Security Now! #980 - 06-25-24

The Mixed Blessing of a Crappy PRNG

This week on Security Now!

How long did it take for Windows' recent horrific WiFi flaw to be weaponized? What are the implications of the U.S. Commerce Department's total ban on Kaspersky? How is the Kremlin reacting? Why would an EU privacy watchdog file a complaint against Google for their Privacy Sandbox? When is an email tracking bug not a tracking bug? What can this podcast do to help a well known security researcher present his work at DEFCON and BlackHat this summer? What's another near-certainty for Microsoft's plan for Recall? What two mistakes have I been making on this podcast? And why might a really bad password generator wind up being a good thing?

Correlation is not Causation

Security News

Expected follow-up on CVE-2024-30078

Last week we opened with the news that the previous week's monthly Windows patchfest had quietly closed a remarkably worrisome flaw that had apparently been sitting undiscovered in every Windows native WiFi network stack since the last time Microsoft poked at it, and there's been no definitive statement about this because it appears that even Microsoft is quite freaked out by this one.

A listener, "Stephen CW" sent a relevant question:

Stephen CW / @DrStephenCW

> *Hi Steve, long time listener. Our corp IT group vets Windows patches thus delaying them. In the meantime, does turning off the Wi-Fi adaptor prevent the attack you described?*

Given the havoc that past mistakes in Windows updates have caused for corporate IT, especially a couple years ago when Microsoft kept wiping out all printing capability enterprise-wide each month, I suspect that many organizations may have adopted a wait-and-test to avoid subjecting their users to such mistakes. And it's typically the case that even though fifty to more than one hundred flaws may be fixed, nothing is happening that's highly time sensitive. But that's not the case with this month's revelations.

What I saw and mentioned last week at GitHub didn't make any sense to me since it appeared to be too high level. Since then, someone else appears to have found a way to overflow the oversized 512-byte buffer Windows WiFi driver provides for SSIDs. He wrote, thinking that this was the critical 30078 CVE:

> *CVE-2024-30078 describes a vulnerability in the way Windows handles SSIDs (Service Set Identifiers) in WiFi networks. Windows has a buffer for SSIDs up to 512 bytes long, which exceeds the WiFi standard. By sending chunked frames to increase the SSID size beyond 512 bytes, a buffer overflow can be triggered. This exploit leverages this vulnerability to cause a buffer overflow by creating and sending WiFi beacon frames with oversized SSID fields.*

But then he realized that he had found a different flaw. So in an update, he added:

> *#INFO : This REPO does not seem to be hitting the same bug as in the stated CVE. New information has come to my attention thanks to FarmPoet. The CVE-2024-30078 vulnerability is in the function "Dot11Translate80211ToEthernetNdisPacket()" of the native wifi windows driver (nwifi.sys) where a very specific frame needs to be constructed to get to the vulnerable code path (which this code does not).*
>
> *I'm working on it. I have identified the changes in the [patched] function and am now working on reversing to construct the relevant frame required to gain code flow into this segment.*

Meanwhile, it may be that anyone who has a spare $5000 may be able to purchase a working exploit without waiting for a freebie on GitHub.

The online publication the "DailyDarkWeb" writes:

> *A threat actor has announced the sale of an exploit for CVE-2024-30078, a Remote Code Execution (RCE) vulnerability in the WiFi driver affecting all Windows Vista and later devices.*
>
> *In their announcement, the threat actor details that the exploit allows for remote code execution over WiFi, leveraging compromised access points or saved WiFi networks. The exploit reportedly works by infecting a victim through [WiFi] router-based malware or simply by having the victim's device be within range of a WiFi network they've previously connected to.*
>
> *The exploit code is offered for sale at $5,000 USD, with the price being negotiable. The seller also offers to develop custom solutions tailored to the buyer's needs. Anastasia, the new owner of the forum, is listed as the escrow for this transaction. Interested parties are instructed to send a private message to the threat actor, with a warning that time wasters and scammers will be ignored.*

Now, in the first place, while we have no way to confirm this, from what we've seen before, it is entirely believable that several weeks downstream from the release of a patch which will have altered the binary of some WiFi component of Windows, that by "diffing" – in hacker parlance – the pre- and post- patched files, the change that Microsoft made to repair the original driver's defect can be readily found. And this is exactly what the earlier GitHub guy was already into.

But the really interesting attack vector that had not occurred to me when we first talked about this last week, but obviously has occurred to the author of this $5000 exploit, is the idea of infecting vulnerable consumer routers or corporate wireless access points – which might well be half the world's circumference away. In other words, if a vulnerable WiFi router is available – anywhere in the world – it could be infected with knowledge of this critical Windows flaw, so that any unpatched Windows WiFi laptop within wireless range of **that** router could be compromised, very remotely! It's clear that the only reason Microsoft was able to get away with labeling this flaw as only being "important" with a CVSS of 8.8, instead of "critical" with a CVSS of 9.8, is that it required a nearby attacker. But in reality, all it requires is a nearby hostile radio, and thanks to the historical vulnerability of consumer and enterprise routers, that's not a high bar.

The observation here is that a maliciously infected router may not be able to attack the machines connected to it by **wire** because there are no known exploitable vulnerabilities in their wired Ethernet network stacks. But that same router may now be able to successfully attack those same or other machines within its wireless reach thanks to the known presence of a – by Microsoft's own assessment – readily exploitable, low-complexity, highly reliable, likely-to-succeed flaw that exists in any Windows machine since Vista which has not yet received the patch that first appeared two weeks ago.

To answer "Stephen CW's" question: **Yes.** Everything we know informs us that turning off Windows WiFi adapters **will** completely protect any unpatched machine from the exploitation of this vulnerability.

