Deep-dive:
MikroTik exploits - a security analysis

Analysis of exploits and malware utilizing them in recent RouterOS versions

Presenter information

Tomas Kirnak

System & Network Architect
Automation & Monitoring

MikroTik Certified Trainer
MikroTik Certified Consultant

About Unimus

Automation

(Mass Config Push, network-wide conf. search, etc.)

Configuration management

(change notifications, historic diffs, etc.)

Disaster recovery

(configuration backup)

Unimus

Note for posterity

- If you find this presentation online in a .pdf, please watch the video
- Proper explanations to every slide and much more information available

https://www.youtube.com/c/TomasKirnak/videos

Why are we here?

- Number of attacks against ROS increasing dramatically in the last 3 months (many news articles around the web)
- To learn how to defend, we will analyze past ROS attack vectors and exploits
- We will then discuss the current situation and the ongoing exploits currently running wild

Preface

- RouterOS runs on Linux

  (if you have access to the underlaying Linux system, you can do anything you can with a normal Linux machine)

- RouterOS runs on many architectures (MIPS, ARM, TILE, etc.)

  (as long as the payload is compiled for the target architecture, this is not a problem for attackers)

- Shortcuts / Terms often used that might need explaining:

  WikiLeaks, CIA / NSA, Vault7, RCE, C&C

Before we even begin

- MikroTik default configurations were NEVER affected by any of these exploits
- All of these exploits would NOT be possible if proper firewall was present
- If you were affected:
  1) you modified the default firewall
  2) you reset configuration and didn't configure firewall at all
  3) you had firewall, but you were not protecting management services (web, ssh, winbox, api, etc.)

A note about security

- We are not here to point out "MikroTik is bad at security"
- Every single piece of software has bugs and vulnerabilities
- Cisco ASA
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1
- Juniper
  https://kb.juniper.net/InfoCenter/index?page=content&channel=SECURITY_ADVISORIES

What is the point of this presentation?

- We are here to learn how to protect ourselves from bad actors present on the internet
- We are here to see how to make a MikroTik network secure against outside exploitation *

* nothing is ever 100% secure, but that doesn't mean we should not do our best

How did all of this happen?
Vault7

WikiLeaks publishes CIA / NSA attack tools

Starting at the beginning

- March 2017 - CIA / NSA attack tools leaked on WikiLeaks - known as Vault7

- These leaks contained attack utilities for multiple systems (Windows, Linux in general, and routers)

https://wikileaks.org/ciav7p1/

Vault7 and MikroTik

- A part of these leaks was a RouterOS attack module, named Chimay Red

- This module contained 2 exploits:
  - http server exploit that allowed RCE
  - Winbox exploit that allowed arbitrary file read

Part 1:
RouterOS web server vulnerability

RCE on routers just by seeing TCP port 80 open

Chimay Red – exploit 1

- Chimay Red used a vulnerability in RouterOS web server (running Webfig, graphs, etc.)
- This vuln. allowed the attacker direct RCE on the router

- This means the attacker could directly execute commands on the underlaying Linux system
  (and also access any RouterOS functions)

What did Chimay Red exploit?

- Chimay was meant (and could be used) to deliver arbitrary payloads)

- No exact payloads were available in the Vault7 leaks, so it is unknown what the original intent of CIA / NSA was to deliver by this exploit

What was it used for

- The http server vuln. was not widely used (compared to what we will be discussing next)

- There is not much public data on how bad actors used this vuln.

  (since exploitation was not very wide-spread)

How did MikroTik respond?

MikroTik released fixes to all branches of RouterOS pretty much imediatelly

What was the impact?

- Impact of module 1 was actually quite small compared to other exploits later in this presentation
- Default config was not affected, and it seems most of publicly available MikroTiks had a firewall for the web service

How could I have defended?

- Simple, have proper firewalling
- Do not allow public access to the web service

- Make sure your RouterOS is up to date

If I was exploited, how to remediate?

- NetInstall
- Since this exploit allow RCE, underlaying Linux might have been compromised.
- Updating RouterOS might not be enough to remediate.
- NetInstall formats the flash, and installs a clean system.

Part 2:
Winbox client-side exploit

Attacking administrator workstations through infected routers

Meanwhile, new exploit

- While module 1 of Chimay Red was being utilized, a new exploit was discovered
- Winbox malicious DLL delivery

What happened?

