characterised by the use of malware in cyberwarfare and the now popular malware as a service.

A security intelligence report [3] collected the the most popular propagation tactics are as follows:

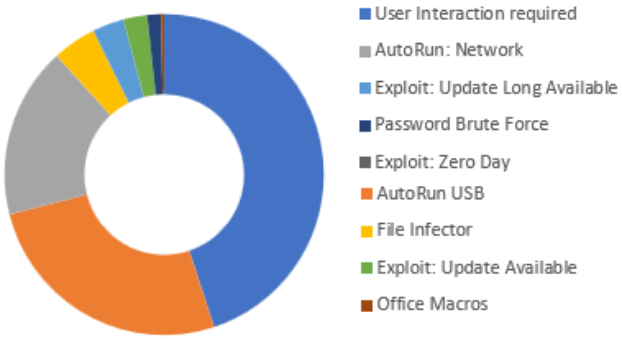


**Figure 2.** Malware propagation tactics

- User Interaction required – 44.8%
- AutoRun USB – 26%
- AutoRun: Network – 17.2%
- File Infector – 4.4%
- Exploit: Update Long Available – 3.2%
- Exploit: Update Available – 2.4%
- Password Brute Force – 1.4%
- Office Macros – 0.3%
- Exploit: Zero Day – 0%

In the industrial world there us Internet of Things (IoT) targeted attacks are also emerging [1].

## 3. Prevention possibilities

The key role of the defense is prevention.

1. Be careful
   a. avoid unknown free software and avoid pirate software
   b. avoid privileged accounts when not necessary
   c. apply secure configurations
   d. keep your machine up-to-date. Apply security updates for your browser, email client, and operating system.
   e. isolate computers that can not be updated
   f. use advanced protection for your browser and emails, use secure email gateway
   g. use anti-malware tools
   h. defense your network in real time
   i. teach users to be suspicious
2. Have access control
   a. use the least privilege required
   b. segment your network
   c. be careful when granting permissions to applications
   d. download applications from reliable places such as app store
   e. have strong user restriction policy on running applications
   f. use whitelists of applications
3. Have backups
   a. it is vital to have automatic backups
   b. you can use online services
   c. ensure your backup containing critical data can not be destroyed
   d. have a backup policy
   e. store your backups on at least two different storage types of which one is offsite
4. Be aware
   a. sensitive data requests
   b. take warnings seriously when clicking on web links
   c. when the computer is slower than usually

Up until a few years ago, cybercriminals focused their efforts on malware attacks because they provided the greatest return on investment. More recently, they've shifted their focus to phishing attacks (~70%) with the goal of harvesting user credentials. [5] Its steps are:

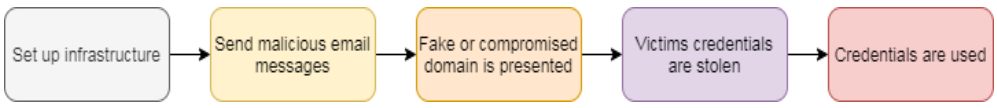


**Figure 3.** Attacks to get user credentials

- Criminals set up their infrastructure: compromitted or fake domains. to gather information on potential targets.
- Send malicious email messages.
- The victim is directed to the fake domain.
- The victim enters credentials into a fake form, or the victim downloads malware that collects credentials on the device.
- Criminals gain access to the victim's network. Criminals use the same credentials on other sites.

## 4. Remote desktop connection log analysis

A comprehensive review is given in [8] on malware detection techniques. These includes:

- signature based malware detection,
- heuristic-based malware detection,
- cloud based malware detection.

There are AI based techniques to detect malware. Another overview is given in [10], which identifies

- host based,
- network based and
- hybrid malware detection systems.

There are many commercial malware detection systems. However if they were not in use at the time the attack happened, then there is nothing much to do. In this section a case study is given how to investigate a potential Remote Desktop Connection arrack.

Once the attackers got access to the target computer, they may log in through the Remote desktop connection (RDC). To find some evidence to the attack you can uses Window's event logging facility.

