Microsoft pinky swears that THIS TIME they'll make security a priority:
The monopolist's bargain was made to be broken.

https://pluralistic.net/2024/06/14/patch-tuesday/#fool-me-twice-we-dont-get-fooled-again

Microsoft pinky swears that THIS TIME they'll make security a priority

As the old saying goes, "When someone tells you who they are and you get fooled again, shame on you." That goes double for Microsoft, especially when it comes to security promises.

Microsoft is, was, always has been, and always will be a rotten company. At every turn, throughout their history, they have learned the wrong lessons, over and over again.

That starts from the very earliest days, when the company was still called "Micro-Soft." Young Bill Gates was given a sweetheart deal to supply the operating system for IBM's PC, thanks to his mother's connection. The nepo-baby enlisted his pal, Paul Allen (whom he'd later rip off for billions) and together, they bought someone else's OS (and took credit for creating it - AKA, the "Musk gambit").

Microsoft then proceeded to make a fortune by monopolizing the OS market through illegal, collusive arrangements with the PC clone industry - an industry that only existed because they could source third-party PC ROMs from Phoenix:

https://www.eff.org/deeplinks/2019/08/ibm-pc-compatible-how-adversarial-interoperability-saved-pcs-monopolization

Bill Gates didn't become one of the richest people on earth simply by emerging from a lucky orifice; he also owed his success to vigorous antitrust enforcement. The IBM PC was the company's first major initiative after it was targeted by the DOJ for a 12-year antitrust enforcement action. IBM tapped its vast monopoly profits to fight the DOJ, spending more on outside counsel to fight the DOJ antitrust division than the DOJ spent on *all* its antitrust lawyers, every year, for 12 years.

IBM's delaying tactic paid off. When Reagan took the White House, he let IBM off the hook. But the company was still seriously scarred by its ordeal, and when the PC project kicked off, the company kept the OS separate from the hardware (one of the DOJ's major issues with IBM's previous behavior was its vertical monopoly on hardware *and* software). IBM didn't hire Gates and Allen to provide it with DOS because it was incapable of writing a PC operating system: they did it to keep the DOJ from kicking down their door again.

The post-antitrust, gunshy IBM kept delivering dividends for Microsoft. When IBM turned a blind eye to the cloned PC-ROM and allowed companies like Compaq, Dell and Gateway to compete directly with Big Blue, this produced a whole cohort of customers for Microsoft - customers Microsoft could play off on each other, ensuring that every PC sold generated income for Microsoft, creating a wide moat around the

OS business that kept other OS vendors out of the market. Why invest in making an OS when every hardware company already had an exclusive arrangement with Microsoft?

The IBM PC story teaches us two things: stronger antitrust enforcement spurs innovation and opens markets for scrappy startups to grow to big, important firms; as do weaker IP protections.

Microsoft learned the opposite: monopolies are wildly profitable; expansive IP protects monopolies; you can violate antitrust laws so long as you have enough monopoly profits rolling in to outspend the government until a Republican bootlicker takes the White House (Microsoft's antitrust ordeal ended after GW Bush stole the 2000 election and dropped the charges against them). Microsoft embodies the idea that you either die a rebel hero or live long enough to become the evil emperor you dethroned.

From the first, Microsoft has pursued three goals:

1. Get too big to fail;

2. Get too big to jail;

3. Get too big to care.

It has succeeded on all three counts. Much of Microsoft's enduring power comes from succeeded IBM as the company that mediocre IT managers can safely buy from without being blamed for the poor quality of Microsoft's products: "Nobody ever got fired for buying Microsoft" is 2024's answer to "Nobody ever got fired for buying IBM."

Microsoft's secret sauce is *impunity*. The PC companies that bundle Windows with their hardware are held blameless for the glaring defects in Windows. The IT managers who buy company-wide Windows licenses are likewise insulated from the rage of the workers who have to use Windows and other Microsoft products.

Microsoft doesn't have to care if you hate it because, for the most part, it's not selling to you. It's selling to a few decision-makers who can be wined and dined and flattered. And since we all have to use its products, developers have to target its platform if they want to sell us their software.

This rarified position has afforded Microsoft enormous freedom to roll out harebrained "features" that made things briefly attractive for some group of developers it was hoping to tempt into its sticky-trap. Remember when it put a Turing-complete scripting environment into Microsoft Office and unleashed a plague of macro viruses that wiped out *years* worth of work for entire businesses?

https://web.archive.org/web/20060325224147/http://www3.ca.com/securityadvisor/newsinfo/collateral.aspx?cid=33338

It wasn't just Office; Microsoft's operating systems have harbored festering swamps of godawful defects that were weaponized by trolls, script kiddies, and nation-states:

https://en.wikipedia.org/wiki/EternalBlue

Microsoft blamed everyone *except* themselves for these defects, claiming that their poor code quality was no worse than others, insisting that the bulging arsenal of Windows-specific malware was the result of being the juiciest target and thus the subject of the most malicious attention.