- Winbox would load and execute arbitrary DLLs delivered as a part of connecting to older RouterOS versions

  (DLL delivery was used with ROS v5 and older, not in v6 anymore)

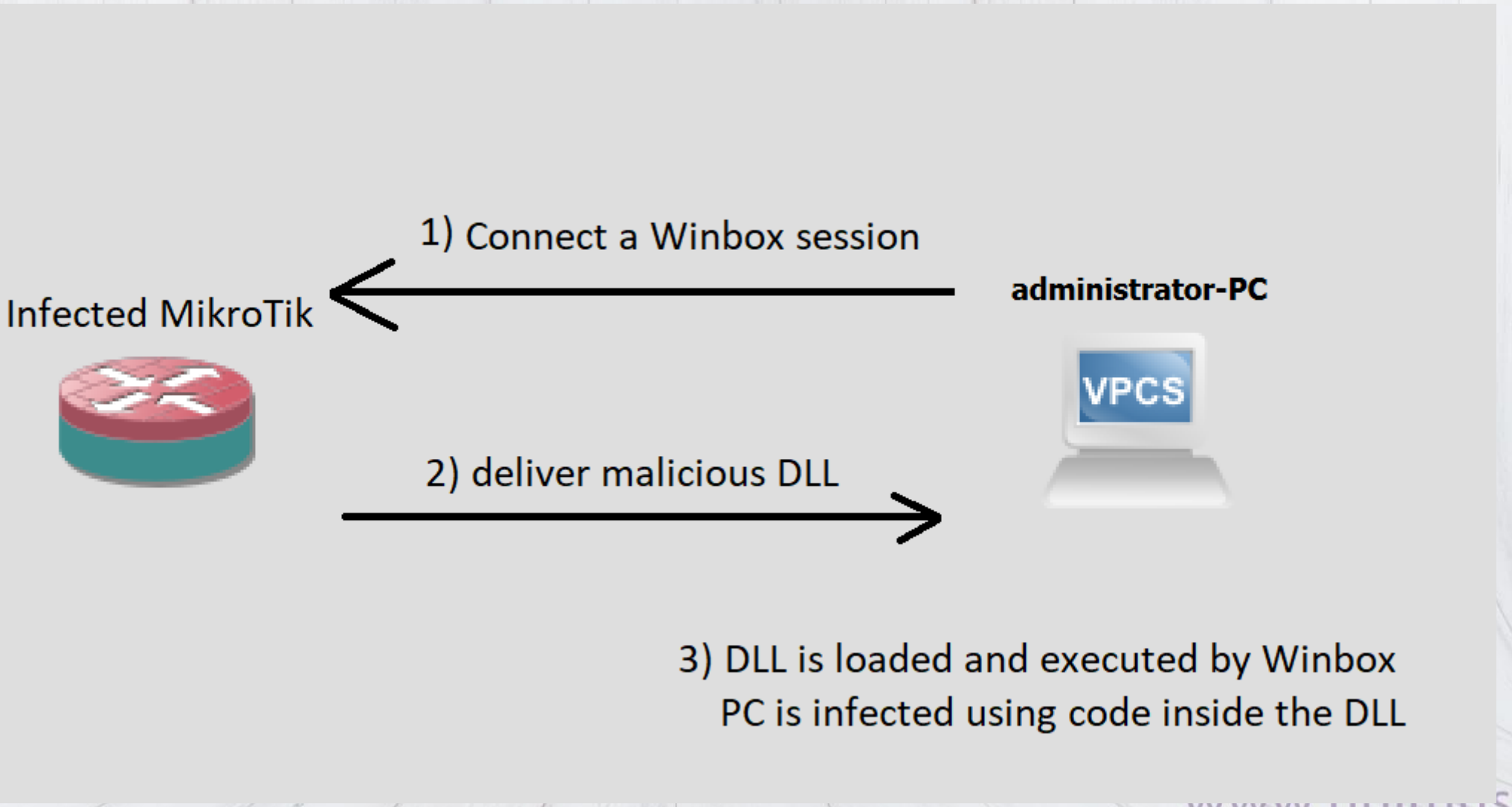
- Winbox supported this for backwards compatibility reasons

More details

- No signing or verification of delivered DLLs was done, so this allowed arbitrary code execution on the system running Winbox
- (this was an attack on the computer the admin of the MikroTik was using)

- In effect, someone could compromise your PC when you connected to a router seeding attack DLLs

Visualizing the exploit



When did this appear?

- In March 2018, exploits utilizing Winbox DLL injection were discovered in the wild
- Chimay was used to deliver payload to routers, routers injected payload into Winbox sessions

MikroTik response

A new version of Winbox was released is short order that does not support DLL loading anymore

(side-effect - connectivity to older ROS devices no longer possible)

Impact of this?

- Impact of this exploit is unknown - but likely extremely small
- Exploiting this required exploiting the router first
  (or having the admin connect to a router the attacker controlled)
- It is speculated that this attacks was used with very narrow focus by state actors against specific targets
  (rumors, no "official" confirmations available)

How could we have defended?

