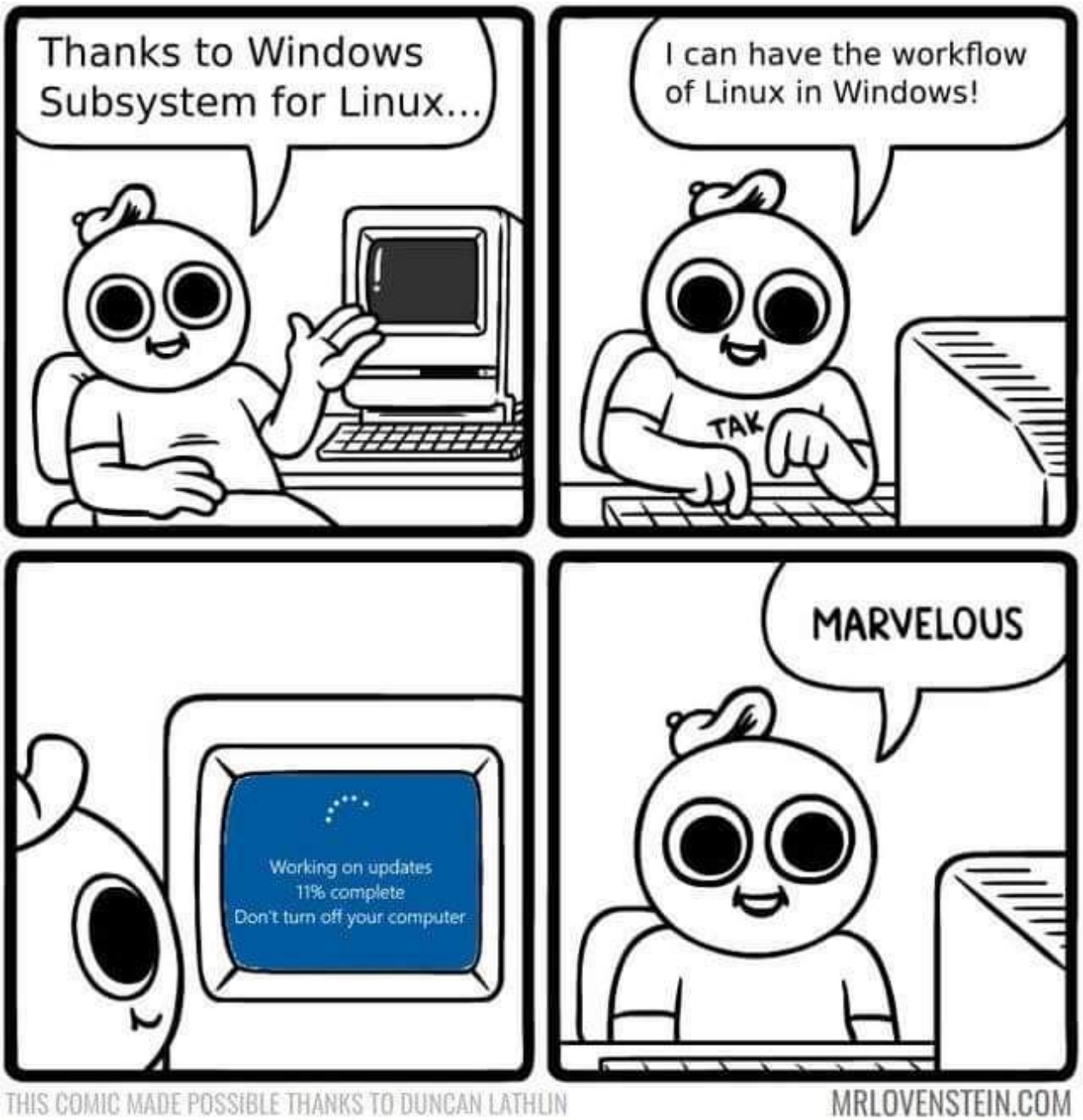
Security Now! #725 - 07-30-19

Urgent / 11

This week on Security Now!

This week we close the chapter on the Marcus Hutchins saga, the US Attorney General weighs-in in "warrant proof" data encryption, we look at what's popular with the underground, we update on the latest four new Ransomware attacks, we examine three different attacks on exposed network attached storage (NAS) servers, we cover a bit of miscellany, then take a close look at the news of the just-released-yesterday vulnerabilities in the 2 Billion strong VxWorks embedded OS and see why it is aptly named "Urgent/11."



