IoT in 2016: a serious overview of IoT today and a technical preview of HoneyVNC

By Yonathan Klijnsma
Yonathan Klijnsma
Senior Threat Intelligence Analyst

Perform threat intelligence analysis at Fox IT keeping track of current events and work on new upcoming threats.

I do my part in:

• Malware analysis (reverse engineering)
• Network Forensics
• Programming

Besides $DAYJOB I like to ‘play around’ with security related things. This varies from malware analysis to random programming projects ending in POC status 99% of the time.

I occasionally write about my findings on my blog.
Large industrial controllers for everyone!

The Internet: a fun place of interconnected devices
by Yonathan Klijnsma
FIRST TC Amsterdam 2015

Cheapest printing/faxing/scanning!

Cheapest: Marriott / Hyatt Hotels - 1$

Most expensive: Intercontinental - 5.43$

Random finds: Getting creepy
It was getting pretty bad back then right?....

We were the firemen taking pictures with the small fires just smiling and laughing.
Did it get better?
No..
No.... no really
It's currently even worse...
It doesn’t seem to get better...
Security Camera “IoT”
Security Camera “IoT”
Internet of Things Conference
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.
They aren’t getting it, hackers are having fun.

IoT security breach forces kitchen devices to reject junk food

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’
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

AUGH. I got back from flying, completely forgot I left this on. Just about shit my pants.
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

Yonathan Klijnsma
@ydklijnsma

And there you have it, a machine controlling an X-Ray device on VNC with patient data open..
shodan.io/host/189.70.24...
Some notes on publishing these screenshots.

Some people complain to Dan, Shodan or Me about some of the screenshots. Let me explain some of the data I published in talks or Twitter:

- The severe items (f.e medical devices or power control) are already fixed

- Some of the data I post on Twitter is in fact more than a year old, because it took a long time to fix

- There is tons more than I actually publish or Tweet, its too problematic to expose or contains way too sensitive data
Some notes on publishing these screenshots.

I usually cooperate with ICS-CERT or direct vendors / organisations for the things I find that are serious.

I used to send out bulk data but it was quite unworkable for most so I filter out most of the data before sending it. I do this in my spare time.
I 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.

The numbers are higher than my last talk, due to better scan results and actually more devices coming online!
Let's look at some statistics for VNC.

These should not exist?!
Let's look at some statistics for VNC.
IoT in 2016: a serious overview of today and a technical preview of HoneyVNC
images.shodan.io - RDP
Total results: 3,680,165

Remote Desktop Protocol
\x03\x00\x00\x0b\x05\xd0\x00\x00\x124\x00

Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00

Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00

Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00

Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00
images.shodan.io - RDP

Carver Technologies - Usage notice

NOTICE TO USERS

THIS IS A PRIVATE COMPUTER SYSTEM. It is for authorized use only.
Any or all uses of this system and all files on this system may
be intercepted, monitored, recorded, copied, audited, inspected,
and disclosed to authorized site and law enforcement personnel,
as well as authorized officials of other agencies, both domestic
and foreign. By using this system, the user consents to such
interception, monitoring, recording, copying, auditing, inspection,
and disclosure at the discretion of authorized site personnel.
Unauthorized or improper use of this system may result in
administrative disciplinary action and civil and criminal penalties.
By continuing to use this system you indicate your awareness of and
consent to these terms and conditions of use. LOG OFF IMMEDIATELY
if you do not agree to the conditions stated in this warning.
IoT in 2016: a serious overview of today and a technical preview of HoneyVNC
HoneyVNC

With all of the scans I do I couldn’t find any proper honeypot that would allow actual interaction. Most of the half-working honeypots support the authentication step but that’s about it, no visual data or anything.

I decided to make one, because I like VNC and was wondering who was also poking these devices besides Dan, Shodan and Me.
HoneyVNC

I implemented a ‘full interaction’ VNC honeypot I’ve named ‘HoneyVNC’. It is still under development but currently features:

- Password authentication on/off (allows you to see brute force attempts)
- Visuals (Actual screen data is being send over to give the impression of a real device on the other end)
- Input can be used to browse around the fake virtual appliance behind the VNC server.
- Sessions are logged for every time a successfully negotiated connection is seen. Everything is logged with a replay-able timestamped file format (mouse and keyboard)
HoneyVNC

There are items I’m still working on to incorporate properly:

- A web application to replay the session logfiles with actual visual representation of what happened in a session.

- Virtual environment design: A honeypot owner can design its own virtual appliance behind the honeypot.
HoneyVNC - Virtual appliances
HoneyVNC

Why not run an actual VNC server:

- Annoying to setup and secure properly, you have to think about all the routes the attacker could go

- HoneyVNC is just a consolidated Python program, there’s no jail to break out of because it doesn’t have one

- Its Python, runs pretty much anywhere which makes HoneyVNC very portable
HoneyVNC - Findings

I ran a basic version (you could login and get a random screen with uninitialised memory) for about 3 months on a couple different environments.

I had some interesting (unexpected) results.
- Targeted scanning
  - Scans that hit my residential uplinks didn’t pass by at data center
  - Known webhosting ranges were not scanned
HoneyVNC - Findings

- Brute forcing
  - When I presented no authentication some would still attempt logins
  - Some were using lists (although I didn’t have proper logging)
HoneyVNC - Findings

- Lots of automated interaction
  - Even though I presented garbage in the screen buffer there was automated keyboard input. Most of the input contained sentences similar to:
    - `del` / `rm` variants
    - `echo “r00ted by <insert some lame nickname>”`
HoneyVNC - Findings

- Some manual interaction:

  - There were some manual interaction moments. Mostly people not understanding the garbage and just randomly clicking and moving (probably thinking to ‘refresh’ the screen to get a proper image), the classic “if I click faster and harder it will respond” pattern

  - When I was (finally) able to present a screenshot I stole from another VNC appliance someone really wanted to see settings.
HoneyVNC - Can I have/run it?!

It is not ready for a public release yet, there’s issues to work out and features to implement still. I want to deliver and as-easy-to-use-as-possible honeypot with good (and meaningful) log results.

I’ve had to implement the RFB protocol by hand, which sucks. I like VNC but I don’t like the protocol… at all…. it. is. a. pain.

As soon as I feel its actually usable for other people I will make it public on Github so other people can play around with it.
HoneyVNC - Development timeline

- **First version (August 2015):** single Python file with a fixed statemachine
- **Second version (October 2015):** Tried making a hacky RFB implementation
- **Third version (current):** found the awesome libvnc and currently making Python bindings. The idea is to have precompiled libvnc binaries and a separate HoneyVNC script with configuration.

Can’t run the current version (completely overhauled)… :( sorry no demo.
RFB logging in Bro!

At my company (Fox-IT) we’ve implemented the RFB protocol in Bro. It features the full protocol and logs the start of sessions and the end (so you can get actual sessions worked out over the network). It currently logs:

- Source / Destination
- Client & server versioning (minor & major)
- Authentication method
- Which auth was used (based on auth list)
- Session sharing flag
- Desktop name
- Width and Height
RFB logging in Bro!

Committed last Wednesday:

- https://github.com/bro/bro/commit/9d0899325a6a4391764cc541f4c41b4353ff79e6
- https://goo.gl/6G5Aun
To come, a Bro policy to dump screenshots from live VNC sessions.
Thanks for your time & attention, let's get back to our fires :(