



2020-21
Zombie Apocalypse
and
Dental Office Security
(available for download!)





ADULT LANGUAGE

TONIGHT'S TOPICS (in under an hour):

- ♦ WHAT I READ (you should, too!)
- ♦ NARROW DOWN GOOGLE SEARCH RESULTS
- ♦ PASSWORD MANAGER
- ♦ UPDATE ALL YOUR CRAP!
- ♦ GONE PHISHING
- ♦ FIREWALL – Do you even have one??

♦ INCREASE SECURITY BY THIS SIMPLE STEP!

- ♦ KREB'S RULES
- ♦ CREATE SHORTCUTS
- ♦ BACKUPS
- ♦ PENETRATION TESTING:
grc.com, Nessus, Kali Linux

TONIGHT IS A
COMBINATION OF.....

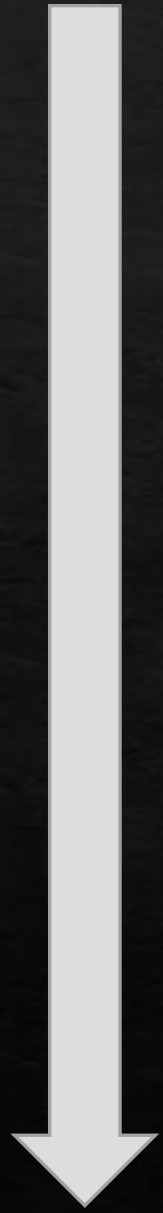


DEBBIE



DOWNER

G
e
e
k
i
e
r



My frequent IT news sources (make them **YOURS!**)

- ♦ Kim Komando (speaks in English, not geek!): <https://www.komando.com/>
- ♦ PcMagazine: <https://www.pcmag.com/categories/security>
- ♦ ZDNet: <https://www.zdnet.com/topic/security/>
- ♦ iPhone: News and Google News APPS
- ♦ Krebs on Security: <https://krebsonsecurity.com/>
- ♦ Ars Technica, TechRepublic, CNET, others: <https://arstechnica.com/>
<https://www.techrepublic.com/> <https://www.cnet.com/>

KIMKOMANDO® 400+ radio stations in the USA and on demand


WATCH LISTEN GET NEWSLETTERS BE A CALLER

NEWS HOW-TOS VIDEOS SHOPPING REVIEWS KIM'S SHOW FIND A STATION PODCASTS COMMUNITY Search ...


Security & privacy

Learn how to stay safe and protected against malware, data breaches and online scams.


Filter by: SECURITY & PRIVACY




Data breach alert: 3 million customer credit card details exposed




FBI: 4 new ways fraudsters are trying to steal your money online




Windows alert: Fake Office updates trick you into downloading malware



Fake customer support scam is wiping out bank accounts – don't fall for it!



Check this list! Android phones Google says are in danger of being hacked



Have an older iPhone or Mac? Don't miss this security warning

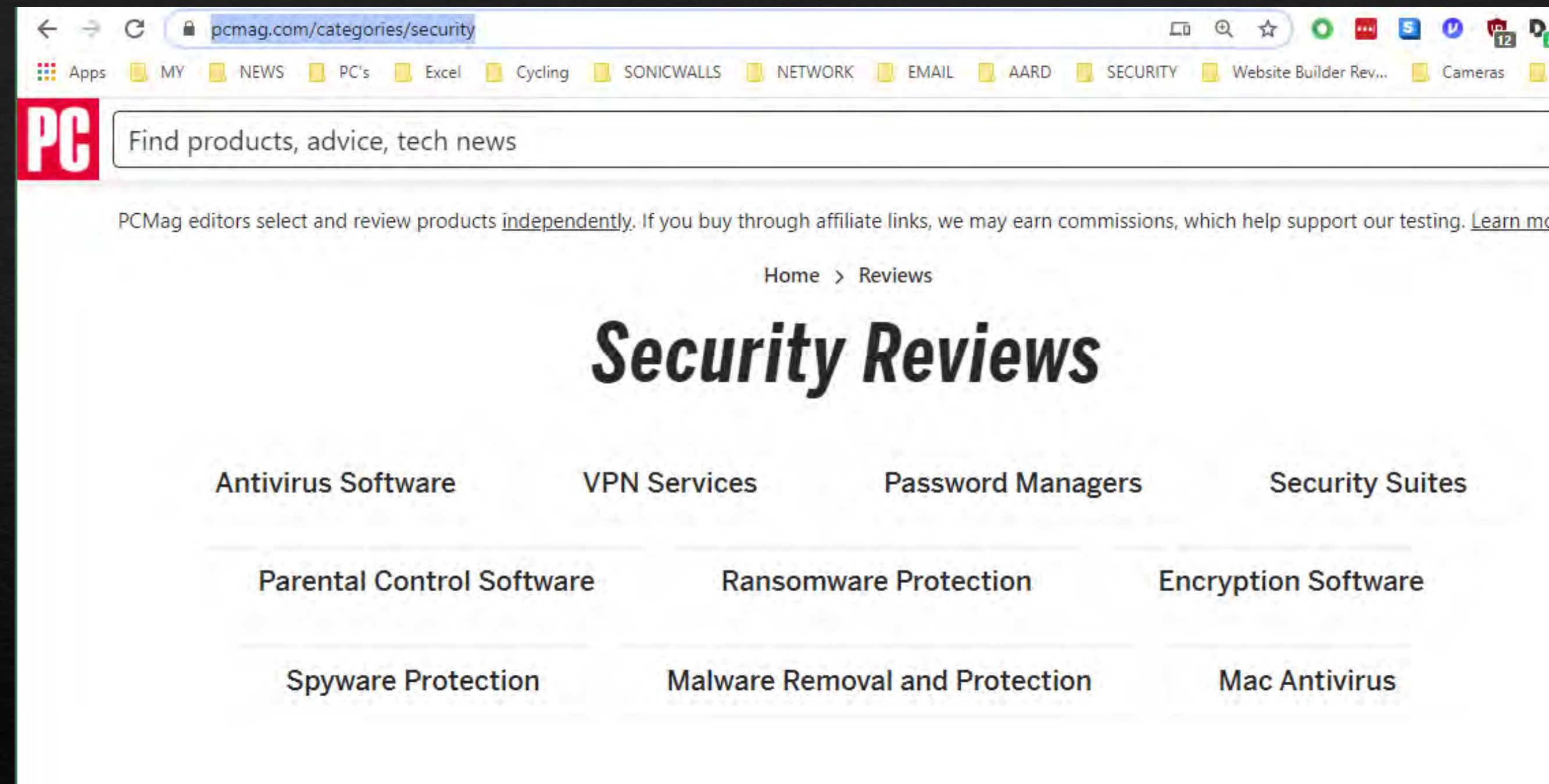
Kim Komando speaks English!

<https://www.komando.com/category/news/security-privacy/>

You may see her column in Fox News, CNN, USA Today, etc.

<https://www.pcmag.com/categories/security>

They (pcmag, zdnet, cnet -
where I first go for answers)
also have daily newsletters I
subscribe to...



CURRENT HEADLINES (today, groan)...

 MUST READ: [Everything you need to know about the Microsoft Exchange Server hack](#)

These two unusual versions of ransomware tell us a lot about how attacks are evolving

Researchers detail two new types of ransomware - AlumniLocker and Humble. Both are new and have very different ways of doing things, demonstrating the diversity in a space attackers are keen to get involved in.

The ransomware is delivered to victims via a **malicious PDF attachment** claiming to be an invoice that is distributed in **phishing emails**. The PDF contains a link that will extract a ZIP archive that runs a PowerShell script to drop the payload and execute the ransomware.

Like an increasing number of ransomware campaigns, the attackers behind AlumniLocker threaten to publish data stolen from the network of their victim if they're not paid within 48 hours – although given the ransom demand is so large, victims may decide it's too much to pay.

Organisations can help protect themselves from ransomware attacks with cybersecurity procedures including applying patches and using multi-factor authentication.

HINT: WHAT IS TOMORROW??



Do you have Microsoft
Exchange Email Server?

(some of my colleagues do!)

KrebsOnSecurity

In-depth security news and investigation



ADVERTISING/SPEAKING

Latest Warnings / The Coming Storm / Time to Patch — 47 comments

05 At Least 30,000 U.S. Organizations Newly MAR 21 Hacked Via Holes in Microsoft's Email Software

At least 30,000 organizations across the United States — including a significant number of small businesses, towns, cities and local governments — have over the past few days been hacked by an unusually aggressive Chinese cyber espionage unit that's focused on stealing email from victim organizations, multiple sources tell KrebsOnSecurity. The espionage group is exploiting four newly-discovered flaws in **Microsoft Exchange Server** email software, and has seeded hundreds of thousands of victim organizations worldwide with tools that give the attackers total, remote control over affected systems.

FINALLY, YOU
CAN BE P

BEYOND
IDENTITY

Researchers Find 3 New Malware Strains Used by SolarWinds Hackers

March 05, 2021 Ravie Lakshmanan

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	F2	1F	D7	0B	AB	6C	8A	B4	97	FA	00	76	18	68	05	5B	ò × «lŠ'—ú v h [
00000010	36	62	65	38	39	37	32	33	37	37	30	32	34	36	63	32	6be89723770246c2
00000020	61	34	36	65	33	34	32	63	35	34	66	63	65	65	37	34	a46e342c54fcee74
00000030	7C	35	2D	31	35	7C	30	7C	30	7C	54	57	39	36	61	57	5-15 0 0 IW96aW
00000040	78	73	59	53	38	31	4C	6A	41	67	4B	46	64	70	62	6D	xsYS81LjAgKFdpbm
00000050	52	76	64	33	4D	67	54	6C	51	67	4D	54	41	75	4D	44	Rvd3MgTlQgMTAuMD
00000060	73	67	56	32	6C	75	4E	6A	51	37	49	48	67	32	4E	44	sgV21uNjQ7IHg2ND
00000070	73	67	63	6E	59	36	4E	7A	55	75	4D	43	6B	67	52	32	sgcnY6NaUuMCkgR2
00000080	56	6A	61	32	38	76	4D	6A	41	78	4D	44	41	78	4D	44	Vja28vMjAxMDAxMD
00000090	45	67	52	6D	6C	79	5A	57	5A	76	65	43	38	33	4E	53	EgRmlyZWZveC83NS
000000A0	34	77	0E	0E	0E	0E	0E	0E	0E	0E	0E	0E	0E	0E	0E	0E	4w
Pseudo-randomly generated data (using the Go crypto/rand package)																	
MD5 hash of the current date/time value obtained by calling time.Now() and time.Time.String()																	
Range used by a custom PRNG																	
Decoy traffic activation value (if set to 1, GoldMax issues decoy HTTP requests)																	
GoldMax activation date represented as an ASCII Unix/Epoch time (e.g., "1609459200" for January 1, 2021 12:00:00 AM), '0' is interpreted as always active																	
Base64 encoded version of the following User-Agent string: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0																	
Padding bytes added to ensure the total size of the structure is a multiple of 16 (AES block																	

FireEye and Microsoft on Thursday said they discovered three more malware strains in connection with the SolarWinds supply-chain attack, including a "sophisticated second-stage backdoor," as the

Popular This Week



New Chrome 0-day Bug
Under Active Attacks –
Update Your Browser ASAP!



SolarWinds Blames Intern
for 'solarwinds123'
Password Lapse



URGENT – 4 Actively
Exploited 0-Day Flaws Found
in Microsoft Exchange



Extortion Gang Breaches
Cybersecurity Firm Qualys
Using Accellion Exploit



Hackers Now Hiding
ObliqueRAT Payload in
Images to Evade Detection

I was contacted
by a DDS who
has SolarWinds
on his system...

[Application Security](#) , [Cybercrime](#) , [Fraud Management & Cybercrime](#)

Severe SolarWinds Hacking: 250 Organizations Affected?

Investigators Reportedly Finding Many More Victims Suffered Serious Intrusions

solarwinds123
????

Microsoft: We've open-sourced this tool we used to hunt for code by SolarWinds hackers

ZDNet · Feb 26



Former SolarWinds CEO blames intern for 'solarwinds123' password leak

CNN · Feb 26



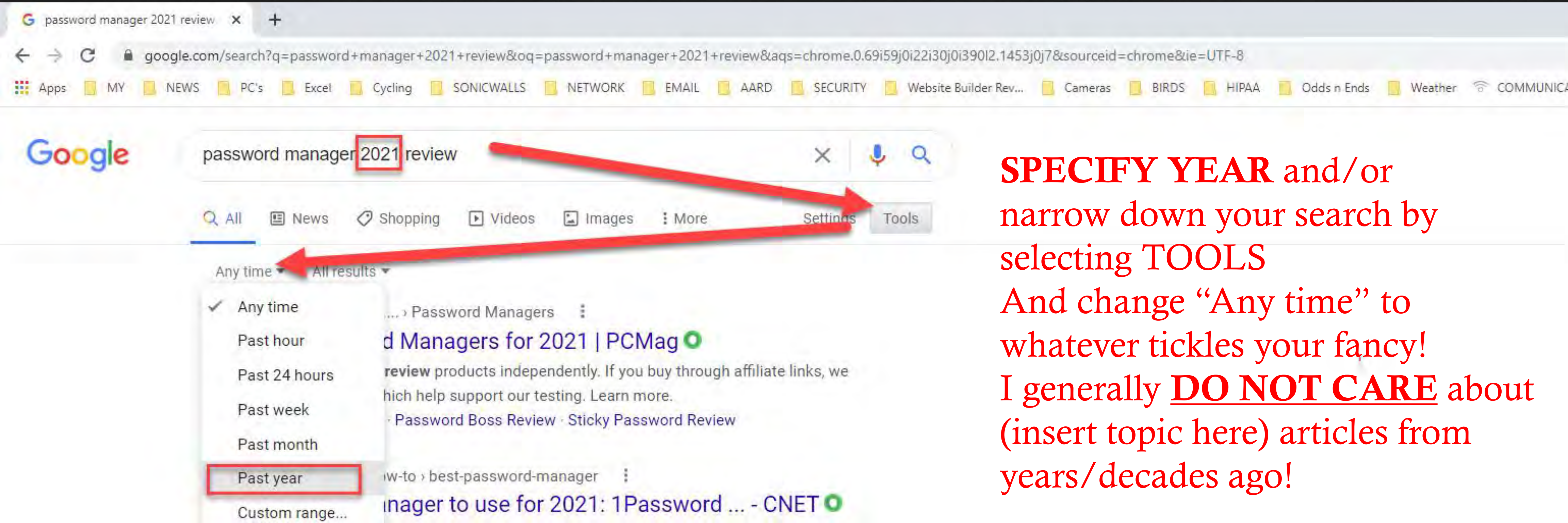
SolarWinds blaming intern is symptom of "security failures"

SC Magazine · 5 days ago



GOOGLE – tweak(s)

◆(or any other search engine – MAYBE)



SPECIFY YEAR and/or narrow down your search by selecting **TOOLS**
And change “Any time” to whatever tickles your fancy!
I generally **DO NOT CARE** about (insert topic here) articles from years/decades ago!

Google

password manager 2021 review

All News Shopping Videos Images More Settings Tools

About 488,000,000 results (0.74 seconds)

<https://www.pcmag.com> › ... › Password Managers

The Best Password Managers for 2021 | PCMag

PCMag editors select and review products independently. If you buy through affiliate links, we may earn commissions, which help support our testing. Learn more.

[The Best Free Password...](#) · [Password Boss Review](#) · [Sticky Password Review](#)

<https://www.cnet.com> › how-to › best-password-manager

Best password manager to use for 2021: 1Password ... - CNET

Feb 16, 2021 — CNET's Apple Report newsletter delivers news, reviews and advice on iPhones, iPads, Macs and software. Yes, I also want to receive the CNET ...



***GET A PASSWORD
MANAGER!***

*Use PHRASES,
not WORDS!!!!!!*



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

[CLOUD](#)[SMALL BUSINESS TV](#)[SECURITY](#)[AI](#)[MORE ▾](#)[NEWSLETTERS](#)[ALL WRITERS](#)

MUST READ: [A little known feature of your iPhone is about to completely change how your doctor talks to you](#)

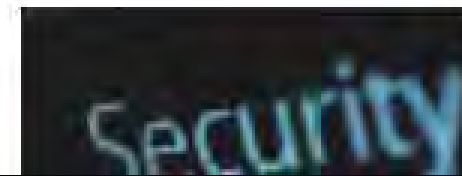
FBI recommends passphrases over password complexity

Longer passwords, even consisting of simpler words or constructs, are better than short passwords with special characters.

MORE FROM CATALIN CIMPANU

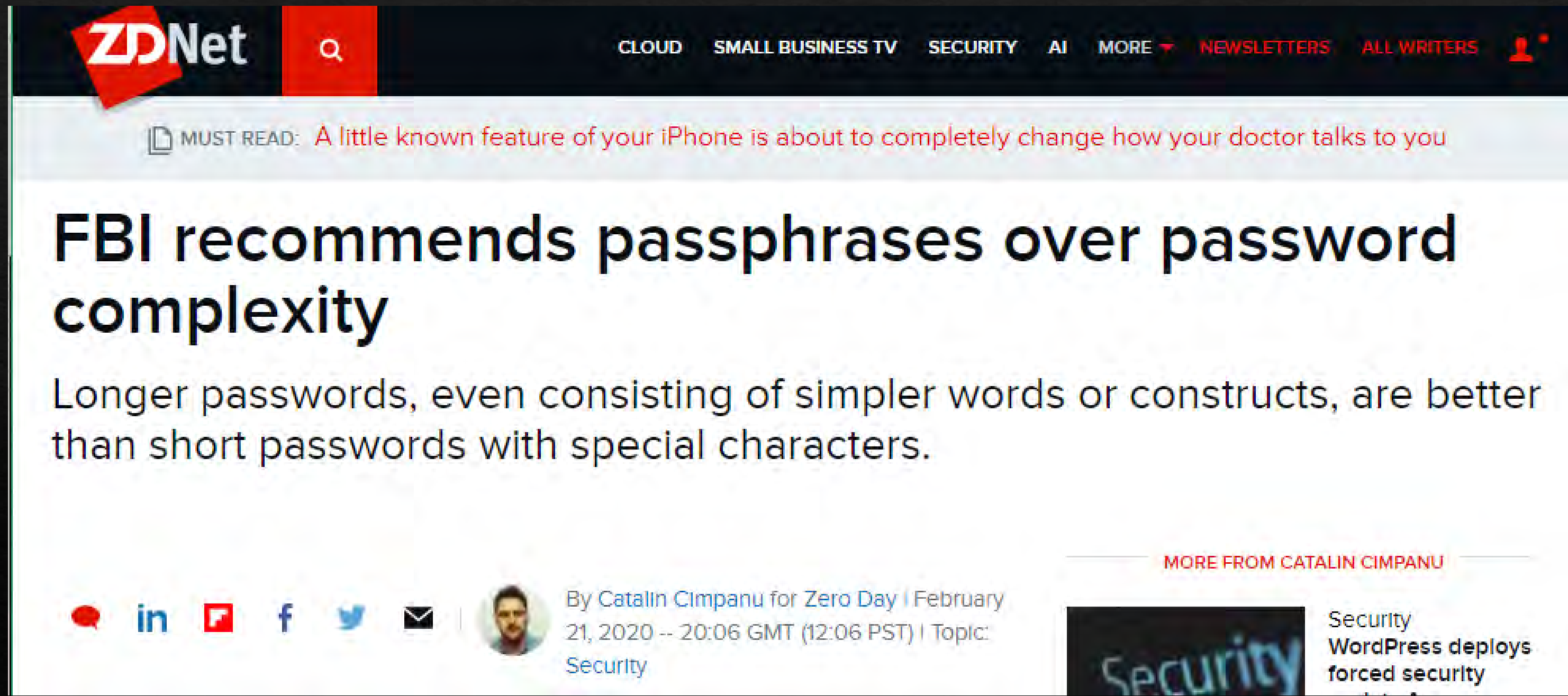


By [Catalin Cimpanu](#) for Zero Day | February 21, 2020 -- 20:06 GMT (12:06 PST) | Topic: [Security](#)



Security
[WordPress deploys forced security](#)

"This involves **combining multiple words** into a long string of at least 15 characters," it added. "The extra length of a passphrase makes it harder to crack while also making it easier for you to remember."



The screenshot shows the Zero Day Net website header with navigation links for CLOUD, SMALL BUSINESS TV, SECURITY, AI, MORE, NEWSLETTERS, and ALL WRITERS. A red search bar is also present. Below the header, a 'MUST READ' banner features a link about an iPhone feature. The main article title is 'FBI recommends passphrases over password complexity'. The sub-headline states: 'Longer passwords, even consisting of simpler words or constructs, are better than short passwords with special characters.' The article is by Catalin Cimpanu for Zero Day, dated February 21, 2020. Social media sharing icons for Reddit, LinkedIn, YouTube, Facebook, Twitter, and Email are provided. A 'MORE FROM CATALIN CIMPANU' section is visible at the bottom right, featuring a thumbnail for a security article about WordPress.

Zero Day Net 🔍

CLOUD SMALL BUSINESS TV SECURITY AI MORE NEWSLETTERS ALL WRITERS

MUST READ: A little known feature of your iPhone is about to completely change how your doctor talks to you

FBI recommends passphrases over password complexity

Longer passwords, even consisting of simpler words or constructs, are better than short passwords with special characters.

By Catalin Cimpanu for Zero Day | February 21, 2020 -- 20:06 GMT (12:06 PST) | Topic: Security

More from Catalin Cimpanu

Security
WordPress deploys forced security

What rattles thru my brain:
"Kittyhawk Golf Center" -- that's 21 characters
"Kitty Hawk Golf Center" – 22 characters!
"Kitty Hawk CVA-63 Golf Center"

I use golf courses, zip codes, hobbies, birds, streets I grew up near, schools, obscenities, **SPACES (if allowed)**, special characters, the list goes on!!

AND THEN MIX 'EM UP!
AND YOUR PASSWORD MANAGER REMEMBERS THEM!

A COUPLE PHRASES...(what if I MIXED the words?)

281 W Lane Ave, Columbus, OH 43210

The Ohio State University, Address



500 S State St, Ann Arbor, MI 48109

University of Michigan, Address



Don't
be
these
idiots

<https://www.cybersecurity-insiders.com/password-123...>

✓ Password 123456 was hacked over 23 million times ...

Password 123456 was hacked over 23 million times worldwide. Posted By Naveen Goud. 691. National Cyber Security Center(NCSC) said that ...

<https://it.slashdot.org/story/more-than-23-million-pe...>

✓ More Than 23 Million People Use the Password '123456' ...

Apr 21, 2019 — So what are the top ten most-frequently used passwords? 123456; 123456789; qwerty; password; 111111; 12345678; abc123; 1234567 ...

<https://www.customonline.com/tech-insights/are-yo...>

✓ Using 123456 as password | Custom Computer Specialists

Using 123456 as your password? It's the most commonly used password. No wonder cyber-intruders have easy access to personal information.

<https://www.techrepublic.com/topic/security/>

<https://www.techrepublic.com/topic/security/>

✓ "123456" tops list of most common passwords for 2020 ...

Nov 18, 2020 — Passwords that lead to data breaches. Among the 200 most commonly used passwords this year, "123456" took first place, used by more than 2.5 ...

<https://www.cnn.com/common-passwords-2020-trnd>

✓ Yes, people are still using '123456' and 'password' as ... - CNN

Nov 19, 2020 — Despite several reminders from cybersecurity experts, NordPass says that after comparing the list of the most common passwords of 2020 to that ...

Images for password 123456

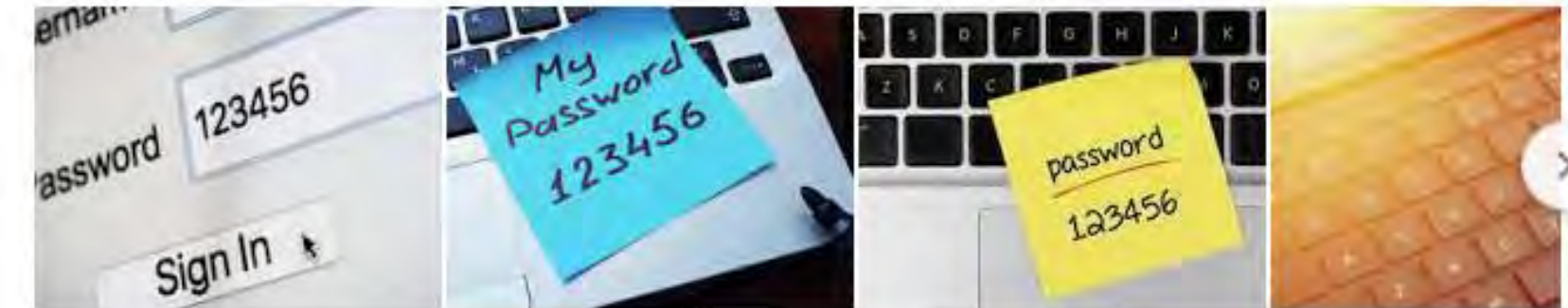
cyber security

every 142

cybersecurity

common passwords

splashdata



Report images

Is EVERY workstation and server in your office using a
DIFFERENT password???

