



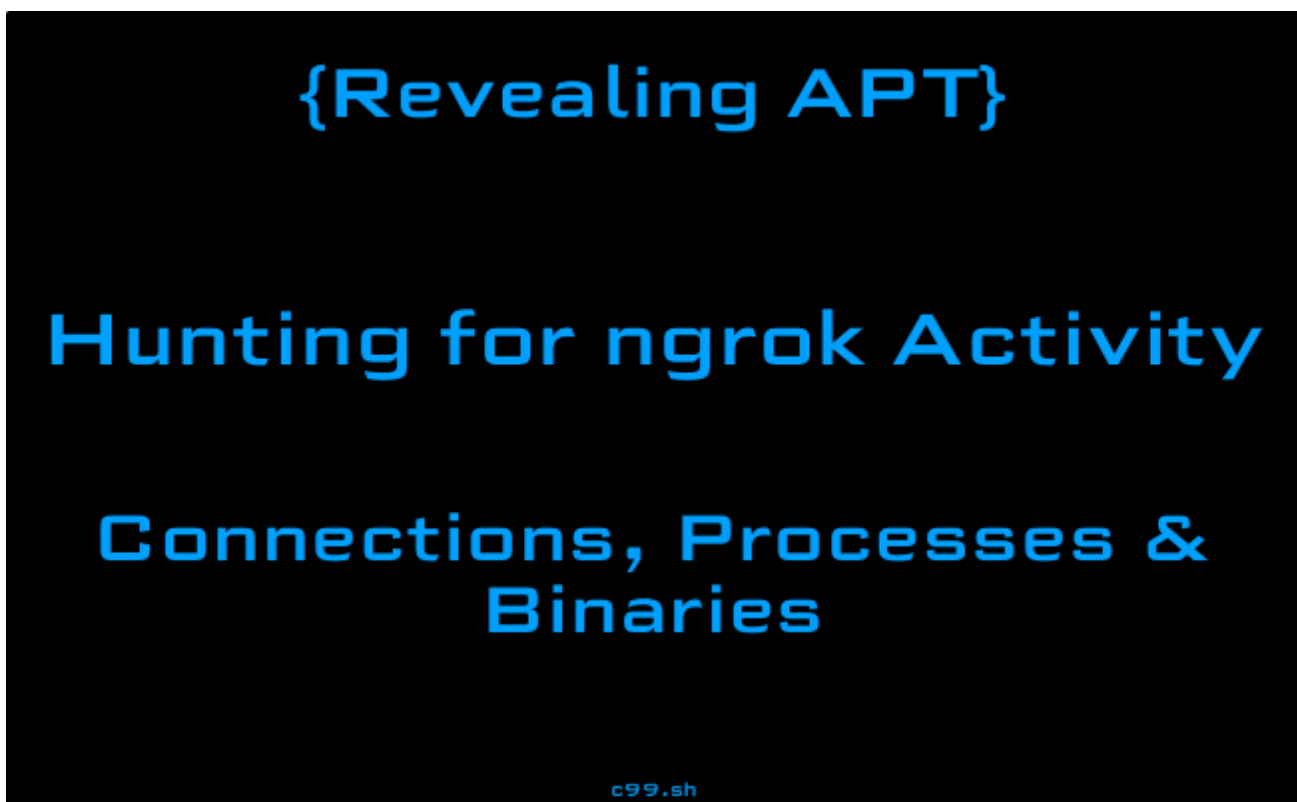
... Security Focus ...