So I want to conclude this week's follow-up on CVE-2024-30078 by making sure everyone understands that the addition of the remote router extension to this vulnerability really does

change the game for it. Tens of thousands of routers have already been and are taken over, and are being used for a multitude of nefarious purposes; to launch DDoS attacks, to forward SPAM email, as proxies to probe the Internet for other known weaknesses and on and on. So the bad guys are going to realize that by updating the malware that's within their already-compromised router fleets, they'll be able to start attacking and hijacking any Windows machines that haven't yet been updated. And for whatever reason, history tells us there will be many. That opportunity is going to be difficult to resist.

From Russia with Love

I'll share this piece of news and interject some thoughts along the way. Last Thursday, Kim Zetter, writing for Zero-Day, posted:

> *The U.S. government has expanded its ban on Kaspersky software in a new move aimed at getting consumers and critical infrastructure to stop using the Russian company's software products, citing national security concerns.*
>
> *The ban, using new powers granted to the U.S. Commerce Department, would prohibit the sale of Kaspersky software anywhere in the U.S. and would also prevent the company from distributing software security updates or malware signatures to customers in the U.S.*
>
> *Signatures are the part of antivirus software that detect malicious threats; antivirus vendors push new signatures to customer machines often on a daily basis to keep their customers protected from new malware and threats as the vendors discover them. Without the ability to update the signatures of customers in the U.S., the ability of Kaspersky software to detect threats on those systems will significantly degrade over time.*
>
> *The U.S. Commerce Department announced the ban on Thursday after what it said was an "extremely thorough investigation" but did not elaborate on the nature of the investigation or what it uncovered.*
>
> *U.S. Secretary of Commerce Gina Raimondo told reporters in a phone call: "Given the Russian government's continued offensive cyber capabilities and capacities to influence Kaspersky's operations ... we have to take the significant measure of a full prohibition if we're going to protect Americans and their personal data. Russia has shown it has the capacity and, even more than that, the intent to exploit Russian companies like Kaspersky to collect and weaponize the personal information of Americans, and that's why we are compelled to take the action we're taking today."*

Wow. In other words, we don't like their zipcode so we're going to deny a company, against whom we have no actionable evidence of wrongdoing, all access to the American market because, being a Russian company, they could be forced to act against us.

I'd say that I'm evenly divided on this. Through the years we've covered countless instances where Kaspersky has been hugely beneficial to Western software and Internet security. Thanks to their work for the past many years, the world is a safer place than it would otherwise be. So to say *"we don't like where you live so we cannot trust you"* is a bit brutal. But at the same time it is also understandable because, being in Russia, it's possible that their actions may not always reflect their values. And it's not as if operating within a state where we democratically elect our

representatives is all that much different. After all, in the U.S. we have "warrant canaries".

Wikipedia explains warrant canaries by writing:

> *A warrant canary is a method by which a communications service provider aims to implicitly inform its users that the provider has been served with a government subpoena despite legal prohibitions on revealing the existence of the subpoena. The warrant canary typically informs users that there has not been a court-issued subpoena as of a particular date. If the canary is not updated for the period specified by the host or if the warning is removed, users might assume the host **has** been served with such a subpoena. The intention is for a provider to passively warn users of the existence of a subpoena, albeit violating the spirit of a court order not to do so, while not violating the letter of the order.*

Right. In other words, in the U.S. our courts are able to say: *"We demand that you turn over information within a certain scope and, by the way, you are legally forbidden from disclosing that we have asked and that you have complied."* It's not my intent to pass moral judgment here. I'm just saying that what we see is that all nation states will act to protect their interests and that their client citizens have little choice other than compliance or prison.

Kim's piece continues:

> *Asked what evidence the government found to support concerns that the Russian government **is** using Kaspersky software to spy on customers, Raimondo and other government officials on the call declined to provide specifics. One senior Commerce official said on background: "In terms of specific ... instances of the Russian government using [Kaspersky software to spy] we generally know that the Russian government uses whatever resources are available to perpetrate various malicious cyber activities. We do not name any particular actions in this final determination, but we certainly **believe** that it's more than just a theoretical threat that we describe."*

That's right, because these days "belief" is all that's needed.

> *The ban will not go into effect until September 29 to give existing Kaspersky customers in the U.S time to find a replacement for their antivirus software. The ban on new sales of Kaspersky software in the U.S., however, goes into effect on July 20th. Sellers and resellers who violate the ban could be subject to fines from the Commerce Department and potentially criminal action.*
>
> *In addition to the ban, the Commerce Department also put three Kaspersky entities on its trade-restrictions entities list, which would prohibit U.S.-based suppliers from selling to Kaspersky, though it's unclear if Kaspersky currently has U.S. suppliers.*
> *A Kaspersky spokesman, in a statement to Zero Day, accused the Commerce Department of making its decision "based on the present geopolitical climate and theoretical concerns, rather than on a comprehensive evaluation of the integrity of Kaspersky's products and services."*
> *He said the company "intends to pursue all legally available options" to challenge the ban.*
>
> *"We ... will continue to defend ourselves against actions that seek to unfairly harm our reputation and commercial interests," he said in an email.*

The Department of Homeland Security had previously issued a directive in 2017 banning federal government agencies and departments from installing Kaspersky software on their systems. DHS had also not cited any specific justification for its ban at the time, but media reports citing anonymous government officials at the time cited two incidents. According to one story, an NSA contractor developing offensive hacking tools for the spy agency had Kaspersky software installed on his home computer where he was developing the NSA tools, and the software detected the source code as malicious and extracted it from the computer, as antivirus software is designed to do. A second story claimed that Israeli spies caught Russian government hackers using Kaspersky software to search customer systems for files containing U.S. secrets.

