Stargate: pivoting through VNC to own internal networks

By Yonathan Klijnsma & Dan Tentler
Stargate: pivoting through VNC to own internal networks

Yonathan Klijnsma
Shodan professional, VNC voyeur, watches attackers and contemplates their motives.

@ydklijnsma

Dan Tentler
Dark overlord of Shodan, VNC voyeur, security guy with a security company.

@Viss
Shit on the internet is getting pretty bad....

Welcome to the internet - we shall be your guides

Stargate: pivoting through VNC to own internal networks
Does it get better?

Stargate: pivoting through VNC to own internal networks
Stargate: pivoting through VNC to own internal networks

No..
No…. no really
Its currently even worse...
It doesn’t seem to get better...
Security Camera “IoT”

Stargate: pivoting through VNC to own internal networks
Internet of Things Conference

Stargate: pivoting through VNC to own internal networks
Internet of Things Conference

Stargate: pivoting through VNC to own internal networks
Everything is being invented again
Everything is being invented again

- They have Wifi
- They have telnet
- Nobody added authentication
- There is actually a CVE for not having authentication
- WHAT.

Stargate: pivoting through VNC to own internal networks
They aren’t getting it, hackers are having fun.

Smart fridges, toasters and microwaves are forcing consumers into reconsidering eating habits due to an exploited flaw that could spread to millions of devices worldwide.

Bitdefender conducted several tests in its labs where it found that smart toasters refuse to toast their owners' food unless they 'feed' them with wholemeal bread.

Furthermore, fridges and freezers across the UK are shutting down as soon as ice cream or frozen goods of a similar consistency are detected.
Besides ancient industrial devices we see new ‘toys’
Besides ancient industrial devices we see new ‘toys’
Besides ancient industrial devices we see new ‘toys’

... is this an exercise bike?! shodan.io/host/128.171.2...
German 'Sonnenbatterie' solar-cell power storage systems
Boats…

Dan Tentler
@Viss

holy shit, I found a yacht. do I win, @ydklijnsma? :D (cc @shodanhq)
We can find criminals(!?) on VNC....

Found open VNC on a server where a criminal was cashing out paypal accounts, talk about getting caught in the act...
Maldives fishes! :D

Dan Tentler
@Vis

soo... my third monitor is kind of a fishtank now.

AUGH. I got back from flying, completely forgot I left this on.

Just about shit my pants

shodan.io/host

Stargate: pivoting through VNC to own internal networks
Cardiac imaging on Shodan....

More open & unauthenticated VNC on medical devices: a cardiac imaging device: shodan.io/host/201.231.2... (cc @shodanhq)
Fingerprints....

Stealing fingerprints from unauthenticated VNC; @shodanhq never ceases to amaze me :)
shodan.io/host/190.255.2...
Swatting 2.0....
Medical devices

And there you have it, a machine controlling an X-Ray device on VNC with patient data open..

shodan.io/host/189.70.24…
Let's look at some statistics for VNC

Decided to scan the globe (with some Shodan help) for the RFB protocol header. It came back with 335K~ results, of those there are 8K~ which use no authentication.
Lets look at some statistics for VNC

These should not exist?!
Let's look at some statistics for VNC.
Stargate: pivoting through VNC to own internal networks

Let's look at some statistics for VNC

Something else was responding with “RFB 000.000”

3.5K somethings named ‘RealVNC repeaters’.
Stargate: pivoting through VNC to own internal networks

uvnc.com/products/uvnc-

Ever seen one of these?

shodan.io/host/109.125.9...

RFB 000.000 sort of triggered me...

Feb 13
"The repeater acts like a proxy, sitting in the middle between the server and viewer. All data for the session is passed through the repeater meaning that the viewer and server can both be behind a NAT firewall, without having to worry about forwarding ports or anything else (providing the repeater is visible to both viewer and server)."