MENU



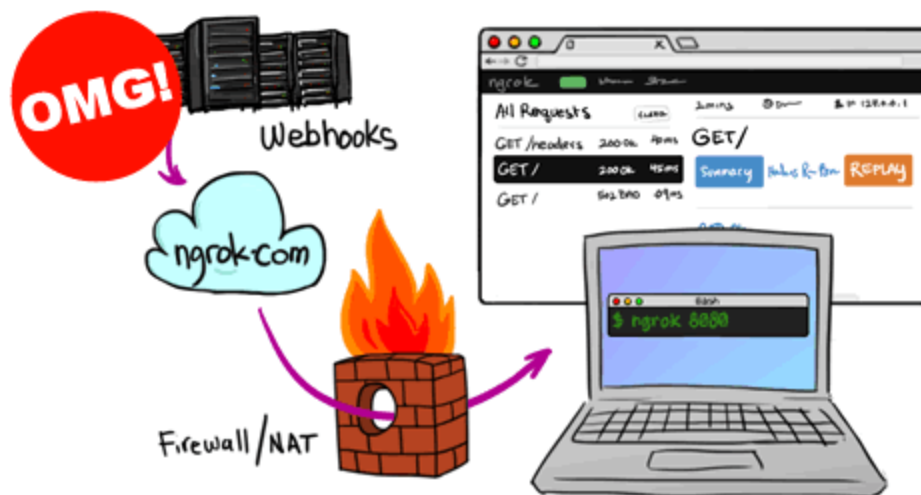
Hunting ngrok Activity

posted in [Threat Hunting](#) on [September 30, 2021](#) by [Moath Maharmeh](#) [SHARE](#)



Ngrok is a genuine software and mainly used by developers to expose local web servers or any other TCP service to the internet. However, ngrok is now widely abused by threat actors and abused in multiple ways including persistence & data exfiltration purposes.

ngrok exposes local services to the internet by wrapping TCP connections under HTTPS, which means that the Workstation that has ngrok agent software installed will be connected with ngrok proxy-servers, on the other side; inside the ngrok website control panel, the user is given a public URL for accessing the exposed services.



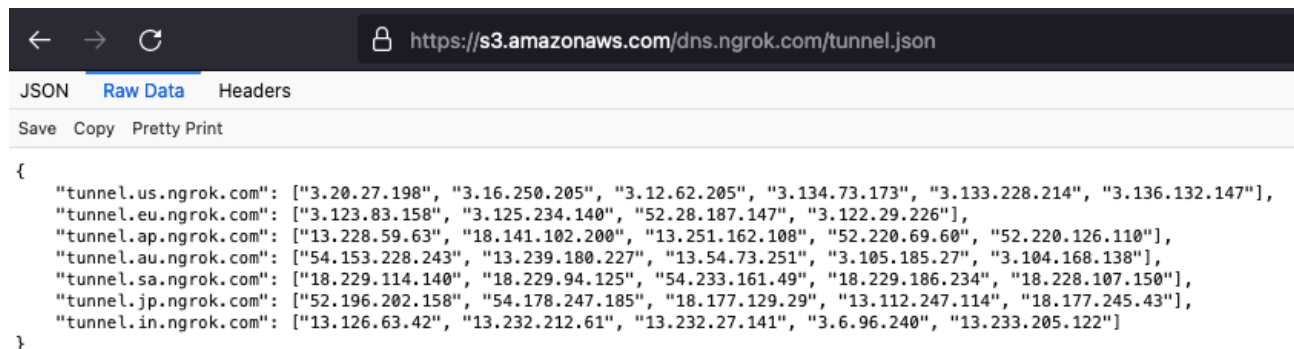
ngrok tunneling

Based on my previous investigations, the ngrok is mostly used for persistence by exposing the RDP service TCP-3389. Usually, with a Windows scheduled task to run the ngrok agent.

Hunting ngrok Network Connections

before the ngrok agent establishes it's tunnel, it will first fetch the ngrok tunneling servers domains & IP addresses list from this URL:

<https://s3.amazonaws.com/dns.ngrok.com/tunnel.json>



Using these artifacts, we can query the firewall or DNS logs for any of the ngrok domain names or IP addresses and find which endpoint is communicating with ngrok servers.