Hmmmm???

Update **ALL** your crap!

Program: “Advanced IP Scanner”

(Scan done on a quiet Saturday)
and THANK YOU !!!!!

What is ‘idrac’ doing here??!!

Advanced IP Scanner

File View Settings Help

Stop || IP C

192.168.17.1-192.168.17.254

Results Favorites

Status	Name	IP	Manufacturer
	192.168.17.11	192.168.17.11	Sonicwall
	FrontRv2	192.168.17.86	
	m6700	192.168.17.94	Dell Inc.
	192.168.17.95	192.168.17.95	Dell Inc.
>	192.168.17.98	192.168.17.98	NETGEAR
>	m7740	192.168.17.103	
>	IQEYE014751	192.168.17.141	IQinVision
>	hp527	192.168.17.224	Hewlett Packard
	idrac	192.168.17.240	Dell Inc.

System
root , Admin

Properties Service Module Job Queue

Summary Details System Inventory

System Summary



Server Health

- ✓ Batteries
- ✓ Voltages
- ✓ Intrusion
- ✓ Power Supplies
- ✓ Removable Flash Media
- ✓ Temperatures

Virtual Console Preview

This feature requires an iDRAC Enterprise license.
For more details on how to obtain a license, visit
[License Page](#).

- Overview
- Server
 - Logs
 - Power / Thermal
 - Alerts
 - Setup
 - Troubleshooting
 - Licenses
 - Intrusion
 - + iDRAC Settings
 - + Hardware
 - + Storage
 - + Host OS

And 'idrac' no longer
showing up in my IP Scan!

Advanced IP Scanner

FileViewSettingsHelp









Stop

IP

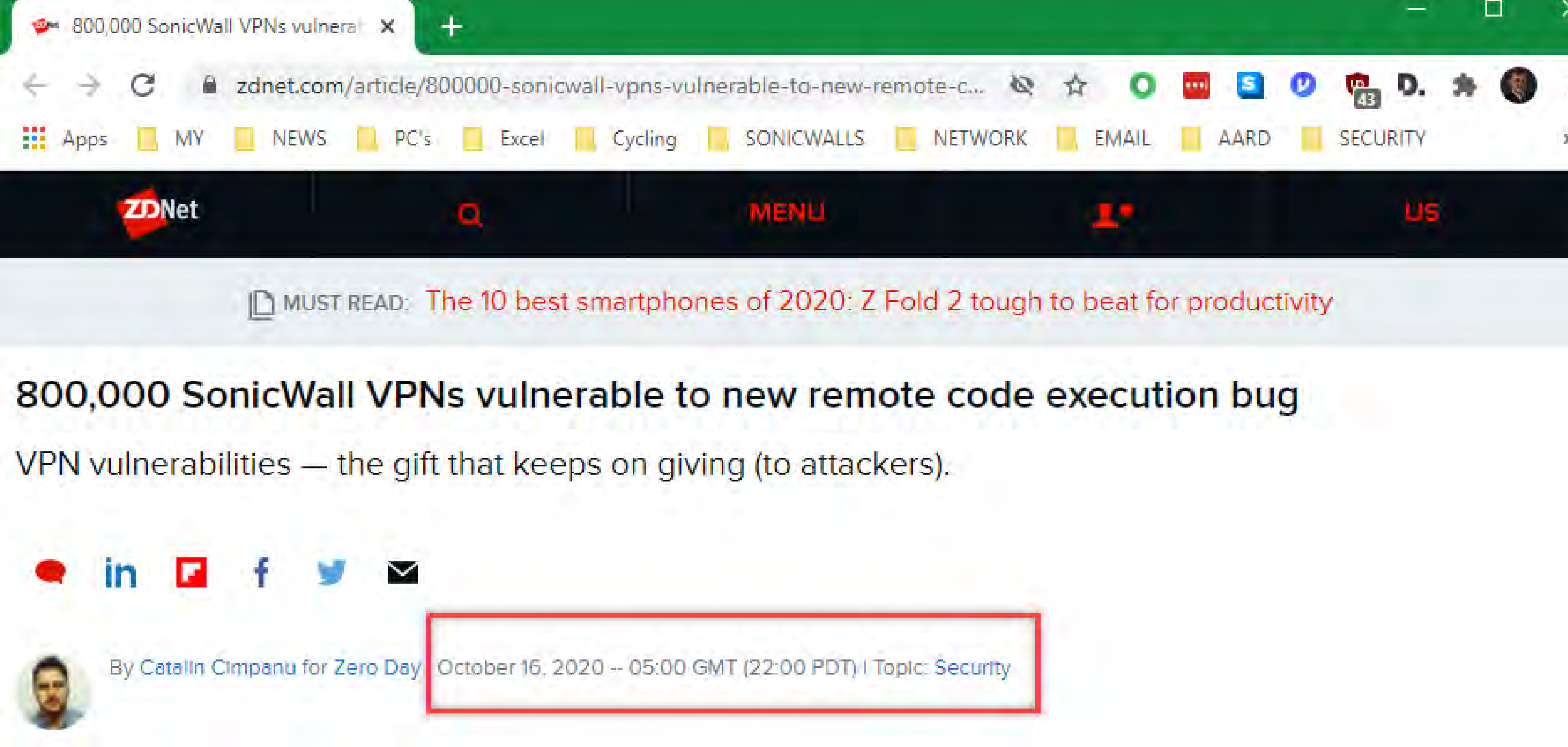
C

192.168.17.1-192.168.17.254

ResultsFavorites

Status	Name	IP	Manufacturer
	192.168.17.11	192.168.17.11	Sonicwall
	FrontRv2	192.168.17.86	
	m6700	192.168.17.94	Dell Inc.
	192.168.17.95	192.168.17.95	Dell Inc.
> 	192.168.17.98	192.168.17.98	NETGEAR
> 	m7740	192.168.17.103	
> 	IQEYE014751	192.168.17.141	IQinVision
	hp527	192.168.17.224	Hewlett Packard

99%, 8 alive, 11 dead, 235 unknown



I mentioned
‘update **ALL**
your crap!’”

And I
use Sonicwalls!

(and applied
the patch!)



MUST READ: [The 10 best smartphones of 2020: Z Fold 2 tough to beat for productivity](#)

Update now: Cisco warns over 25 high-impact flaws in its IOS and IOS XE software

Cisco urges customers using IOS and IOS XE devices and software to apply updates for dozens of high-severity vulnerabilities.

RANSOMWARE

Health & Fitness

Data Hack Impacts Local Patients

Patients may soon receive letters from Froedtert & the Medical College of Wisconsin Community Physicians, Inc.

By Rebecca Collett, Patch Staff 

Oct 14, 2020 9:40 am CT



Yet another
hospital
hacked...

To: Mark Benavides

Thu 10/15/2020 6:14 AM

This major criminal hacking group just switched to ransomware attacks

A newly detailed financial cyber crime group has been conducting attacks around the world since 2016 - but now they've switched to ransomware because it's the biggest and easiest pay day.

Read in ZDNet: <https://apple.news/A4NisNzVkSj2nNS5pojEicA>

Shared from [Apple News](#)

Barnes & Noble hit by cyberattack that exposed customer data

By [Lawrence Abrams](#)

October 14, 2020

11:25 PM

0



U.S. Bookstore giant Barnes & Noble has disclosed that they were victims of a cyberattack that may have exposed customers' data.

CHANGE
YOUR
PASSWORD(s)!
(every 90 days??)



Bitdefender Total Security



Data breach alert for Barnes & Noble



A security incident was reported for mail.barnesandnoble.com. Barnes & Noble Cyberattack May Have Exposed Personal Information of Shoppers. The attack did more than cripple Barnes & Noble corporate network. According to a notice sent to customers, the security incident may have exposed email addresses, billing, shipping information and telephone numbers of shoppers. CHECK IF YOU WERE AFFECTED!

Read more [here](#)

Protect yourself



To Mark Benavides

Sat 10/10/2020 6:20 AM

Hackers Share Fairfax County Schools Employees' SSNs Online

Hackers are sharing more private information after hacking a Virginia public school system's computer system.

Read in NBC Washington: <https://apple.news/ASCzImmeHSMqjgRaCCMeJ1Q>

threatpost.com › Malware ▾

Las Vegas Students' Personal Data Leaked, Post ... - Threatpost

Sep 29, 2020 — Personal information for students in the Clark County School District, which ... after school began online, on August 27, it found many of the school's files to be ... When Threatpost reached out to Emsisoft for more details on the data cache, ... a similar attack in July on the Athens school district in Texas led to ...

A researcher said he discovered an open data cache with names, grades, birthdates and more, after the Clark County School District refused to pay the ransom.



To Mark Benavides

Mon 10/12/2020 6:01 AM

North American Governments Hit Hardest by Rise in Ransomware Attacks

Ransomware is out of control in 2020, and those most likely hit by an attack are governments and small businesses that are ill-equipped to protect themselves.

Read in PCMag: <https://apple.news/AtCR7D4HzQpiYR6fdqGsqHQ>

Shared from [Apple News](#)

How are we most likely going to catch ransomware?

KEY!



most likely way to get ransomware



All

News

Videos

Images

Shopping

More

Settings

Tools

About 87,400,000 results (0.62 seconds)

These are the four most common ways ransomware infects its victims.

1. Phishing Emails. ...
2. Remote Desktop Protocol. ... **PORT 3389**
3. Drive-By Downloads From a Compromised Website. ...
4. USB and Removable Media.

Aug 9, 2018

www.itproportal.com › features › the-four-most-popula... ▼

The four most popular methods hackers use to spread ...

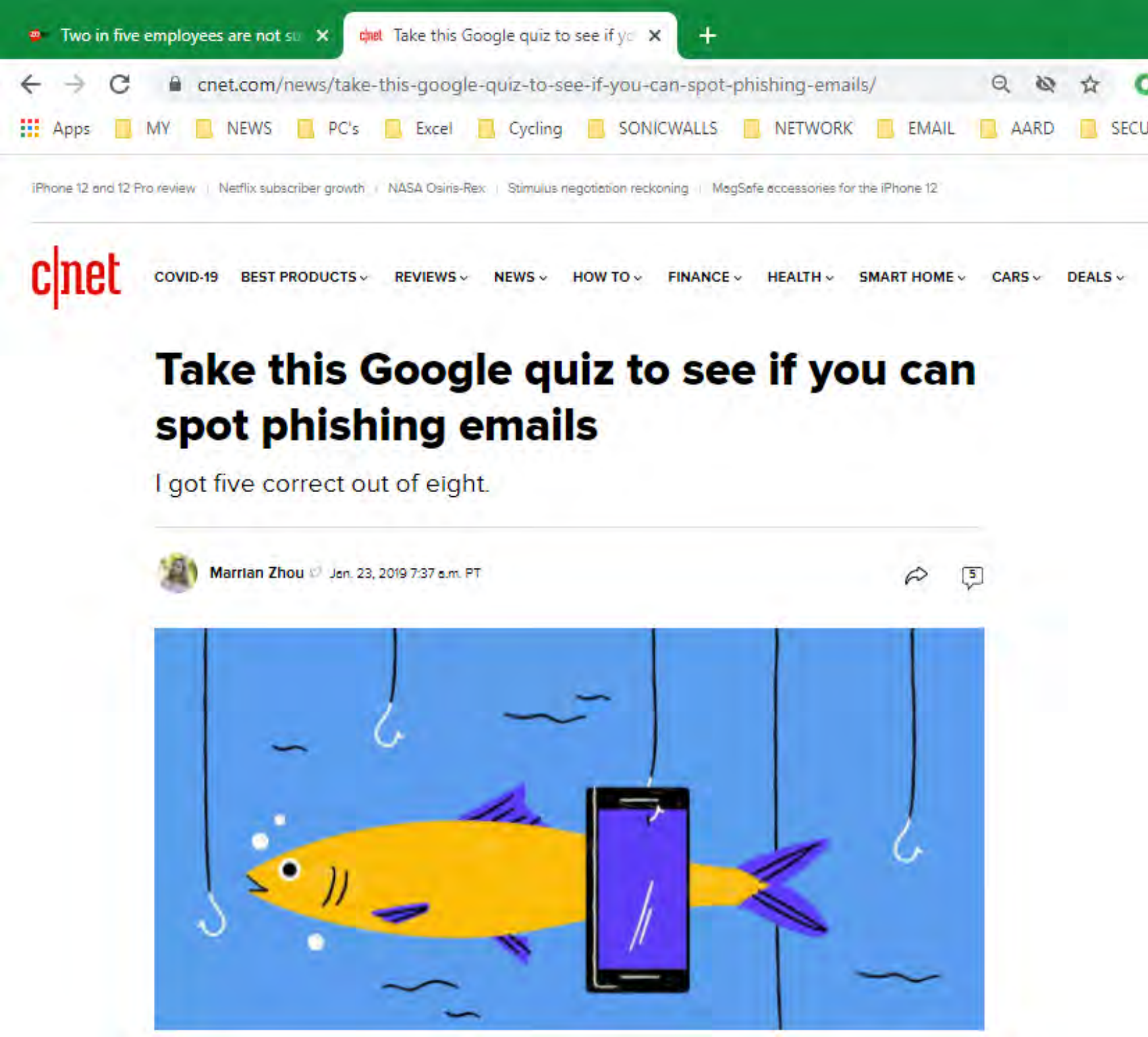


‘local bank’ won’t
allow some
employees email
since they
FLUNK phishing
tests!

The image is a screenshot of a web browser displaying a ZDNet article. The browser's address bar shows the URL: zdnet.com/article/two-in-five-employees-are-not-sure-what-a-mobile-phishing-attack-is/. The ZDNet logo is visible in the top left of the page. A navigation bar at the top right includes links for CLOUD, SMALL BUSINESS TV, SECURITY, AI, MORE, NEWSLETTERS, and ALL WRITERS. Below this, a 'MUST READ' section highlights the article being viewed. The article title is 'Two in five employees are not sure what a mobile phishing attack is'. The introductory paragraph states: 'The COVID-19 pandemic presents a significant challenge for businesses around the world as it seems their dispersed workforce have little regard for IT security and mobile phishing - a threat vector being increasingly used to target remote workers.'

Two in five employees are not sure what a mobile phishing attack is

The COVID-19 pandemic presents a significant challenge for businesses around the world as it seems their dispersed workforce have little regard for IT security and mobile phishing - a threat vector being increasingly used to target remote workers.



<https://phishingquiz.withgoogle.com/>

Can you spot when you're being phished?

Identifying phishing can be harder than you think. Phishing is an attempt to trick you into giving up your personal information by pretending to be someone you know. Can you tell what's fake?

TAKE THE QUIZ



I use multiple
ways of
checking
website
safety...

In this article, we'll show you some of the most common ways ransomware propagates and how you can reduce the risk of infection.

- Email attachments. ...
- Malicious URLs. ...
- Remote desktop protocol. ...
- MSPs and RMMs. ...
- Malvertising. ...
- Drive-by downloads. ...
- Network propagation. ...
- Pirated software.

[More items...](#) • Dec 19, 2019

[blog.emsisoft.com › how-ransomware-spreads-9-most-c...](#)

[How ransomware spreads: 9 most common infection methods ...](#)

“Web of Trust”

https://www.cantarus.com › News › Blogs › Details

✓ SonicWALL VPN Tunnel Configuration Best Practice for ...

SonicWALL VPN Tunnel Configuration **Best** Practice for Remote Desktop Services ... connections over VPN tunnels is due to TCP timeout **settings** that are too low. ... AS and **IPs**) to obtain the **best** RDS performance and connection reliability.

https://www.fastvue.co › sonicwall › blog › the-best-so...

WEBROOT - Caution

This site may contain content that could affect your online security.

ed Logging and ...

mmendations to get the ...

Syslog **Settings** with Reporting Software **Settings** in Log | Syslog that forces the ... that is required for the Fastvue Server to resolve **IPs** in the first place.

https://www.sonicguard.com › datasheets › SonicWAL... PDF

✓ SonicWall TZ series - SonicGuard.com

SonicWall **TZ300** series firewall combines effective **intrusion prevention**, ... Manage security **settings** of additional ports, including POE and POE+, under a single ...

http://www.warez.com


Warez.com


No information is available

Learn why

Security

Reputation





SUSPICIOUS!

★ ★ ★ ★ ★

WOT

View full scorecard

This popup shows you the reputation score of this website.

Next

Warez Wars. For the Inner underground, collecting i

Warez (pronounced as though spelled "wares" or possibly by some pronounced like the city of "Juarez") is a term used b

Definition of wa

(soft "wares") Pirated software distributed over the internet. A **warez** site may also provide hackers with viruses and Trojans as well as tips, techniques and ...

If multi-million dollar companies, hospitals, schools,
governments, etc cannot thwart ransomware,
what are you and I to do?

Videos



Debbie Downer: Disney World - SNL

Saturday Night Live
YouTube - Sep 25, 2013



Debbie Downer Wedding Reception - SNL

Saturday Night Live
YouTube - Mar 7, 2020



This Day in SNL History: Debbie Downer

Saturday Night Live
YouTube - May 1, 2020

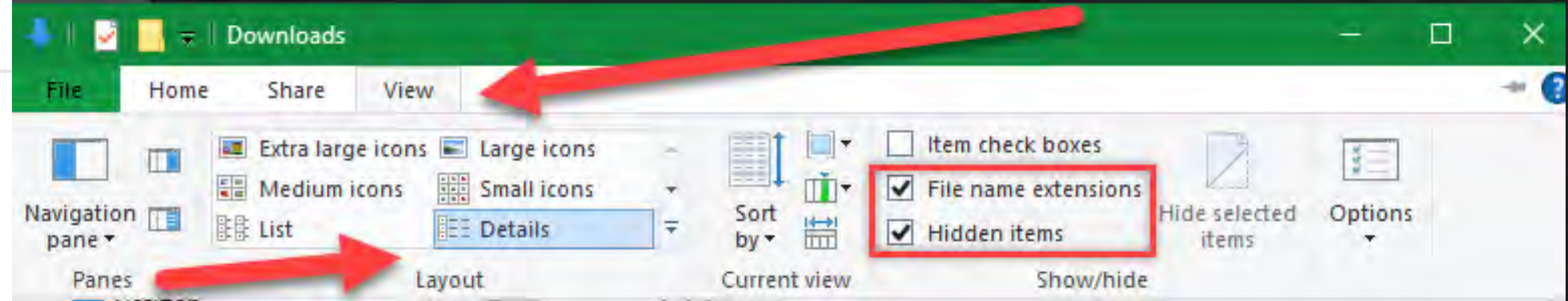


View all



Earlier this year (16)

- pia-windows-x64-2.2.1-05193
- GKM541R
- ChromeSetup
- sonicwall-TZ_400-6_5_4_6-79n-1593886218.exp
- sw_tz-400_eng_6.5.4.6-79n.sig
- Printer_3110cn_APP_WIN_A08
- Setup.Def.en-us_O365BusinessRetail_04ca2e19-b6c...
- SupportAssistLauncher
- W9
- tableclinics2020
- Panasonic KX-TA824
- KX-TA824.Operating Manual
- Panasonic Voice Mail Installation_Manual
- dpfsetupg_dpfw-site
- Printer_3110cn_APP_WIN_A08
- Stardock



EASY:

change your PC to see
file suffix- WHY??

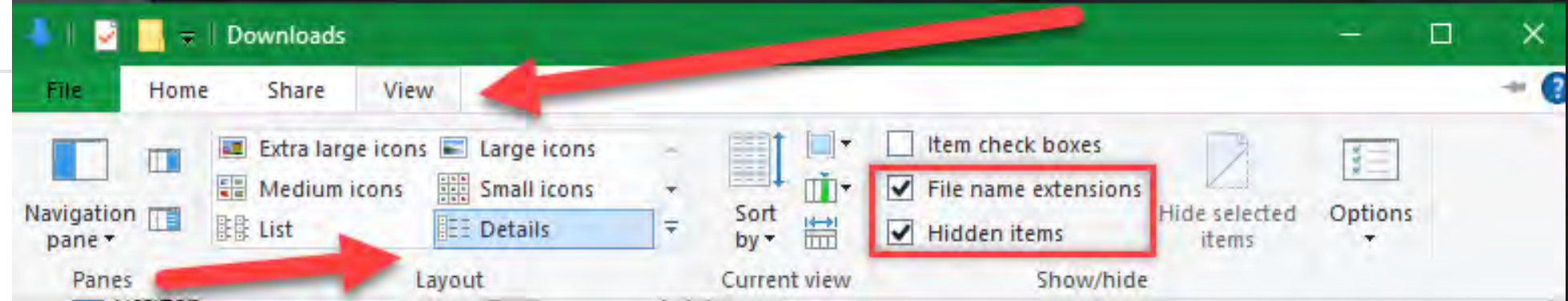
icons can be spoofed...

Earlier this year (16)

- pia-windows-x64-2.2.1-05193.exe
- GKM541R.pdf
- ChromeSetup.exe
- sonicwall-TZ_400-6_5_4_6-79n-1593886218.exp
- sw_tz-400_eng_6.5.4.6-79n.sig
- Printer_3110cn_APP_WIN_A08.zip
- Setup.Def.en-us_O365BusinessRetail_04ca2e19-b6c...
- SupportAssistLauncher.exe
- W9.pdf
- tableclinics2020.zip
- Panasonic KX-TA824.pdf
- KX-TA824.Operating Manual.pdf
- Panasonic Voice Mail Installation_Manual.pdf
- dpfsetupg_dpfw-site.exe
- Printer_3110cn_APP_WIN_A08
- Stardock

Earlier this year (16)

- pia-windows-x64-2.2.1-05193
- GKM541R
- ChromeSetup
- sonicwall-TZ_400-6_5_4_6-79n-1593886218.exp
- sw_tz-400_eng_6.5.4.6-79n.sig
- Printer_3110cn_APP_WIN_A08
- Setup.Def.en-us_O365BusinessRetail_04ca2e19-b6c...
- SupportAssistLauncher
- W9
- tableclinics2020
- Panasonic KX-TA824
- KX-TA824.Operating Manual
- Panasonic Voice Mail Installation_Manual
- dpfsetupg_dpfw-site
- Printer_3110cn_APP_WIN_A08
- Stardock



What if it's a **PDF icon**
but really a **.exe???**

Earlier this year (16)

- pia-windows-x64-2.2.1-05193.exe
- GKM541R.pdf
- ChromeSetup.exe
- sonicwall-TZ_400-6_5_4_6-79n-1593886218.exp
- sw_tz-400_eng_6.5.4.6-79n.sig
- Printer_3110cn_APP_WIN_A08.zip
- Setup.Def.en-us_O365BusinessRetail_04ca2e19-b6c...
- SupportAssistLauncher.exe
- W9.pdf
- tableclinics2020.zip
- Panasonic KX-TA824.pdf
- KX-TA824.Operating Manual.pdf
- Panasonic Voice Mail Installation_Manual.pdf
- dpfsetupg_dpfw-site.exe
- Printer_3110cn_APP_WIN_A08
- Stardock

FIREWALL LOGS: From the Office on a quiet Saturday

Threat Prevention Summary

Threats Blocked

Intrusion Prevention



21

Geo-IP Filter




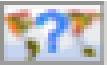
17


Not ALL firewalls can do this (GEO-IP BLOCK)...