Security News

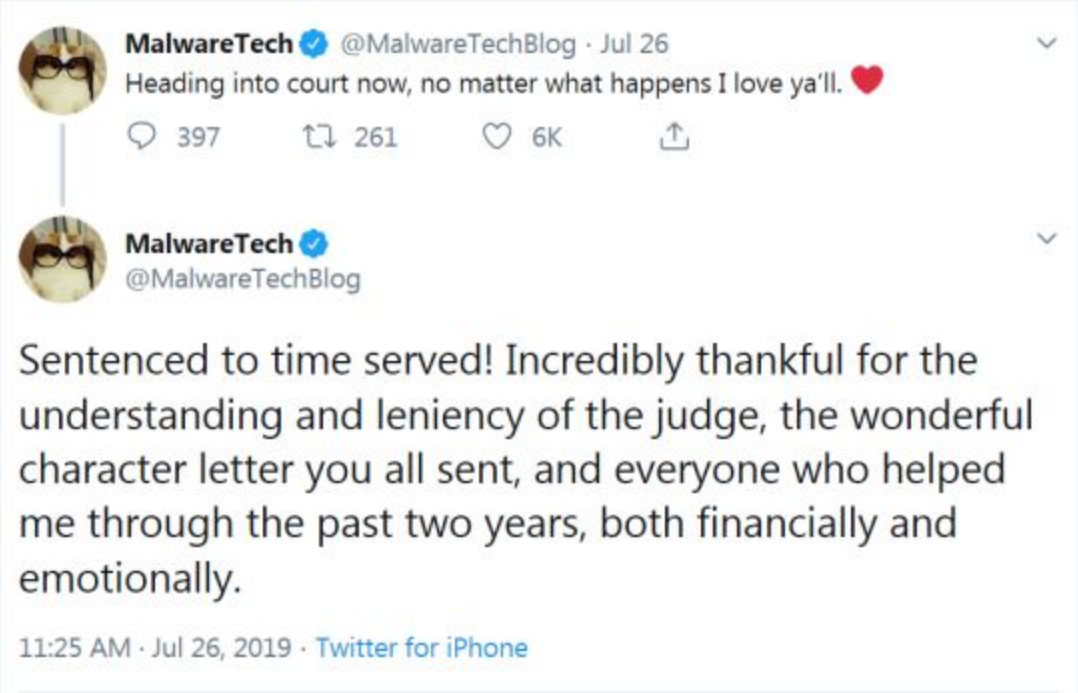
Marcus Hutchins ... is Free!
It was two years ago this summer, after the annual 2017 DEFCON security conference, as he was walking through the Las Vegas airport preparing to return to his home in the UK, that Marcus Hutchins, having been for many years a good guy White Hat, was nabbed by local law enforcement and held on charges of computer hacking, fraud and abuse.

Pretty soon afterward he was released from jail, but his passport was withheld and he was under travel restrictions. For that past two year he's been working with his defense team on the charges and legal attending hearings.

Although he did have a darker and more sketchy adolescence, he had outgrown those interests and clearly regretted any trouble his earlier activities may have caused. (And let us not forget that what originally brought Steve Jobs and Steve Wozniak together was their interest in "Blue Boxing" which allowed the long distance billing system of the U.S. telephone system to be quickly bypassed for making free long distance calls.)

However, shortly before his arrest, Marcus was studying the alarming emergence and rapid propagation of the incredibly prolific and dangerous WannaCry Internet worm. His research serendipitously halted its propagation and doubtless saved a great many entities connected to the Internet a great deal of time and trouble.

So... US district judge Joseph Peter Stadtmueller said that the malware Hutchins helped stop was much more damaging than the two programs he created, and sentenced him to time served with a year of supervised release.



Marcus had faced a maximum sentence of 10 years in prison. He is now free to return to the UK.

However, US authorities will need to decide whether he's barred from returning to the US due to his criminal record. Doing so would be really dumb… but we did say "US authorities."

U.S. Attorney General Bill Barr on "Warrant Proof data encryption"
The Associated Press posted a 2-minute video of U.S. Attorney General, William Barr. It's worth two minutes of the podcast for everyone to hear this in his words:
https://www.youtube.com/watch?v=c-QQwv1U2aY

What's popular underground?
https://www.recordedfuture.com/measuring-malware-popularity/
https://go.recordedfuture.com/hubfs/reports/cta-2019-0724.pdf

"Recorded Future" has assembled a beautiful report titled: "Bestsellers in the Underground Economy: Measuring Malware Popularity by Forum"

By analyzing over 3.9 million posts from May 2018 to May 2019 across all underground forums indexed by the Recorded Future platform, Recorded Future's Insikt Group identified the top malware variants being referenced on underground forums. The Insikt Group also attempted to find real-world events that correlated with a higher number of malware references on these forums, as well as differences in tools advertised in forums of different languages, to see if any differences existed.

Insikt Group discovered that a majority of the top 10 mentions of malware in multiple languages included openly available dual-use tools, open-source malware, or cracked malware. Some of these malware families were also over three years old or could be mitigated with basic security precautions. Activity in underground forums that correlated to growth in malware references included: sale of malware in a larger bundle, advertising updates to the malware, advertisements of the malware on a new forum in which the malware was not previously sold, news articles related to malware shared on forums, and community engagement.

Insikt Group also discovered that underground communities in different languages did indeed focus on different malware, malware categories, and attack vectors. English- and Chinese-speaking underground communities, for example, focused more on Android malware than other communities. By separating forum advertisements by language, Insikt Group found that forum members occasionally used online translation services to attract business partners and buyers from different language communities.

Key Judgments

- The top 10 mentions of malware across Recorded Future underground forum collections suggest that underground forum members are discussing and using tools readily available to them more often than paying for or inventing new tools.