Sample Splunk Search Query:

```
index=dns ("tunnel.us.ngrok.com" OR "tunnel.eu.ngrok.com" OR "tunnel.ap.ngrok.com" OR
"tunnel.au.ngrok.com" OR "tunnel.sa.ngrok.com" OR "tunnel.jp.ngrok.com" OR
"tunnel.in.ngrok.com" OR "/*.ngrok.io")
```

```
index=firewall ("3.20.27.198" OR "3.16.250.205" OR "3.12.62.205" OR "3.134.73.173" OR  
"3.133.228.214" OR "3.136.132.147" OR "3.123.83.158" OR "3.125.234.140" OR "52.28.187.147" OR  
"3.122.29.226" OR "13.228.59.63" OR "18.141.102.200" OR "13.251.162.108" OR "52.220.69.60" OR  
"52.220.126.110" OR "54.153.228.243" OR "13.239.180.227" OR "13.54.73.251" OR "3.105.185.27"  
OR "3.104.168.138" OR "18.229.114.140" OR "18.229.94.125" OR "54.233.161.49" OR  
"18.229.186.234" OR "18.228.107.150" OR "52.196.202.158" OR "54.178.247.185" OR  
"18.177.129.29" OR "13.112.247.114" OR "18.177.245.43" OR "13.126.63.42" OR "13.232.212.61"  
OR "13.232.27.141" OR "3.6.96.240" OR "13.233.205.122")
```

Hunting ngrok Windows Processes

I've seen multiple APTs placing ngrok under "c:\windows\" directory or sub-directories

C:\windows**

Examples command line parameters for launching ngrok:

```
c:\windows\abc.exe tcp -config=help.txt 3389  
c:\windows\abc.exe tcp -config=svc19.dll 3389  
c:\windows\abc.exe tcp -config=HELP 3389
```

Where:

- abc.exe: the ngrok binary
- tcp: protocol type of the service will be exposed
- -config=: the config file contain ngrok config, usually contain user access token
- 3389: the port will be exposed

You read more on the ngrok documentation page: <https://ngrok.com/docs>

To find ngrok running process, you can use process explorer and inspect processes Command Line column, or if you have SIEM in place you can use the following Splunk search query or SIGMA rule:

Sample Splunk Search query

```
index=windows dest_port=4040 dest_ip=127.0.0.1 transport=TCP
```

```
index=windows CommandLine="*.exe tcp -config=*
```

Sigma Rule

Source: https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_ngrok_pua.yml

```
title: Ngrok Usage
id: ee37eb7c-a4e7-4cd5-8fa4-efa27f1c3f31
description: Detects the use of Ngrok, a utility used for port forwarding and tunneling,
often used by threat actors to make local protected services publicly available. Involved
domains are bin.equinox.io for download and *.ngrok.io for connections.
status: experimental
references:
  - https://ngrok.com/docs
  - https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-
ransomware-operations.html
  - https://stackoverflow.com/questions/42442320/ssh-tunnel-to-ngrok-and-initiate-rdp
  - https://www.virustotal.com/gui/file
/58d21840d915aaf4040ceb89522396124c82f325282f805d1085527e1e2ccfa1/detection
  - https://cybleinc.com/2021/02/15/ngrok-platform-abused-by-hackers-to-deliver-a-new-wave-
of-phishing-attacks/.
author: Florian Roth
date: 2021/05/14
modified: 2021/06/07
tags:
  - attack.command_and_control
  - attack.t1572
logsource:
  category: process_creation
  product: windows
detection:
  selection1:
    CommandLine|contains:
      - ' tcp 139'
      - ' tcp 445'
      - ' tcp 3389'
      - ' tcp 5985'
      - ' tcp 5986'
  selection2:
    CommandLine|contains|all:
      - ' start '
      - '--all'
      - '--config'
      - '.yml'
  selection3:
    Image|endswith:
      - 'ngrok.exe'
    CommandLine|contains:
      - ' tcp '
      - ' http '
      - ' authToken '
  condition: 1 of them
falsepositives:
  - Another tool that uses the command line switches of Ngrok
  - ngrok http 3978 (https://docs.microsoft.com/en-us/azure/bot-service/bot-service-debug-
```

```
channel-ngrok?view=azure-bot-service-4.0)
level: high
```

Hunting ngrok binaries on-disk

Ngrok agent executable can be detected on disk using several ways, including hash compassion & imphash and YARA rules. We will use YARA rules as the hashes are regularly changed.