Kaspersky denied that anyone used its software to explicitly search for secret information on customer machines and said that the tools detected on the NSA worker's machine were detected in the same way that all antivirus software is designed to detect malware on customer machines and quarantine or extract it for analysis. Once Kaspersky discovered that the code its antivirus software detected on the NSA worker's machine was not actually malware but appeared to be source code in development by the U.S. government for its hacking operations, CEO Eugene Kaspersky says he ordered workers to delete the code.

Following the 2017 DHS directive, Best Buy and other commercial computer sellers that had contracts with Kaspersky to sell computers with Kaspersky antivirus software pre-installed on those systems subsequently announced they would no longer install the software on computers they sold. This didn't, however, put an end to existing customers using Kaspersky software or prevent new customers from purchasing the software on their own.

Today's ban is designed to convince those customers to stop using the software as well.

Commerce Secretary Raimondo told reporters: "When Americans have software from companies owned or controlled by countries of concern – such as Russia and China – integrated into their systems, it makes all Americans vulnerable. Those countries can use their authority over those companies to abuse that software to access and potentially exploit sensitive U.S. technology and data."

And I'll just note that the United States is no different in that regard. It's just that we're here and they're there. We've covered the news that China's government is similarly urging its businesses to stop using Windows. We clearly have a new cyber cold war heating up, and unfortunately, choosing sides and cutting ties is part of this process.

In announcing the move, Raimondo emphasized that users of the software will not face legal penalties for continuing to use Kaspersky products. But she noted that the government has already launched an aggressive education campaign designed to discourage them from using Kaspersky.
Raimondo said: "U.S. individuals and businesses that continue to use or have existing Kaspersky products and services are not in violation of the law. However, I would encourage you in as strong as possible terms to immediately stop using that software and switch to an alternative in order to protect yourself and your data and your family."

<sigh>

It's not clear how large Kaspersky's U.S. customer base is. The Commerce Department said the company's business in the U.S. is "significant" but did not release any numbers to reporters. Jake Williams, founder of the security firm Rendition Infosec and a former NSA hacker, told Zero Day that the ban on Kaspersky software could prove problematic for critical infrastructures that have the software embedded in devices and can't easily swap it out in the time frame set by Commerce. He said: "I'm less concerned about your average user who has a Kaspersky antivirus running on their endpoint than somebody who has it running in a security appliance like a router or firewall. They cannot easily swap that out. I know I've seen Kaspersky embedded on an ATM." He noted that the time frame for updating embedded devices (if ever) is often "measured in years not months."

He says that anyone using an embedded device that has Kaspersky installed on it will have to rely on the maker of that device to provide an updated system that doesn't use Kaspersky, which will force customers to replace their hardware device.

Unlike Jake, I've never encountered an embedded device that had any specific A/V vendor's product built-in. In general, regardless of whom, that just seems like a very poor design. At the same time, we know there are many ATMs still running Windows XP. So having Kaspersky installed there is probably the least of anyone's worries (and frankly, I'd be surprised if any such A/V was still delivering its services.)

Kaspersky's spokesman noted that the ban on the sale of the company's software does not extend to its threat intelligence reports, which it can still sell to U.S. customers. But he said that the ban will likely impact international cooperation between cybersecurity experts. Kaspersky for years has collaborated with security firms and law enforcement agencies in the U.S. to help fight cybercrime and nation-state threats, sharing data and intelligence about known threats. He noted that the new ban will <quote> "restrict those efforts" <unquote> but did not elaborate on whether the company will completely halt this cooperation going forward.

I would imagine that Kaspersky's employees love their mother Russia as much as I love these United States. So it's easy for me to wish that they had seen the writing on the wall with the rising tensions with the West, and had quietly relocated their operations away from Russia and into a nearby neutral location. But it's probably the case that for most of them this is just a job and not worth giving up their national heritage. Presumably, they still have plenty of market until and unless the EU decides to follow suit.

Before I leave this topic I want to quote the first Q&A from the U.S. Government's FAQ about this:

Q: *Why is the Department of Commerce (Department) taking this action?*

A: *The Department is taking this action to address threats to U.S. national security posed by Russian-based entity Kaspersky Lab, Inc. (together with all affiliates, subsidiaries, and parent companies, Kaspersky). This action was not taken lightly—it is the result of a lengthy and thorough investigation into the company's Information and Communications Technology and Services (ICTS) transactions, their potential risks, and evaluation of other options to address the risks. The Department has determined that Kaspersky's products and services pose an unacceptable risk to United States national security and the safety of U.S. persons, and an*

undue risk of subversion of or sabotage to the integrity and operation of ICTS in the United States.

The U.S. Government has concluded that the risks posed by Kaspersky's continued ICTS transactions are too great to be mitigated, and, with the issuance of the Final Determination in this matter, the Department is taking action to protect Americans' national security.

This is a legitimate national security concern – which doesn't make it right, but it does make it legitimate. How many times have I bemoaned the fact that all of our $5 IoT light switches and wall plugs are phoning home to Chinese servers? For years I've been urging everyone to arrange to put their high-value PCs on their own separate network, so that if anything ever did get loose from a wayward thermostat, it could not get into anyone's PCs. All of those IoT devices would have their own playground ... which we would turn into a secure sandbox.

The Kaspersky AntiVirus model is far more worrisome than concerns over IoT misbehavior, since A/V software is operating in the system's kernel where there's literally nothing it could not do if it were to turn malicious. The entire country could be largely taken over by Kaspersky. All that's needed are a sufficient number of endpoints that are connected to enough others and you have critical mass. It's never happened. It probably never would. But could it? Yeah... and that's just the sort of threat that keeps the military mind laying awake through the night.

I feel that I ought to also observe that Kasapersky makes a password manager that's used by a great many people. Right now Kaspersky claims, and I'm sure it's true, that it uses a zero-trust design which performs TNO or PIE in its design. Or longtime listeners will know that TNO is "Trust No One" and PIE is "Pre-Internet Encryption." The threat is that a remote "security" update to the password manager could remove its client-side encryption and allow "Russia" to obtain the usernames and passwords of every one of their users.