- Based on the prevalence and longevity of the malware, Insikt Group assesses with medium confidence that there likely exist enough victims who do not comply with basic security precautions for forum members to successfully infect.

- Approximately 50% of all activity concerning ransomware on underground forums are either requests for any generic ransomware or sales posts for generic ransomware from lower-level vendors. We believe this reflects a growing number of low-level actors developing and sharing generic ransomware on underground forums.

- Insikt Group assesses with medium confidence that, due to the number of underground forum members sharing, deploying, and providing reviews about malware and its functionality, the 10 most popular malware on underground forums hit host computers with higher frequency, but are low to moderate threats compared to other malware due to their age, ineffectiveness without a delivery vehicle or crypter, and existing antivirus detections.

Pulling all that together, this suggests a few things. For example, I scanned the charts and graphs for any mention of Ryuk Ransomware. It is nowhere. Why? Because it's high-end proprietary upper-crust ransomware. The ransomware that is for sale in these forums is the equivalent of second-hand non-state-of-the-art hand-me-downs. Those who are capable of writing state-of-the-art ransomware are NOT selling it here. They are not selling it at all. They're deploying it. Perhaps, in five years, Ryuk will be seen changing hands within the underground community. But not today. Today it is earning a reputation that will evolve into mythology. And that mythology will eventually be driving its aftermarket resale... long after Ryuk's authors have moved onto the next scam.

"This Week in Ransomware"
Lawrence Abrams headlined his weekly snapshot Ransomware coverage for BleepingComputer "State of Emergency" and started with a declaration that I think is all too true. He wrote:

"*Now that ransomware developers know that they can earn monstrous payouts from local cities and insurance policies, we see a new government agency, school district, or large company getting hit with a ransomware attack every day. For example, this week the Governor of Louisiana declared a state of emergency for the wave of attacks targeting school districts in the state.*"

So what happened?? Louisiana's Governor John Bel Edwards, last Wednesday, declared a formal state of emergency after three public school districts were taken over by ransomware. The reason for making it a declaration of a state of emergency is interesting. We'll get to that in a second.

http://gov.louisiana.gov/assets/EmergencyProclamations/115-JBE-2019-State-of-Emergency-Cybersecurity-Incident.pdf

One of the three public school districts, Sabine Parish in northern Louisiana, released the following statement:

The Sabine Parish School System was hit with an electronic virus early Sunday morning. This virus has disabled some of our technology systems and our central office phone system. The district staff reported this electronic viral attack to local law enforcement, state officials and the FBI. All available resources are being utilized to get the district systems back online. An investigation involving local, state and federal law enforcement is ongoing at this time. The

school phone systems were not affected by this attack. The central office phone system is being repaired and service will be restored as soon as possible. According to the Louisiana Department of Education, several other school districts were attacked by the same virus this week.

No details have emerged yet about what ransomware variant was used, but does anyone want to place a bet that it WASN'T Ryuk? State officials have not yet released a full list of the affected systems.

Eddie Jones, principal of Florien High School in Sabine Parish, told the local television news station KSLA that his technology supervisor got an alert on his phone around 4am Sunday about a surge in bandwidth usage. It was particularly unusual given the time of day and the fact that the schools are all on summer break.

When technical staff investigated, Jones said, they found ransomware on the servers.

The principal said that he doesn't believe that any sensitive information was lost. What was lost: "anything and everything" stored on the school district's servers, including 17 years' worth of Jones' personal documents – his speeches, test schedules, master schedules and more.

The declaration of a state of emergency means that state resources will be made available and that assistance will be coming from cybersecurity experts from the Louisiana National Guard, Louisiana State Police, the Office of Technology Services and others to assist local governments in responding to the crisis and in preventing further data loss. Interestingly, the declaration of an emergency also includes protection from being price-gouged for the extra help and resources. Language concerning that protection, from a Louisiana proclamation about states of emergency reads:

"*During a declared state of emergency, the prices charged or value received for goods and services sold within the designated emergency area may not exceed the prices ordinarily charged for comparable goods and services in the same market area at or immediately before the time of the state of emergency, unless the price by the seller is attributable to fluctuations in applicable commodity markets, fluctuations in applicable regional or national market trends, or to reasonable expenses and charges and attendant business risk incurred in procuring or selling the goods or services during the state of emergency.*"

This is the first time that Louisiana has activated its emergency cybersecurity powers, which were created for just this type of cyberattack. The response is being handled by the state's newly formed Cyber Security Commission, which was established two years ago in 2017. It brings together the state's key stakeholders, subject matter experts, and cybersecurity professionals from Louisiana's public sector, private industry, academia, and law enforcement.

The Governor's Office of Homeland Security and Emergency Preparedness has also activated its Crisis Action Team and the Emergency Services Function-17 to coordinate a response.

The Governor's office said: "The state was made aware of a malware attack on a few north Louisiana school systems and we have been coordinating a response ever since. This is exactly why we established the Cyber Security Commission, focused on preparing for, responding to and preventing cybersecurity attacks, and we are well-positioned to assist local governments as they

battle this current threat."