09:52:53 Oct 17	83	Security Services	Alert	Probable port scan detected
09:52:53 Oct 17	82	Security Services	Alert	Possible port scan detected
09:51:51 Oct 17	1199	Security Services	Alert	Responder from country blocked: Responder IP:20.189.118.208 Country Name:Hong Kong
09:39:27 Oct 17	82	Security Services	Alert	Possible port scan detected
09:37:23 Oct 17	82	Security Services	Alert	Possible port scan detected
09:26:01 Oct 17	82	Security Services	Alert	Possible port scan detected
09:15:34 Oct 17	1199	Security Services	Alert	Responder from country blocked: Responder IP:52.229.171.202 Country Name:Hong Kong
09:09:11 Oct 17	1198	Security Services	Alert	Initiator from country blocked: Initiator IP:129.227.129.187 Country Name:Hong Kong
08:37:54 Oct 17	82	Security Services	Alert	Possible port scan detected


Blocked Countries:


 Afghanistan

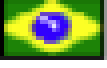
 Anonymous Proxy/Private IP


 Azerbaijan


 Bahrain


 Belarus


 Bhutan


 Brazil


 Bulgaria


 China


 Croatia

 Czech Republic

 Hong Kong

 Iran, Islamic Republic of

 Iraq

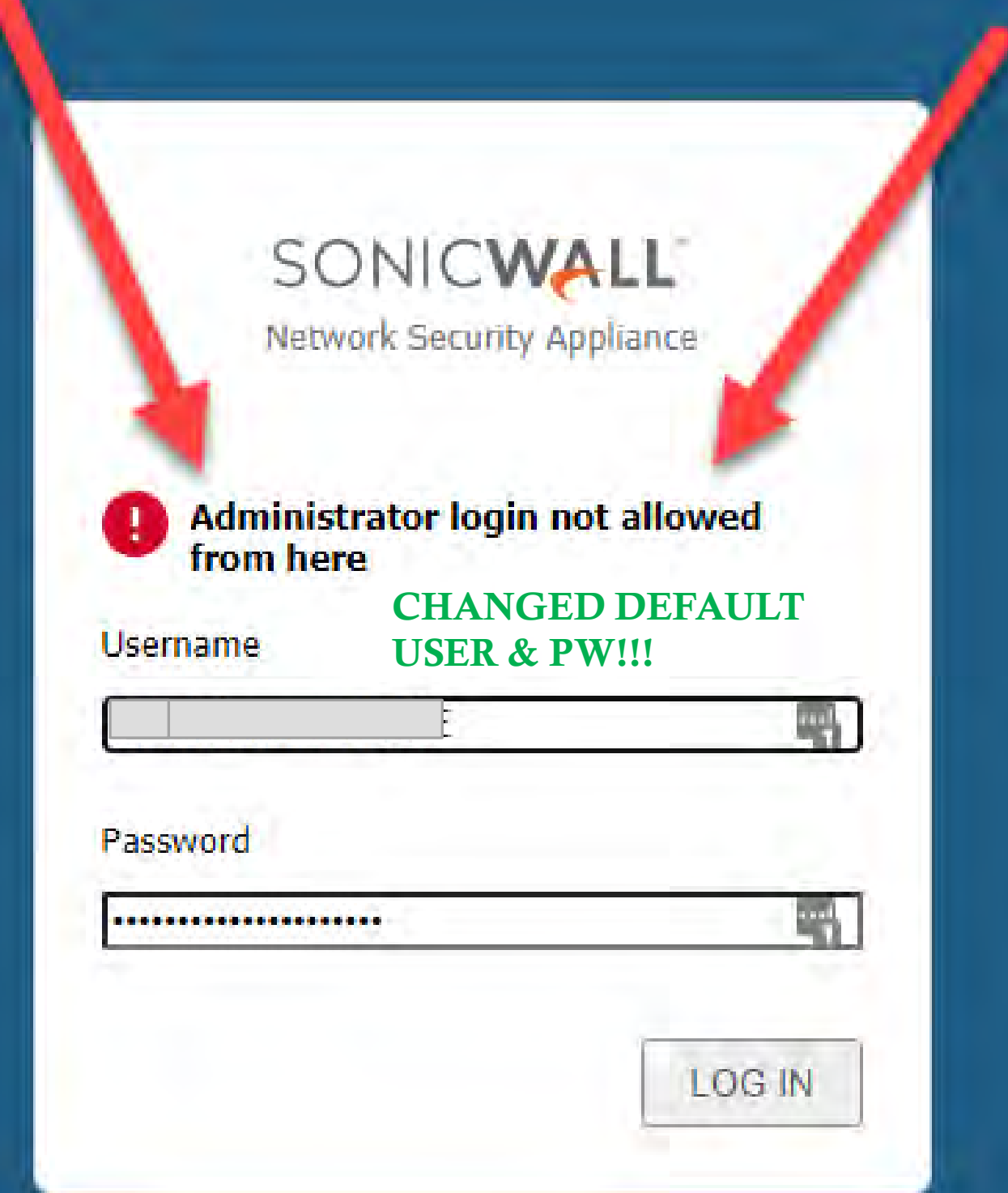
 Kazakhstan

And when I try to login to my HOME firewall from the OFFICE

NOT ALLOWED to access the **firewall administration** from the internet - ONLY FROM HOME
(by MY design!)

I've even **DELETED** the VPN between home/office,
as VPN's are now at risk (see Sonicwall slide)

I'll bet SOME OF YOU don't have office FIREWALL, and > 95% of you do NOT have a firewall at home...
perhaps upgrade the office Firewall and use old one at home (it's ALSO what I do with old SERVERS!)



Threats Blocked

Intrusion Prevention



21288

Botnet Filter



339

Geo-IP Filter



8

I went home and accessed the Sonicwall's home logs.....

This graphic shows the HOME activity

What's going on at YOUR HOME?? Especially those with teenagers??

Easiest way to keep your office secure....



2 KEYS!

Wake up!!

Even a DDS adverse to anything IT can do this!

Easiest Way to keep your
office secure:
FIREWALL!!!

And....
What's **WRONG** with
this picture??



Best Firewall Hardware for Small Businesses in 2021

comparitech

VPN Antivirus Online backup Streaming Blog More Comparisons


Blog » Information Security » Best Firewall Hardware for Small Businesses in 2021

We are reader supported and may earn a commission when you buy through links on our site

Best Firewall Hardware for Small Businesses in 2021

Shopping for firewall hardware and confused by the options? We reveal our top picks for the best firewall hardware for small businesses.

AIMEE O'DRISCOLL - VPN AND CYBERSECURITY EXPERT
October 8, 2020



Best Firewall Hardware for Small Businesses

What's in this article?

- Best firewall hardware for small businesses
- SonicWall TZ400 Security Firewall
- Ubiquiti UniFi Security Gateway

Best firewall hardware for small businesses:

1. [SonicWall TZ400 Security Firewall](#): A customizable, versatile solution for small businesses with possible expansion goals.
2. [Ubiquiti UniFi Security Gateway](#): This budget option is easy to install and manage.
3. [WatchGuard Firebox T35](#): Ideal for businesses with up to 20 employees, the T35 comes with optional built-in wifi.
4. [Protectli Vault – 4 Port](#): A robust firewall hardware for use with open source firewall distributions.
5. [Cisco Meraki MX68](#): This all-in-one router and firewall is backed by advanced cloud-managed security.
6. [Sophos XG 86](#): A next-generation firewall with optional wifi and centralized management.

(1st)? 2nd

Easiest Way to keep your
office secure:

“A Timer”

KEY!!



My internet **MODEM** is **ON**
6:45a-5:30p DAILY
8:00a – 12Noon (or less!) On
WEEKENDS

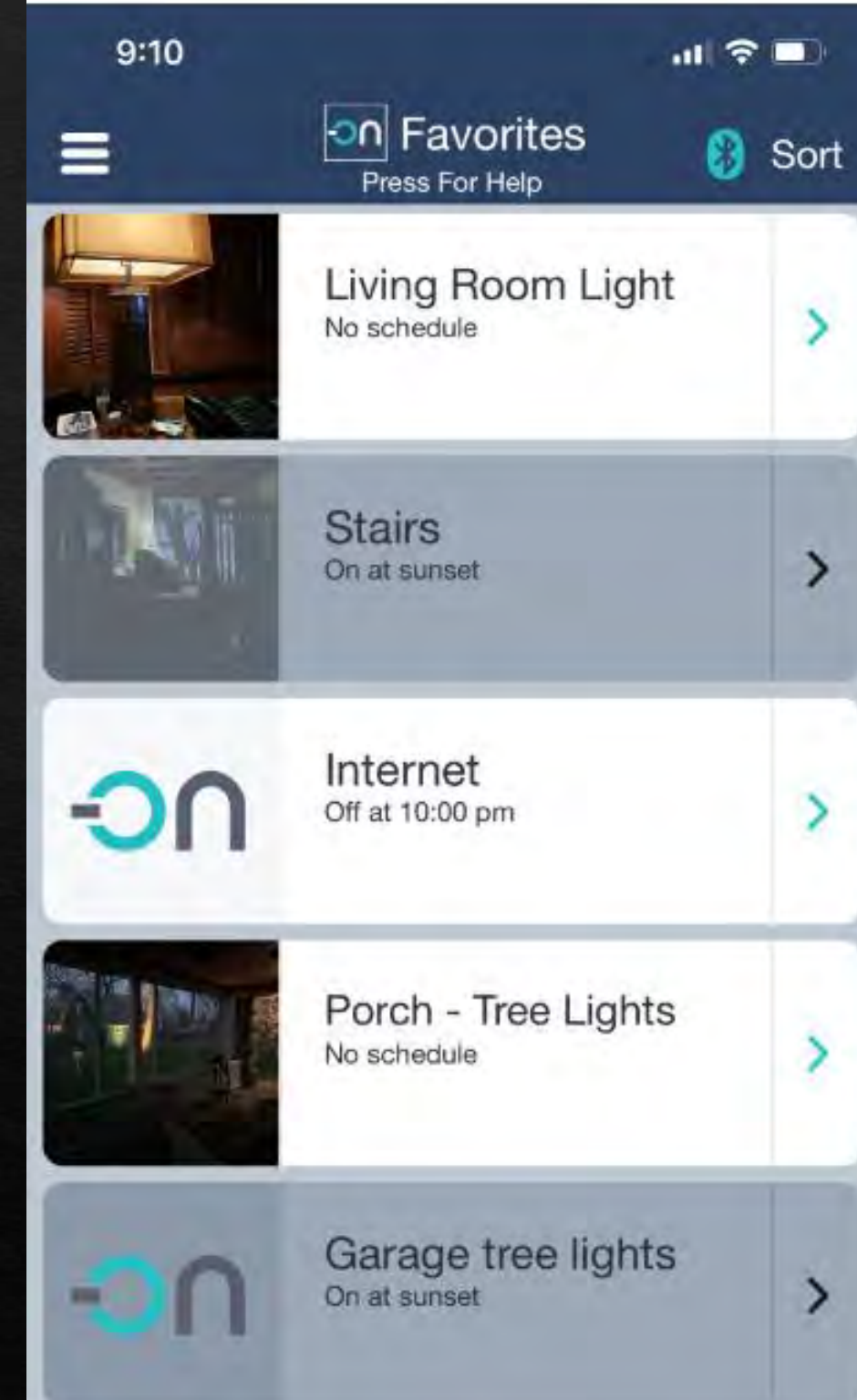
OTHERWISE **OFF**

“if it’s **OFF**, it can’t be hacked”





I NOW DO THE SAME AT MY
HOME
(which ALSO has a FIREWALL)
HIGHSPEED **MODEM OFF** overnight
(Google “GE Smart Switch”)



CAUTION USING A TIMER...

- ◆ My front desk informed me “we haven’t received any electronic-filed insurance payments in about a month...”
- ◆ That’s because that task was scheduled to run after hours (~11pm and now the internet **OFF**)
- ◆ I changed this to run at 7am after internet back online, and before staff arrives
 - ◆ And the next month had excellent collections....

“If it’s OFF, it can’t be hacked”

- ◆ I know two LOCAL dentists who have NO INTERNET to their dental management network and workstations/server!
- ◆ My office? Email and online ordering on a dedicated workstation on its **OWN NETWORK**, with no access to the dental management network.
- ◆ ALL but ONE workstation OFF at 530p!
- ◆ I NOW turn OFF my SERVER 1p Fri until I walk into office 645a Mon!!!
- ◆ **Attacks changed from up to 1500/day (!) to WAY LESS than a few per hour!**

WORKSTATIONS and SERVERS (and PRINTERS and SWITCHES and NAS and and and...)

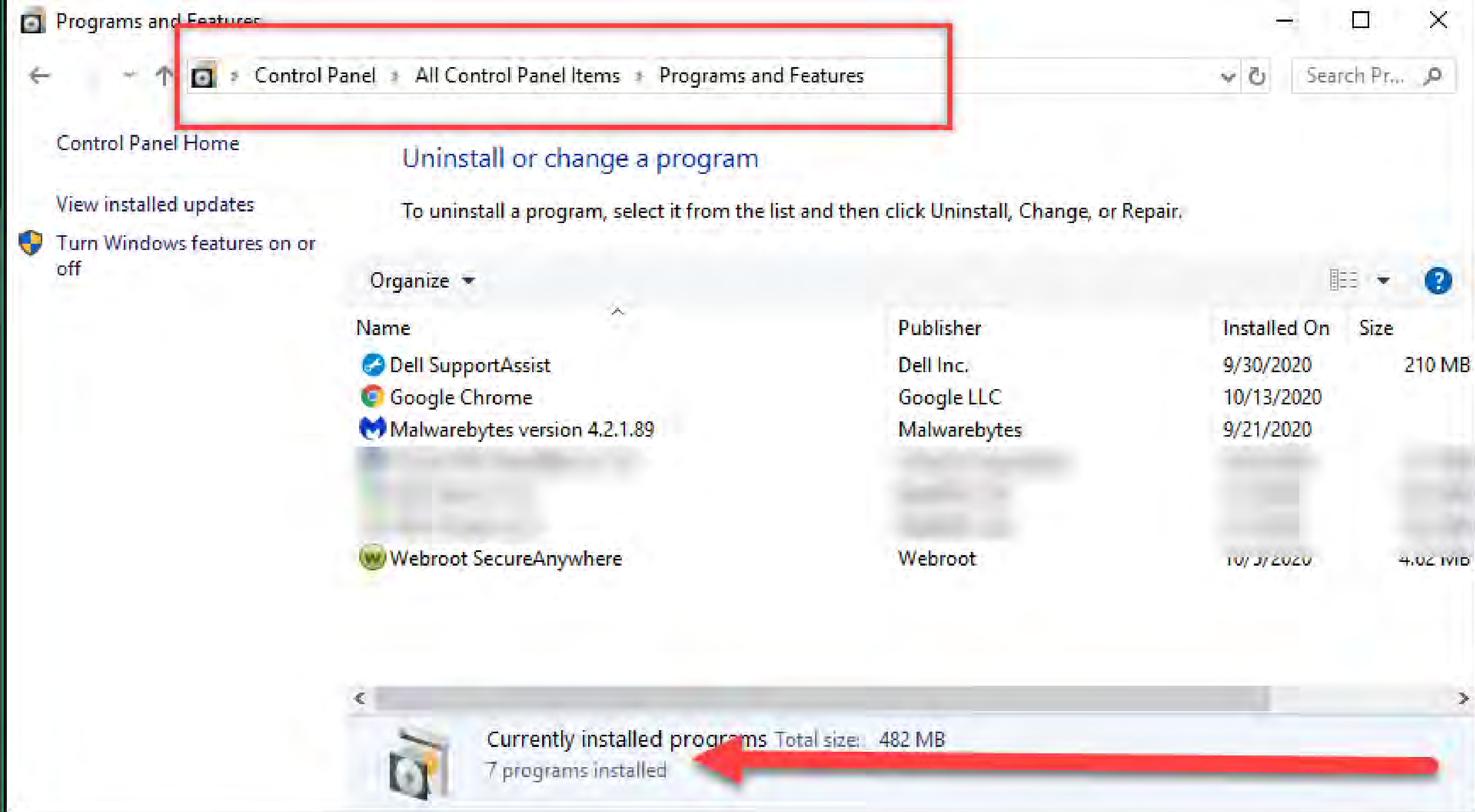


Kreb's 3 Rules for Staying Safe Online (2011!):

- ◆Krebs's Rule #1 for Staying Safe Online: *"If you didn't go looking for it, don't install it!"*
- ◆Krebs's Rule #2 for Staying Safe Online: *"If you installed it, update it."*
- ◆Krebs's Rule #3 for Staying Safe Online: *"If you no longer need it, remove it."*
 - ◆Example: "TeamViewer," "Citrix GoToWebinar" and ~45 other programs on colleague's server(!)
 - ◆Do you REALLY need the Office Music System on your SERVER? (saw this in a different office).
 - ◆I WILL UNINSTALL TEAMS AFTER THIS EVENING! (OR may format my drive!)

MY SERVER:
7 programs installed, and
2 for security!
THAT'S IT!!

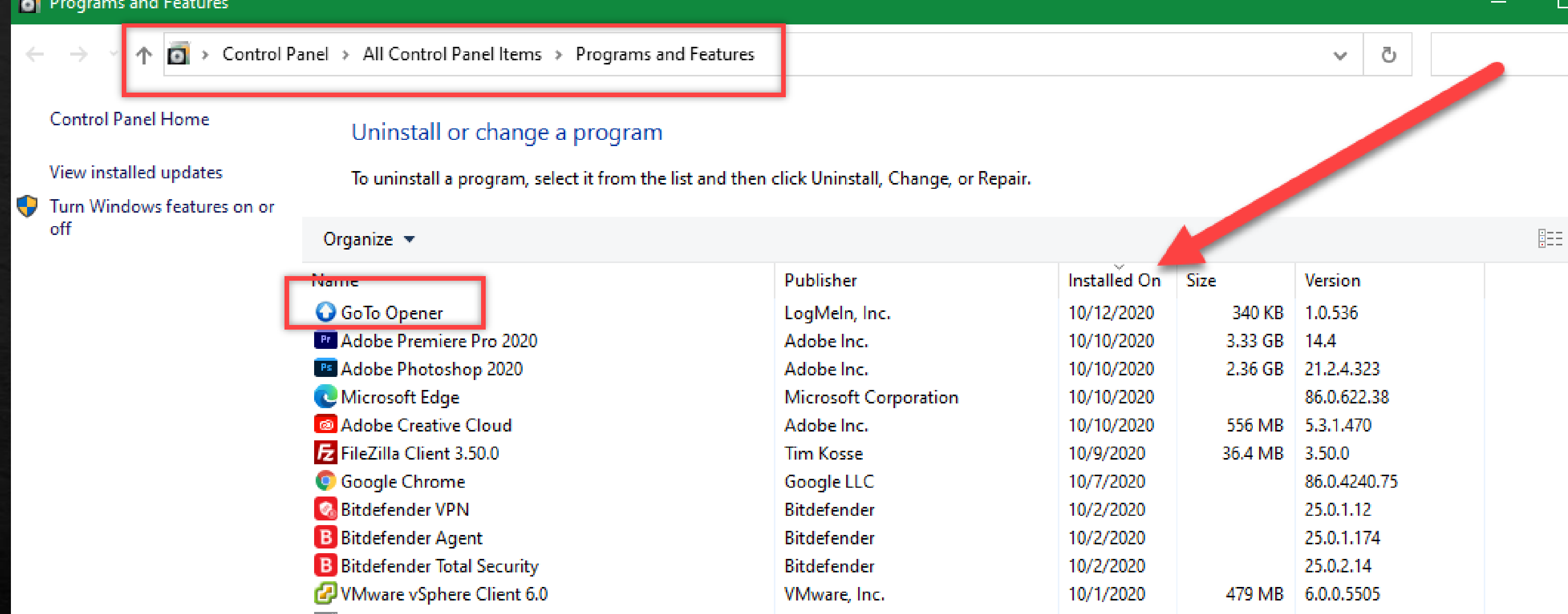
“If you no longer need it, remove it.”
and NO RDP ACCESS!!
To ANYTHING!
(see **KEY** slide , POINT #2)



My laptop:
Once tech support was finished
accessing my server (via my laptop), I
mosey to “Control Panel:

-sort by ‘installed on’
- delete the software

“If you no longer need it, remove it.”



My Laptop screen and the toolbar on the bottom....

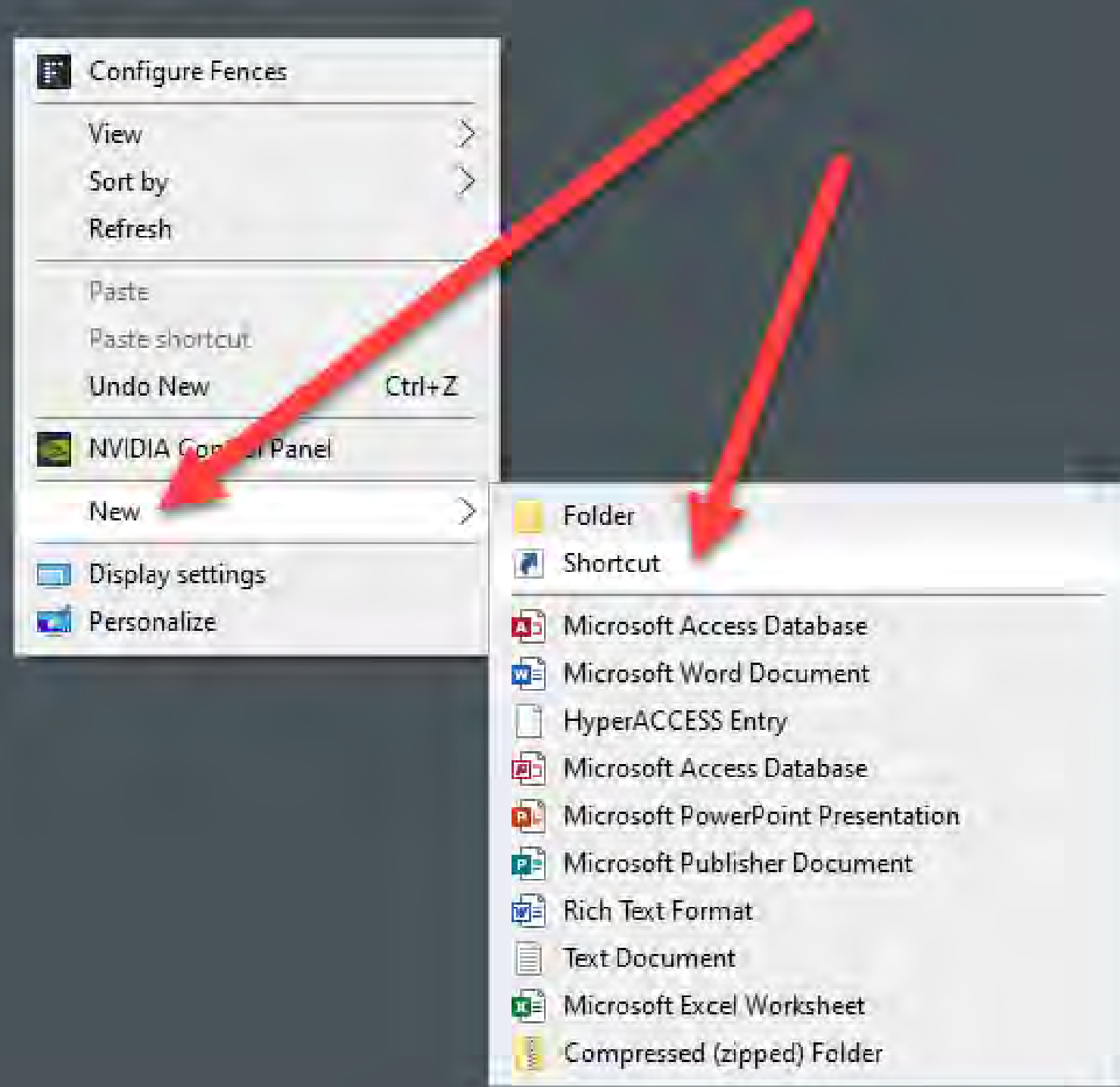




EVERY machine in my home and office sports these 3 shortcuts

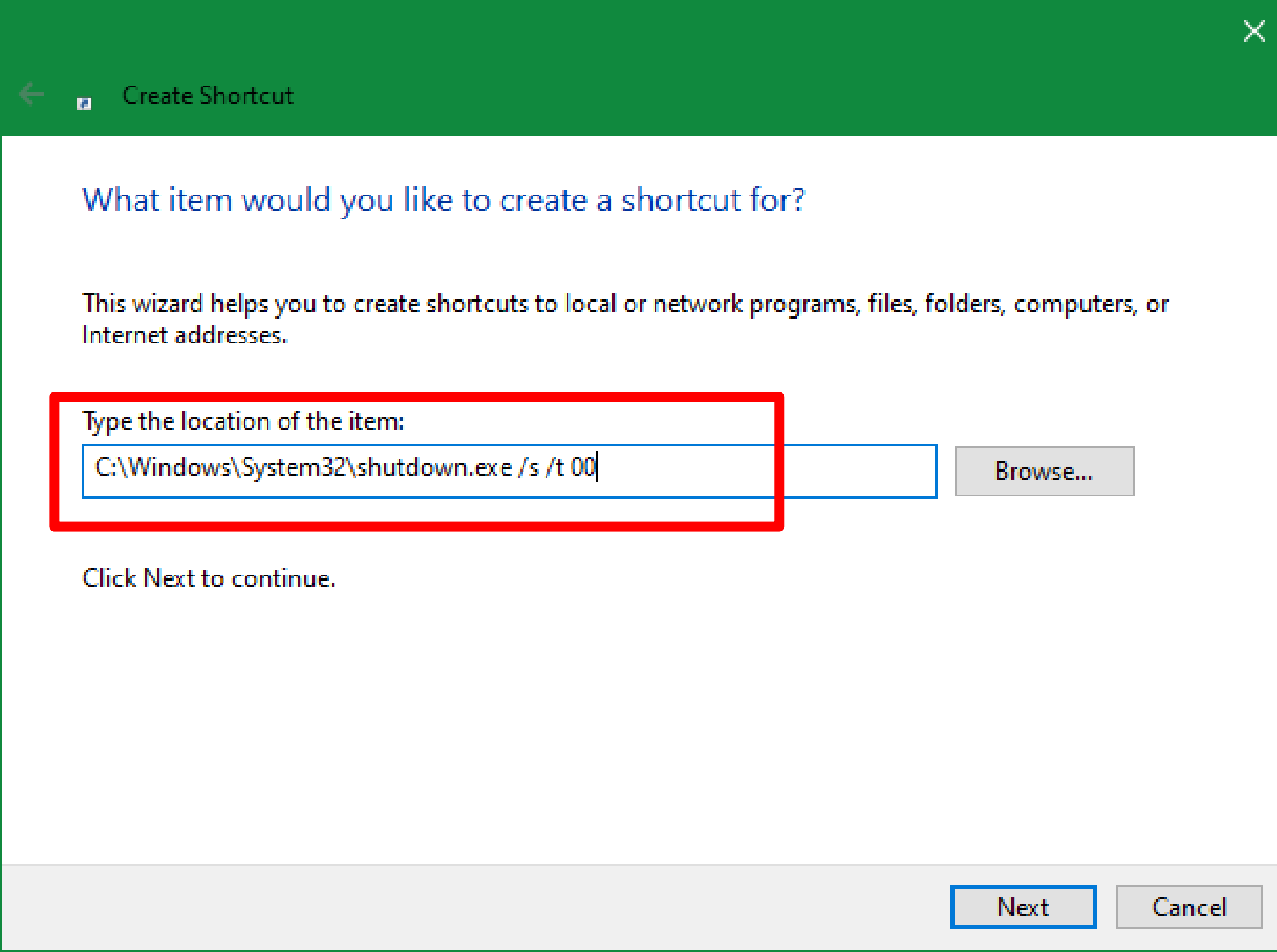
How to create 'shortcuts' in Windows: I will walk you thru ONE,
the other two are just as easy!