Tit for tat

And in what might be known as "tit for tat", the Kremlin has just extended the duration on its ban on Russian government agencies and critical organizations using IT security services from "unfriendly" countries. The new ban will enter into effect on January 1, 2025, when the previous one was set to expire.

An EU privacy agency complains about Google's Privacy Sandbox?

I saw a short blurb in the Risky Business newsletter, it read:

Google Chrome complaint: European privacy organization noyb has filed a complaint with Austria's data protection agency against Google for its new Privacy Sandbox technology. Noyb says Google is tricking users to enable Privacy Sandbox by falsely advertising it as an ad privacy feature.

Since my reaction to that was "... What?!" I dug a bit deeper. I went over to the NOYB.EU website and found their article with the headline: "Google Chrome: Agree to 'privacy feature', but get tracking!"

Their piece begins with "*After years of growing criticism over invasive ad tracking, Google announced in September 2023 that it would phase out third-party cookies from its Chrome browser.*" Okay. First off, this is already misleading, because while it's true that Google has been using the same ad tracking that the rest of the advertising and data aggregation industry uses, the growing criticism has been over the entire ***industry's*** use of ad tracking, not just Google's.

As we have been carefully covering here, what Google is hoping to do with their Privacy Sandbox is to change the entire model of the way advertising and its user profiling operates by inventing an entirely new way for a user's browser to intelligently select from among available advertisements that are seen at websites. And we've already heard from one of our listeners, whose job it is to implement server-side technology, that the rest of the non-Google industry is massively pushing back against Google's attempt to end tracking. Anyway, the beginning of this article reads:

> *After years of growing criticism over invasive ad tracking, Google announced in September 2023 that it would phase out third-party cookies from its Chrome browser . Since then, users have been gradually tricked into enabling a supposed "ad privacy feature" that actually tracks people. While the so-called "Privacy Sandbox" is advertised as an improvement over extremely invasive third-party tracking, the tracking is now simply done within the browser by Google itself. To do this, the company theoretically needs the same informed consent from users. Instead, Google is tricking people by pretending to "Turn on an ad privacy feature". noyb has therefore filed a complaint with the Austrian data protection authority.*

The article goes on at length and it never gets any more accurate so there's no point in dragging everyone through it. It's full of misconceptions and an utter lack of understanding of what Google is trying to do. Google's Privacy Sandbox system explicitly does not track users, which is precisely why the rest of the well established tracking industry is freaking out over it and scurrying around trying to come up with alternative tracking solutions.

This NOYB is a privacy watchdog agency based in Austria. I looked around at their site and they appear to gauge their value to the world by the number of complaints they're able to file per day. They're complaining about everyone and everything. So they're like a rabid version of the IETF – like the IETF, they are never going to be happy with anything short of total and complete legally and technically enforced Internet anonymity. And in a perfect world that would be great.

Giving the author of this the most sweeping benefit of the doubt available, the only thing I can imagine is that he confuses "tracking" with "profiling". Those two words are different, and so is what they mean. Perhaps he sees no difference. Perhaps he doesn't consider Google's Privacy Sandbox to be the "ad privacy feature" that Google does.

We're told that websites which are able to offer identification of the viewers of the ads they display, or at least some reasonable assurance of the relevance to them of the ads, can double their revenue from that advertising. The problem, therefore, is not Google, who has been working long and hard to find a way to do this without tracking. The problem now is becoming websites and their advertisers who are refusing to change their own thinking.

And speaking of tracking. . .

Email @ GRC

After last week's podcast, as planned, I finished the implementation of GRC's subscription management front-end and turned to the email sending side. I designed a layout and template for the weekly podcast announcements I plan to start sending. And Saturday afternoon, U.S. Pacific time, I sent the first podcast summary email to this podcast list's 4,239 subscribers.

Rob in Britain

> *Hi Steve, As Apple broke their imap message read flag a while back I have been using the Blue Mail app to get my email. Blue Mail includes a "tracking image detector" and guess what, it flagged your message below as containing one. As a Brit, the irony of a security podcast "tracking me" does not escape me!!*

Rob was one of a couple of people who replied with a "What The ...?" when their email clients reported that a so-called "tracking bug" was present in the email from me. And since that's what **their** client calls it, it's natural for concern to be raised. So I wanted to correct the record about when an email bug is "tracking" someone, and when it's not.

The TL;DR is: It's not "tracking you" if it's a bug you indirectly ASKED FOR and if it's only linked back to whom you asked from. The confusion arises because our email clients have no way of knowing that this incoming email is **not** unwanted SPAM, and that makes all the difference in the world about the purpose and implications of the bug; because it if it **were** an unwanted SPAM email, as opposed to email everyone has been clamoring for, you would definitely **not** want your opening of that email to send a ping back to the cretins who are despoiling the world with SPAM.

But in this case, no one is being "tracked" because the image link points only back to me — back to GRC — the source of the email that was just sent to you, which only those who jumped through some hoops to ask for it would have received. Also, unlike pretty much everyone else, and against the advice of some well informed others, I (GRC) am sending email myself, NOT through any of the typical 3rd-party cloud providers that most organizations now use. As a consequence, the email address our subscribers have entrusted to me will **never** be disclosed to **any** 3rd party, and as I noted, that single pixel "bug" is only coming back to me to allow me to obtain statistics about the percentage of email I send that's opened and viewed.

And I'll note that the Security Now! emails also contain links to the full-size picture of the week, the show notes and GRC's Security Now! summary page. So it's not as if anyone who receives these emails from me and clicks any of their links is being stealth. Also, I chose to embed the reduced-size picture of the week as a thumbnail image so that the email would be self-contained and complete. But I could have linked back to GRC for its retrieval when viewed. In that way I would have obtained the same feedback that single-pixel image provided.