Even if you take them at their word here, that's still no excuse. Microsoft didn't slip and accidentally become an operating system monopolist. They relentlessly, deliberately, *illegally* pursued the goal of extinguishing every OS except their own. It's *completely foreseeable* that this dominance would make their products the subject of continuous attacks.

There's an implicit bargain that every monopolist makes: allow me to dominate my market and I will be a benevolent dictator who spends his windfall profits on maintaining product quality and security. Indeed, if we permit "wasteful competition" to erode the margins of operating system vendors, who will have a surplus sufficient to meet the security investment demands of the digital world?

But monopolists *always* violate this bargain. When faced with the decision to either invest in quality and security, or hand billions of dollars to their shareholders, they'll always take the latter. Why wouldn't they? Once they have a monopoly, they don't have to worry about losing customers to a competitor, so why invest in customer satisfaction? That's how Google can piss away $80b on a stock buyback and fire 12,000 technical employees at the same time as its flagship search product (with a 90% market-share) is turning into an unusable pile of shit:

https://pluralistic.net/2024/02/21/im-feeling-unlucky/#not-up-to-the-task

Microsoft reneged on this bargain from day one, and they never stopped. When the company moved Office to the cloud, it added an "analytics" suite that lets bosses spy on and stack-rank their employees ("Sorry, fella, Office365 says you're the slowest typist in the company, so you're fired"). Microsoft will also sell you internal data on the Office365 usage of your industry competitors (they'll sell your data to your competitors, too, natch). But most of all, Microsoft harvest, analyzes and sells this data for its *own* purposes:

https://pluralistic.net/2020/11/25/the-peoples-amazon/#clippys-revenge

Leave aside how creepy, gross and exploitative this is - it's also *incredibly reckless*. Microsoft is creating a two-way conduit into the majority of the world's businesses that insider threats, security services and hackers can exploit to spy on and wreck Microsoft's customers' business. You don't get more "too big to care" than this.

Or at least, not until now. Microsoft recently announced a product called "Recall" that would record every keystroke, click and screen element, nominally in the name of helping you figure out what you've done and either do it again, or go back and fix it. The problem here is that anyone who gains access to your system - your boss, a spy, a cop, a Microsoft insider, a stalker, an abusive partner or a hacker - now has access to *everything*, on a platter. Naturally, this system - which Microsoft billed as ultra-

secure - was wildly *insecure* and after a series of blockbuster exploits, the company was forced to hit pause on the rollout:

https://arstechnica.com/gadgets/2024/06/microsoft-delays-data-scraping-recall-feature-again-commits-to-public-beta-test/

For years, Microsoft waged a war on the single most important security practice in software development: transparency. This is the company that branded the GPL Free Software license a "virus" and called open source "a cancer." The company argued that allowing public scrutiny of code would be a disaster because bad guys would spot and weaponize defects.

This is "security through obscurity" and it's an idea that was discredited nearly 500 years ago with the advent of the scientific method. The crux of that method: we are so good at bullshiting ourselves into thinking that our experiment was successful that the only way to make sure we know *anything* is to tell our enemies what we think we've proved so they can try to tear us down.

Or, as Bruce Schneier puts it: "Anyone can design a security system that you yourself can't think of a way of breaking. That doesn't mean it works, it just means that it works against people stupider than you."

And yet, Microsoft - whose made more widely and consequentially exploited software than anyone else in the history of the human race - claimed that free and open code was insecure, and spent millions on deceptive PR campaigns intended to discredit the scientific method in favor of a kind of software alchemy, in which every coder toils in secret, assuring themselves that drinking mercury is the secret to eternal life.

Access to source code isn't sufficient to make software secure - nothing about access to code guarantees that anyone will review that code and repair its defects. Indeed, there've been some high profile examples of "supply chain attacks" in the free/open source software world:

https://www.securityweek.com/supply-chain-attack-major-linux-distributions-impacted-by-xz-utils-backdoor/

But there's no good argument that this code would have been *more* secure if it had been *harder* for the good guys to spot its bugs. When it comes to secure code, transparency is an essential, but it's not a sufficency.