Ars Technica put some interesting context around Louisiana's response: it's modeled on Colorado's response a year and a half ago in the wake of two SamSam ransomware attacks. The first hit in February 2018, and the second came the following week. The attacks wound up costing the state $1.5 million to disinfect its systems after officials decided against paying anything to the attackers.

In Sophos' reporting they noted that contemporary ransomware attacks don't just encrypt data, they also encrypt parts of the computer's operating system too so that backup plans need to account for how entire machines will be restored, not just databases.

It'll be interesting to learn what decision is made in this case. Since it's summertime with school in recess, they may be under less time pressure than the municipalities that have recently been hit. Do they pay or don't they?

But wait... there's more!!
"Cyberattackers strike fourth Louisiana school district, Tangipahoa Parish, others taking precautions."
https://www.theadvocate.com/baton_rouge/news/education/article_8a4bd37c-b214-11e9-87ff-a39b5f997ee8.html
Just yesterday a fourth Louisiana school district was attacked. In the local reporting of that attack, the comment was made that the timing was especially troublesome since school was scheduled to resume in about a week. So… I guess they are under significant time pressure after all. And I suppose it's convenient that the State is already in a formally declared state of emergency.

What a mess.

Your NAS is Grass!

One by one, service by service, we have been seeing attackers targeting anything that's exposed and is either deliberately or inadvertently offering services to the Internet. Last week's podcast was titled "Hide Your RDP Now!" because even non-BlueKeep-vulnerable RDP services were under attack to a sobering degree with password guessing. So, in keeping with last week's theme, and as a result of there being three separate instances of NAS attacks, this week we caution our listeners that unless measures are taken to protect their devices, they may find that their NAS is Grass!

In the case of Network Attached Storage (NAS) devices, since these devices are presumably storing important and valuable documents, they are an obvious target for Ransomware. And, indeed, that's what we're seeing.

QNAP:
Earlier this month, a campaign targeting the NAS devices produced by the Taiwanese company QNAP Systems, Inc., was uncovered by researchers at Anomali Labs. They found that QNAP's devices were being compromised by brute forcing weak credentials and exploiting known vulnerabilities. And, once infected, a malicious payload was encrypting specific file extensions on the NAS using AES encryption and appending ".encrypt" extension to the encrypted files. Once complete, the following ransom note was created and left behind:

```
All your data has been locked(crypted).
How to unclock(decrypt) instruction located in this TOR website:
http://sg3dwqfpnr4sl5hh.onion/order/[Bitcoin address]
Use TOR browser for access .onion websites:
https://duckduckgo.com/html?q=tor+browser+how+to

Do NOT remove this file and NOT remove last line in this file!
[base64 encoded encrypted data]
```

The researchers reverse-engineered the malware, discovering that it had been written and compiled in the GP programming language. The Ransomware is quite straightforward and not very complex, consisting of fewer than 400 lines of code. Upon execution, the malware first reaches out to its Command & Control server, which is listening on IP [192].[99].[206].[61] to notify it that the encryption process has started. It then walks the file system hierarchy for files to encrypt that have not already been encrypted. When it locates one it encrypts it, changes its file extension, and move on to the next file. When finished it produces the ransom note.

Of note is that NAS devices are not normally running any form of Anti-Virus software since they are considered turnkey embedded systems. But even so, at the time of its discovery, VirusTotal reported that only 2 or 3 A/V scanners were detecting this malware as being malicious.

In their conclusion, the researchers recommended that external access to QNAP NAS devices be restricted, to ensure that the device's firmware is current and up to date with security patches, and that strong credentials are being used with all devices, especially those which are exposed to the Internet.

And I'll add, in the spirit of "hide your NAS", if the device offers an OpenVPN server/service as an access option, seriously consider using it, even if it's somewhat inconvenient. One of the things that OpenVPN offers is very strong authentication security. You can use it to hide all manner of sins.

https://www.anomali.com/blog/the-ech0raix-ransomware

Synology:
Meanwhile, last week, another major NAS vendor, Synology, issued an urgent warning titled: "Synology Urges All Users to Take Immediate Action to Protect Data from Ransomware Attack"

TAIPEI, Taiwan—July 23, 2019—Synology® recently found that several users were under a ransomware attack, where admins' credentials were stolen by brute-force login attacks, and their data was encrypted as a result. We investigated and found that the causes of these attacks were due to dictionary attacks instead of specific system vulnerabilities. This large-scale attack was targeted at various NAS models from different vendors; [in otherr words, this is NAS-wide, not just Synology] therefore we strongly recommend users check network and account settings to protect data from ransomware.

Ken Lee, Manager of Security Incident Response Team at Synology said: "We believe this is an organized attack. After an intensive investigation into this matter, we found that the attacker used botnet addresses to hide the real source IP. After collecting admin account passwords with brute-force attacks, the attack was launched on July 19 and caught users off guard. We therefore informed TWCERT/CC and CERT/CC immediately of this matter in hopes of accelerating the collaborative efforts to resolve this incident."