Let's start with
turn your computer OFF at the touch of a button




Right mouse-click a blank spot on your
desktop screen

select “New”
Select “Shortcut”



Copy and paste the following:

**C:\Windows\System32\shutdown
.exe /s /t 00**

 Create Shortcut

What would you like to name the shortcut?

Type a name for this shortcut:

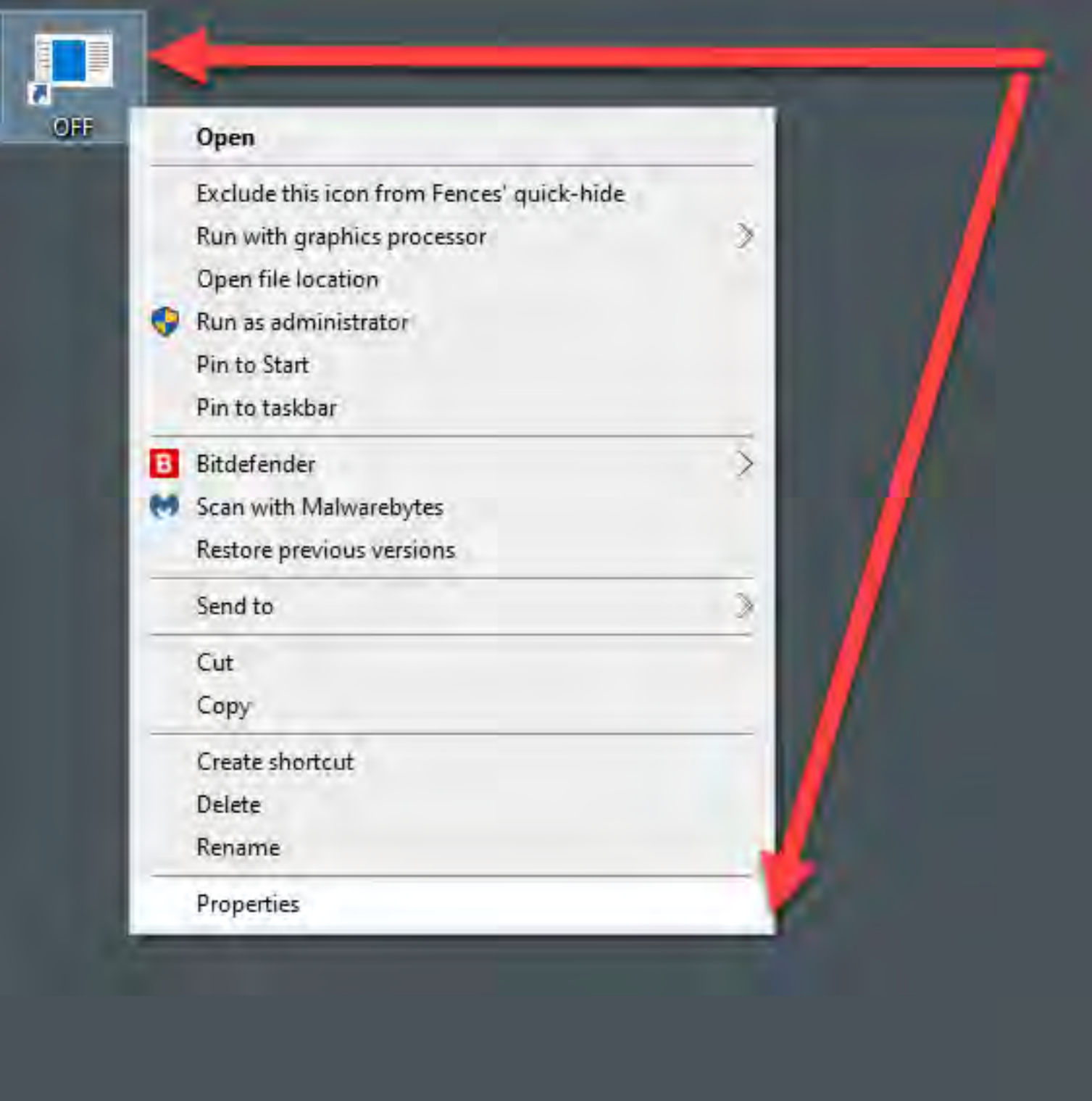
OFF

Click Finish to create the shortcut.

Finish

Cancel

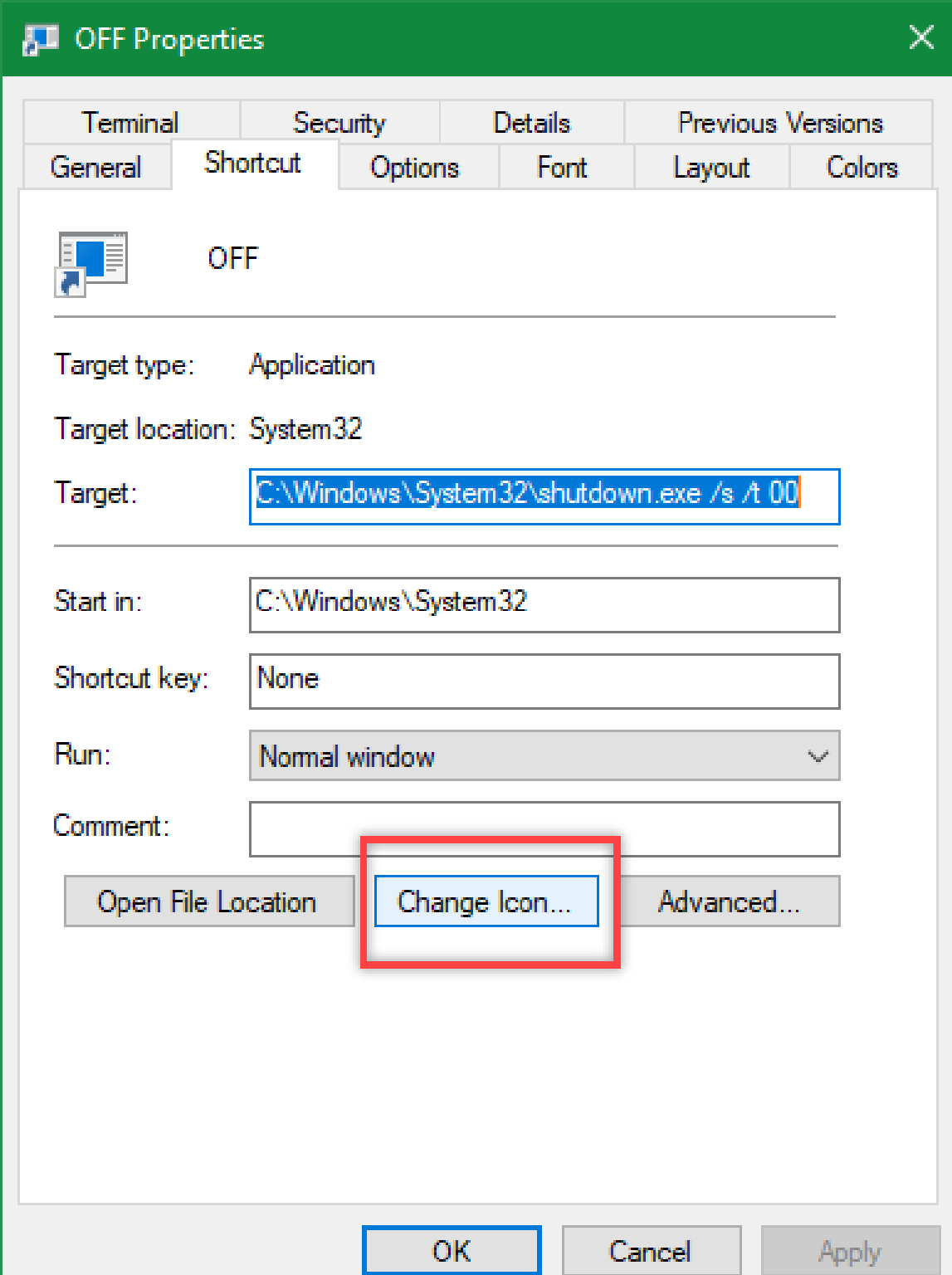
Now give it a name...

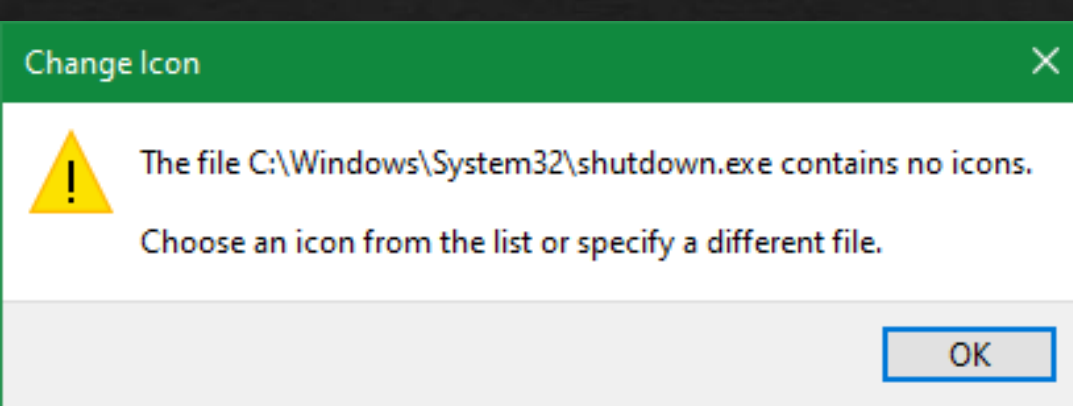


Let's change that ugly icon:

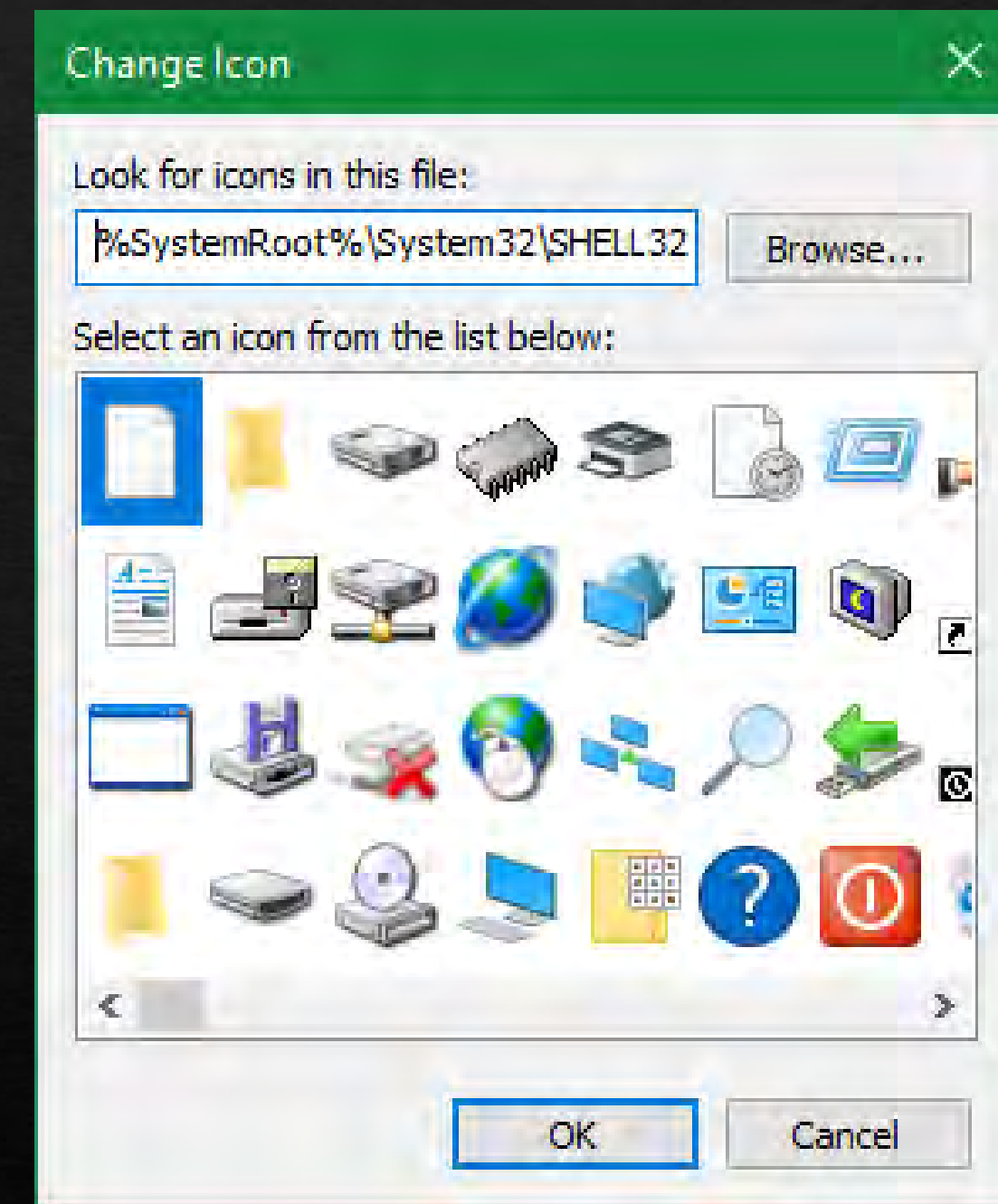
- Right click your new shortcut icon
- Select "Properties"

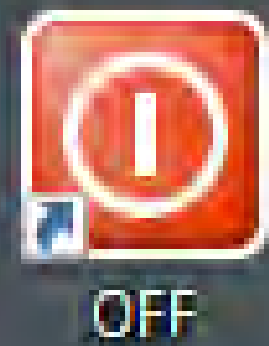
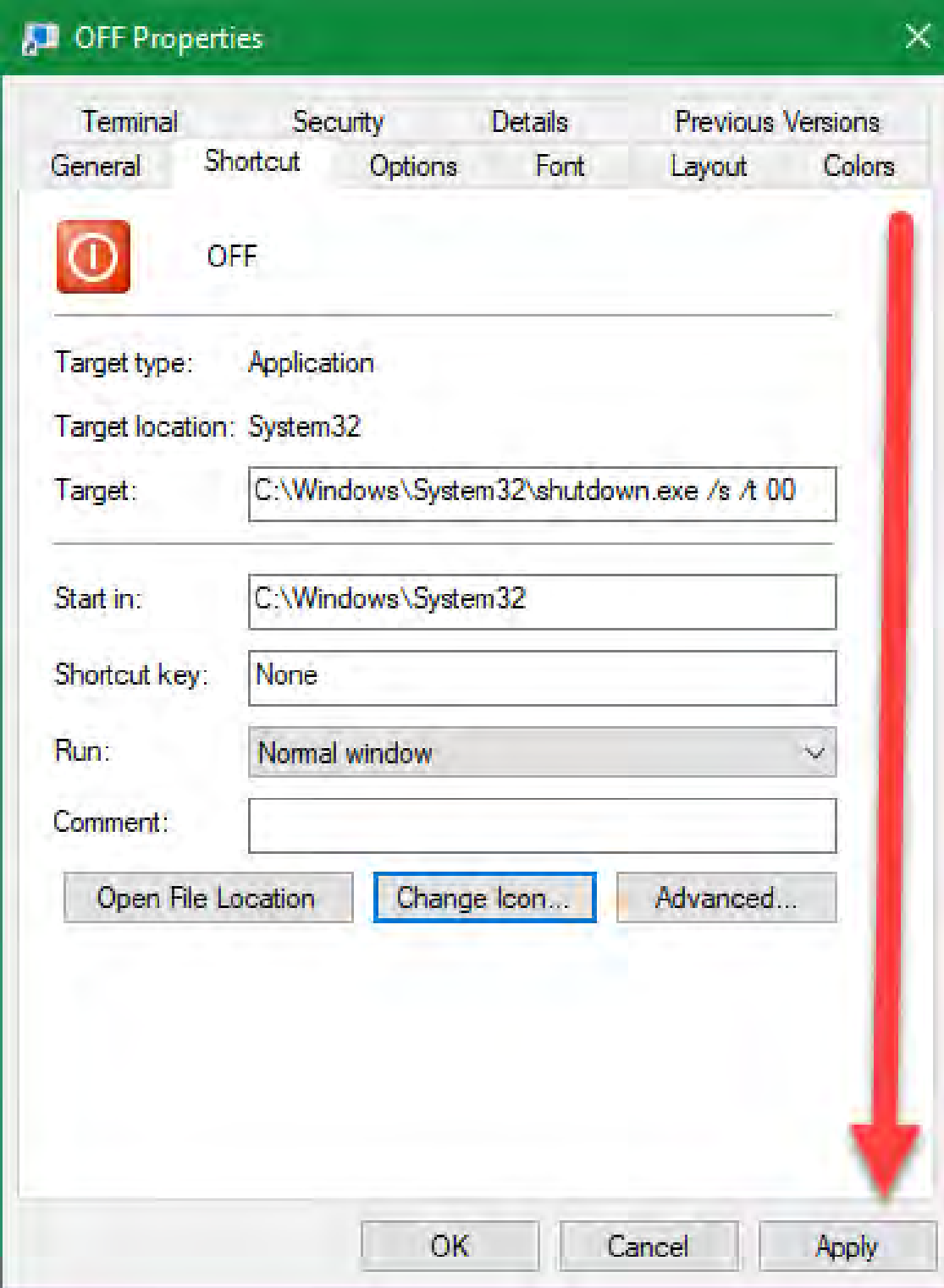
“Change Icon”





Select “OK” on the next screen,
then pick whatever icon you
want for your shortcut,
hit “OK” one more time.





“Apply” the change, and there’s your new icon.

I drag mine to the toolbar on the bottom of my screen.

Summary: **TAKE A PICTURE OF THIS SLIDE!**

OFF:

C:\Windows\System32\shutdown.exe /s /t 00

KEY!!!

LOCK:

C:\Windows\System32\rundll32.exe user32.dll,LockWorkStation

UPDATE:

ms-settings:windowsupdate

and I run 'update' **DAILY**, and generally do it 2-3 times! WHY????

MANY

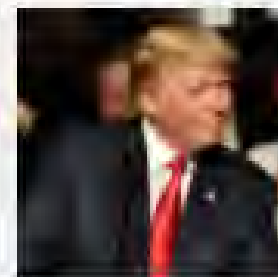
OTHER

DATES

6  GOT TIPS?

SHARE

// MOST READ



Let's check in with that
30,000-job \$10bn Trump-
Foxconn Wisconsin plant.
Wow, way worse than we'd
imagined

BTW: TOMORROW
is “PATCH TUESDAY”

Writing Batchfile(s)

Slightly harder...

and I might be losing a few of you so

TIME OUT!

(Or watch a 3min Sam Kineson
Video):