1) keep your Winbox up to date

2) protect your router so it doesn’t get seeded with malicious DLLs

3) do not connect to unknown routers

How to remediate?

- Since the attack was against the OS of the administrator, remediation is not simple.
- Reinstall OS might not be enough, since malware can hide in MBR, recovery partitions, even BIOS.
  (or even chip firmware - especially with recent Meltdown / Spectre / Ryzenfall / Masterkey / Foreshadow exploits)
- How to remediate user workstations is out-of-scope of this presentation

Part 3:
Winbox arbitrary file read vulnerability

Read any file on routers just by seeing TCP port 8291 open

New saga - current ROS exploits

- All of the previously discussed exploits were very low impact compared to what has been happening in the recent 3 months

- Let's talk about the current situation, and the exploits running wild around the world right now

What happened?

- Chimay Red module 2 allowed arbitrary file access through a Winbox vulnerability
- Essentially, this allowed anyone to retrieve the contents of the file-system of the router through the Winbox port
- When you can read any files on the file system – you can read the user database file

How was this exploited?

- Winbox directory traversal vuln. allow unauthenticated attackers to retrieve the user database of the router
- After this, attackers could connect using Winbox (or any other management service), since they had valid passwords.
- Essentially, if the Winbox port (TCP 8291) was available to the attacker, they could take over the router

A huge wave of exploits started

- In the first days of August 2018, a botnet attacked and successfully exploited over 200k routers in Latin America.

- This was the first time the Winbox vuln. was successfully used for an attack

MikroTik response?

Well, this was actually patched back in April 2018

Patched versions:

Fixed in 6.40.8 and 6.42.1

What was done after routers were exploited?

- There are many variants of malware running wild using this exploit.
- We know of at least 6 separate "families" of malware distributed by various botnets.

What was the impact?

- The impact of this was huge - since many routers had Winbox publicly available
- In Latin America alone – 200k routers exploited
- Since the discovery of this exploits, estimates put the number of exploited routers at 400k+
- Currently world-wide – 500k+ of routers still vulnerable

Variant 1 - original

- The "original" malware family hit Latin America in August

- Its goal was simple:
- Insert crypto mining JS into websites visited by clients behind the router
- This would cause clients to mine Monero simply by browsing the web

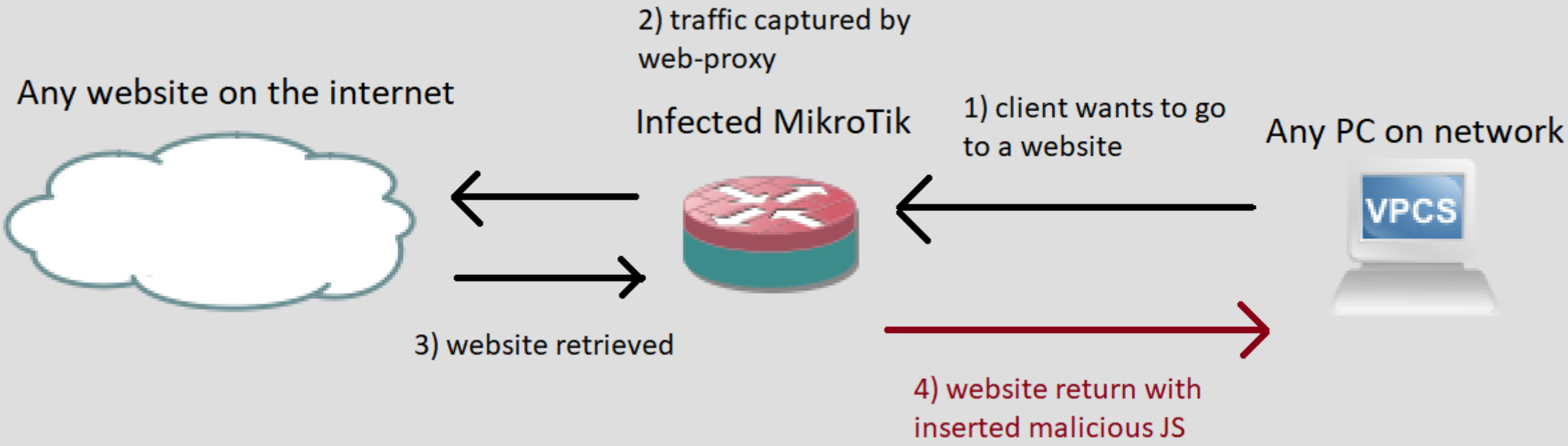
- Multiple target Monero wallets were identified, some seized

How was this done?