The following YARA rules can find ngrok binaries on Windows systems.

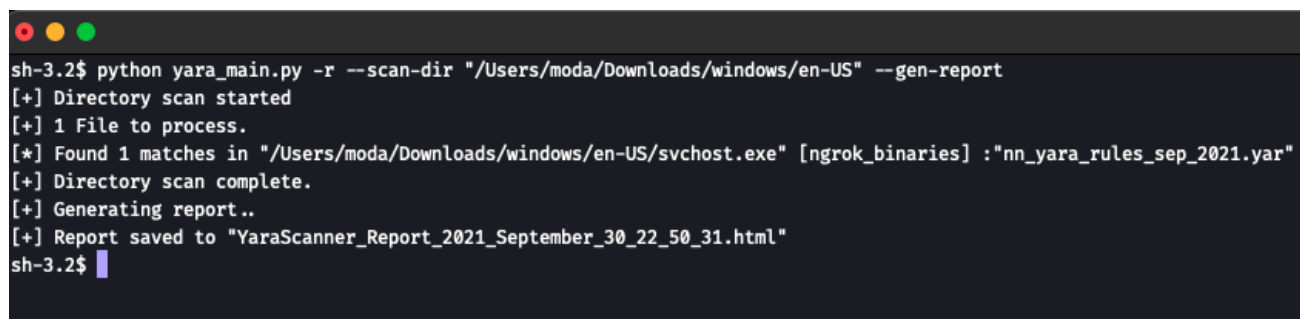
```
import "pe"

rule ngrok_binaries {
  meta:
    author      = "Moath Maharmeh"
    date        = "2021/Sep/28"
    description = "Find NGROK agent binaries"
    filetype    = "exe"
  strings:
    $s1 = "ngrok" fullword
    $s2 = "go.ngrok.com"
    $s3 = "https://s3.amazonaws.com/dns.ngrok.com/tunnel.json"
    $s4 = "ngrokService"
    $s5 = "HTTPRoundTrip_KeyVal"
  condition:
    (
      uint16(0) == 0x5a4d
    ) and
    (3 of ($s*))
}
```

Either **yara-scanner** or **Loki** tool can be used to run a YARA scan

If using yara-scanner, save the code above in a new file with the extension “yar” and place it in the directory “yara-rules-src”

```
python yara_main.py -r --scan-dir "c:\\windows" --gen-report
```



```
sh-3.2$ python yara_main.py -r --scan-dir "/Users/moda/Downloads/windows/en-US" --gen-report
[+] Directory scan started
[+] 1 File to process.
[*] Found 1 matches in "/Users/moda/Downloads/windows/en-US/svchost.exe" [ngrok_binaries] : "nn_yara_rules_sep_2021.yar"
[+] Directory scan complete.
[+] Generating report..
[+] Report saved to "YaraScanner_Report_2021_September_30_22_50_31.html"
sh-3.2$
```

yara-scan tool using the rule “ngrok_binaries”

YaraScanner - Scan Report

2021-09-30 22:50:31

	File Path	Rules Matched	Yara Rules
1	/Users/moda/Downloads/windows/en-US/svchost.exe	[ngrok_binaries]	nn_yara_rules_sep_2021.yar

Generated by [Yara Scanner](#)

yara-scan HTML report



ngrok, persistence, threat-hunting

ABOUT THE AUTHOR



MOATH MAHARMEH

Purple Teamer @Moaaz_0x

PREVIOUS POST

← [SharpSpray | Active Directory Password Spraying Tool](#)

NEXT POST

[Establishing a secure communication channel over HTTP](#) →