The main stages of an RDC are:

- establish a network connection,
- authenticate,
- logon,
- disconnect or reconnect session,
- logoff.

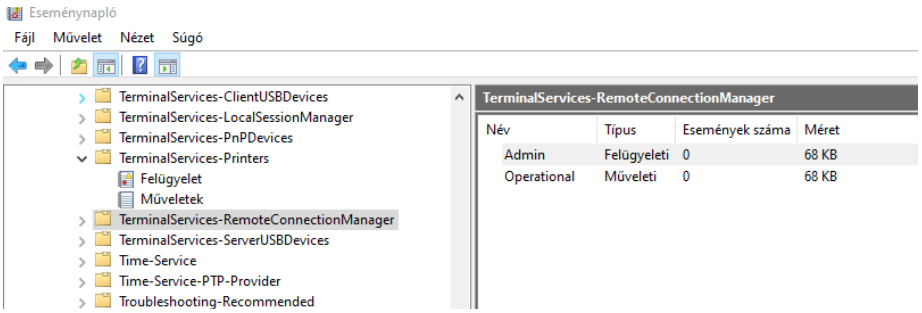


**Figure 4.** Sample figure

Figure 4 depicts the event log viewer at "Applications and Services Logs → Microsoft → Windows → Terminal-Services-RemoteConnectionManager → Operational".

Whenever a network connection happens an event log is created with EventID 1149. This event indicates the connection only.

Authenticate events have the ID of 4624: "An account was successfully logged on" or 4625 in case of failure: "An account failed to log on". In the event description field, there is a logon type that may contain further information:

**Table 1.** Sample table

| Logon Type | Description |
|---|---|
| 2 | Interactive (logon credentials typed manually) |
| 3 | Network connection |
| 4 | Batch – e.g. a task |
| 5 | Service startup |
| 7 | Unlock (i.e. logon when the screen saver is locked by a password) |
| 8 | Logon with clear text credentials |
| 9 | Practically not used |
| 10 | Remote Interactive logon (Terminal Services, Remote Desktop or Remote Assistance) |
| 11 | Cached Interactive Logon |

A sample 4624 event looks like:

```
An account was successfully logged on.

Subject:
    Security ID: SYSTEM
    Account Name: DESKTOP-5MRKQIP$
    Account Domain: LABOR
    Logon ID: 0x3E7

Logon Information:
    Logon Type: 7
    Restricted Admin Mode: -
```

```
    Virtual Account: No
    Elevated Token: No

Impersonation Level: Impersonation

New Logon:
    Security ID: Oliver
    Account Name: oliver.hornyak@uni-miskolc.hu
    Account Domain: LABOR
    Logon ID: 0xFD5113F
    Linked Logon ID: 0xFD5112A
    Network Account Name: -
    Network Account Domain: -
    Logon GUID: {00000000-0000-0000-0000-000000000000}
Process Information:
    Process ID: 0x30c
    Process Name: C:\Windows\System32\lsass.exe

Network Information:
    Workstation Name: DESKTOP-5MRKQIP
    Source Network Address: -
    Source Port: -

Detailed Authentication Information:
    Logon Process: Negotiat
    Authentication Package: Negotiate
    Transited Services: -
    Package Name (NTLM only): -
    Key Length: 0
```

## 5. Prevent brute force remote desktop attacks

Attackers may endeavor a brute force attack. This results in continuous remote desktop connection attempts. The system administrator can block the attacker's IP by a Windows firewall rule [6]. The following PowerShell script gets the failed logon attempts (at least 5 attempts from the same IP) of the last 12 hours and extracts the attacker's IP address.

```
$timeFrame = [DateTime]::Now.AddHours(-12)
$failedRDPAttempts = Get-EventLog -LogName 'Security' -after
$timeFrame -InstanceId 4625 | ?{$_.Message -match 'logon
type:\s+(3)\s'} | Select-Object
@{n='IpAddress';e={$_.ReplacementStrings[-2]} }
$attackerIP = $failedRDPAttempts | group-object -property IpAddress
| where {$_.Count -gt 5} | Select -property Name
```

Now you can list **`$attackerIP`**. To drop all connection attempts the administrator can create a custom Windows firewall event.