It is certainly the case that unsolicited commercial SPAM email contains tracking bugs to inform their senders when their obnoxious unwanted SPAM has been opened. Anyone who thinks that describes the weekly podcast summaries they signed up for, will be glad that every one of my emails contains a very clearly marked unsubscribe link. And, of course, it has immediate effect. There's none of this "please allow two weeks for your unsubscribe to be processed" nonsense!

My work after today's podcast will be to automate the sending of these weekly podcast summaries. Sending a new email to a list is not difficult but it does involve a large number of steps and redundant decisions. So I want to take a bit more time to build some infrastructure to make it dead simple and mistake proof.

Closing The Loop

Orange Tsai

Subject: Seeking Assistance for Black Hat USA Visa Issue

Hello Steve Gibson and Leo Laporte,

My name is Orange Tsai, a security researcher from Taiwan! While I'm not a listener of the show, Jonathan Leitschuh, a friend of mine says you've featured my work and spoke about my name many times on the show. I've won the Pwn2Own championship and Pwnie Awards several times, as well as having been the researcher behind impactful research such as Exchange Server RCEs (mentioned in Security Now! sn-809, sn-819, sn-833, sn-844, sn-916 for ProxyLogon & ProxyShell), Samba RCE (sn-857), Facebook RCE (sn-795 for MobileIron RCE), SSL VPN RCEs (sn-814 for Fortigate & Pulse Secure), and the recent PHP RCE.

I come to you with a plea for support from either you or your listeners. I've been accepted to speak at Black Hat USA this year. Unfortunately, due to United States border control, I've been unable to enter the country the past few years. I was wondering if you or your listeners had any connections that would be of assistance in this.

Here's a brief intro to give you some of the context:

I have previously traveled to the US seven times through ESTA (US Visa Waiver Program) and have presented in person at DEFCON and Black Hat USA (BHUSA) many times without any issues. However, after I reported several critical vulnerabilities to Microsoft in 2021, my ESTA was rejected. My guess is because one of my reported bugs has a collision with a China APT Group. I believe this may have resulted in me being flagged by the US. Since then, I have been unable to enter the United States to present at DEFCON/BHUSA in person.

In 2022, I tried applying for a business/tourist visa at the embassy. However, the consular officer couldn't decide, and my application had to be sent to DHS for further administrative processing. After several months of review, I never got a response and missed the 2022 DEFCON/BHUSA dates.

This year, I submitted my latest research and was accepted by BHUSA in May 2024. To catch up with the visa this time, I reapplied for the B1/B2 visa in January and had the interview on March 19th. However, three months have passed and there's still no update. As a security researcher, I try to do the most impactful research and I'm keen on having my research seen by the world, especially at the top hacker gatherings like BHUSA. I'm currently seeking all the help I can get to break through this situation.

I hope this gives you a better understanding of the situation I am facing. This has been a long and troubling issue for me. If you have any advice or guidance to offer, it would be greatly appreciated. Here is my contact information in case anyone needs it.

Thank you!
- Orange Tsai

Okay. So the moment I saw Orange Tsai's name in my Security Now! email, my eyes opened wider because of course I recognized his name from the **many** times through the years we've covered his leading edge significant contributions to the security of this industry and its software

systems. I don't actively maintain the sorts of contacts that he needs for this, but I'm always surprised and flattered when I learn about the roles of many of the people who **are** listening to this podcast and who consider it to be worth their time. So I am sharing Orange Tsai's plea in the sincere hope that do we have listeners here who may have the connections required to solve this problem for him. This year's DEFCON and BlackHat USA conferences are being held near the start of August, and today is our last podcast of June. So there's only a month to go.

I wrote back to Orange Tsai to tell him that I would be honored to do anything I could to help by giving his situation a larger audience. I also asked how someone who was in a position of authority might contact him if they needed further clarification. He replied:

> *Hi Steve, Thank you for your response. I really appreciate your help! My only concern comes via a friend, in that the U.S. government can be very sensitive to "media pressure," and there have been cases where this has led to a permanent ban on entry. Although Security Now! is not "traditional media," I still hope that when mentioning my case, it can be done in a neutral manner. When seeking help, please ask listeners to do so in their personal capacity, rather than representing me, the media, or any other sensitive identities.*

So I would ask anyone who might be in a position to help to please heed his concerns and to be gentle as they determine what's going on and why. I asked him for a link to a page of contact information which he provided, but all he write there was: https://orange.tw/contact-for-sn.txt

> *Hi, I'm Orange Tsai, a security researcher from Taiwan. I really want to go to the US to present my latest research at Black Hat USA 2024 in person. If you have any suggestions, please feel free to email me at orange[at]chroot.org! Thank you!*

So I'm leaving this in the hands of our wonderful listeners. PLEASE to not do anything if you are not the right person, since I would hate to make things worse. But if you are the right person, or have a sufficiently close relationship with someone who is, then it would be wonderful if we were able to help him. His years of past work have shown that he is exactly the sort of security researcher whose work we ***should*** be encouraging.

markzip @Markzip@twit.social

> *Steve, it seems to me that an overlooked problem with Recall is third party leakage. Listeners to Security Now may lock down their machines and opt out of Recall, whereas the people with whom we interact may not. If I write an email to a friend, their Recall instance now knows of our correspondence. We can think of other leakage easily. For instance, people frequently share passwords via email. More examples should be easy to imagine.*

So first of all, I think Mark makes a great point. Many people who've been critical of Recall have likened it to spyware or malware that being "factory installed." Though our first podcast about this **was** titled "The 50 gigabyte privacy bomb", I've never characterized Recall as spyware or malware because both of those things require malicious **intent**, and at no point have I believed, or do I believe, that Microsoft has ever had a shred of malicious intent for Recall.