<https://www.youtube.com/watch?v=PRbnTNL4UAM>





2015
vs
2020



1, 2, 3, 30, 31, 32



2020/09/17

3, 4, 5, 28, 29, 30



2020/09/17

12, 13, 14, 19, 20, 21

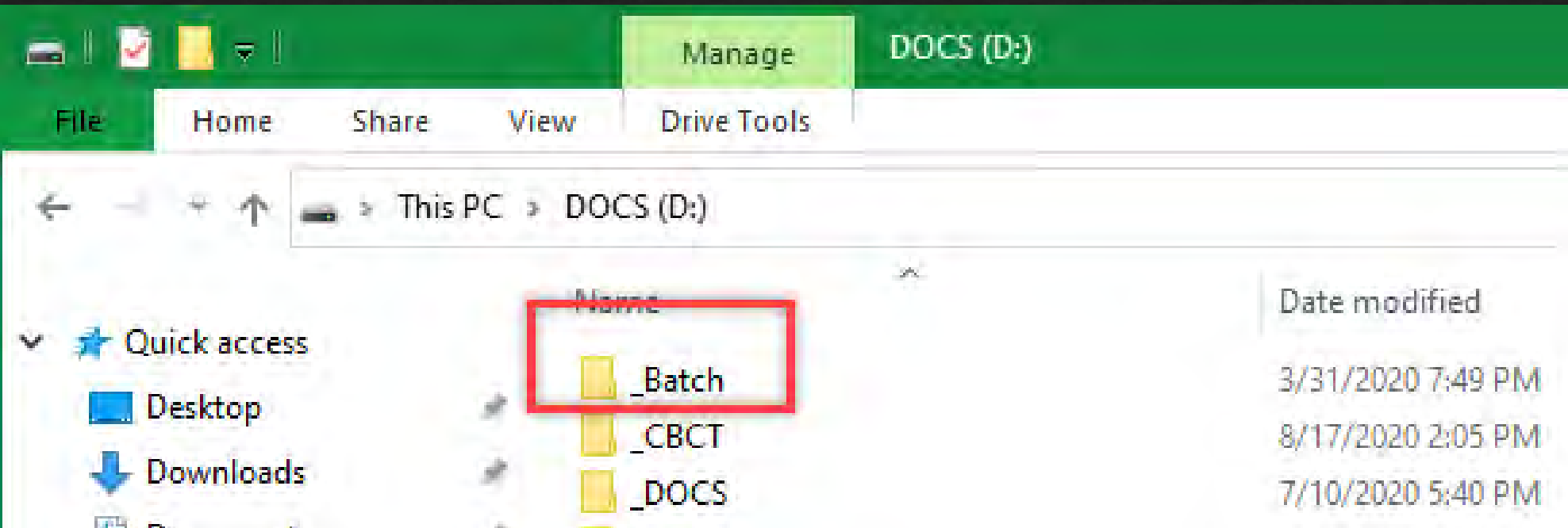


2020/09/17

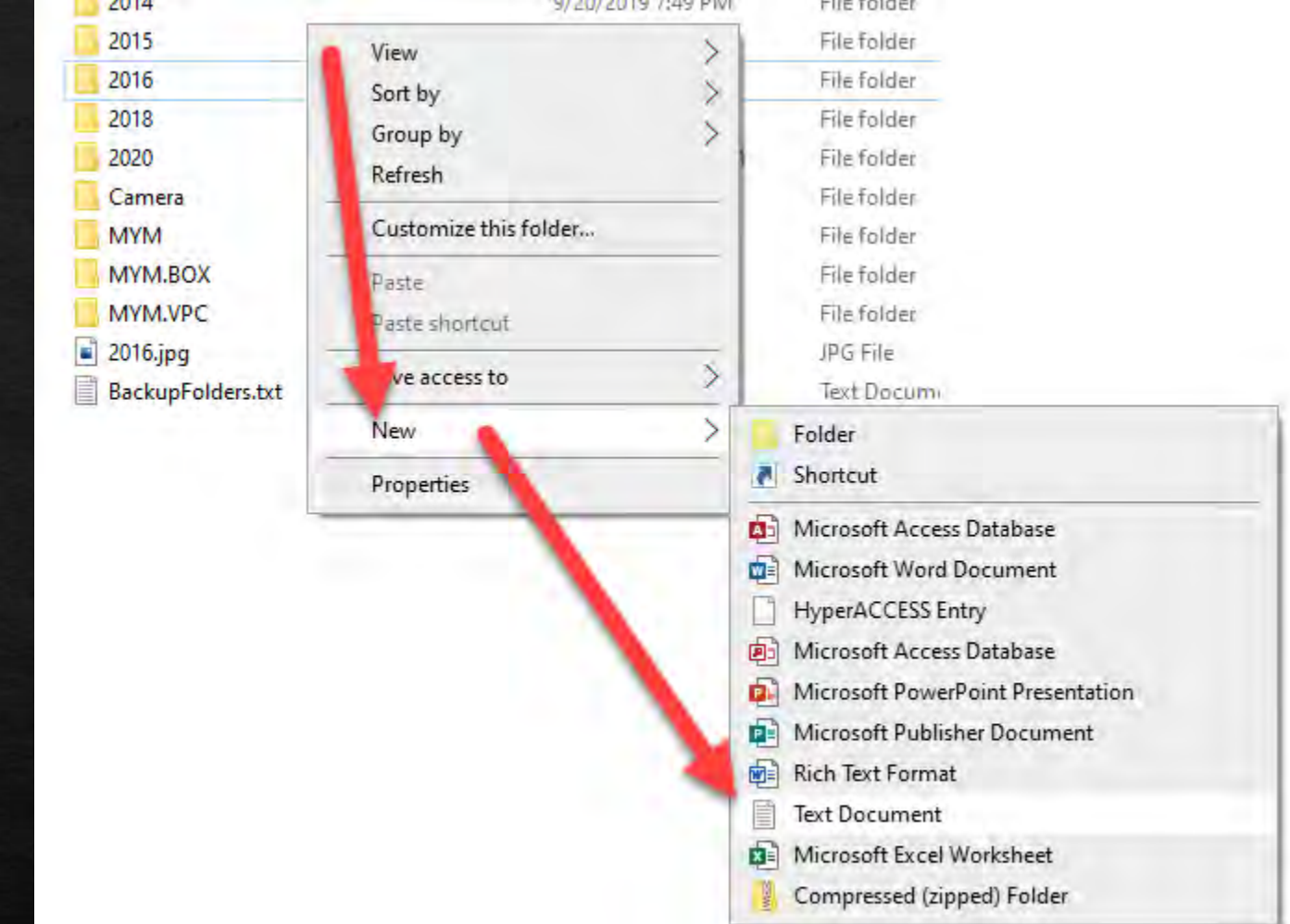
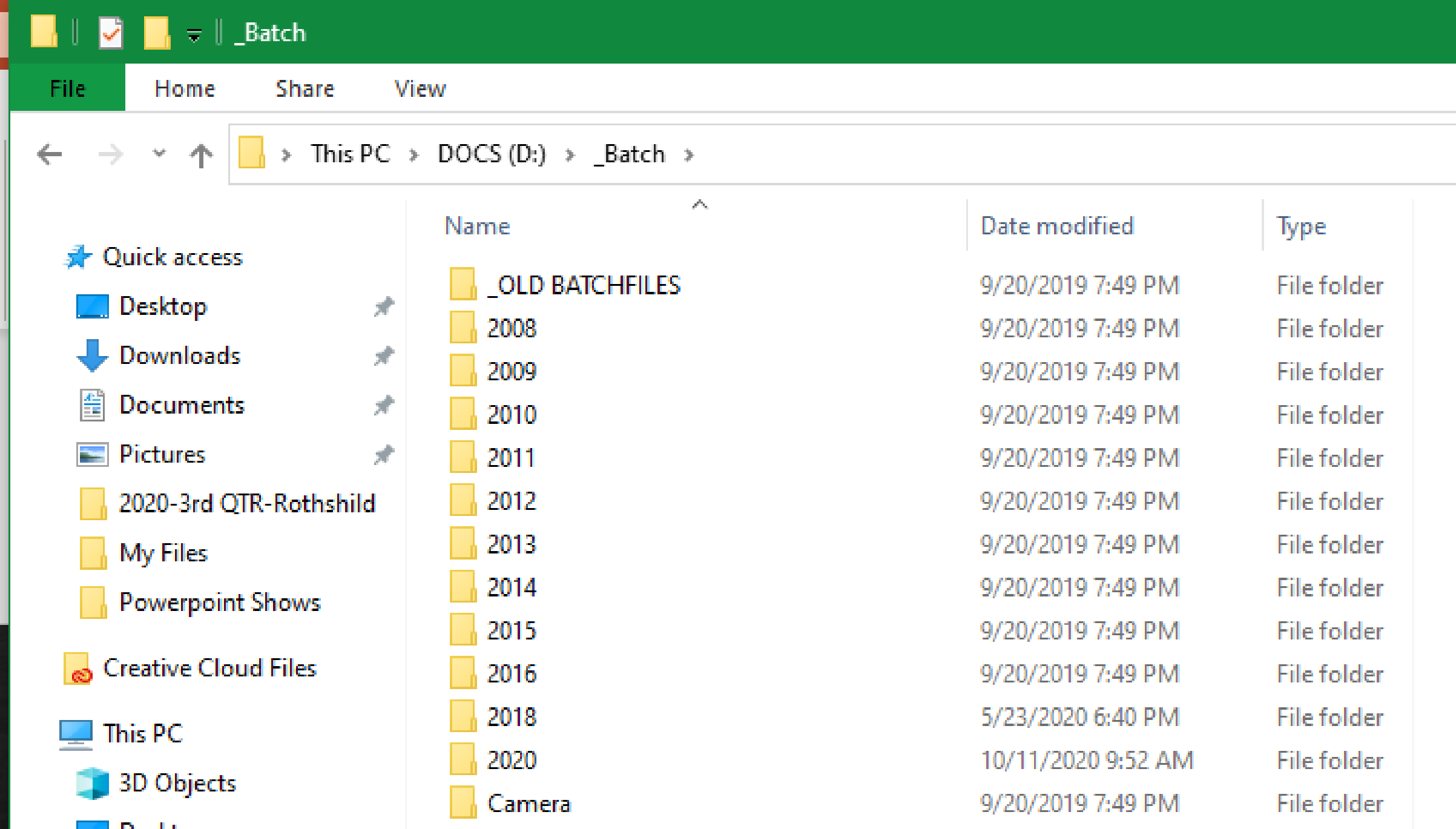
14, 15, 16, 17, 18, 19



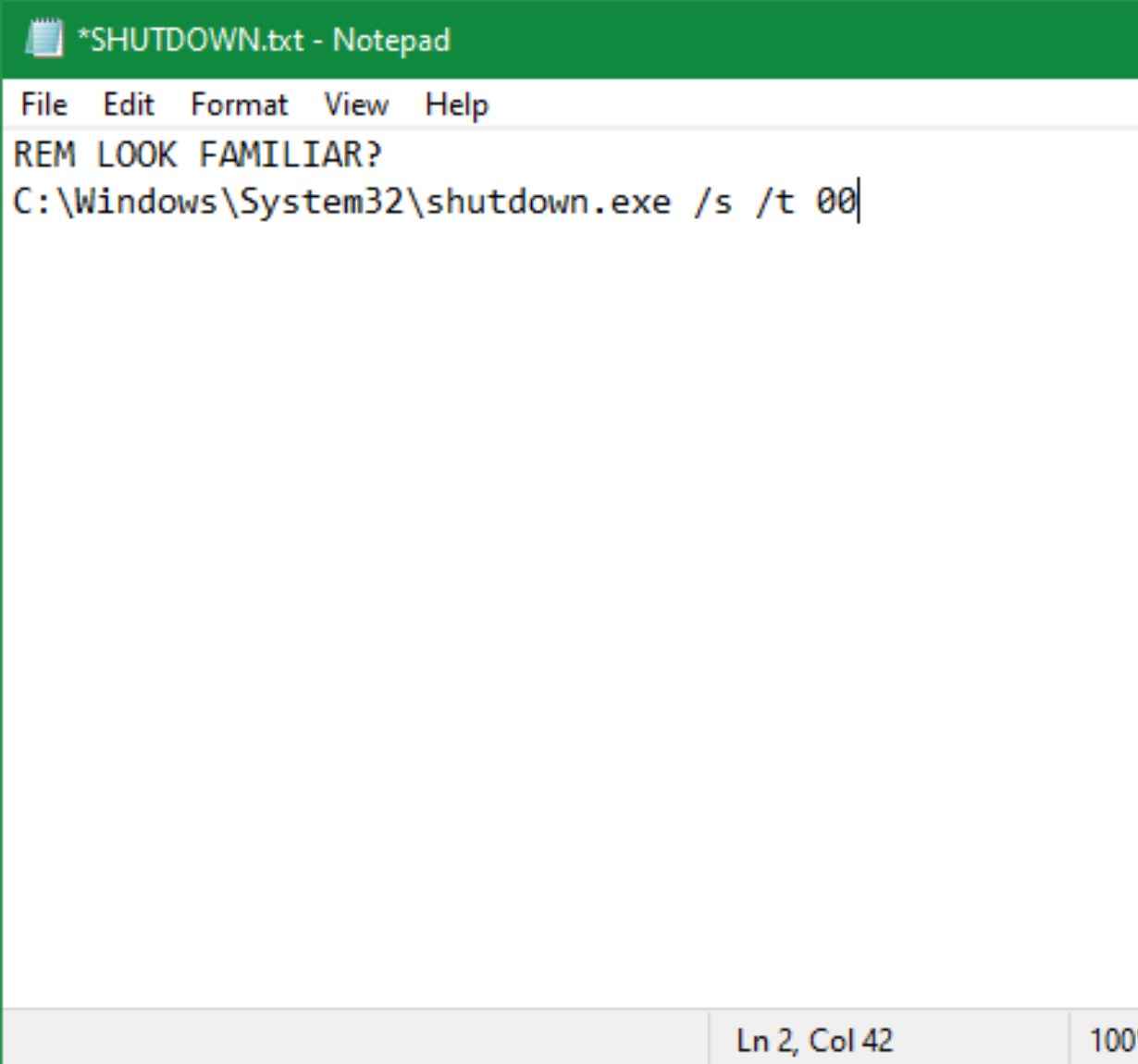
2020/09/17



I write a LOT of batchfiles....
(looks hard but I've taught other dentists to do this!)



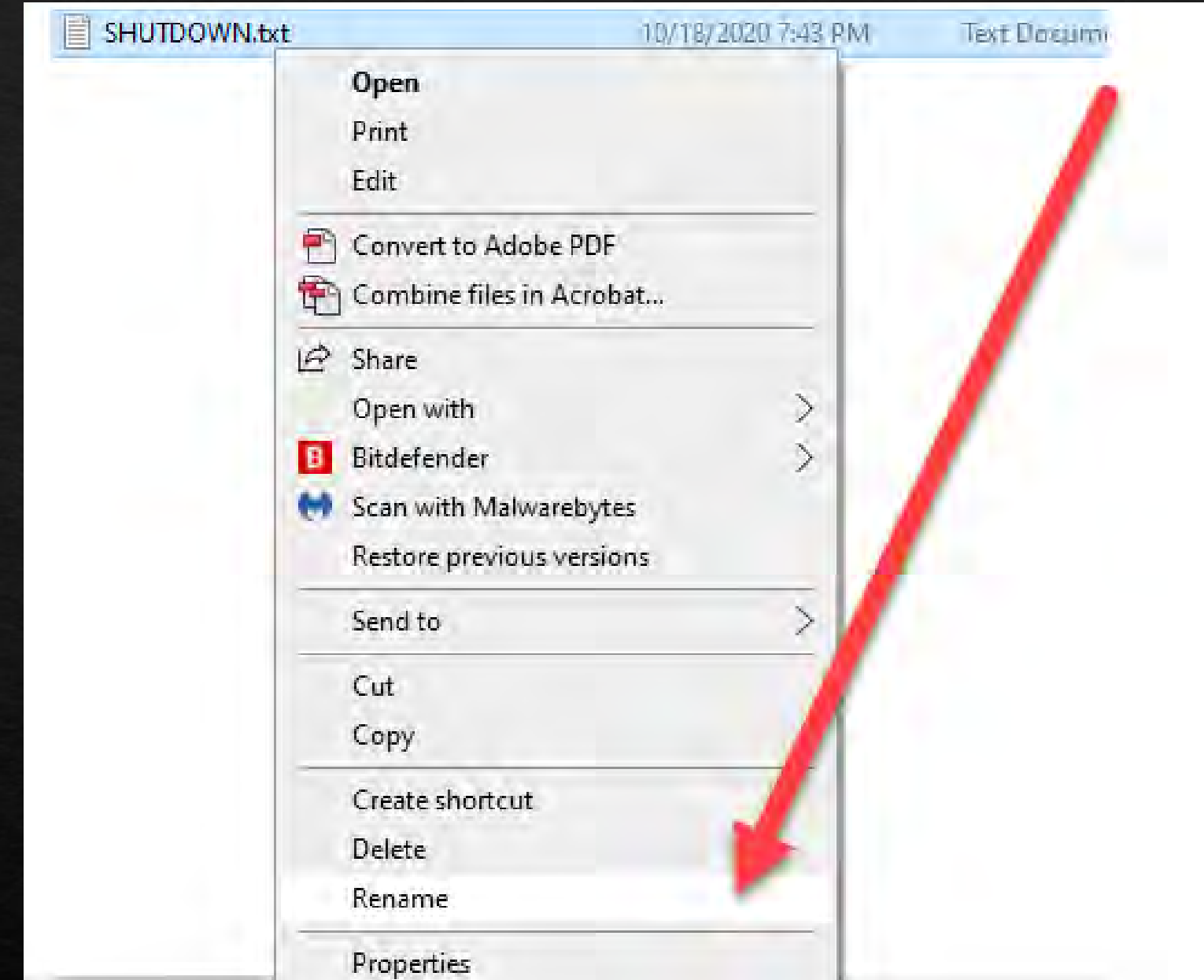
Right click blank screen & select
New | Text Document



A screenshot of the Notepad application window titled '*SHUTDOWN.txt - Notepad'. The menu bar includes File, Edit, Format, View, and Help. The text area contains the command: REM LOOK FAMILIAR? C:\Windows\System32\shutdown.exe /s /t 00. The status bar at the bottom indicates 'Ln 2, Col 42' and '100%' zoom.

```
File Edit Format View Help
REM LOOK FAMILIAR?
C:\Windows\System32\shutdown.exe /s /t 00
Ln 2, Col 42 100%
```

Use the same command
you used for the
shortcut on your toolbar
or desktop and place in
a txt document you
called 'shutdown.txt'



RENAME to shutdown.bat



BackupFolders.txt

3/31/2020 7:06 PM

Text Document



SHUTDOWN.bat

10/18/2020 7:43 PM

Text Document

Rename



If you change a file name extension, the file might become unusable.

Are you sure you want to change it?

Yes

No

YES you do!

Another way and Harder still.....

I want my damn computer **workstations** OFF at 5:30pm every day! **PERIOD**

I want my damn **SERVER** off 1pm Fridays. **PERIOD**

YES, I tell my staff to turn 'em off at the end of the day but...has your assistant ever asked YOU “Do you want to etch before you bond that tooth?”

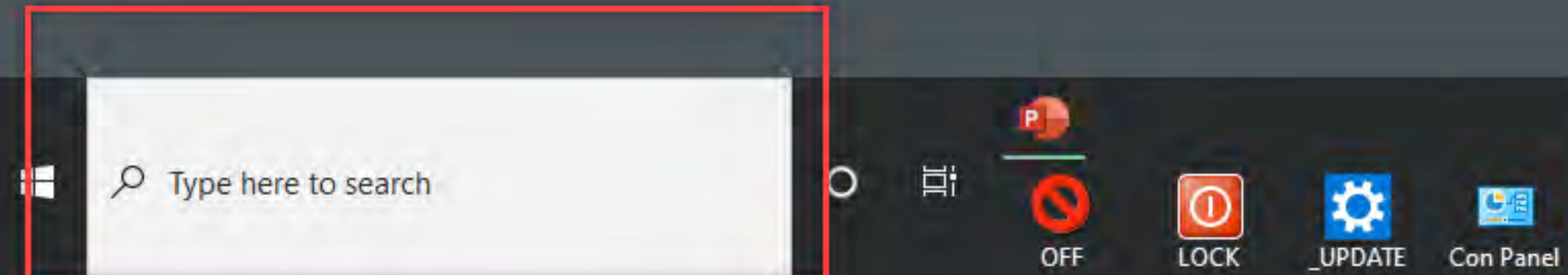
NONE OF US IS SMARTER THAN ALL OF US!

Windows Task: SHUTDOWN

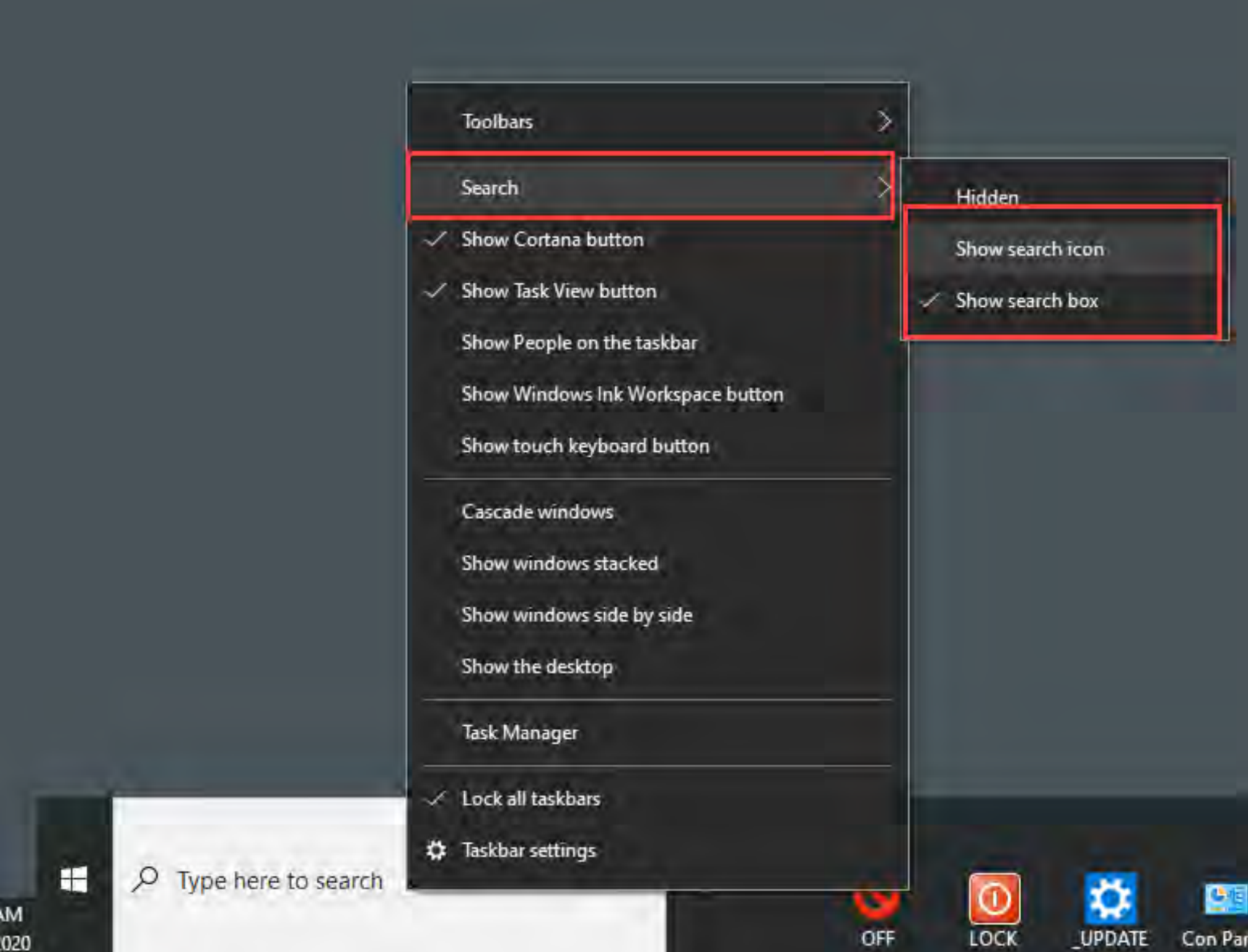
“To-may-to”
search icon

or

“to-mah-to”
search box



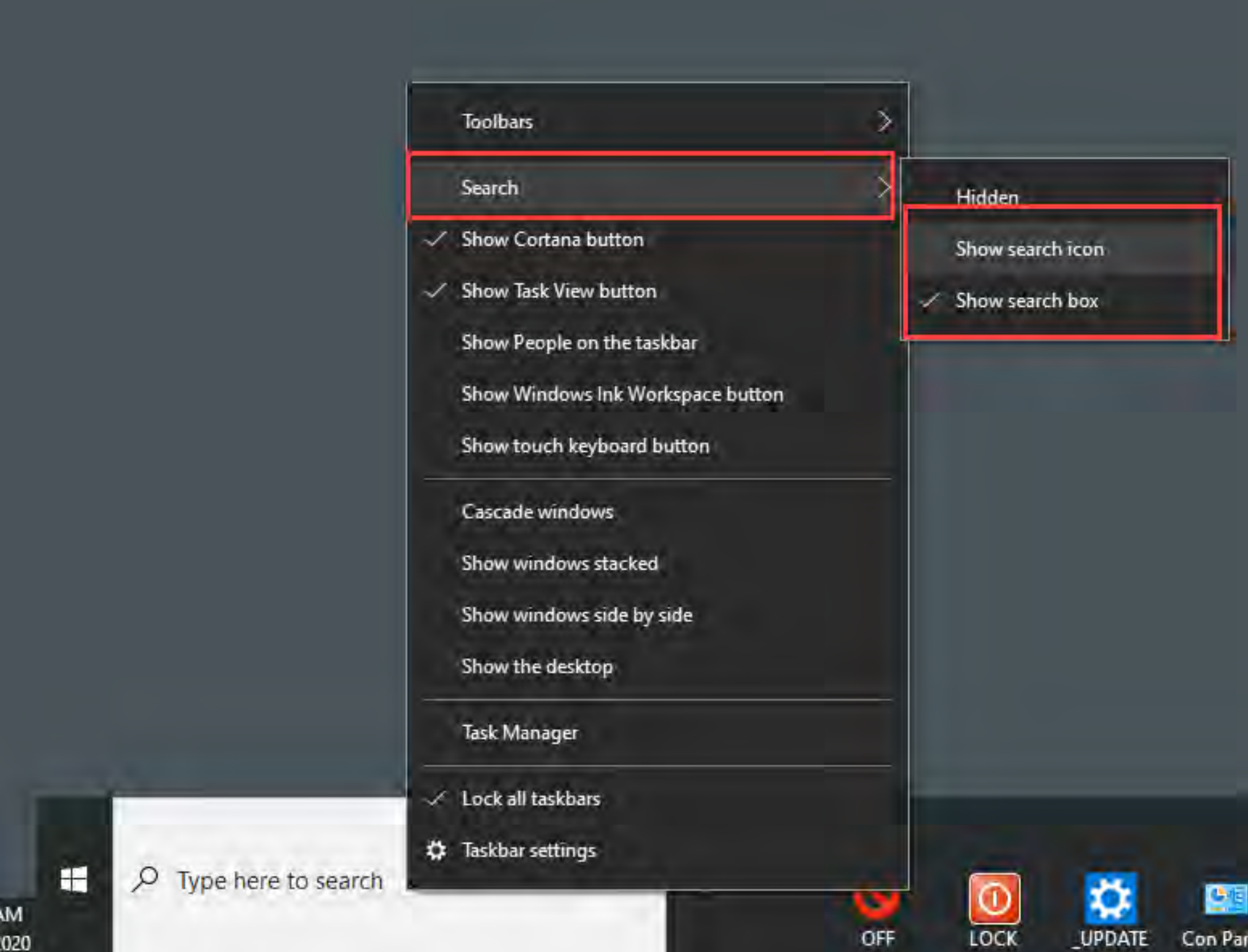
Right click the search box or icon
and:
(icon or box)