- Web proxy was enabled on the router
- NAT rules were inserted to redirect web traffic to the web proxy

- Multiple scripts were put on the router that served as command delivery methods
- Schedulers were configured to pull command scripts from C&C servers

Visualizing attack



Common symptoms:

- "service" user was created
- new scripts added to router
- new "Scheduler" entries added
- web proxy was enabled
- NAT and firewall were modified

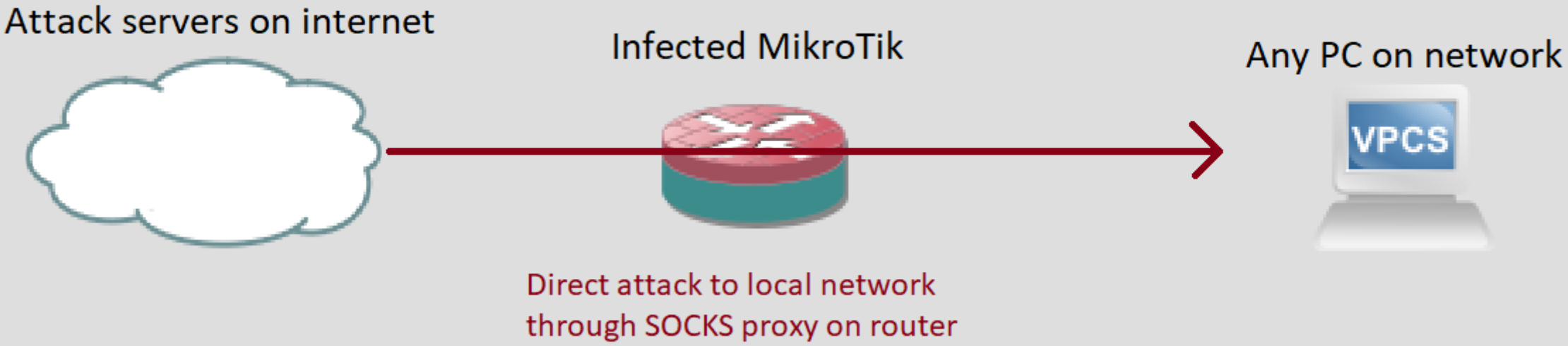
Variant 2: 2nd generation

- Another variant shortly appeared that setup SOCKS proxy to allow direct LAN attacks
- Proxy was also used to attack 3rd party services anonymously

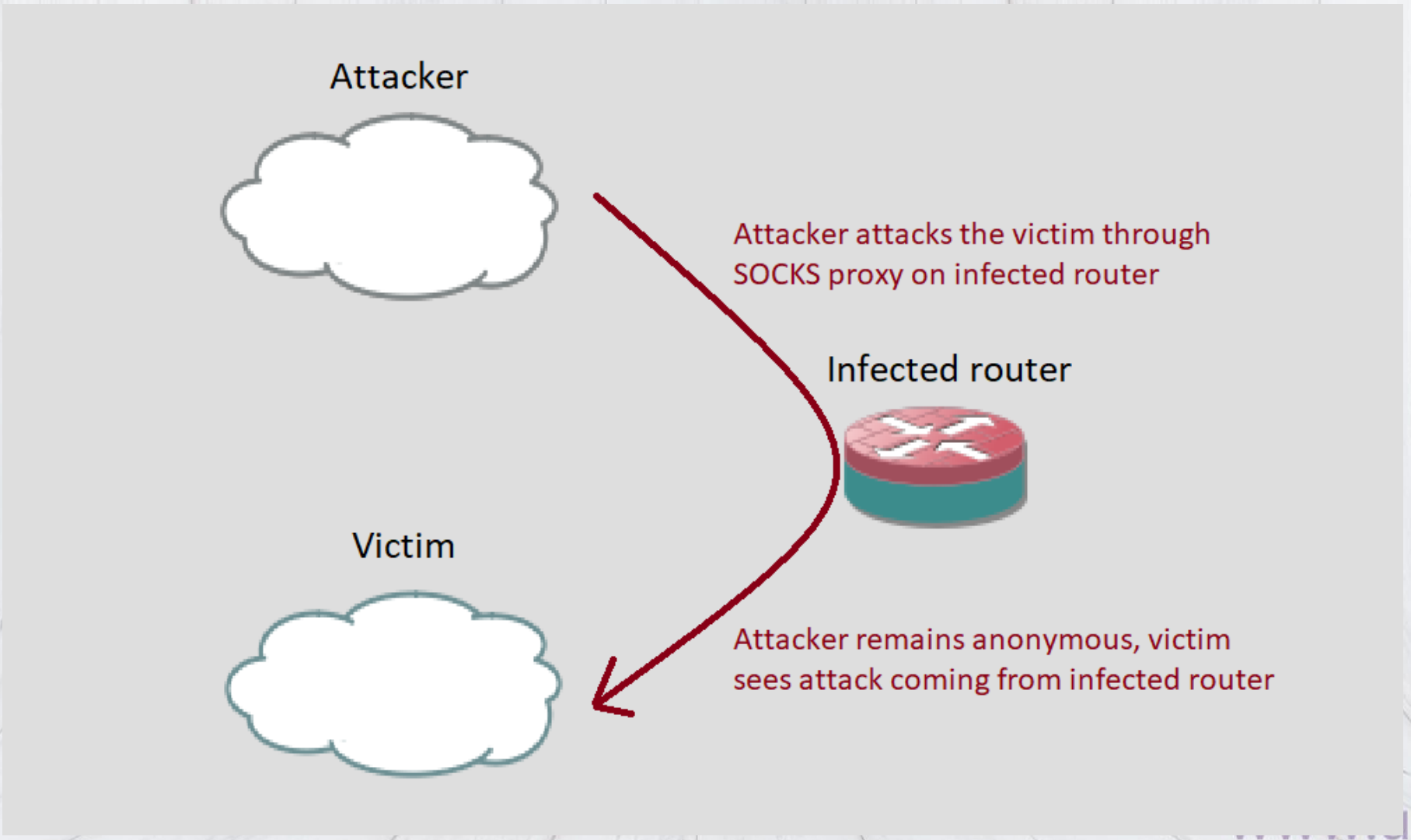
How was this done?