I've seen other commentators suggesting that the entire purpose of Recall is to send the collected data back to the Redmond Washington mothership. I think that's irresponsible nonsense, and it's a failure of imagination. For one thing, Microsoft knows that in today's world they could never do that without being found out. And besides, why would they? The details of some grandmother's management of her canasta group is nothing that Microsoft cares about.

But that's not to say that there would not be some value to having the AI residing in grandma's **computer** be "aware" of her interest in canasta. If Windows continues to evolve (or devolve) into an advertising platform – which would be unfortunate but seems quite likely – Microsoft would be crazy **not** to use their Recall AI's digested history and understanding of its machine's user to improve the relevance of such advertising. And, as we know, this could all be done locally on the machine, much as Google's privacy sandbox will be doing in the user's web browser. In this case, the Windows OS itself would be pulling the most relevant ads from the Internet for display either in Windows or in their Bing web browser.

So we now have one declared and two undeclared but obvious uses for Recall; and none of these applications for Recall's data requires it to ever leave its local machine environment.

The concern Mark raised about 3rd-party leakage is a good one. It probably hadn't occurred to most of us that not only would our own machines be recording our every move, but that all of our personal interactions with others would also be captured by their instances of Recall.

Last week we quoted Matthew Green on the topic of Apple's Cloud Compute design. He wrote:

> *TL;DR: it is not easy. Building trustworthy computers is literally the hardest problem in computer security. Honestly, it's almost the only problem in computer security. But while it remains a challenging problem, we've made a lot of advances. Apple is using almost all of them.*

Now in Apple's case, they have the comparative luxury of housing their Cloud Compute infrastructure in data center facilities surrounded by strong physical security. Even so, the architecture Apple has designed does not require its physical security to hold in the presence of an infiltrating adversary. But they have physical access security nevertheless. That's something Microsoft does not have with their widely distributed Windows workstations. Grandma always leaves her CoPilot+ PC open, logged in and unlocked, just like her back door. So Microsoft's challenge is greater than Apple's, which Matthew Green just made clear is already the hardest problem in computer security. And as we've seen with last week's revelation of a super-critical WiFi proximity remote code execution flaw that's apparently been present in Windows forever, whatever solution Microsoft finally implements will need to be something we've not yet seen them successfully accomplish.

Let me say that again because I think this is really important and it's exactly the right way to think about this: *"Whatever solution Microsoft finally implements will need to be something we've not yet seen them successfully accomplish."* What everyone **else** other than Microsoft clearly sees is just how much having Recall running in a PC raises the stakes for Windows security. But so far, we've seen **zero** indication that Microsoft **truly** understands that this is not

something they can just wave their hands around and claim is now safe – because they said so. What's not clear is whether they'll be able to use the hardware that's already present in those CoPilot+ PCs to implement the sort of super-secure enclave they're going to need... and that makes it even more doubtful that they'll be able to securely retrofit the inventory of existing Windows 11 hardware to provide the required level of security. Apple has only managed to do it for their iPhone handsets because their hardware architecture is so tightly closed. Windows never has been since it's an OS designed to run on 3rd-party OEM hardware. So, for example, the phrase "Secure Boot" is an oxymoron since secure boot bypasses are continually surfacing.

I realize that I'm spending a great deal of time on Recall. This is now the 4th podcast where it's been a significant topic of discussion and the first two podcasts it was our title topic. But given the security and privacy significance of Microsoft's proposal, it would be difficult to give it more time than it deserves.

Errata

I have two pieces of podcast errata to share.

Do the math!

The first came from someone who wanted to correct my recent statement about the duration of this podcast. He noted that since we started in 2005 we're still in our **19th** year of the podcast, not, as I have been erroneously saying, in our 20th year. So in two months, we will be having our 19th birthday, not our 20th. He said "The reason we listen is that we know you care about getting the details right." I'm glad that comes through so I'm happy to correct the record.

It was Service Pack 2... not 3!

The second mistake several of our astute listeners have spotted is that I've been erroneously saying that the big security changes in Windows XP – its built-in firewall being enabled by default and its users' access to raw sockets being restricted – came about with the release of XP's final service pack 3. That's wrong. It was the release of XP's service pack 2 where Microsoft finally decided that they needed to get more serious about XP's security and made those important changes. So, a thank you to everyone who said "Ah… Steve…"

The Mixed Blessing of a Crappy PRNG

— or —

When are you very glad that your old password manager
used a very crappy pseudo-random number generator?

Today I want to share the true story of a guy named Michael who, after generating 43.6 Bitcoin, lost the password that was used to protect it. With Bitcoin currently trading at around $60,000 USD each, that's around $2.6 million dollars worth of Bitcoin waiting for him at the other side of the proper password. Unlike many similar stories, this one has a happy ending. But it's the reason for the happy ending that makes this such an interesting story for this podcast and offers so many lessons for us.

By pure coincidence, the story was recently written up by the same guy, Kim Zetter, who wrote that piece about Kaspersky for Zero Day that we were discussing earlier. Kim's story in WIRED is titled: "How Researchers Cracked an 11-Year-Old Password to a $3 Million Crypto Wallet."

Two years ago when "Michael," an owner of cryptocurrency, contacted Joe Grand to help him recover access to about $2 million worth of bitcoin he had stored in encrypted format on his computer, Grand turned him down.

Michael, who is based in Europe and asked to remain anonymous, stored the cryptocurrency in a password-protected digital wallet. He generated a password using the RoboForm password manager and stored that password in a file encrypted with a tool called TrueCrypt. At some point, that file got corrupted and Michael lost access to the 20-character password he had generated to secure his 43.6 BTC (worth a total of about €4,000, or $5,300, back in 2013 when it was generated and stored). Michael used the RoboForm password manager to generate the password, but did not store it in his manager. He worried that someone would hack his computer and obtain the password.