Since this attack is not related to system security vulnerabilities, it is recommended that Synology users utilize built-in network and account management settings to enhance system security level, preventing malicious attacks from the Internet.

Hewitt Lee, Director of Product Management at Synology said: "We urge all Synology users to take immediate action to protect their NAS from the ransomware attack. Users' data security is always our priority. For those who are not using Synology NAS, we still recommend you take corresponding actions to protect your precious data."

Please make sure you go through the checklist below:

- Use a complex and strong password, and Apply password strength rules to all users.
- Create a new account in administrator group and disable the system default "admin" account.
- Enable Auto Block in Control Panel to block IP addresses with too many failed login attempts.
- Run Security Advisor to make sure there are no weak passwords in the system.

To ensure the security of your Synology NAS, we strongly recommend you enable Firewall in Control Panel and only allow public ports for services when necessary, and enable 2-step verification to prevent unauthorized login attempts. You may also want to enable Snapshot to keep your NAS immune to encryption-based ransomware.

["Snapshot" is Synology's backup versioning solution]

https://www.synology.com/en-us/company/news/article/2019JulyRansomware/Synology%C2%AE%20Urges%20All%20Users%20to%20Take%20Immediate%20Action%20to%20Protect%20Data%20from%20Ransomware%20Attack

Lenovo-EMC & Iomega NAS Flaw:
Wait!, What? Iomega? They're still around? Eleven years ago, back in 2008, EMC bought up the company. Then five years later, a Lenovo-EMC joint venture relaunched Iomega as "LenovoEMC." So today we have a Iomega / LenovoEMC vulnerability announcement:

Our story begins with an intrepid employee with the infosec firm Vertical Structure, based in Northern Ireland, first discovered files apparently being publicly exposed on the Internet via Shodan late last year. After a bit of additional sleuthing, they confirmed that documents (a great many documents, actually) were being publicly exposed to the Internet without any password or other authentication checks through an unauthenticated API call.

The exposed API was eventually tracked down to an older set of Iomega NAS boxes that were, thanks to this widely exposed and unauthenticated API, leaving many millions of files -- more than 3 million files totally 36 terabytes of information -- exposed to the web.

Simon Whittaker, a director at Vertical Structure said: "There were a significant number of files containing sensitive financial information including card numbers and financial records. Vertical Structure was able to track down the common source, a legacy Iomega storage product acquired by EMC and co-branded LenovoEMC in a joint venture."

Of those three million files, Whittaker said 405,398 were images, 20,055 were documents, 13,677 were spreadsheets, and 13,972 were text documents.

After realizing the extent of the exposure, Vertical Structure called in WhiteHat, who ran their own investigation of the leak, and confirmed that public-facing Iomega-LenovoEMC devices were in fact spewing all of their data onto the internet. The two companies then alerted Lenovo to the problem, and the vendor responded by bringing the software out of retirement to address the bug. Details of the API flaw were not shared, as the patch for the hole has only just been released.

Lenovo has responded with a security vulnerability announcement and updates:

Iomega and LenovoEMC NAS Vulnerability
Lenovo Security Advisory: LEN-25557
Potential Impact: Information disclosure
Severity: High
Scope of Impact: Lenovo-specific
CVE Identifier: CVE-2019-6160

https://support.lenovo.com/us/en/product_security/LEN-25557

So the bottom line is, anyone or any firm using older Iomega-brand or LenovoEMC NAS devices should immediately check with Lenovo for updates and be certain that you're running the latest firmware for your NAS to protect against attack.

Although absolutely nothing has been disclosed about the vulnerability, it sounds as though the devices were opening and offering services on additional "other" ports aside from the ports used for primary NAS services. If that's the case, it sounds as through these NAS devices were given

their own public IPs and were simply placed out onto the Internet.

This makes me shake my head since even consumer NAT routers provide more security than that. In an IP-constrained environment, we're forced to share an IP among many devices. So, if a user wishes to publicly expose a NAS, they need to create a static port mapping through the NAT router to the internal IP of the NAS box. In this way, ONLY the specifically-configured NAS ports would be made publicly available and any other "off the book" services being offered would remain hidden, just as they should be.

So, one way or another, NEVER hang your whole NAS box out on the Internet where all of its 65,535 TCP and UDP ports can -- and definitely will -- be scanned. ALWAYS place it inside your network and only allow external public access to the one port or few ports that you need to have configured for its intended use.

And, yes, of course, if it's feasible to only make it accessible via a VPN, then so much the better. :)

Miscellany

- **Netflix "*Another Life*"** -- OMG!
  @SGgrc: "The best thing about Netflix's much anticipated incredibly unbelievably awful and disappointing science fiction series "Another Life" are the reviews on IMDB. Believe them: https://www.imdb.com/title/tt8369840/reviews?ref_=tt_ql_3

- **The Great Hack**
  This is a just-released Netflix original documentary, primarily about Cambridge Analytica and somewhat secondarily about its role in the 2016 US Presidential election. It is predominantly a human interest piece, obtaining a look inside Cambridge Analytica and several related organizations through the eyes of a young woman who got a bit swept up in the power, was very much on the inside, and later saw what this thing had become. The sense I got was that we have her story because she's still the only one talking. The main guy isn't talking. There's doubtless more to be told and presumably over time more will emerge. But anyone watching this 2-hour documentary will definitely come away with a much deeper appreciation of the true influential power of big data mining and the power to manipulate popular sentiment.