- SOCKS proxy was setup on the router
- This allowed attackers to directly attack machines in the LAN behind the router utilizing SOCKS proxied connections to the internal network
- Also allowed anonymous attack on 3rd parties

Visualization 1



Visualization 2



Symptoms

- usually very similar as variant 1
- SOCKS proxy was also enabled and reconfigured

Evolutions...

- Variant 1 and 2 soon merged to become a single malware family
- You could find web proxy and socks proxy deployed alongside commonly

Variant 3 - 2nd generation

- Not long after the "1st generation" of malwares, new ones appeared
- This time, DNS interception and redirection was the goal

What was done?

- On the router, DNS server was enabled, and used malicious upstream DNS servers
- In NAT a transparent DNS hijack was performed (redirect all tcp/udp 53 traffic to the router)

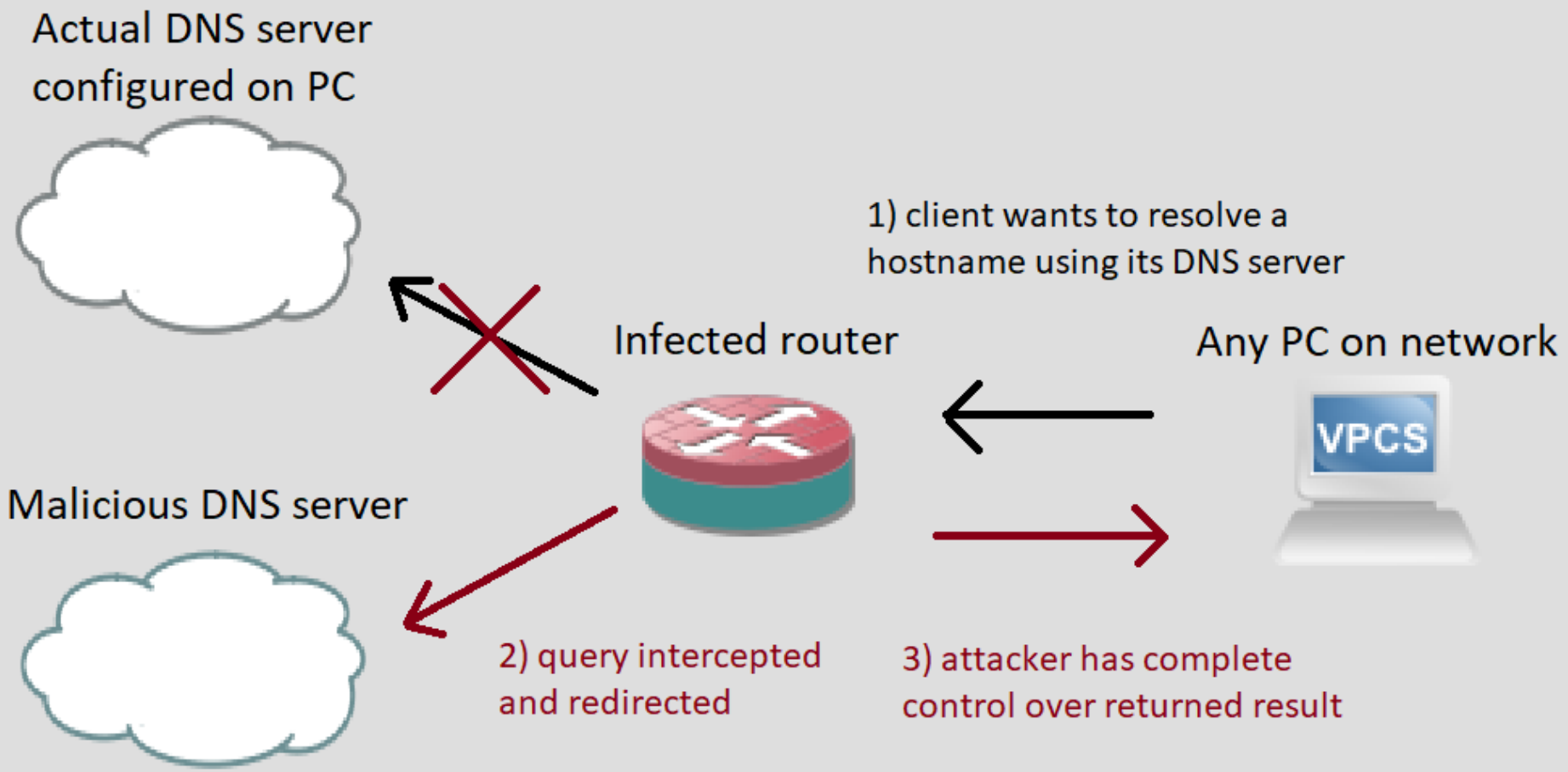
What was the goal?