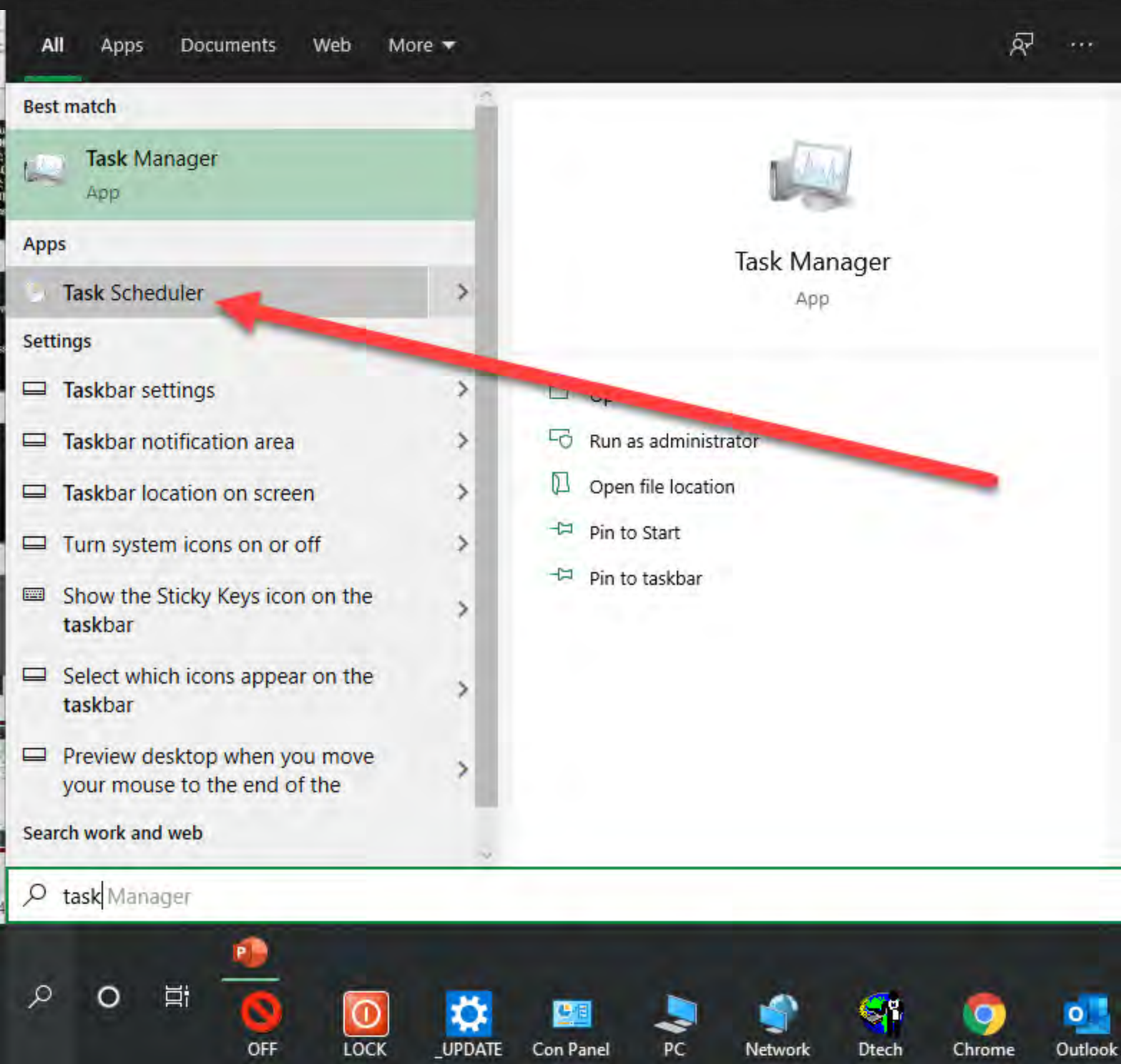


... and type:
task

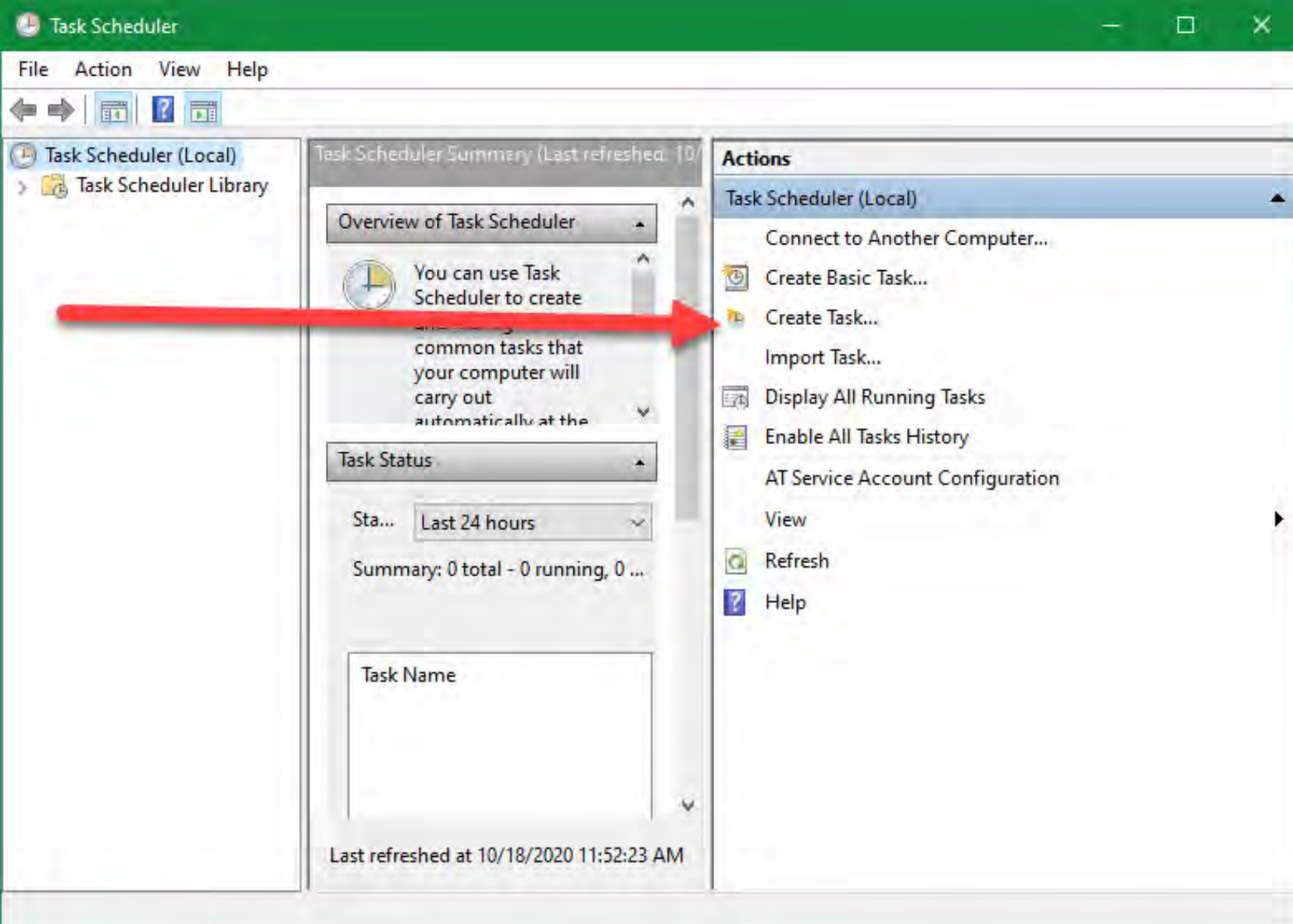
Choices....

Select **Task Scheduler**

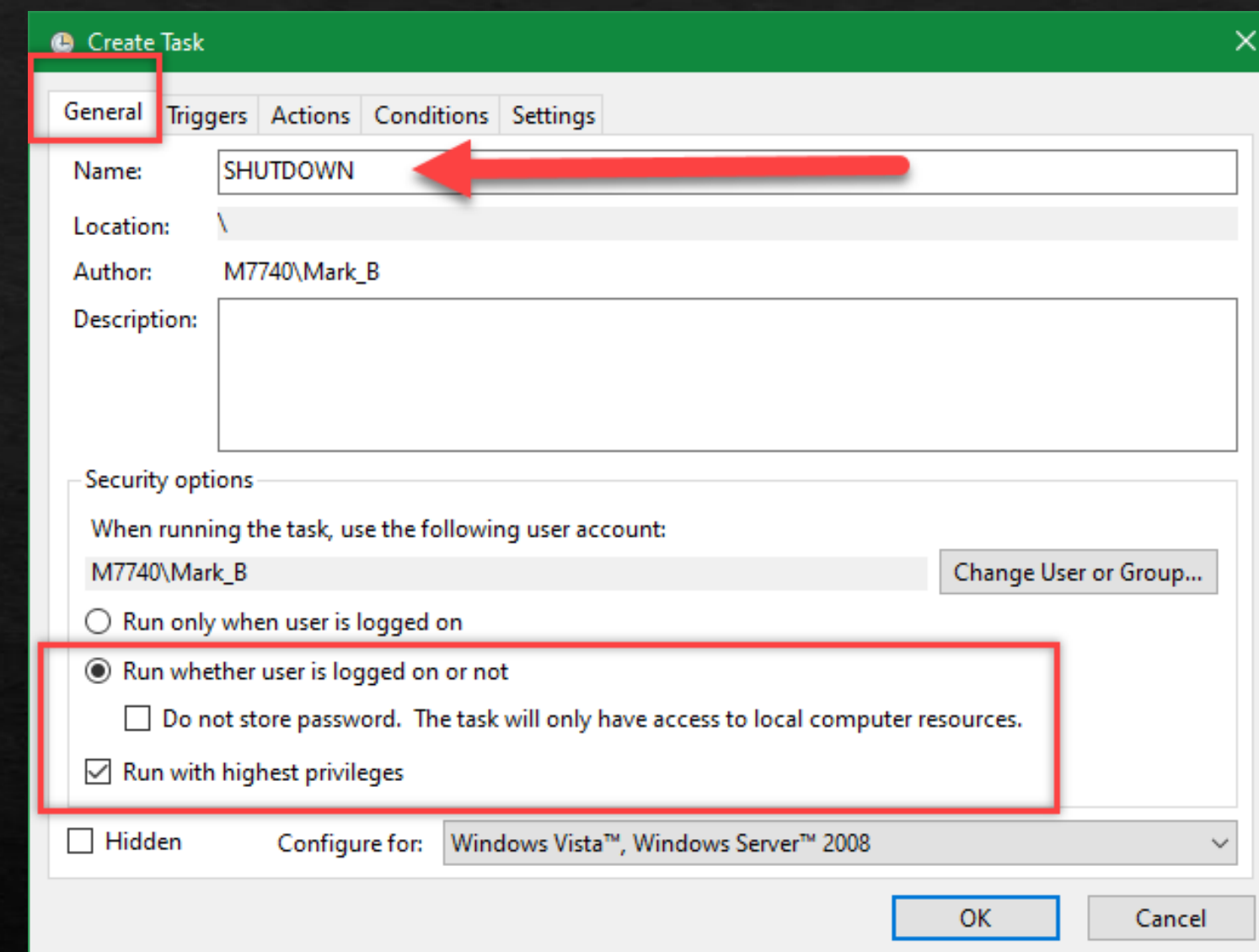


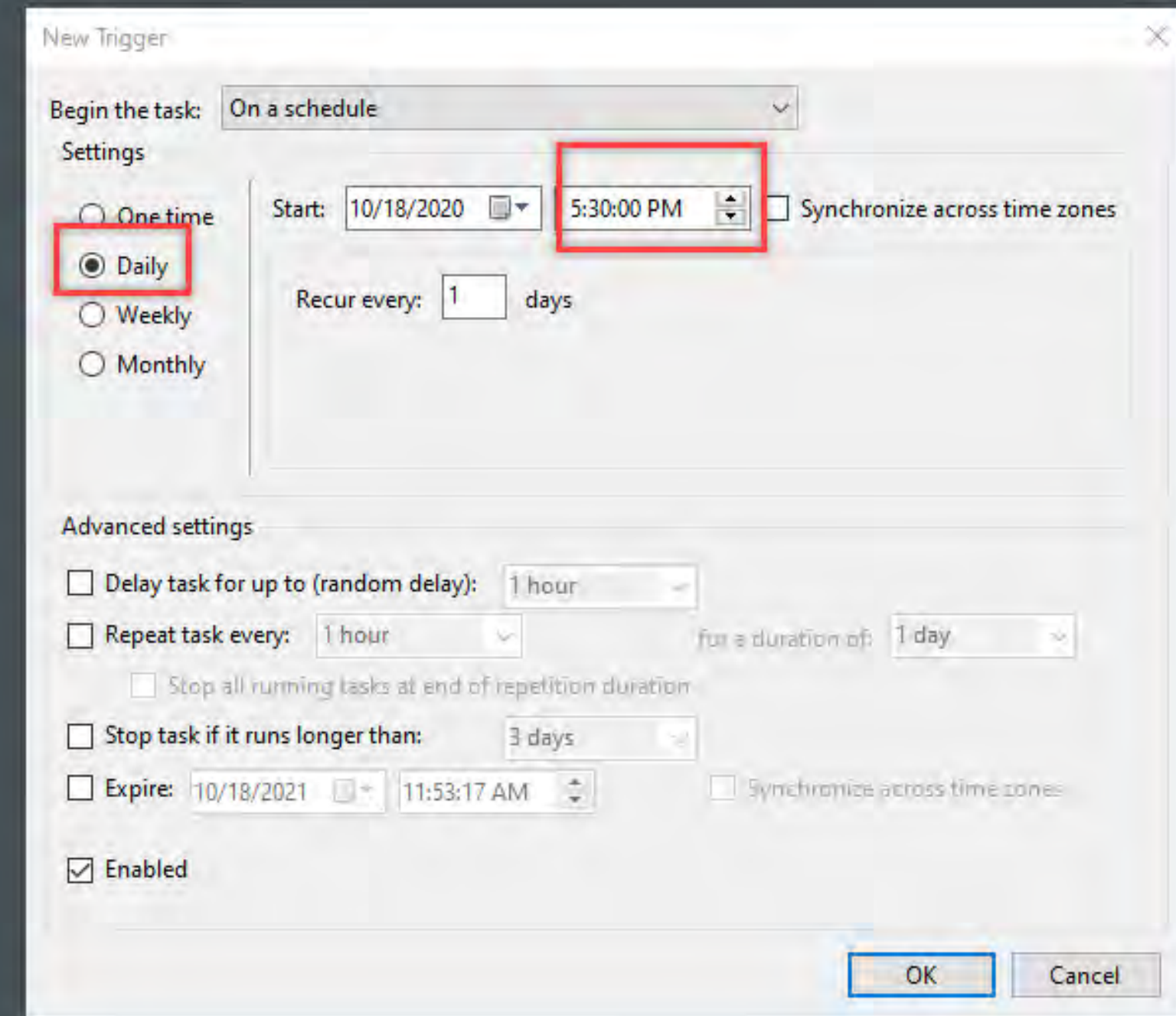
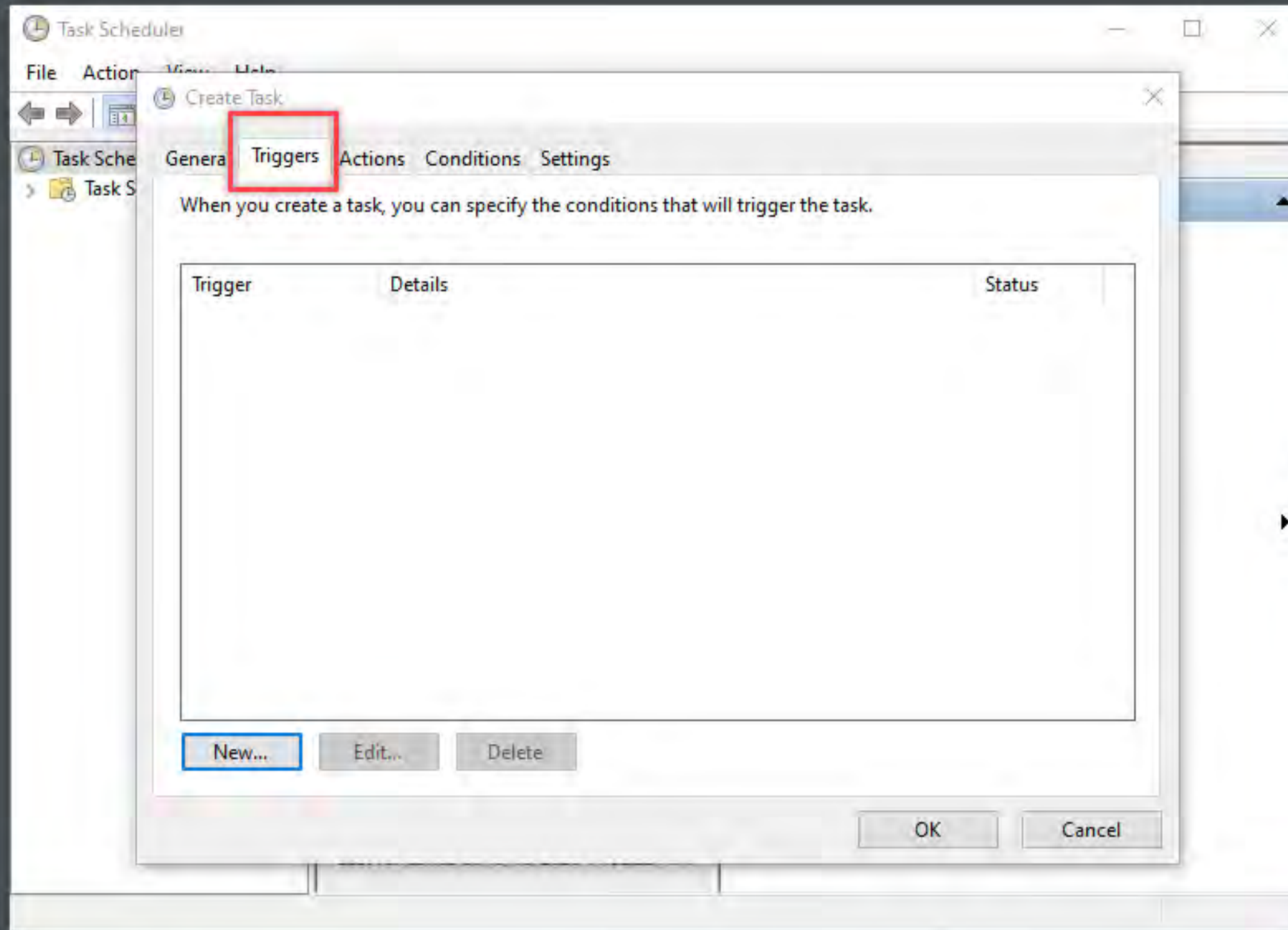


Select “Task Scheduler”



-Create task
-give it a name
and
-check the options

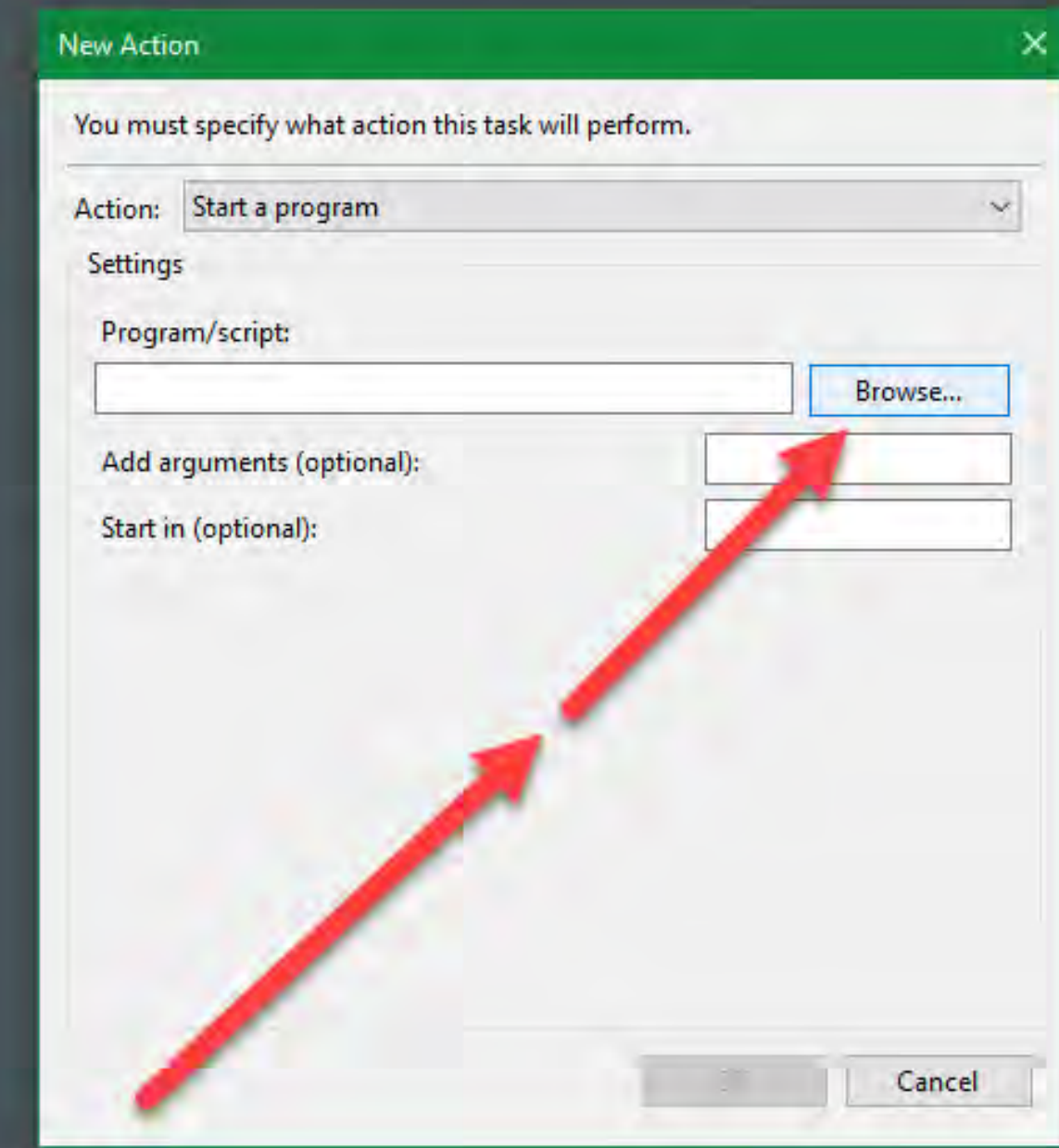
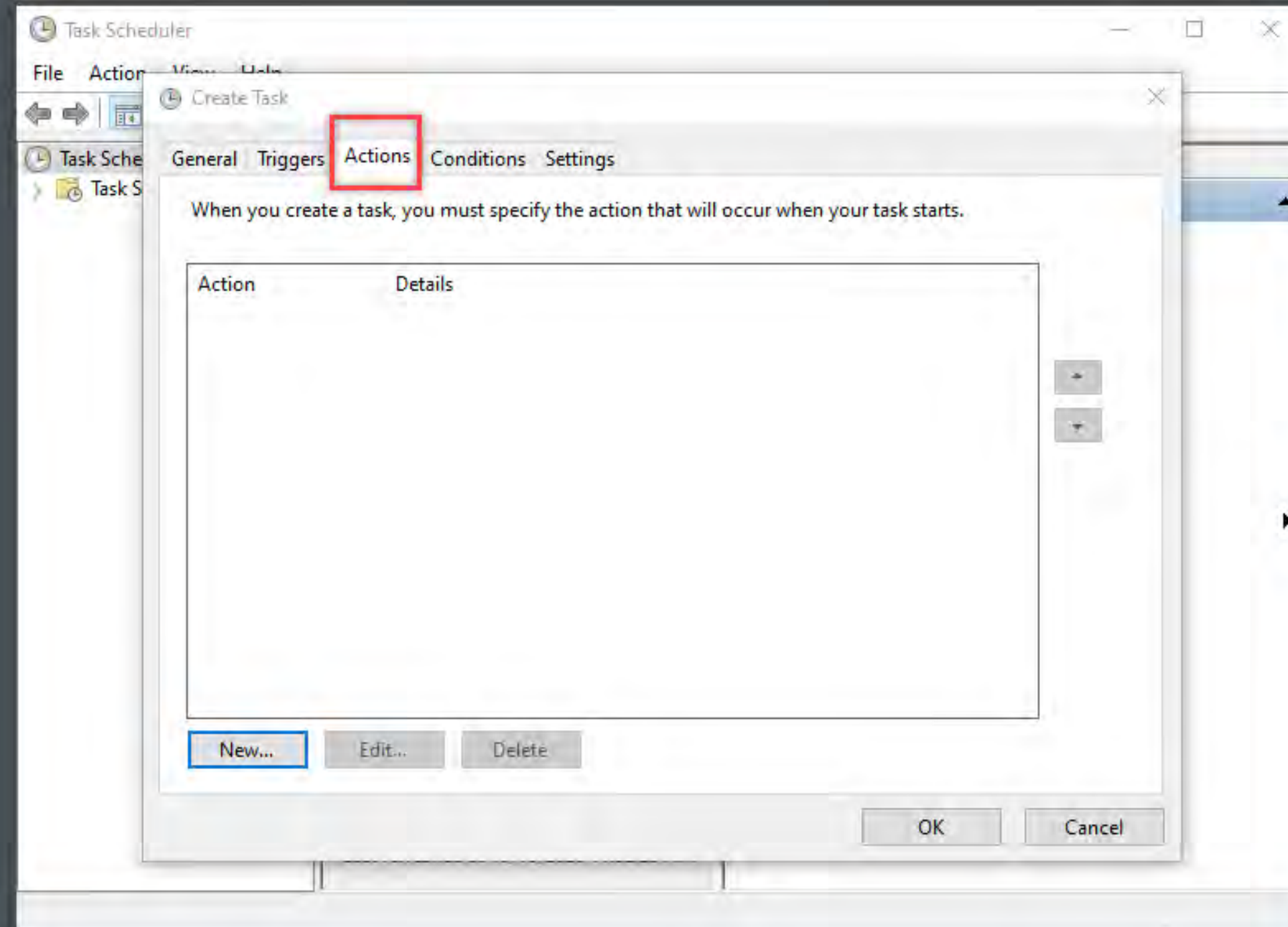