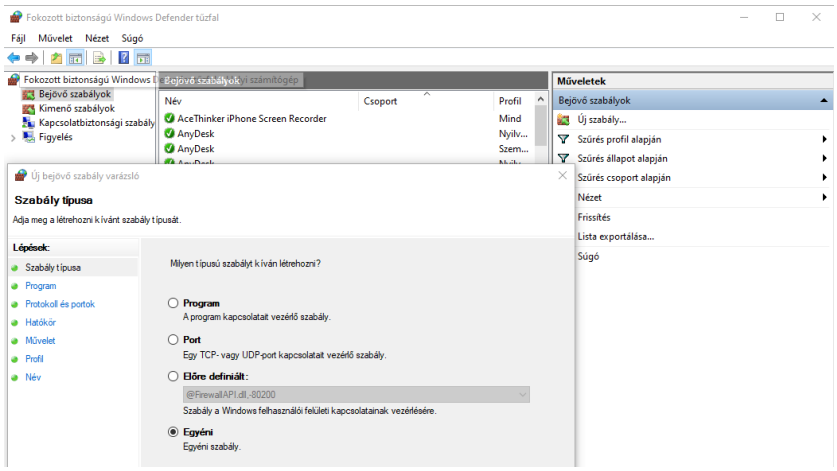


**Figure 5.** Windows firewall rule

## 6. Summary

In this paper, an overview was given on the most common attack types against a Windows computer. An analysis tool was presented that can detect remote desktop connection attempts. Although there are commercial malware detection tools, this do not provide help in finding the traces of such an analysis of the attack. In this article a detailed proposal was given. Following an attack, the system administrator needs to prevent further attacks. After the attacker's IP address(es) are determined the system administrator can block those IP addresses by a firewall rule which is also detailed. Unfortunately, there is no out of the box solution for this specific analysis and prevention. The advantage the proposed method is that it is free, it requires basic system administration knowledge to run.

## References

[1] Ervural, B. C., Ervural, B.: Overview of cyber security in the industry 4.0 era. *Industry 4.0: managing the digital transformation*. Springer, Cham, 2018, pp. 267–284. https://doi.org/10.1007/978-3-319-57870-5_16

[2] Cox, K. J., Gerg, C.: *Managing Security with Snort & IDS Tools: Intrusion Detection with Open Source Tools*. O'Reilly Media, Inc., 2004.

[3] https://www.zdnet.com/article/which-is-the-most-popular-malware-propagation-tactic/.

[4] Microsoft Security Intelligence Report (last accessed 28. 09. 2022). https://clouddamcdnprodep.azureedge.net/gdc/gdc09FrGq/original

[5] Microsoft Digital Defense Report | September 2020.

[6] http://woshub.com/rdp-connection-logs-forensics-windows/#h2_1.

[7] Aslan, Ö. A., Samet, R.: A comprehensive review on malware detection approaches. *IEEE Access*, 8 (2020), pp. 6249–6271, https://doi.org/10.1109/ACCESS.2019.2963724.

[8] Ye, Y. et al.: A survey on malware detection using data mining techniques. *ACM Computing Surveys (CSUR)*, 50, 3 (2017), pp. 1–40. https://doi.org/10.1145/3073559.

[9] Gandotra, E., Bansal, D., Sofat, S.: Malware analysis and classification: A survey. *Journal of Information Security*, 2014, https://doi.org/10.4236/jis.2014.52006.

[10] Saeed, I. A., Selamat, A., Abuagoub, A. M. A.: A survey on malware and malware detection systems. *International Journal of Computer Applications*, 67, 16 (2013).

[11] Ligh, M. W., Adair, S., Hartstein, B., Richard, M.: *Malware analyst's cookbook and DVD: Tools and Techniques for Fighting Malicious Code*. Wiley Pub., Inc, 2010.