- By controlling DNS for the entire network behind the router, attackers gained control to route traffic from the network as they wished

  (even if PCs used explicit DNS configuration due to DNS hijack through NAT)

- Many attacks are possible here, since attackers are in complete control of where traffic from clients goes

Visualizing



More generations

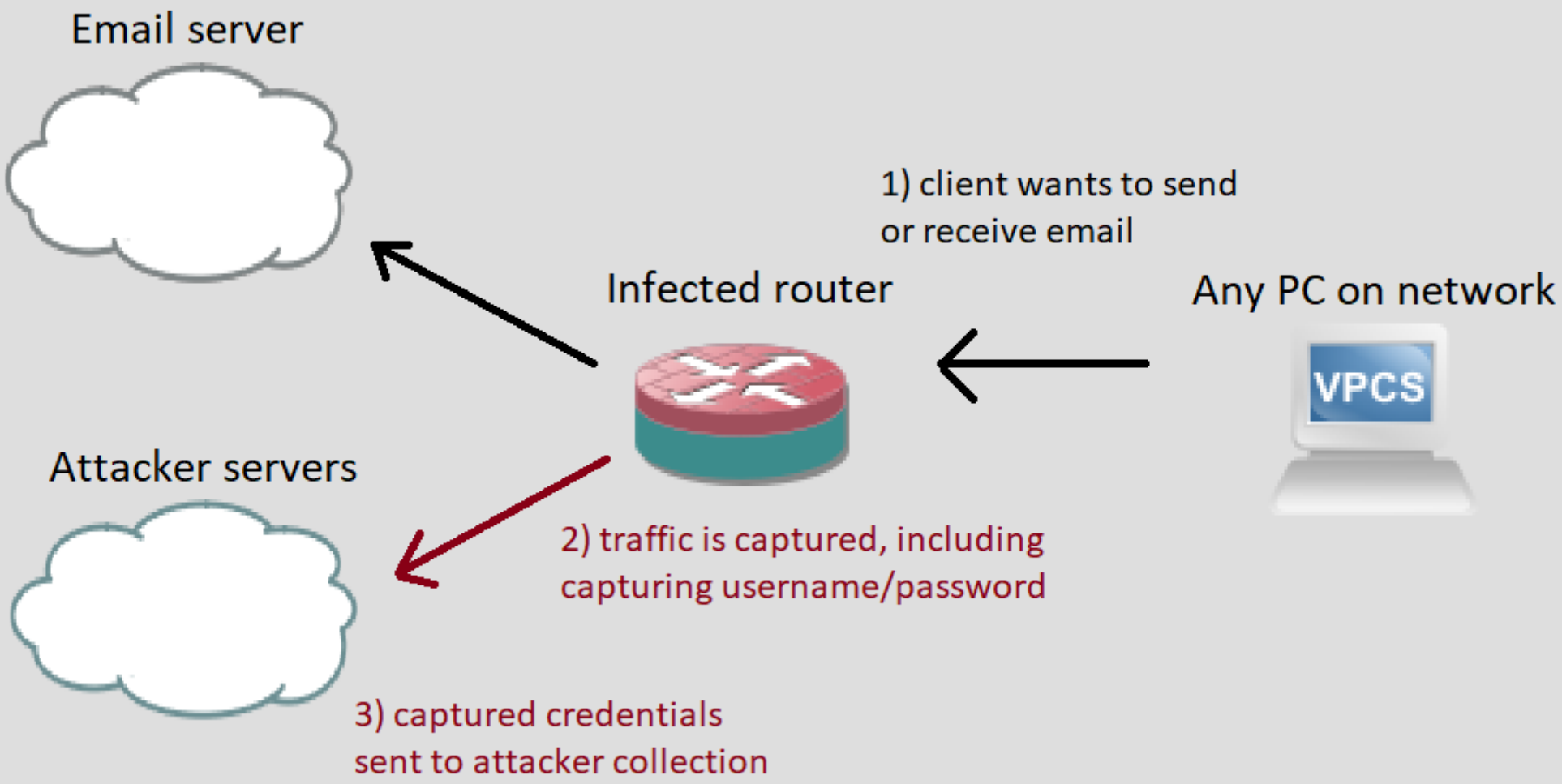
- Since the 2nd generation, many more new variants of exploits have appeared.
- We even saw variants that checked against the C&C servers with MAC of ether1 as identifier.
- This allows attackers to instruct individual routers what to do, or use groups of routers for geo-focused attacks.