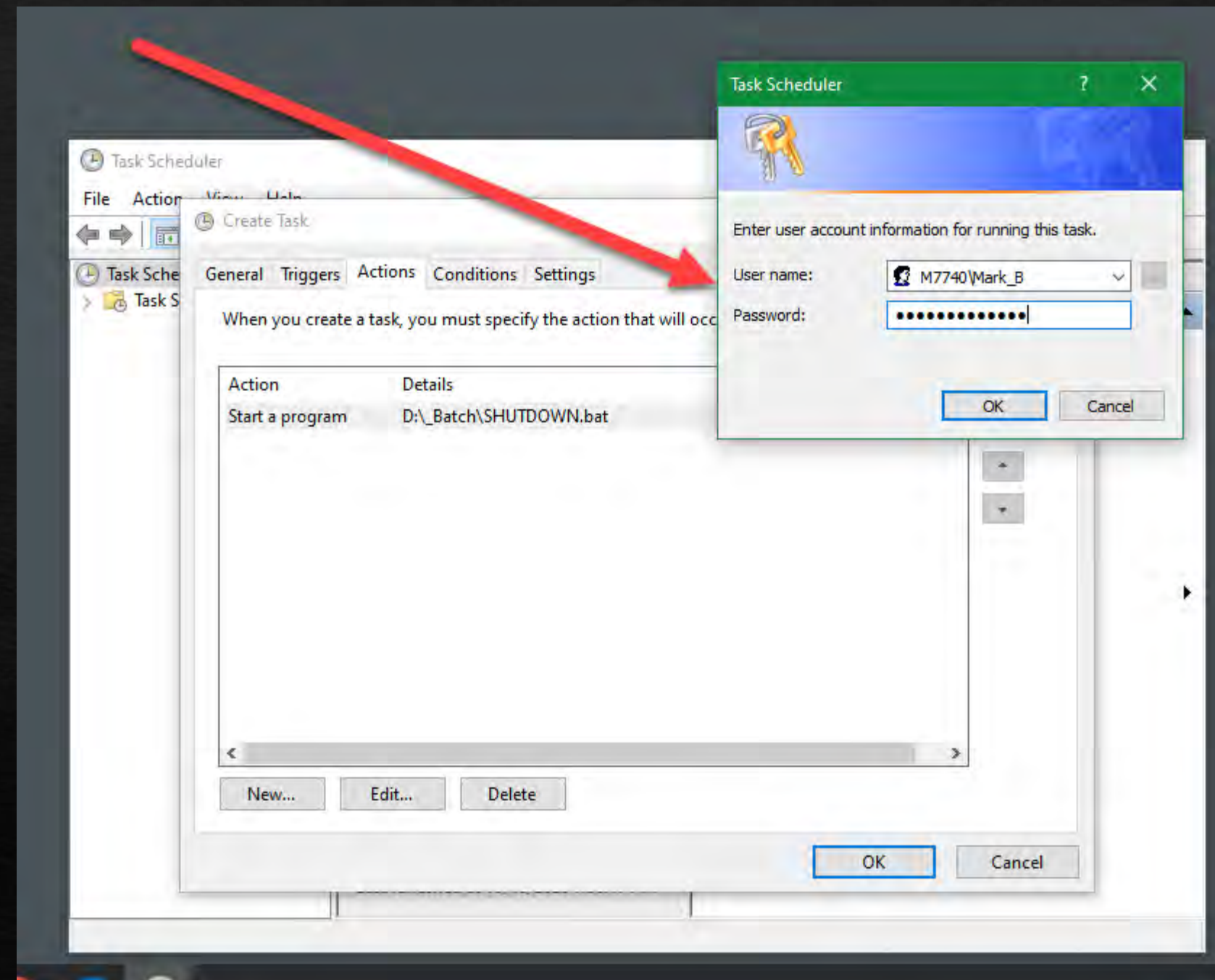
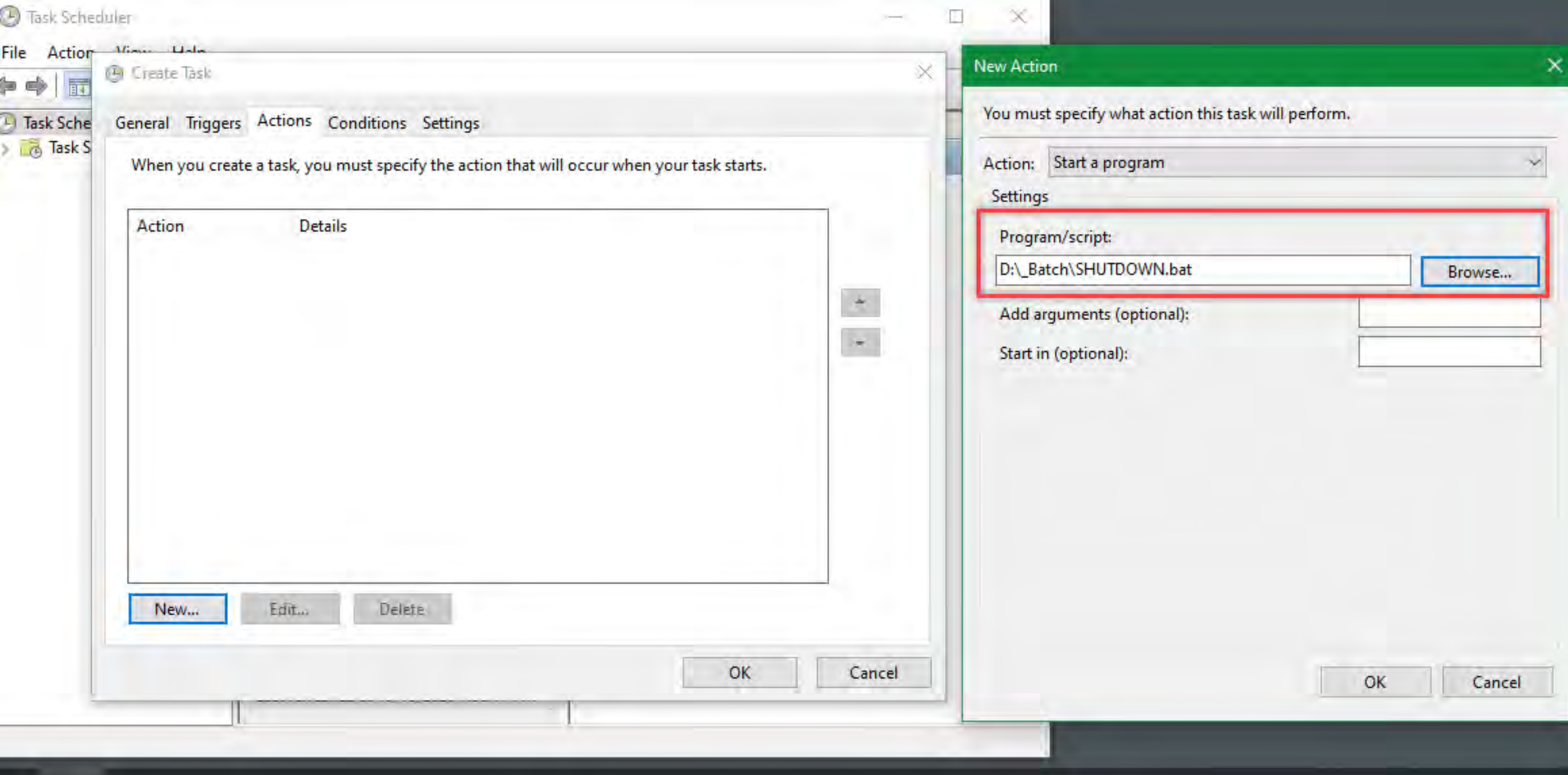


When you create a task, you can specify the conditions that will trigger the task.

Trigger	Details	Status
Daily	At 5:30 PM every day	Enabled

We're going to
'browse' to a
batchfile you've
created (next slide)





Task Scheduler

FileActionViewHelp

Task Scheduler (Local)

Task Scheduler Library

Agent Activation Runt...

Apple

Microsoft

Name	Status	Triggers	Next Run Time
Adobe Acro...	Ready	Multiple triggers defined	10/19/2020 5:00:00 PM
AdobeGCInv...	Ready	At 6:19 PM every day	10/19/2020 6:19:00 PM
Bitdefender ...	Ready	At log on of any user - After triggered, repeat every 1.00:00:00 indefinitely.	
Bitdefender ...	Running	At log on of any user	
CCleaner Up...	Ready	Multiple triggers defined	10/19/2020 5:46:51 AM
CCleanerSki...	Ready		
Dell Support...	Ready	At 1:55 PM every Saturday of every week, starting 9/19/2020	10/24/2020 1:55:05 PM
GarminUpda...	Ready	At 2:00 AM every day	10/19/2020 4:38:48 AM
GoogleUpda...	Ready	Multiple triggers defined	10/19/2020 10:39:14 AM
GoogleUpda...	Ready	At 10:39 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.	10/18/2020 8:39:14 PM
MicrosoftEd...	Ready	Multiple triggers defined	10/19/2020 6:28:24 PM
MicrosoftEd...	Ready	At 6:28 PM every day - After triggered, repeat every 1 hour for a duration of 1 day.	10/18/2020 8:28:24 PM
npcapwatch...	Ready	At system startup	
SHUTDOWN	Ready	At 5:30 PM every day	10/19/2020 5:30:00 PM

If it's OFF, it can't be hacked!

(how many times have I mentioned this?)

KEY!!!

BACKUPS! (EASY!!!!)

3-2-1 and 'Off and Away' backup strategy (FROM 2017)

Most IT professionals recommend a "3-2-1 backup strategy". The idea is to have at least three copies of every file, two of which are on different physical devices, and one of which is located off-site. Hardware fails, so it's clear why you'd want a copy of your data on different hardware. As for why you'd want a backup offsite, Rael LaBreche, information services director at McFarlanes' Manufacturing, explains:

"One of our saving graces prior to a business fire in 2013 was that we had backups offsite, so the only data information we lost was from the day of the fire. I would caution every business to seriously consider implementing a business disaster plan that includes regularly replacing and storing backups offsite -- it's a small task that in return could save your business."

The "off" strategy: Keep one backup in storage, powered off and not connected to anything. This protects you from situations like ransomware, where a virus propagates throughout a network and encrypts files, **even your (CLOUD!!) backups**. If you have an unplugged, powered off, unconnected backup, it's safe.

The "away" strategy: I live in Florida, where we have hurricanes. While it's good to have an offsite backup, it's even better to have an offsite backup that's outside of your region. That way, if your entire state gets knocked back to the Stone Age, your data is still alive and available. Cloud backup services are ideal for the away strategy. They often keep multiple copies of your data, and keep them in multiple data centers.

MY OFFLINE BACKUPS:
Bitlocker Encrypted “in case” they’re
pried from my cold dead fingers

2TB NVME SSD’s
USB3.1 and/or Thunderbolt

Google ‘Sabrent’
Google ‘fastest NVME 2Tb’



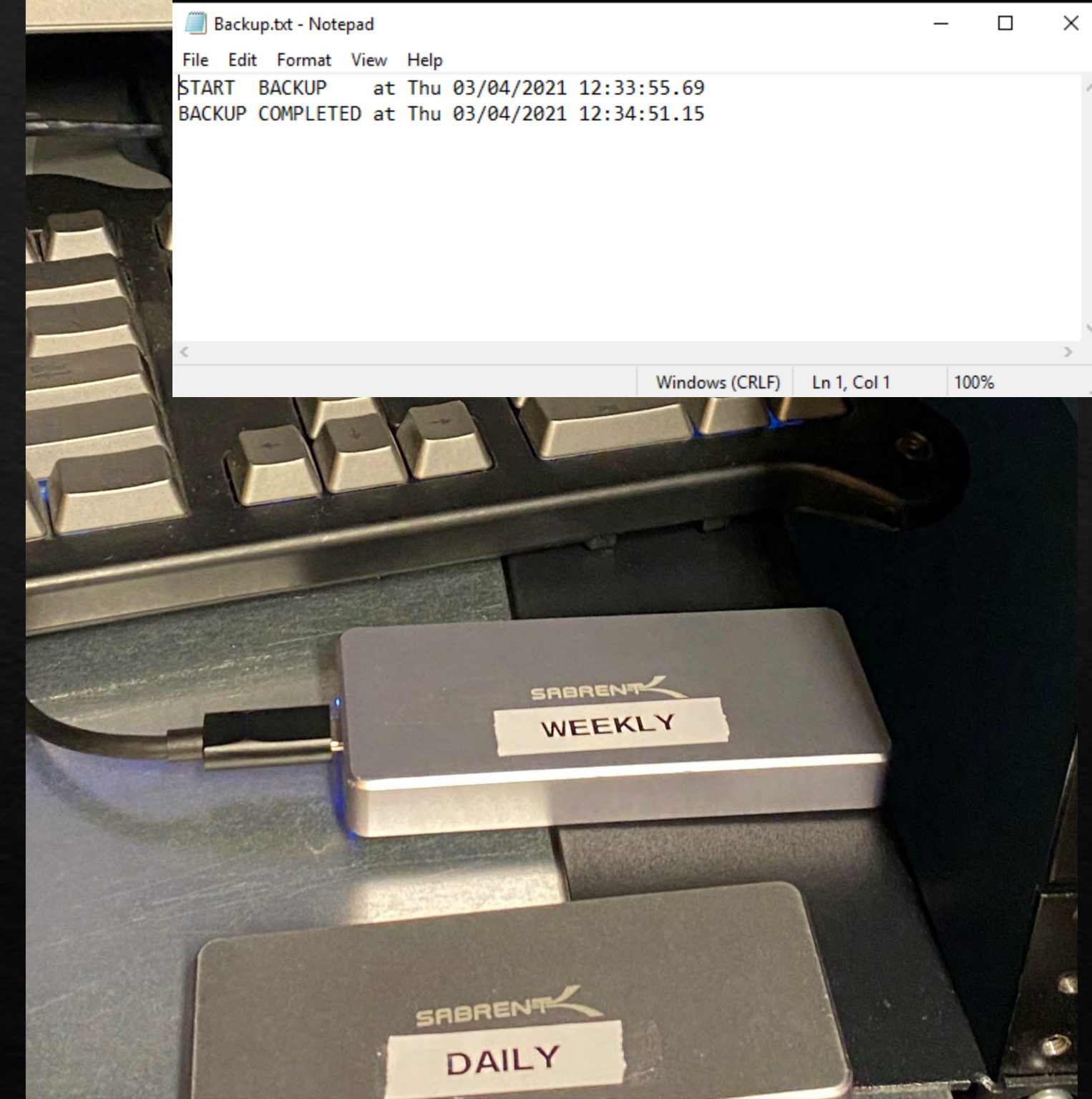


BACKUPS:

My Sabrent NVME backup
takes **1 min!**

I also use NAS and it's...
OFF 23.50hrs/day!

I also...
RSYNC to multiple machines



REM **PATH** ADDED or else Robocopy runs!! (hell if I know why!)

C:\Windows\System32\xcopy **D:_Batch** U:\m7720_Batch /c/s/i/f/y/d/r

C:\Windows\System32\xcopy **D:_CBCT** U:\m7720_CBCT /c/s/i/f/y/d/r

C:\Windows\System32\xcopy **D:_DOCS** U:\m7720_DOCS /c/s/i/f/y/d/r

C:\Windows\System32\xcopy **P:_PATIENTS** U:\m7720_PATIENTS /c/s/i/f/y/d/r

I'm **ALSO** copying from my laptop hard drive(s) (D, P) to an external drive –
DAILY!

My laptop is backed up both at HOME and at OFFICE to external drives
External drives then turned **OFF (WHY???)**

SERVER

Daily Master Backup to a NAS

Backup (~7min)
Verify (~4min)

SW Compression	= 76%
Elapsed Time	= 00:06:51
Data Transfer Speed	= 19.328 GB/hr = 330.009 MB/min = 5767337 bytes/sec
Relative Speed	= 63.512 GB/hr = 1084.121 MB/min = 18946389 bytes/sec
Exit Status	= 0
Actual Medium Usage	= 96%
Non-reclaimable Usage	= 3%
[Verify of dtech430:system]	
Archive ID: 5f8e1ccc00006e63	
Instance ID: 5f8e2a2700007442	
SUMMARY - BYTE-BY-BYTE VERIFICATION	
Serial Number	:
Date	= Tue Oct 20 00:15:08 2020
Segments Used	= 2
Data Read	= 1.86GB
Elapsed Time	= 00:03:15
Data Transfer Speed	= 65.375 GB/hr = 1116.009 MB/min = 19503684 bytes/sec
Files Encountered	= 355946
Files Excluded	= 4
Special Files	= 31152
Verified Successfully	= 324790
Change Log	= /usr/lib/edge/lists/simple_job/

HOW SECURE IS YOUR OFFICE? Or HOME?

“This stuff is over my head, Mark!
I’ll delegate it!”

Former SolarWinds CEO blames intern for 'solarwinds123' password leak

CNN · 2 days ago

- **SolarWinds Officials Blame Intern for 'solarwinds123' Password**

Gizmodo · 22 hours ago

 [View Full Coverage](#)

Microsoft: We've open-sourced this tool we used to hunt for code by SolarWinds hackers

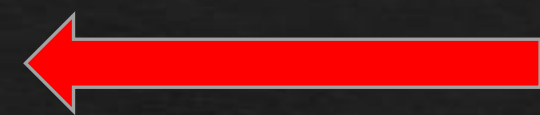
ZDNet · 2 days ago

SolarWinds Hack Pits Microsoft Against Dell, IBM Over How Companies Store Data

The Wall Street Journal · Yesterday

The SolarWinds Body Count Now Includes NASA and the FAA

WIRED · Yesterday



SOLARWINDS

AND

PERCSOFT

29 Ransomware Bites Dental Data Backup Firm

AUG 19

PerCSoft, a Wisconsin-based company that manages a remote data backup service relied upon by hundreds of dental offices across the country, is struggling to restore access to client systems after falling victim to a ransomware attack.

THE DIGITAL
Dental Record

SEARCH



IMPORTANT MESSAGE FOR DDS SAFE CLIENTS

DIGITAL SOLUTIONS

ESERVICE BUNDLES

HIPAA SOLUTIONS

FORMS & CHARTS

MORE

Encrypted. Integrated.
SIMPLIFIED.



West Allis, Wis.-based **PerCSoft** is a cloud management provider for **Digital Dental Record** (DDR), which operates an online data backup service called **DDS Safe** that archives medical records, charts, insurance documents and other personal information for various dental offices across the United States.

The ransomware attack hit PerCSoft on the morning of Monday, Aug. 26, and encrypted dental records for some — but not all — of the practices that rely on DDS Safe.

blackbaud data breach 2020 - Gr

google.com/search?q=blackbaud+data+breach+2020&oq=blackbau...

Google

blackbaud data breach 2020

All News Images Videos Maps More Settings Tools

About 168,000 results (0.51 seconds)

www.thenonproftimes.com › npt_articles › the-hack-o-...
The Hack Of Blackbaud: Damage Is Still Being Assessed - The ...
Aug 6, 2020 — August 6, 2020 ... The cloud software company **Blackbaud** has reported a **data breach** incident which has potentially affected a large number of ...

portswigger.net › daily-swig › blackbaud-hack-us-healt...
Blackbaud hack: US healthcare organizations confirm data ...
Sep 16, 2020 — **Blackbaud** hack: US healthcare organizations confirm **data breach** impacted 190,000 patients. Jessica Haworth 16 September 2020 at 14:15 ...

www.welivesecurity.com › 2020/08/06 › blackbaud-dat...
Blackbaud data breach: What you should know | WeLiveSecurity
Aug 6, 2020 — Has your personal **data** been stolen in the **breach** at **Blackbaud**? ... In the 30 days of June 2020, there are 38 such notifications listed on the ...

healthitsecurity.com › news › blackbaud-confirms-hack...
Blackbaud Confirms Hackers Stole Some SSNs, as Lawsuits ...
Sep 30, 2020 — The **Blackbaud** breach victim tally is piling up, as is its impact: an SEC filing shows ... September 30, 2020 - The ransomware hackers behind the massive **Blackbaud** ransomware attack and subsequent **data breach** likely had ...

www.eidebailly.com › insights › articles › 2020 › black...
Blackbaud Data Breach: What You Need to Know
Aug 26, 2020 — On May 14, 2020, **Blackbaud** was hit with a ransomware attack that wasn't

uhs cyber attack - Google Search

google.com/search?q=uhs+cyber+attack&oq=uhs+&aqs=chrome.3.6...

Google

uhs cyber attack

www.healthcareitnews.com › news › uhs-says-all-us-fac...
UHS says all U.S. facilities affected by apparent ransomware ...
Oct 2, 2020 — **UHS** says all U.S. facilities affected by apparent ransomware attack ... AI and machine learning: a gift, and a curse, for **cybersecurity**. By.

www.healthcareitnews.com › news › uhs-says-recovery...
UHS says recovery process complete for corporate data ...
Oct 5, 2020 — **UHS** says recovery process complete for corporate data centers after **cyberattack**. The Pennsylvania-based chain was targeted by an apparent ...

medcitynews.com › 2020/09 › uhs-breach-signals-grief...
UHS breach signals grief ahead for hospitals - MedCity News
Sep 30, 2020 — A malware attack brought hospital chain **Universal Health Services**' IT systems down at the beginning of the week. **Cybersecurity** experts said

healthitsecurity.com › news › 3-weeks-after-ransomwar...
3 Weeks After Ransomware Attack, All 400 UHS Systems ...
Oct 13, 2020 — The **UHS** IT team brought all 400 US health system sites back online, ... healthcare data breach ransomware attack **cybersecurity** **cyberattack** ...

www.fiercehealthcare.com › tech › uhs-breach-shows-d...
UHS breach shows the dangers facing hospitals with growing ...
Oct 2, 2020 — The **UHS** **cyberattack** is just the latest example of the growing cyber ... illustration of healthcare cybersecurity with text medical data breach on a ...

www.fiercehealthcare.com › tech › uhs-hit-massive-cyb...
UHS hit with massive cyberattack as hospitals reportedly ...
Sep 28, 2020 — A major hospital chain has been hit by a massive **cyberattack** that reportedly has

KrebsonSecurity
In-depth security news and investigation

29 Ransomware Bites Dental Data Backup Firm
AUG 19

PerCSOft, a Wisconsin-based company that manages a remote data backup service relied upon by hundreds of dental offices across the country, is struggling to restore access to client systems after falling victim to a ransomware attack.

THE DIGITAL Dental Record

SEARCH

*****IMPORTANT MESSAGE FOR DDS SAFE CLIENTS*****

DIGITAL SOLUTIONS ESERVICE BUNDLES HIPAA SOLUTIONS FORMS & CHARTS MORE

Encrypted. Integrated.
SIMPLIFIED.

West Allis, Wis.-based **PerCSOft** is a cloud management provider for **Digital Dental Record** (DDR), which operates an online data backup service called **DDS Safe** that archives medical

How secure is your home or office?

[HOME](#) ▸ [TECHNOLOGY EXPLAINED](#)

What Is Port Scanning and How Does It Work?

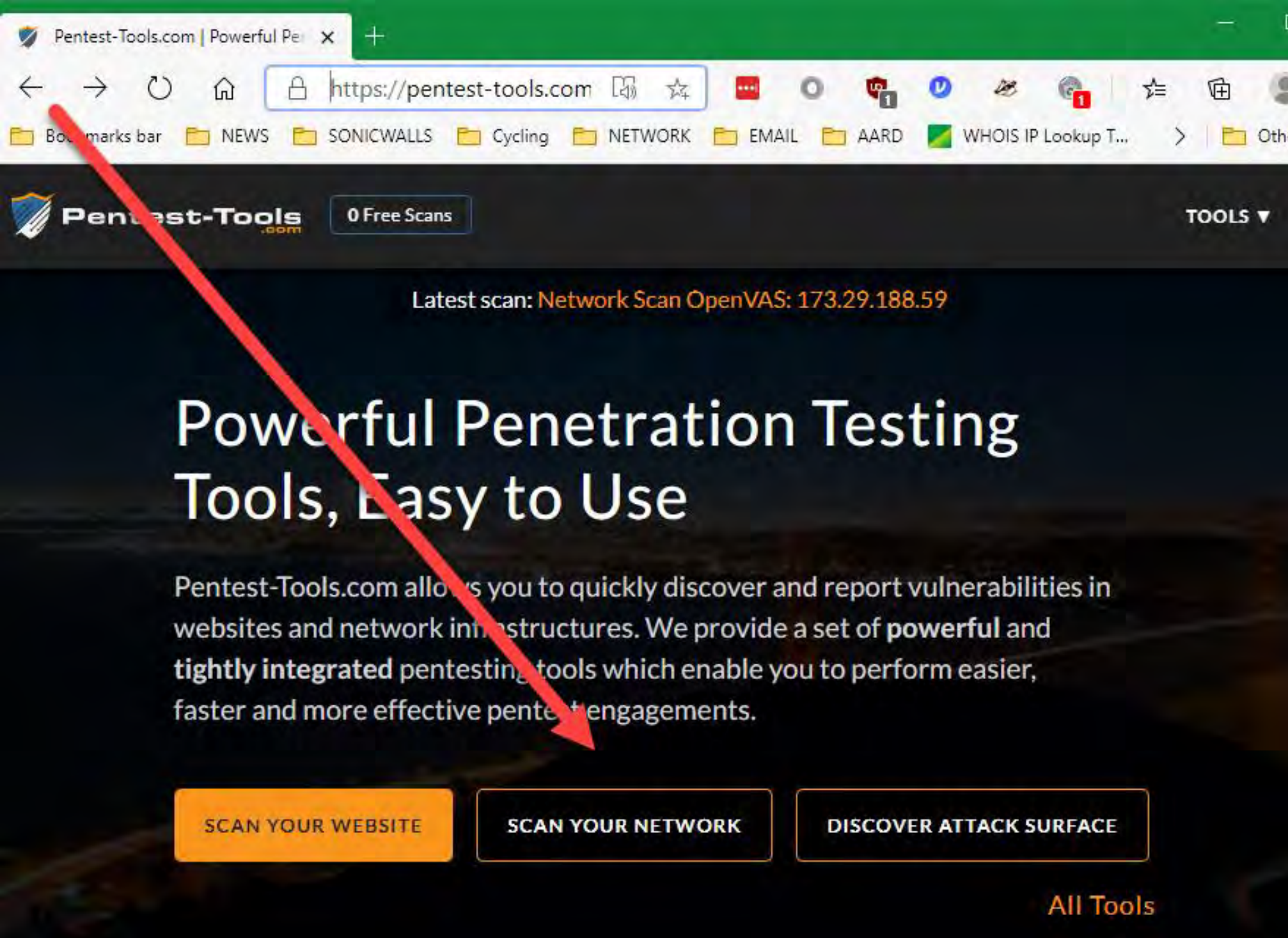
Is it safe to leave your ports open?