  We are direct eye witnesses to only a tiny portion of what we believe we know to be an accurate depiction of reality. EVERYTHING ELSE we receive is relayed through a channel that has some purpose for doing so.

- **Once Upon a Time in Hollywood...**
  Quentin Tarrantino

Urgent / 11

We were just talking recently, in the context of the idea of China rolling their own Internet operating system, how ridiculously improbable that really is. I used as an example the huge amount of trouble the entire industry had just getting TCP/IP stacks running solidly and correctly due to the extreme complexity and corner-cases of the evolving TCP/IP specification over time.

Well... the entire industry just got bitten by a set of 11 vulnerabilities found to affect VxWorks' TCP/IP stack… **which has been quietly embedded into more than 2 BILLION devices!**

Now, since VxWorks is not a common household name, we need to step back for a moment to understand what VxWorks is and why it matters. I've talked about so-called "embedded operating systems" in the past. A microwave oven will have an embedded operating system. All modern automobiles have at least one and probably several. The Amazon Kindle is based upon an embedded Linux kernel that's been stripped down for embedding. All of our consumer NAT routers will have one, as will commercial firewall devices. Certainly all modern printers are written on top of an embedded OS. And... somewhat more worrisomely... virtually all sophisticated IoT devices will have an embedded OS at their heart.

The #1 most popular and widely-used OS, with a 32 year history, is Wind River Systems VxWorks.

Wikipedia has the following to say about VxWorks:

> VxWorks is a real-time operating system (RTOS) developed as proprietary software by Wind River Systems, a wholly owned subsidiary of TPG Capital, US. First released in 1987, VxWorks is designed for use in embedded systems requiring real-time, deterministic performance and, in many cases, safety and security certification, for industries, such as aerospace and defense, medical devices, industrial equipment, robotics, energy, transportation, network infrastructure, automotive, and consumer electronics.
>
> VxWorks supports Intel architecture, POWER architecture, and ARM architectures. The RTOS can be used in multicore asymmetric multiprocessing (AMP), symmetric multiprocessing (SMP), and mixed modes and multi-OS (via Type 1 hypervisor) designs on 32- and 64-bit processors.
>
> VxWorks comes with the kernel, middleware, board support packages, Wind River Workbench development suite and complementary third-party software and hardware technologies. In its latest release, VxWorks 7, the RTOS has been re-engineered for modularity and upgradeability so the OS kernel is separate from middleware, applications and other packages. Scalability, security, safety, connectivity, and graphics have been improved to address Internet of Things (IoT) needs.

Under "Notable Uses" Wikipedia enumerates a few which is worth sharing to get a better sense for the popularity and broad sweep of this OS:

Spacecraft

- The Mars 2020 rover scheduled to launch in 2020
- The Mars Reconnaissance Orbiter
- The Mars Science Laboratory, also known as the Curiosity rover
- NASA Mars rovers (Sojourner, Spirit, Opportunity)
- The Deep Space Program Science Experiment (DSPSE) also known as Clementine (spacecraft)[33] Clementine launched in 1994 running VxWorks 5.1 on a MIPS-based CPU responsible for the Star Tracker and image processing algorithms. The use of a commercial RTOS on board a spacecraft was considered experimental at the time[citation needed]
- Phoenix Mars lander
- The Deep Impact space probe
- The Mars Pathfinder mission
- The SpaceX Dragon
- NASA's Juno space probe sent to Jupiter

Aircraft

- AgustaWestland Project Zero[39]
- Northrop Grumman X-47B Unmanned Combat Air System
- Airbus A400M Airlifter
- BAE Systems Tornado Advanced Radar Display Information System (TARDIS) used in the Tornado GR4 aircraft for the U.K. Royal Air Force
- Lockheed Martin RQ-170 Sentinel UAV

Space telescopes

- Fermi Gamma-ray Space Telescope(FGST)
- James Webb Space Telescope (in development)

Others

- European Geostationary Navigation Overlay System (EGNOS)[46]
- TacNet Tracker, Sandia National Laboratory’s rugged handheld communication device[47]
- BAE Systems SCC500TM series of infrared camera cores[48]
- Barco CDMS-3000 next generation control display and management system[49]

Automotive

- Toshiba TMPV75 Series image recognition SoCs for advanced driver assistance systems (ADAS)
- Bosch Motor Sports race car telemetry system
- Clarion AX1 Android-based automotive In-Vehicle Infotainment system (IVI)
- Hyundai Mobis IVI system
- Magneti Marelli's telemetry logger and GENIVI®-compliant infotainment system[54]
- BMW iDrive system after 2008
- Siemens VDO automotive navigation systems
- Most of Renault Trucks T, K and C trucks' electronic control units.
- European Volkswagen RNS 510 navigation systems.