Grand is a famed hardware hacker who in 2022 helped another crypto wallet owner recover access to $2 million in cryptocurrency he thought he'd lost forever after forgetting the PIN to his Trezor wallet. Since then, dozens of people have contacted Grand to help them recover their treasure. But Grand, known by the hacker handle "Kingpin," turns down most of them, for various reasons.

Grand is an electrical engineer who began hacking computing hardware at age 10 and in 2008 cohosted the Discovery Channel's "Prototype This" show. He now consults with companies that build complex digital systems to help them understand how hardware hackers like him might subvert their systems. He cracked the Trezor wallet in 2022 using hardware techniques that forced the USB-style wallet to reveal its password.

But Michael stored his cryptocurrency in a software-based wallet, which meant none of Grand's hardware skills were relevant this time. He considered brute-forcing Michael's password—writing a script to automatically guess millions of possible passwords to find the correct one—but determined this wasn't feasible. He briefly considered that the RoboForm password manager Michael used to generate his password might have a flaw in the way it generated passwords, which would allow him to guess the password more easily. Grand, however, doubted such a flaw existed.

Michael contacted multiple people who specialize in cracking cryptography; they all told him "there's no chance" of retrieving his money. But last June he approached Grand again, hoping to convince him to help, and this time Grand agreed to give it a try, working with a friend named Bruno in Germany who also hacks digital wallets.

*Grand and Bruno spent months reverse engineering the version of the RoboForm program that they thought Michael had used in 2013 and found that the pseudo-random number generator used to generate passwords in that version—and subsequent versions until 2015—**did indeed have a significant flaw** that made the random number generator not so random. The RoboForm program unwisely tied the random passwords it generated to the date and time on the user's computer—it determined the computer's date and time, and then generated passwords that were predictable. If you knew the date and time and other parameters, you could compute any password that would have been generated on a certain date and time in the past.*

If Michael knew the day or general time frame in 2013 when he generated it, as well as the parameters he used to generate the password (for example, the number of characters in the password, including lower- and upper-case letters, figures, and special characters), this would narrow the possible password guesses to a manageable number. Then they could hijack the RoboForm function responsible for checking the date and time on a computer and get it to travel back in time, believing the current date was a day in the 2013 time frame when Michael generated his password. RoboForm would then spit out the same passwords it generated on the days in 2013.

There was one problem: Michael couldn't remember when he created the password.

According to the log on his software wallet, Michael moved bitcoin the into his wallet for the first time on April 14, 2013. But he couldn't remember if he generated the password the same day or some time before or after this. So, looking at the parameters of other passwords he generated using RoboForm, Grand and Bruno configured RoboForm to generate 20-character passwords with upper- and lower-case letters, numbers, and eight special characters from March 1 to April 20, 2013.

It failed to generate the right password. So Grand and Bruno lengthened the time frame from April 20 to June 1, 2013, using the same parameters. Still no luck.

Michael says that Grand and Bruno kept coming back to him, asking if he was sure about the parameters he'd used. He stuck to his first answer. Michael said: "They really annoyed me, because who knows what I did 10 years ago." He found other passwords he generated with RoboForm in 2013, and two of them did not use any special characters, so Grand and Bruno adjusted. Last November, they reached out to Michael to set up a meeting in person. Michael said: "I thought, 'Oh my God, they're going to ask me again for the settings."

Instead, they revealed that they had finally found the correct password—no special characters. And it was generated on May 15, 2013, at 4:10:40 pm GMT.

Grand wrote in an email to WIRED: "We ultimately got lucky that our parameters and time range was correct. If either of those were wrong, we would have continued to take guesses and shots in the dark and it would have taken significantly longer to precompute all the possible passwords."

Kim then provides a bit of background about RoboForm, writing:

RoboForm, made by US-based Siber [spelled with an 'S'] Systems, was one of the first password managers on the market, and currently has more than 6 million users worldwide, according to a company report. In 2015, Siber seemed to fix the RoboForm password manager. In a cursory glance, Grand and Bruno couldn't find any sign that the pseudo-random number generator in the 2015 version used the computer's time, which makes them think they removed it to fix the flaw, though Grand says they would need to examine it more thoroughly to be certain.

Siber Systems confirmed to WIRED that it did fix the issue with version 7.9.14 of RoboForm, released June 10, 2015, but a spokesperson wouldn't answer questions about how it did so. In a changelog on the company's website, it mentions only that Siber programmers made changes to "increase randomness of generated passwords," but it doesn't say how they did this. Siber spokesman Simon Davis says that "RoboForm 7 was discontinued in 2017."

Grand says that, without knowing how Siber fixed the issue, attackers may still be able to regenerate passwords generated by versions of RoboForm released before the fix in 2015. He's also not sure if current versions contain the problem. He said: "I'm still not sure I would trust it without knowing how they actually improved the password generation in more recent versions. I'm not sure if RoboForm knew how bad this particular weakness was."

Customers may also still be using passwords that were generated with the early versions of the program before the fix. It doesn't appear that Siber ever notified customers when it released the fixed version 7.9.14 in 2015 that they should generate new passwords for critical accounts or data. The company didn't respond to a question about this.

If Siber didn't inform customers, this would mean that anyone like Michael who used RoboForm to generate passwords prior to 2015—and are still using those passwords—may have vulnerable passwords that hackers can regenerate. Grand said: "We know that most people don't change passwords unless they're prompted to do so." He added that: "Out of 935 passwords in my password manager (not RoboForm), 220 of them are from 2015 and earlier, and most of them are [for] sites I still use."