The architects of that campaign are genuinely awful people, and yet they're revered as heroes by Microsoft's current leadership. There's Steve "Linux Is Cancer" Ballmer, star of *Propublica*'s IRS Files, where he is shown to be the king of "tax loss harvesting":

https://pluralistic.net/2023/04/24/tax-loss-harvesting/#mego

And also the most prominent example of the disgusting tax cheats practiced by rich sports-team owners:

https://pluralistic.net/2021/07/08/tuyul-apps/#economic-substance-doctrine

Microsoft may give lip service to open source these days (mostly through buying, stripmining and enclosing Github) but Ballmer's legacy lives on within the company, through its wildly illegal tax-evasion tactics:

https://pluralistic.net/2023/10/13/pour-encoragez-les-autres/#micros-tilde-one

But Ballmer is an angel compared to his boss, Bill Gates, last seen some paragraphs above, stealing the credit for MS DOS from Tim Paterson and billions of dollars from his co-founder Paul Allen. Gates is an odious creep who made billions through corrupt tech industry practices, then used them to wield influence over the world's politics and policy. The Gates Foundation (and Gates personally) invented vaccine apartheid, helped kill access to AIDS vaccines in Sub-Saharan Africa, then repeated the trick to keep covid vaccines out of reach of the Global South:

https://pluralistic.net/2021/04/13/public-interest-pharma/#gates-foundation

The Gates Foundation wants us to think of it as malaria-fighting heroes, but they're also the leaders of the war against public education, and have been key to the replacement of public schools with charter schools, where the poorest kids in America serve as experimental subjects for the failed pet theories of billionaire dilettantes:

https://www.ineteconomics.org/perspectives/blog/millionaire-driven-education-reform-has-failed-heres-what-works

(On a personal level, Gates is also a serial sexual abuser who harassed multiple subordinates into having sexual affairs with him:)

https://www.nytimes.com/2022/01/13/technology/microsoft-sexual-harassment-policy-review.html

The management culture of Microsoft started rotten and never improved. It's a company with corruption and monopoly in its blood, a firm that would always rather build market power to insulate itself from the consequences of making defective products than actually make good products. This is true of ever division, from cloud computing:

https://pluralistic.net/2022/09/28/other-peoples-computers/#clouded-over

To gaming:

https://pluralistic.net/2023/04/27/convicted-monopolist/#microsquish

No one should ever trust Microsoft to do anything that benefits anyone except Microsoft. One of the low points in the otherwise wonderful surge of tech worker labor organizing was when the Communications Workers of America endorsed Microsoft's acquisition of Activision because Microsoft promised not to union-bust Activision employees. They lied:

https://80.lv/articles/qa-workers-contracted-by-microsoft-say-they-were-fired-for-trying-to-unionize/

Repeatedly:

https://www.reuters.com/technology/activision-fired-staff-using-strong-language-about-remote-work-policy-union-2023-03-01/

Why wouldn't they lie? They've never faced any consequences for lying in the past. Remember: the secret to Microsoft's billions is *impunity*.

Which brings me to Solarwinds. Solarwinds is an enterprise management tool that allows IT managers to see, patch and control the computers they oversee. Foreign spies hacked Solarwinds and accessed a variety of US federal agencies, including National Nuclear Security Administration (who oversee nuclear weapons stockpiles), the NIH, and the Treasury Department.

When the Solarwinds story broke, Microsoft strenuously denied that the Solarwinds hack relied on exploiting defects in Microsoft software. They said this to everyone: the press, the Pentagon, and Congress.

This was a lie. As Renee Dudley and Doris Burke reported for *Propublica*, the Solarwinds attack relied on defects in the SAML authentication system that Microsoft's own senior security staff had identified and repeatedly warned management about. Microsoft's leadership ignored these warnings, buried the research, prohibited anyone from warning Microsoft customers, and sidelined Andrew Harris, the researcher who discovered the defect:

https://www.propublica.org/article/microsoft-solarwinds-golden-saml-data-breach-russian-hackers

The single most consequential cyberattack on the US government was only possible because Microsoft decided not to fix a profound and dangerous bug in its code, and declined to warn anyone who relied on this defective software.

Yesterday, Microsoft president Brad Smith testified about this to Congress, and promised that the company would henceforth prioritize security over gimmicks like AI:

https://arstechnica.com/tech-policy/2024/06/microsoft-in-damage-control-mode-says-it-will-prioritize-security-over-ai/

Despite all the reasons to mistrust this promise, the company is hoping Congress will believe it. More importantly, it's hoping that the *Pentagon* will believe it, because the Pentagon is about to award billions in free no-bid military contract profits to Microsoft:

https://www.axios.com/2024/05/17/pentagon-weighs-microsoft-licensing-upgrades

You know what? I bet they'll sell this lie. It won't be the first time they've convinced Serious People in charge of billions of dollars and/or lives to ignore that all-important

maxim, "When someone tells you who they are and you get fooled again, shame on you."