Unencrypted traffic capture

- One new attack these malware can utilize is capturing all interesting unencrypted traffic passing the router

- This includes:
  - Telnet, FTP
  - POP, IMAP, SMTP
  - HTTP, SNMP
  - etc.

Visualizing



All together now…

- In most currently active exploits, attack patterns stayed the same as discussed above

- web traffic interception and injection using HTTP proxy
- Using SOCKS proxy to attack local network, or redirect traffic for spoofing
- DNS hijack to redirect traffic from local network
- Traffic capture for unencrypted protocols

Signs of "infection"

- In general look for:
  - modified HTTP proxy settings
  - new users created on the router
  - SOCKS enabled / reconfigured
  - suspicious scripts present
  - strange Schedulers present
  - DNS reconfigured
  - NAT / firewall reconfigured
  - Packet Sniffer enabled for unencrypted traffic

How could have we defended against this?

- Simple, have proper firewalling

- Do not allow public access to the Winbox service
- (secure access to Winbox with an address-list, use management VPN, port knocking, etc.)

- Make sure your RouterOS is up to date

Repeating what we said in the beginning

- MikroTik default configurations were NEVER affected by any of these exploits
- If you were affected, it is because you reconfigured the router in an unsecured way

Side note - how to protect yourself going forward?

- Configuration change notifications.
- Make sure you have config monitoring that notifies you on config changes.
- (configuration management software - check Unimus)

How to remediate?

- For var1 and var2, we have an article on our website:
- https://unimus.net/blog/validating-security-of-mikrotik-routers-network-wide.html

- For Gen2 (DNS hijack), fix DNS and NAT

How to remediate part 2

- For newer exploits... this is more complicated.
- 1) Check your entire configuration for things that should not be there
- 2) reset config and reconfigure from scratch

- Optionally, recover config from older backups
  (have a configuration backup solution, like Unimus)

How to remediate part 3

- CHANGE PASSWORD!
- Since the user DB was retrieved using the vulnerability, make sure to not reuse passwords
- If you reset config (or even update RouterOS) and don't change your management credentials, attackers will just get right back in
- Many people have been re-infected this way

Latest news (from last week)

- The Winbox directory traversal vulnerability can now be used for RCE
- This means that things much worse than what was happening in last 3 months are about to come soon.

What’s going to happen?

- 500k MikroTiks around the world are still vulnerable to the Winbox exploit

- Now that RCE has been discovered through this exploit, it opens a whole new world of possibilities for attackers.
- (since they can now issue commands to underlaying Linux just by seeing TCP 8291 opened)

What can attackers do now?

- Attackers will be able to:
- Install crypto mining software directly on routers
- Install malware that won't go away when reseting configuration

- Attack local network directly from the router
- Attack ISPs infrastructure from routers of their clients

- etc., etc., etc.