BY SIMON BATT

PUBLISHED 22 HOURS AGO



When your computer goes on the internet, it uses "ports" to help do its job. Both network administrators and hackers are keen to scan these ports for weaknesses, but what is a port, and why are people scanning them?



EASY!

Penetration Testing

<https://pentest-tools.com/home>

GRC.com

(both)

Pen-Testing

and

Password Strength

Home of Gibson Research Corp. X +

grc.com/intro.htm

Apps MY NEWS PC's Excel Cycling SONICWALLS NETWORK EMAIL AARD SECURITY Website Builder Rev... Cameras BIRDS HIPAA Od

Gibson Research Corporation • Security

Home ▾ SpinRite ▾ Services ▾ Freeware ▾ Research ▾ Other ▾

Gibson Research Corporation Proudly Announces



The industry's #1 hard drive data recovery software is NOW COMPATIBLE with NTFS, FAT, Linux, and ALL OTHER file systems!

And the exclusive home of . . .

ShieldsUP!!™

More than 104,876,723 shields tested!

To proceed, click the logos or select from the menu above.

GRC | ShieldsUP! — Internet Vuln x

grc.com/x/ne.dll?bh0bkyd2

AppsMYNEWSPC'sExcelCyclingSONICWALLSNETWORKEMAILAARDSECURITYWebsite Builder Rev...CamerasBIRDSHIPAAweatherCOMMUNICATOR

Gibson Research Corporation • Data Recovery

Home ▾SpinRite ▾Services ▾ShieldsUP!Certificate RevocationPassword HaystacksHTTPS FingerprintsSecurity Now!DNS Spoofability TestPerfect PasswordsPPP PasswordsTech TV video clipsNewsgroup Discussions

Research ▾Other ▾

Search

Welcome to ShieldsUP!

If you have not visited for some time, please note that:

- Our new **Perfect Passwords** facility is used by thousands of people every day to generate ultra-high-quality random passwords for securing WiFi and other services.
- Our weekly **Security Now!** audio podcast has covered **every security issue** you might have. These mp3 audio files are freely downloadable, and since we have transcripts of every podcast, you can use our sitewide search to find any podcast by keyword.

If you are new to this site and our services:

Please take just a moment to read and consider these three points:

Your use of the Internet security vulnerability profiling services on this site constitutes your FORMAL PERMISSION for us to conduct these tests and requests our transmission of Internet packets to your computer. ShieldsUP!! benignly probes the target computer at your location. Since these probings must travel from **our** server to **your** computer, you should be certain to have administrative right-of-way to conduct probative protocol tests through any and all equipment located between your computer and the Internet.

NO INFORMATION gained from your use of these services will be retained, viewed or used by us or anyone else in any way for any purpose whatsoever.

If you are using a personal firewall product which LOGS contacts by other systems, you should expect to see entries from this site's probing IP addresses: **4.79.142.192** -thru- **4.79.142.207**. Since we own this IP range, these packets will be from us and will NOT BE ANY FORM OF MALICIOUS INTRUSION ATTEMPT OR ATTACK on your computer. You can use the report of their arrival as handy confirmation that your intrusion logging systems are operating correctly, but please do not be concerned with their appearance in your firewall logs. It's expected.

Proceed

ShieldsUP!!

Port Authority Edition – Internet Vulnerability Profiling

by Steve Gibson, Gibson Research Corporation.



Greetings.

Without your knowledge or explicit permission, the Windows networking technology which connects your computer to the Internet **may be offering some or all of your computer's data to the entire world at this very moment!**

- **For orientation and background**, please examine the page links provided below for important information about Internet vulnerabilities, precautions and solutions.
- **First time users** should start by checking their **Windows File Sharing** and **Common Ports** vulnerabilities with the "File Sharing" and "Common Ports" buttons below.
- For orientation and information about the Port Authority system, **click the Home or Help icons** in the titlebar . . .

[Click here to check your router now...](#)

**GRC's Instant UPnP
Exposure Test**

HOME		ShieldsUP!! Services		HELP
File Sharing	Common Ports	All Service Ports	Messenger Spam	Browser Headers
You may select any service from among those listed above . . .				
User Specified Custom Port Probe		Lookup Specific Port Information		
Or enter a port to lookup, or the ports for a custom probe to check, then choose the service. Your computer at IP 108.166.136.253 will be tested.				

TEST

- COMMON PORTS
- ALL SERVICE PORTS
- CUSTOM PORTS (3389)

PORT 3389= RDP
(Remote Desktop Protocol)
= #2 way of getting
Ransomware

ShieldsUP!!

Port Authority Edition – Internet Vulnerability Profiling

by Steve Gibson, Gibson Research Corporation.

Checking the Most Common and Troublesome Internet Ports

This Internet Common Ports Probe attempts to establish standard TCP Internet connections with a collection of standard, well-known, and often vulnerable or troublesome Internet ports on **YOUR** computer. Since this is being done from **our** server, successful connections demonstrate which of your ports are "open" or visible and soliciting connections from passing Internet port scanners.

Your computer at IP:

[REDACTED]

I'm hiding my IP address...

Is being profiled. Please stand by. . .

[REDACTED]

Total elapsed testing time: 5.095 seconds

PASSED

**TruStealth
Analysis**

PASSED

Your system has achieved a **perfect** "TruStealth" rating. **Not a single packet** — solicited or otherwise — was received from your system as a result of our security probing tests. Your system ignored and refused to reply to repeated Pings (ICMP Echo Requests). From the standpoint of the passing probes of any hacker, this machine does not exist on the Internet. Some questionable personal security systems expose their users by attempting to "counter-probe the prober", thus revealing themselves. But your system wisely remained silent in every way. Very nice.

GRC ONLY works at whatever network you are located,
i.e. I cannot remotely test another network

Perform these tests both at home and office
If anything appears open, time to talk with IT!!!

And don't forget to run those OTHER tests

Scanning “all service ports”

Determine the status of your
system's first 1056 ports

- This Internet service ports "grid scan" determines the status — ■ Open, ■ Closed, or ■ Stealth — of your system's first 1056 TCP ports.
- 32 ports, represented by each horizontal row, are probed as a group. The results are posted as the next set of ports are probed.
 - During off-peak hours the entire scan requires just over one minute.
 - For guaranteed accuracy, the scanning time will increase during peak usage when many people are sharing our scanning bandwidth.
 - A scan of a stealthed system is up to four times slower since many more probes must be sent to guarantee against Internet packet loss.
 - The test may be abandoned at any time if you do not wish to wait for the scan to finish.
 - You may hover your mouse cursor over any grid cell to determine which port it represents, or click on the cell to jump to the corresponding Port Authority database page to learn about the port's specific role, history, and security consequences. (Depress SHIFT when clicking to open new window and allow unfinished test to continue.)

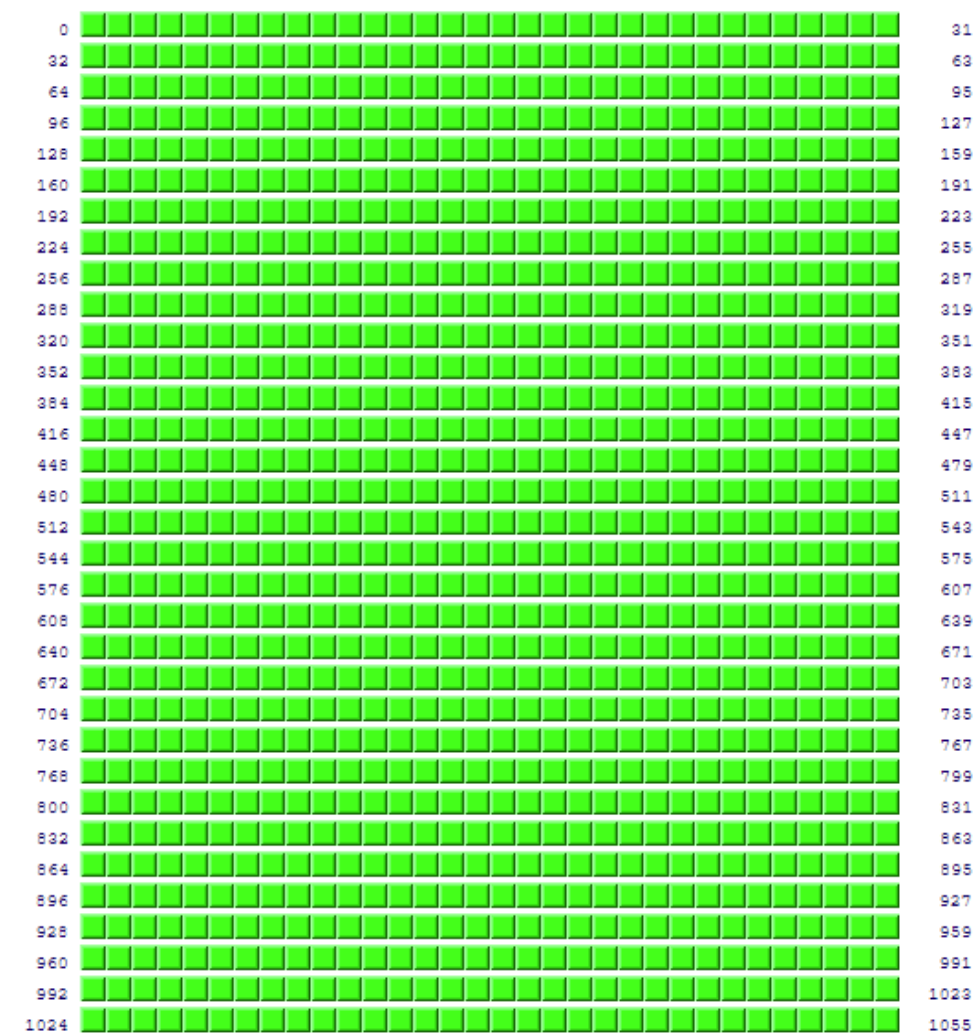
Your computer at IP:

192.168.1.100

Is being carefully examined:

0	<div></div>	31
32	<div></div>	63
64	<div></div>	95
96	<div></div>	127
128	<div></div>	159
160	<div></div>	191
192	<div></div>	223
224	<div></div>	255
256	<div></div>	287
288	<div></div>	319
320	<div></div>	351
352	<div></div>	383
384	<div></div>	415
416	<div></div>	447
448	<div></div>	479
480	<div></div>	511
512	<div></div>	543
544	<div></div>	575
576	<div></div>	607
608	<div></div>	639
640	<div></div>	671
672	<div></div>	703
704	<div></div>	735
736	<div></div>	767
768	<div></div>	799
800	<div></div>	831

Is being carefully examined:



The port number of any location on the grid above may be determined by floating your mouse over the square. Most web browsers will display a pop-up window to identify the port. Otherwise, see the URL display at the bottom of your browser.

Open Closed Stealth

Text Summary

Total elapsed testing time: 69.031 seconds

PASSED

TruStealth
Analysis

PASSED

#2 way to get Ransomware is RDP (port 3389)

[Click here to check your router now...](#)

**GRC's Instant UPnP
Exposure Test**

HOME

ShieldsUP!! Services

File Sharing

Common Ports

All Service Ports

Messenger Sp

You may select any service from among those listed above ...

3389

User Specified Custom Port Probe

Or enter a port to lookup, or the ports for a custom probe to check, then
choose the service. Your computer at IP 108.166.136.253 will be tested.



Gibson Research Corporation is owned and operated by Steve Gibson. The contents of this page are Copyright (c) 2020 Gibson Research Corporation. SpinRite, ShieldsUP, NanoProbe, and any other indicated trademarks are registered trademarks of Gibson Research Corporation, Laguna Hills, CA, USA. GRC's web and customer [privacy policy](#).

Jump
To Top

IF A DDS CAN
DO THIS....
HOPEFULLY
your IT can also!

BELLCURVES

User-Specified Custom Port Probe

This Internet port probe attempts to establish standard TCP Internet connections with any set of up to 64 ports specified by the user.

Your computer at IP:

Is now being examined:

Total elapsed testing time: 5.063 seconds

PASSED

TruStealth Analysis

PASSED

Your system has achieved a **perfect** "TruStealth" rating. **Not a single packet** — solicited or otherwise — was received from your system as a result of our security probing tests. Your system ignored and refused to reply to repeated Pings (ICMP Echo Request). From the standpoint of the passing probes of any hacker, this machine does not exist on the Internet. Some questionable personal security systems expose their users by attempting to "counter-probe the prober", thus revealing themselves. But your system wisely remained silent in every way. Very nice.

Port	Status	Protocol and Application
3389	Stealth	msrdp Microsoft Remote Display Protocol

The ports you specified have been successfully probed. Their open, closed, or stealth status is displayed in the table above. This Text Summary button provides a textual report that can be printed, copied, and saved:

Text Summary

ADVANCED PENETRATION TESTING

Tenable's "NESSUS ESSENTIALS:"
TEST YOUR OFFICE and HOME
FROM ANYWHERE!
FREE version good for scanning 16 IP
addresses!



TENABLE IS

#1 IN
VULNERABILITY
MANAGEMENT



Tenable Ranks #1

in the IDC Worldwide Device
Vulnerability Management
Market Shares, 2019 Report

[Read the Report Excerpt](#)



Tenable Named a Leader
in Vulnerability Risk
Management, Q4 2019 The
Forrester Wave™

[Read the Report](#)



As part of the Nessus family, Nessus® Essentials (formerly Nessus Home) allows you to scan your environment (up to 16 IP addresses per scanner) with the same high-speed, in-depth assessments and agentless scanning convenience that Nessus subscribers enjoy.

Please note that Nessus Essentials does not allow you to perform compliance checks or content audits, Live Results or use the Nessus virtual appliance. If you require these additional features, please purchase a [Nessus Professional](#) subscription.

Using Nessus Essentials for education? Register for Nessus Essentials through the [Tenable for Education](#) program to get started.

Register for an Activation Code

First Name *

Last Name *

Email *

☐ Check to receive updates from Tenable


[Register](#)

T

- tenable.io
- tenable.sc™
- tenable Lumin
- nessus
- tenable.ot™
Powered by Indegy
- tenable.io
Container Security
- tenable.io
PCI ASV
- tenable.io
Web App Scanning

nessus

The #1 vulnerability assessment solution.



[Learn More](#)

tenable® Cyber Exposure Products Solutions Research Support Company Partners Resources [Free Trial](#) [Buy Now](#)

THE NESSUS FAMILY

Nessus is trusted by more than 30,000 organizations worldwide as one of the most widely deployed security technologies on the planet - and the gold standard for vulnerability assessment.

nessus Essentials

FREE DOWNLOAD
Scan 16 IPs

- ✓ High speed, in-depth assessments
- ✓ Free training and guidance
- ✓ Support via Tenable Community

Ideal for: Educators, students and individuals starting their careers in Cyber Security. [Learn more](#) about using Essentials in the classroom with the Tenable for Education program.

nessus Professional

SUBSCRIPTION
Scan Unlimited IPs

- ✓ Unlimited assessments
- ✓ Use anywhere, annual subscription
- ✓ Configuration assessment
- ✓ Live Results
- ✓ Configurable Reports
- ✓ Community Support
- ✓ [Advanced Support](#) available with subscription

Ideal for: Consultants, Pen Testers and Security Practitioners

tenable.io

SUBSCRIPTION
Deploy Unlimited Scanners

- ✓ Unlimited Nessus Scanners
- ✓ Managed in the Cloud
- ✓ Includes Predictive Prioritization
- ✓ Advanced Dashboards and Reports
- ✓ Role-Based Access Control
- ✓ Advanced Support
- ✓ Enterprise Scalability
- ✓ Priced per asset, annual subscription

Ideal for: Vulnerability Management for small, medium and enterprise organizations

Nessus Essentials / Scan Templates

localhost:8834/#/scans/reports/new

AppsMYNEWSPC'sExcelCyclingSONICWALLSNETWORKEMAILAARDSECURITYWebsite Builder Rev...CamerasBIRDSHIPAAOdds n EndsWeatherCOMMUNICATORDocView Print Servi...

There's an error with your feed. [Click here to view your license information.](#)

nessus EssentialsScansSettings

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Scanners

TENABLE

Community

Research

Scan Templates

Back to Scans

Scanner

Search Library

DISCOVERY

Host Discovery

A simple scan to discover live hosts and open ports.

VULNERABILITIES

Basic Network Scan

A full system scan suitable for any host.

Advanced Scan

Configure a scan without using any recommendations.

Advanced Dynamic Scan

Configure a dynamic plugin scan without recommendations.

Malware Scan

Scan for malware on Windows and Unix systems.

Mobile Device Scan

Assess mobile devices via Microsoft Exchange or an MDM.

Web Application Tests

Scan for published and unknown web vulnerabilities.

Credentialed Patch Audit

Authenticate to hosts and enumerate missing updates.

Badlock Detection

Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

Bash Shellshock Detection

Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

DROWN Detection

Remote checks for CVE-2016-0800.

Intel AMT Security Bypass

Remote and local checks for CVE-2017-5689.

Shadow Brokers Scan

Scan for vulnerabilities disclosed in the Shadow Brokers leaks.

Spectre and Meltdown

Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.

WannaCry Ransomware

Remote and local checks for MS17-010.

Waiting for
results.....



Tastes like chicken...



Here's
MY
office
results:

Office ALL PORTS ALL IP's

[← Back to My Scans](#)

Configure

Launch ▼

Report ▼

Export

Hosts 0

Vulnerabilities 0

History 4

Search History

4 Histories

<input type="checkbox"/>	Start Time ▼	Last Modified	Status
<input type="checkbox"/>	Current October 4 at 2:25 PM	October 4 at 2:25 PM	✓ Completed <input type="button" value="✕"/>
<input type="checkbox"/>	October 2 at 3:13 PM	October 2 at 3:14 PM	✓ Completed <input type="button" value="✕"/>
<input type="checkbox"/>	August 29 at 7:09 AM	August 29 at 7:10 AM	✓ Completed <input type="button" value="✕"/>
<input type="checkbox"/>	August 28 at 4:41 PM	August 28 at 4:41 PM	✓ Completed <input type="button" value="✕"/>

Scan Details

Policy:

Basic Network Scan

Status:

Completed

Scanner:

Local Scanner

Start:

October 4 at 2:25 PM

End:

October 4 at 2:25 PM

Elapsed:

a few seconds

Advanced Scan OFFICE.253 ALL PORTS

[Back to My Scans](#)

Configure

Launch

Report

E

Hosts0

Vulnerabilities0

History2

Search History

2 Histories

<input type="checkbox"/>	Start Time ▾	Last Modified	Status
<input type="checkbox"/>	Current October 2 at 3:05 PM	October 2 at 3:06 PM	✓ Completed
<input type="checkbox"/>	August 29 at 7:33 AM	August 29 at 7:33 AM	✓ Completed

Scan Details

Policy:

Advanced Scan

Status:

Completed

Scanner:

Local Scanner

Start:

October 2 at 3:05 PM

End:

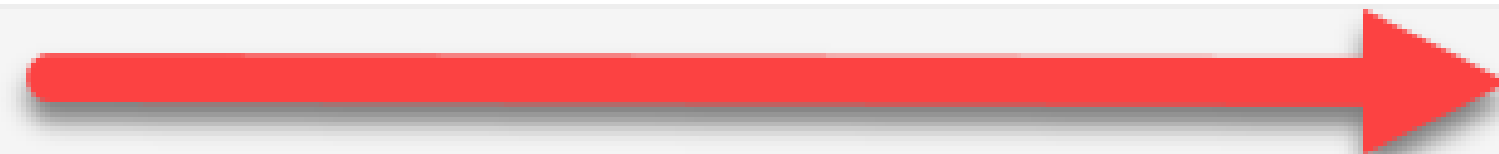
October 2 at 3:06 PM

Elapsed:

a few seconds

Google “What is my IP”
to find your WAN (internet) IP address
do this both at home and office
Those are 2 (of the 16) IP’s I scan

Gateway Anti-Virus Alert: (Cloud Id: 53078257) Agent.FL (Trojan) blocked.	23.39.44.16, 80, X1
Gateway Anti-Virus Alert: (Cloud Id: 53078257) Agent.FL (Trojan) blocked.	23.39.44.16, 80, X1
Gateway Anti-Virus Alert: (Cloud Id: 53078257) Agent.FL (Trojan) blocked.	23.39.44.16, 80, X1
Gateway Anti-Virus Alert: (Cloud Id: 53078257) Agent.FL (Trojan) blocked.	23.39.44.16, 80, X1
Gateway Anti-Virus Alert: (Cloud Id: 53078257) Agent.FL (Trojan) blocked.	23.39.44.16, 80, X1
Gateway Anti-Virus Alert: (Cloud Id: 53078257) Agent.FL (Trojan) blocked.	23.39.44.16, 80, X1
Gateway Anti-Virus Alert: (Cloud Id: 53078257) Agent.FL (Trojan) blocked.	23.39.44.19, 80, X1
Gateway Anti-Virus Alert: (Cloud Id: 53078257) Agent.FL (Trojan) blocked.	23.39.44.16, 80, X1



Meanwhile: TODAY! who is scanning my networks??!!!

<https://www.ultratools.com/tools/ipWhoisLookup>

I also use this webpage to check who is scanning my networks!

Google “whois ip”

whois ip - Google Search

www.ultratools.com

google.com/search?q=whois+ip&oq=whois+ip

MY NEWS PC's Excel Cycling SONICWALLS NETWORK EMAIL AARD SEC

Google

whois ip

All Books News Shopping Videos More Settings Tools

About 1,070,000,000 results (0.76 seconds)

whois ip

The Whois protocol, originally specified in RFC 3912, is a query and response protocol that is used for querying databases that store registered users or assignees of an Internet resource, such as **IP addresses**, Autonomous System Numbers (ASNs) or domain names.

https://www.arin.net > resources > registry > whois

Using Whois - American Registry for Internet Numbers

About featured snippets Feedback

https://www.ultratools.com > tools > ipWhoisLookupRe...

WHOIS IP Lookup Tool | UltraTools

This free WHOIS IP lookup tool from UltraTools shows the WHOIS information on a particular domain name or IP address.

https://www.whatismyip.com > ip-whois-lookup

Lookup IP WHOIS Information - WhatIsMyIP.com

Lookup IP WHOIS information using the IP WHOIS Lookup tool. Find the assigned owner, location, contact information, and abuse reporting details for any ...

DOMAINTOOLS

PROFILE CONNECT MONITOR SUPPORT

Whois Lookup

IP Information for 23.39.44.16

Quick Stats

IP Location	United States Of America Chicago Akamai Technologies Inc.
ASN	AS20940 AKAMAI-ASN1, NL (registered Jul 10, 2001)
Resolve Host	a23-39-44-16.deploy.static.akamaitechnologies.com
Whois Server	whois.arin.net
IP Address	23.39.44.16

NetRange: 23.32.0.0 - 23.67.255.255

CIDR: 23.64.0.0/14, 23.32.0.0/11

NetName: AKAMAI

NetHandle: NET-23-32-0-0-1

Parent: NET23 (NET-23-0-0-0-0)

NetType: Direct Allocation

OriginAS:

Organization: Akamai Technologies, Inc. (AKAMAI)

RegDate: 2011-05-16

Updated: 2012-03-02

Ref: https://rdap.arin.net/registry/ip/23.32.0.0

OrgName: Akamai Technologies, Inc.

OrgId: AKAMAI

Address: 145 Broadway

City: Cambridge

StateProv: MA

PostalCode: 02142

Country: US

RegDate: 1999-01-21

Updated: 2020-08-26

Ref: https://rdap.arin.net/registry/entity/AKAMAI



Kali Linux

I have laptops sporting this, also runs
in Virtualbox, etc

21 Important Penetration Tools in Kali Linux - Make Tech Easier

Images may be subject to copyright. [Learn More](#)

And that's it!

Sincere thanks for getting this far...

questions can be emailed to mark@benavides.org