Consumer electronics

- Apple Airport Extreme
- Drobo data storage robot
- Honda robot ASIMO
- Linksys WRT54G wireless routers (versions 5.0 and later)
- MacroSystem Casablanca-2 digital video editor (Avio, Kron, Prestige, Claro, Renommee, Solitaire)
- Motorola's DCT2500 interactive digital set-top box
- Mobile Technika MobbyTalk and MobbyTalk253 phones
- ReplayTV home digital video recorder

Industrial robots

- ABB industrial robots
- The C5G robotic project by Comau
- KUKA industrial robots
- Stäubli industrial robots
- Yaskawa Electric Corporation's industrial robots
- Comau Robotics SMART5 industrial robot

Test and Measurement

- Teledyne LeCroy WaveRunner LT, WaveRunner2LT and WavePro 900 oscilloscope series
- Hexagon Metrology GLOBAL Silver coordinate measuring machine (CMM)

Transportation

- FITSCO Automatic Train Protection (ATP)system[69]
- Bombardier HMI410 Train Information System[70]

Controllers

- Bachmann M1 Controller System
- Invensys Foxboro PAC System
- National Instruments CompactRIO 901x, 902x 907x controllers
- Mitsubishi's C controller
- The Experimental Physics and Industrial Control System (EPICS)
- Bosch Rexroth Industrial Tightening Control Systems
- MCE iBox elevator controller

Storage systems

- External RAID controllers designed by the LSI Corporation prior to 2011, now designed by NetApp, and used in IBM System Storage's DS3000 and DS4000 (formerly FAStT)
- Fujitsu ETERNUS DX S3 family of unified data storage arrays

Imaging

- Toshiba eBridge based range of photocopiers

Others

- GrandMA Full-Size and Light Console by MA Lighting

Medical

- Varian Medical Systems Truebeam - a radiotherapy device for treating cancer
- Olympus Corporation's surgical generato
- BD Biosciences FACSCount HIV/AIDS Monitoring System
- Fedegari Autoclavi S.p.A. Thema4 process controller
- Sirona Dental Systems: CEREC extraoral X-ray CAD/CAM systems
- General Electric Healthcare: CT and MRI scanners.
- Carl Zeiss Meditec: Humphrey Field Analyzer HFA-II Series

Networking and communication infrastructure

- Arkoon Network Security appliances
- Ubee Interactive's AirWalk EdgePoint
- Kontron's ACTA processor boards
- QQTechnologies's QQSG
- A significant portion of Huawei's telecoms equipment uses VxWorks
- BroadLight's GPON/PON products
- Shiron Satellite Communications' InterSKY
- Sky Pilot's SkyGateway, SkyExtender and SkyControl
- EtherRaptor-1010 by Raptor Network Technology
- CPG-3000 and CPX-5000 routers from Siemens
- Nokia Solutions and Networks FlexiPacket series microwave engineering product
- Acme Packet Net-Net series of Session Border Controllers
- Alcatel-Lucent IP Touch 40x8 IP Deskphones
- Avaya ERS 8600
- Avaya IP400 Office
- Cisco CSS platform
- Cisco ONS platform
- Ciena Common Photonic Layer
- Dell PowerConnect switches that are 'powered by' Broadcom, except latest PCT8100 which runs on Linux platform
- Ericsson SmartEdge routers (SEOS 11 run NetBSD 3.0 and VxWorks for Broadcom BCM1480 version 5.5.1 kernel version 2.6)
- Hewlett Packard HP 9000 Superdome Guardian Service Processor
- Hirschmann EAGLE20 Industrial Firewall
- HughesNet/Direcway satellite internet modems
- Mitel Networks' MiVoice Business (formerly Mitel Communications Director (MCD)), 3300 ICP Media Gateways and SX-200 and SX-200 ICP.
- Motorola Solutions MCD5000 IP Deskset System
- Motorola SB5100 cable modem
- Motorola Cable Headend Equipment including SEM, NC, OM and other lines
- Nortel Passport
- Radware OnDemand Switches
- Samsung DCS and OfficeServ series PBX
- SonicWALL firewalls
- Thuraya SO-2510 satellite phone and ThurayaModule
- Radvision 3G communications equipment
- 3com NBX phone systems
- Zhone Technologies access systems

In short... it's almost easier to answer the question "what DOESN'T use VxWorks"??

And so now, after a 32-year, relatively blemish-free track record, the entire world has just learned of 11 very serious vulnerabilities -- 6 which are remote code execution capable -- in VxWorks.

ARMIS, Inc. found and responsibly reported and disclosed their alarming findings to VxWorks, which has, of course, fixed all of these known problems. The trouble, of course, is that, some of the affected devices are, quite literally, on Mars! The good news is, those devices are not also on the Internet. But the same cannot be said for the 200 million other devices which are!