"the viewer and server can both be behind a NAT firewall, without having to worry about forwarding ports or anything else"

-Feb 13-

yeah - someone was telling me yesterday... i dont remember who

someone on twitter was saying that some of the scada shit we find that has vnc open is only supposed to be using vnc 'internally'

and that vnc shouldn't be exposed - but it is

-Feb 13-
Stargate: pivoting through VNC to own internal networks

hm

that can be upnpx

Feb 13

so it seems like there's some massive glaring architectural deficiency

Feb 13
these repeater things you have to know what you want I think

these forward requests for internal machines (aka we can scan internally :)))

Feb 13

hahaha oh man

that would be a fun thing to write

how to pivot through a vnc forwarder to find hosts?

i wonder how badly it could be abused

Feb 13
ah it has settings

Feb 13

well, based on what we know about these systems so far, my guess is it's a sloppy mess :D

Feb 13

to limit the servers you CAN connect to or you CANT connect to

and ports

Feb 13

yeah, as horrible as it is now this repeater thing can only be worse

Feb 13

"How to pivot through recursive VNC, all hail VNC forwarders"

Feb 13

it would be quadruply awesome if the forwarder was broken, and you could pivot shit through it just like any tcp proxy and it turns out you can just proxy attacks/ddos shit through em

Feb 13

hahahaha

could you imagine?
Stargate: pivoting through VNC to own internal networks

the client, the way it connects to the repeater

Feb 13

the repeater just throws a version your way

Feb 13

and you send the repeater the local IP you want a connection with + port

Feb 13

RFB 000.000
192.168.0.1:5900

Feb 13

then it sends 0bytes every so often as a keepalive to the repeater or smt

Feb 13

so you could flood this thing, analyze responses and enumerate backends

Feb 13

time to run this locally

Feb 13

and test to see how connections are forwarded

Feb 13

because, if its not bound to the VNC protocol, we have a good talk :D
it seems to open a socket to the host you specify

Feb 13

after which it will forward whatever that hosts gives back to the client who requested it

as a mere proxy

Feb 13

oh man

Feb 13

hahah oh god

Feb 13
Stargate: pivoting through VNC to own internal networks

Feb 13

turning vnc into open proxies.
so its just a stupid tcp proxy

 Feb 13

hahahah
it is
it is just a plain stupid tcp proxy
labeled with the word VNC
I just made it talk HTTP

Feb 13
**Stargate:** pivoting through VNC to own internal networks

**Feb 13**

> oh god.

Feb 13

> so if you can like, wrap nmap in it..

Feb 13

> you can scan THROUGH vnc proxies

Feb 13

> :D

Feb 13

> ... dude.

Feb 13

> make a python script

Feb 13

**Feb 13**

> hahahah excellent
but yeah dude, i wager if you can do up a python script that can scan through rfb proxies, shit is gonna get REALLY INTERESTING

haha yeah

or, a script you can setup, by which you can specify as a proxy for nmap

I made this to test it:
import socket
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
host = "172.16.238.128"
port = 5901
s.connect((host, port))
print s.recv(12).decode()

Feb 13
Stargate: pivoting through VNC to own internal networks

Feb 13

response:
RFB 000.000

HTTP/1.1 400 Bad Request
Date: Sat, 13 Feb 2016 22:36:46 GMT
Server: Apache/2.4.17 (Win32) OpenSSL/1.0.2d PHP/5.5.30
Vary: accept-language,accept-charset
Accept-Ranges: bytes
Connection: close
Content-Type: text/html; charset=utf-8
Content-Language: en

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="w3.org/1999/xhtml" lang="en" xml:lang="en">
  <head>
    <title>Bad request!</title>
    <link rel="made" href="mailto:postmaster@localhost" />
    <style type="text/css"/>
  </head>
  <body>
    <p>Bad request!</p>
  </body>
</html>
yeah :D

you have to get the padding with 0bytes right

Feb 13

then you send it

Feb 13

HAHA OH GOD

Feb 13

BLOODBATH

Feb 13

it upstream connects

then you can talk anything you want

Feb 13

once it has a connection
I am both terrified and can't stop smiling about what we could find :D

Feb 13

MUHAHAHA

well

at first glance it appears that it'll be all windows boxes, so doing silly shit like asking for simple netbios information would be a great poc

but turning it into a full on proxy that you can use to scan through the box - that would be killer

or an http proxy through which you can 'tunnel' nmap

Feb 13

Stargate: pivoting through VNC to own internal networks
I should make a better version, where you specify a host and it fixes the padding etc