If your router gets compromised now

- Make sure to NetInstall, not just reset configuration
- With RCE, malware can be installed directly in underlaying Linux

Takeaway from this presentation

- Secure the management ports on your router
  (do not leave them open to the public)

- Have proper firewall
- Update RouterOS & Winbox

- NetInstall and change passwords on compromised routers

- Have configuration change notifications & backups

Additional resources

Things to watch/listen to

My other presentations and talks

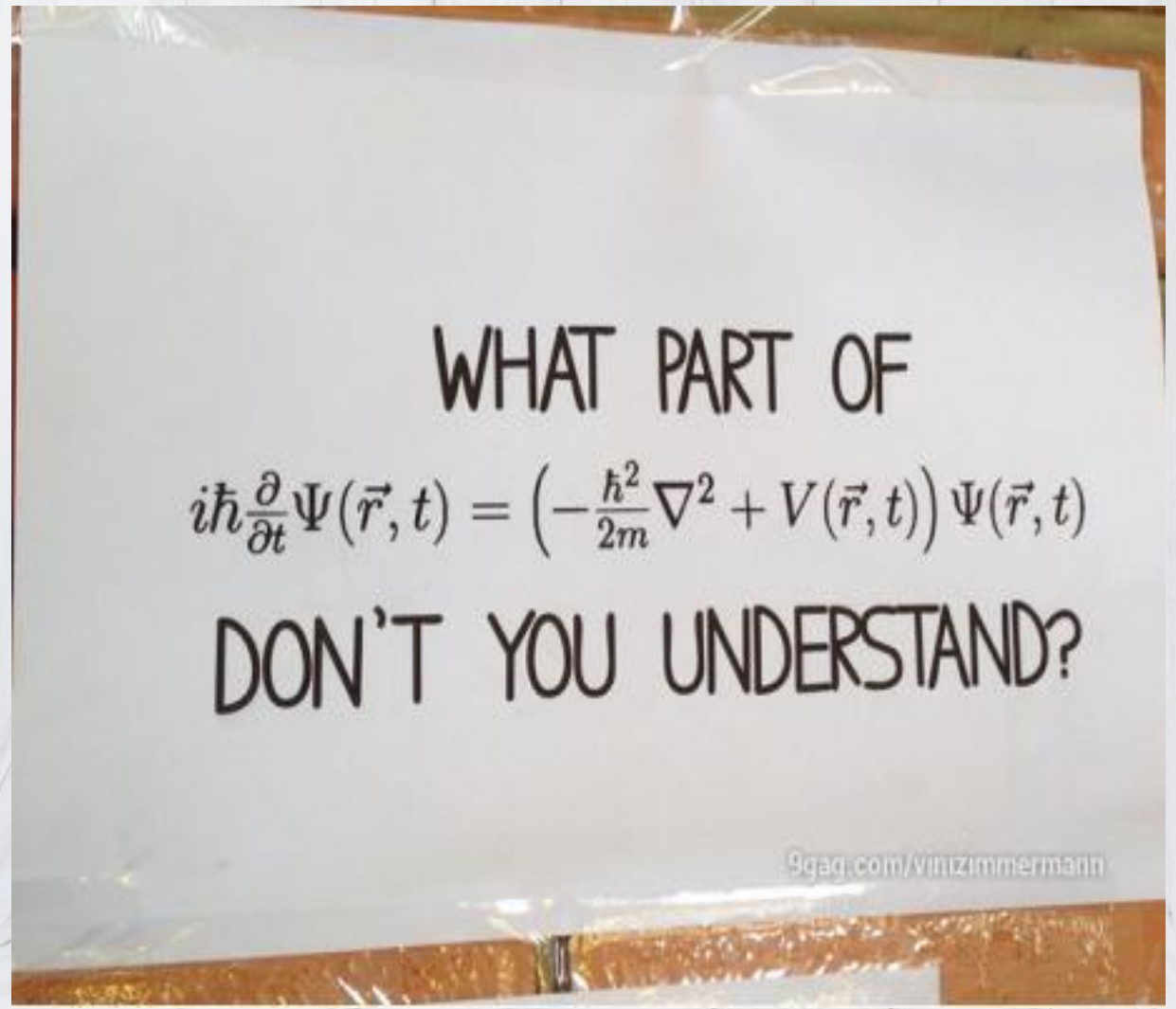
- Find all my other MUM presentations and more on:
  https://www.youtube.com/c/TomasKirnak/videos

  Load Balancing / Mangle deep dive
  L2TP / IPSec deep dive
  IPSec XAuth mode-config deep dive
  MLPS / VPLS / MTU deep dive
  Monitoring / SNMP deep dive
  Automation deep-dive
  etc.

TheBrothersWISP

- I am a part of The Brothers WISP
- We do a bi-weekly networking podcast
  http://thebrotherswisp.com
- Give us a listen if you feel like it!

Thank you very much for your attention!



Tomas Kirnak

tomas@unimus.net