Armis explains what they found:

URGENT/11 is a set of 11 vulnerabilities found to affect VxWorks' TCP/IP stack (IPnet), used by the versions of VxWorks. Six of the vulnerabilities are classified as critical and enable Remote Code Execution (RCE). The remaining vulnerabilities are classified as denial of service, information leaks or logical flaws. As each vulnerability affects a different part of the network stack, it impacts a different set of VxWorks versions. As a group, URGENT/11 affects the VxWorks' versions described above with at least one RCE vulnerability affecting each version. The wide range of affected versions spanning over the last 13 years is a rare occurrence in the cyber arena and is the result of VxWorks' relative obscurity in the research community. This timespan might be even longer, as according to Wind River, three of the vulnerabilities were already existent in IPnet when it acquired the stack from Interpeak in 2006.

URGENT/11 are the most severe vulnerabilities found in VxWorks to date, which has suffered from only 13 public CVEs in its 32-year history. URGENT/11 is a unique group of vulnerabilities that allow attackers to circumvent NAT and firewalls and take control over devices remotely via the TCP/IP stack undetected, with no user interaction required. This is due to the vulnerabilities' low level position inside the TCP/IP stack, which enables attacks to be viewed as legitimate network activity. Such vulnerabilities do not require any adaptations for the various devices using the network stack, making them exceptionally easy to spread. In most operating systems, such fundamental vulnerabilities in the crucial networking stacks have become extinct, after years of scrutiny unravelled and mitigated such flaws.

URGENT/11 is comprised of 11 vulnerabilities, separated to two classes of severity: There Six Critical vulnerabilities, allowing remote-code-execution and five vulnerabilities leading to denial of service, information leak or certain logical flaws.

There's a stack overflow in the parsing of IPv4 options (CVE-2019-12256)

This vulnerability can be triggered by a specially crafted IP packet sent to the target device, even as a broadcast or multicast packet. It does not require any specific application or configuration to be running on the device, and it affects any device running VxWorks v6.9.4 or above with a network connection. The vulnerability causes a stack overflow in the handling of IP options in the IPv4 header, making it easy to reach Remote Code Execution by it.

There are four memory corruption vulnerabilities stemming from erroneous handling of TCP's Urgent Pointer field (CVE-2019-12255, CVE-2019-12260, CVE-2019-12261, CVE-2019-12263)

The four vulnerabilities all stem from erroneous handling of TCP's Urgent Pointer field. This is an esoteric TCP field that is rarely used in modern applications. An attacker can trigger the erroneous handling of this field by either directly connecting to an open TCP port on the target device, or by hijacking an outbound TCP connection originating from the target device. Once triggered, these vulnerabilities will cause the application on the target device to receive more bytes than expected from the system's recv() function, leading to a memory corruption of either the stack, the heap, or of global data section variables — depending on which buffer was passed to the recv() function. This means an attacker can probe the various TCP connections of the target device (either inbound or outbound) and attack the application that is the easiest to exploit.

Since the Urgent Pointer field is a built-in feature of TCP, routers, NATs and even firewalls that stand between the target device and the attacker are likely to transfer it intact. This means that even a TCP connection that travels from a vulnerable device to the Internet through multiple routers, NAT and firewall devices can still be hijacked by an attacker on the Internet and used to trigger the vulnerability. This can enable an attacker to not only take over vulnerable devices that are otherwise secured within internal networks, but also penetrate these networks via this path.

The four variants of this type of attack affecting different VxWorks versions:

- TCP Urgent Pointer = 0 leads to integer underflow (CVE-2019-12255) affects VxWorks versions 6.5 to 6.9.3.
- TCP Urgent Pointer state confusion caused by malformed TCP AO option (CVE-2019-12260) affects VxWorks versions 6.9.4 and above.
- TCP Urgent Pointer state confusion due to race condition (CVE-2019-12263) affects VxWorks versions 6.6 and above.
- TCP Urgent Pointer state confusion during connect to a remote host (CVE-2019-12261) affect VxWorks versions 6.7 and above.

There is also a heap overflow in DHCP Offer/ACK parsing in ipdhcpc (CVE-2019-12257)

This vulnerability is a heap overflow vulnerability triggered when a vulnerable device parses a specially crafted DHCP response packets. These packets are parsed by ipdhcpc, VxWorks' built-in DHCP client, when it attempts to acquire an IP address from a DHCP server. An attacker located in the same subnet as the target device can wait for it to send a DHCP request, and reply quickly with the specially crafted DHCP response. In this scenario the target device waiting for a response from the original DHCP server of the network will be easily fooled by the attacker, and parse the crafted DHCP response message. This would lead to a heap overflow with attacker controlled data that can result in remote-code-execution. This vulnerability affects VxWorks versions from 6.5 to 6.9.3.

... and it goes on and on like that.

Armis researchers made all of this public yesterday, on July 29th and will be detailing this in greater depth during their presentation at Black Hat next week, on August 8, in Las Vegas.

Wind River spokesperson told ZDNet that "These vulnerabilities are not unique to Wind River software. The IPnet stack was acquired by Wind River through its acquisition of Interpeak in 2006. Prior to the acquisition, the stack was broadly licensed to and deployed by a number of other RTOS vendors." Uh huh.

If you have SonicWall and DELL PowerConnect switches you should definitely check for updated firmware immediately. Also, Linksys WRT54G wireless routers (versions 5.0 and later) or a Drobo exposed to the Internet.

~30~