Depending on what the company did to fix the issue in 2015, newer passwords may also be vulnerable.

Last November, Grand and Bruno, having earned their reward, deducted a percentage of bitcoins from Michael's account for the work they did, then gave him the password to access the rest. The bitcoin was worth $38,000 per coin at the time. Michael waited until it rose to $62,000 per coin and sold some of it. He now has 30 BTC, now worth $3 million, and is waiting for the value to rise to $100,000 per coin.

Michael says he was lucky that he lost the password years ago because, otherwise, he would have sold off the bitcoin when it was worth $40,000 per coin and missed out on a greater fortune. He said: "My losing the password was financially a good thing."

Okay. So first of all, RoboForm is probably a well known name to everyone, even those of us who never had occasion to use it. I'm in that camp. I've never used RoboForm, but since this podcast has been going since 2005, we've covered the span of time that RoboForm was apparently using a horrific password generation scheme.

One of this podcast's early and continuing focuses has been on the importance of the strength of pseudorandom number generators used in cryptographic operations. So I was quite curious to learn more about what exactly Grand and Bruno found when they peeled back the covers of RoboForm circa 2013. I'm reminded of a line from the Sci-Fi movie "Serenity" where our villain says to Mel: "It's worse than you know", to which Mel replies "It usually is."

Believe it or not, whenever the user of RoboForm v7.9.0 which was released on June 26th of 2013, pressed its "Generate Password" button, RoboForm, up until its repair two years later with v7.9.14, simply took the Windows system's UNIX time, which is the number of seconds elapsed since January 1st, 1970, and directly and deterministically used that time to produce the user's password. RoboForm didn't even take the trouble to create a unique per-system salt so that differing installations would produce differing bad passwords. This meant that if two users anywhere were to press the "Generate Password" button within the same one-second interval, if they were using the same password parameters identical passwords would be generated.

Grand and Bruno discovered something else when they opened up RoboForm. The designers of this password generator, that should really just be called a "time scrambler", realized that if a user happened to press the "Generate Password" button a second time within the same second the same password would be generated. To cover up this flaw, they subtract a fixed amount of time from the system time for repeats. What an utter disaster.

One thing we don't know is for how long RoboForm's password generator was this horrific before it was changed. (I originally wrote "before it was fixed", but we don't know that it was fixed. We only know that it was changed.) But I have a theory about that. My theory is that this must have been the original implementation of RoboForm's password generator. The reason I think that is that by 2013 no one would have ever designed such a horrifically lame password generation scheme. This had to have been a very early password generator created back in the late 90's or early 2000's before there was much awareness of the proper way to do things. And then, following the well understood property of software inertia, 10 to 15 years went by without anyone at RoboForm bothering to think about it again, because it was, after all, producing random appearing passwords. But for some reason, eventually someone apparently did.

Grand and Bruno note that something did finally change in 2015 with v7.9.14. But since RoboForm is both closed-source and closed-mouthed we have no idea what may have precipitated the change, nor what the new algorithm was changed to. So I'm put in mind of Bitwarden, the password generating sponsor of this network, where we can know anything we want to know about its innards, first because if we ask we'll be told, secondly because it's probably openly documented, and thirdly because the source code of the solution is publicly available. None of which is true for RoboForm.

The final note that's worth repeating is the point that Grand highlights: Regardless of their apparent complexity, we now know that's an illusion — it's just the scrambled time of day and date, without even any per-system salt, which means that all user scramblings are identical. Therefore, ANY PASSWORDS that were EVER generated by RoboForm, presumably until v7.9.14, CAN be reverse engineered, and the set of possible passwords can be further narrowed by the degree to which their approximate date of their creation is known.

Even if the format of the password is not known, there are a limited number of choices available for upper and lower case, special characters, numbers and length. So if someone were determined to crack into something that was being protected by a password that they had reason to believe had been generated by RoboForm and they had some idea of when, such as the date of the protected account's creation, it's not a stretch to imagine that it could be done.

Sure, I would put the chances of this actually being done as extremely remote at best. But anyone who was using RoboForm back then who may have never had the occasion to update their passwords since, should at least be aware that those passwords were simply generated by scrambling the time of day, and with a resolution of only one second. There are not a cryptographically strong number of seconds in a day.

And, while I don't want to throw shade on the RoboForm product of today which might be excellent, given the history that has just been revealed, RoboForm is certainly not something I could ever use or recommend, especially when there are alternatives like Bitwarden which are hiding nothing and RoboForm is hiding everything.

And this brings me to the final and most important point and lesson I want to take away from this. Way back when I and this podcast first endorsed LastPass, I was able to do so with full confidence – and in fact the only reason I was able to do so, and did – was because the product's original designer, Joe Segrist, completely disclosed its detailed operation. It was the 21st century, and Joe understood that the value he was offering was not some secret crypto mumbo jumbo. That was 20th century thinking. Joe understood that the value he was offering was a proper implementation of well understood crypto that was then wrapped into an appealing user experience; the value is not in proprietary secrecy, it's in implementation, maintenance and service. As we know, many years and ownership changes later, LastPass eventually let us down. I hope Joe is relaxing on a beach somewhere, because he earned it.

So the lesson we should take from what can only be considered a RoboForm debacle, is that something like the design of a password generator is too important for us to trust without a full disclosure of the system's operation and its subsequent assessment by independent experts. Any password generator that anyone is using should fully disclose its algorithms. It doesn't need to be open source, but it **must** be open design. No company should be allowed to get away with producing passwords for us while asking us to assume those passwords were properly derived, just because their website looks so nice. What the marketing people say has exactly zero bearing on how the product operates. It's obvious that we cannot assume that just because a company is offering a fancy looking crypto product that they have any idea how to correctly design and produce such a thing. There's no reason to believe that there are not more RoboForm's out there.