Then make some pcaps, do some testing

But

oh it pads out to 250 chars? or it can be 'whatever host' and then 250 chars so total is greater than 250

What is fun is that you can connect to 127.0.01

No max 250 chars
you're making some kind of netbios request type of thing?
because if we can talk to 127.0.0.1 we can for every proxy host ask it to give internal network information
which means you can do some real damage with targeting

nah, im just reformatting the script to take input and auto calculate padding

ahh ok

yeah my plan sort of as well
imagine there being vulnerabilities in this thing hah
seeing the way its been built and the comments I find in the code I wouldn't be surprised
expecting fixed length buffers etc.
Stargate: pivoting through VNC to own internal networks

```python
import socket
import sys

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

host = sys.argv[1]
port = int(sys.argv[2])
remotehost = str(sys.argv[3])
```

i dont have the details worked out yet, but as a test i did tcpdump on one of my boxes, and had some random remote host try to hit me - and it worked

here's my shit code, still working out the details
Stargate:
pivoting through VNC to own internal networks

try to make it a 4 digit port
because the VNC default ports are 5900 something
so 9090
or smth
Feb 14

yah, or do the math to wrap ports
Feb 14

oh god. :D
Feb 14

if you ask for port 65615 or something you get 80
Feb 14

it wraps after 65535
Feb 14

yeah, "yay" for filtering
Feb 14

hahahah
Feb 14
now let me try low ports (2 digit ports) to confirm for sure

Feb 14

its a string format...

Feb 14

if I put my apache on 90 it will request 5990

Feb 14

I'll try to wrap it around

Feb 14

yeah we can do wrapping :D

Feb 14

depending on the port you want to scan you can just wrap it

Feb 14

anything under 1000 you add 65536

Feb 14

'fixed' code

import socket
import sys
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
we have full port control :D

bahahaha thats glorious

I'll see about trying to hit various protocols
Stargate: pivoting through VNC to own internal networks

[iroot@hax6:~/tools# python vncprox.py 96.227.72.58 5900 google.com 80 /
RFB 808.008

Payload is: GET / HTTP/1.0

HTTP/1.0 200 OK
Date: Sun, 14 Feb 2016 19:33:47 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=ISO-8859-1
P3P: CP="This is not a P3P policy! See https://www.google.com/support/accounts/answer/151657?hl=en for more info."
Server: gws
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Set-Cookie: NID=766V_L_zx3m5sRTSc04hcgxKQghjW40q-4Yc62PY5wA6xhE0EMgZj_6Cv0waY9T0Fv16vJAI5Av89kUfKrVgK-Zn1OaUgeCeM-8veVJ3s7xrc701y4p_NpELFiE4tdMj1011Sxj0fNg; expires=Mon, 15-Aug-2016 19:33:47 GMT; path=/; domain=.google.com; HttpOnly
Accept-Ranges: none
Vary: Accept-Encoding

<!doctype html itemscope="" itemtype="http://schema.org/WebPage" lang="en">
<head><meta content="Search the world's information, including webpages, images, videos and more. Google has many special features to help you find exactly what you're looking for." name="description"><meta content="noop" name="robots"><meta content="text/html; charset=UTF-8" http-equiv="Content-Type"><meta content="" root@hax6:~/tools#
Talked to vendor

- Fixed port wrapping

- Will not enforce VNC because own product will stop working

- Will enforce whitelisting instead of blacklisting (I think)

Product will stay as it is, a plain TCP proxy without inspection.
I see your black/white listing but I don’t like it

curl "http://localhost/testaction.cgi?mode2=mode2&server_port=5901&viewer_port=5500&allow_on=allow_on&allow_con=&refuse_con=&id_con=&web_port=80&hidden=": -H "Authorization: Basic YWRtaW46YWRtaW5hZGl0Mg=="
Do not run this.

We call this ‘vulnerability’ stargate, you never know where you end up :)

It's an open proxy, and can be used to pivot into environments.
Have fun!

Here are our (horrible) Python scripts, use at own caution and always: don’t abuse it (too much):

https://www.github.com/0x3a/stargate/

And if you manage to use this in a pentest please tell us the war-stories :D
Stargate: pivoting through VNC to own internal networks

That's all Folks!