Security Now! #1037 - 08-05-25

Chinese Participation in MAPP

This week on Security Now!

• A follow-up to the SharePoint server patch mess. • How Russia arranges to spy on other country's local embassies. • "Dropbox Passwords" manager app is ending in October. • Signal will leave Australia rather than help spy. • YouTube deploys viewing history age-estimation heuristics. • Chrome adds clever lightweight extension signing to prevent abuse. • A domain registrar is coming close to losing its rights. • A TP-Link router that doesn't encrypt its configuration. • What is "TruAge" and might it be useful for age verification. • An update on "Artemis". • With U.S.-China tensions on the rise, should Chinese security companies receive weeks of advance notice of forthcoming Microsoft flaw patches?

Not every solution that works
should be recommended.

Security News

SharePoint Follow-up

A bit of additional interesting information surfaced about the Microsoft Sharepoint 0-day RCE after our coverage of this last week. I'm glad I was skeptical of The Register's allegation that someone within Microsoft's MAPP program had leaked the information about the SharePoint vulnerability. I believe The Register picked up this idea from someone at Trend Micro's Zero-Day Initiative, which was unfortunate. First, remember that, even so, this was not the big issue. It's true that someone was found to be exploiting this vulnerability on July 7th, the day before the official patch was released. But the big mess did not occur until after Microsoft's botched patch was made public. At that point everyone was able to compare the new code against the old code to immediately zero-in on the location of the problem and design a work-around.

But it was still troubling that someone did exploit the original completely unpatched vulnerability the day before anyone was supposed to know about it. How'd that happen? ProPublica offered an interesting theory that did not require any of Microsoft's MAPP program participants to leak anything. Propublica's headline was: *"Microsoft Used China-Based Engineers to Support Product Recently Hacked by China."* In other words... whoops. Propublica's subhead noted: *"Microsoft announced that Chinese state-sponsored hackers had exploited vulnerabilities in its popular SharePoint software but did not mention that it has long used China-based engineers to maintain the product."* Hmmm. ProPublica wrote:

> *Last month, Microsoft announced that Chinese state-sponsored hackers had exploited vulnerabilities in SharePoint, the company's widely used collaboration software, to access the computer systems of hundreds of companies and government agencies, including the National Nuclear Security Administration and the Department of Homeland Security.*
>
> *The company did not include in its announcement, however, that support for SharePoint is handled by a China-based engineering team that has been responsible for maintaining the software for years.*
>
> *ProPublica viewed screenshots of Microsoft's internal work-tracking system that showed China-based employees recently fixing bugs for SharePoint "OnPrem," the version of the software involved in last month's attacks. Microsoft said the China-based team "is supervised by a US-based engineer and subject to all security requirements and manager code review. Work is already underway to shift this work to another location."*
>
> *It's unclear if Microsoft's China-based staff had any role in the SharePoint hack. But experts have said allowing China-based personnel to perform technical support and maintenance on U.S. government systems can pose major security risks. Laws in China grant the country's officials broad authority to collect data, and experts say it is difficult for any Chinese citizen or company to meaningfully resist a direct request from security forces or law enforcement. The Office of the Director of National Intelligence has deemed China the "most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks."*
>
> *ProPublica revealed in a story published last month that Microsoft has for a decade relied on foreign workers — including those based in China — to maintain the Defense Department's cloud systems, with oversight coming from U.S.-based personnel known as digital escorts. But those escorts often don't have the advanced technical expertise to police foreign counterparts with far more advanced skills, leaving highly sensitive information vulnerable, the investigation showed.*

Also, this escort service Microsoft runs would not prevent foreign coders from learning about vulnerabilities. They must know about vulnerabilities in order to fix them. So this entire digital escort concept seems like total crock. ProPublica continued:

> *ProPublica found that Microsoft developed the escort arrangement to satisfy Defense Department officials who were concerned about the company's foreign employees, and to meet the department's requirement that people handling sensitive data be U.S. citizens or permanent residents. Microsoft went on to win federal cloud computing business and has said in earnings reports that it receives "substantial revenue from government contracts." ProPublica also found that Microsoft uses its China-based engineers to maintain the cloud systems of other federal departments, including parts of Justice, Treasury and Commerce.*

Wow. This is where we deploy our favorite: ***"What could possibly go wrong?"***

> *In response to the reporting, Microsoft said that it had halted its use of China-based engineers to support Defense Department cloud computing systems, and that it was considering the same change for other government cloud customers. Additionally, Defense Secretary Pete Hegseth launched a review of tech companies' reliance on foreign-based engineers to support the department. Sens. Tom Cotton, an Arkansas Republican, and Jeanne Shaheen, a New Hampshire Democrat, have written letters to Hegseth, citing ProPublica's investigation, to demand more information about Microsoft's China-based support.*

ProPublica's reporting ended, writing:

> *Microsoft has said that, beginning next July, it will no longer support on-premises versions of SharePoint. It has urged customers to switch to the online version of the product, which generates more revenue because it involves an ongoing software subscription as well as usage of Microsoft's Azure cloud computing platform. The strength of the Azure cloud computing business has propelled Microsoft's share price in recent years. On Thursday, it became the second company in history to be valued at more than $4 trillion.*

So, it might be that the call was coming from inside the house. Microsoft's own China-based coders were the maintainers of the SharePoint codebase. This means that **they were the ones** who directly received the early information about the SharePoint vulnerability from the Pwn2Own competition by way of Trend Micro's Zero-day Initiative. It was Chinese coders who prepared the patch. But knowing this begs another even greater and far more worrisome question: Could the patch, whose initially defective design caused the majority of the damage, been deliberately botched by its Chinese developers? I'm not saying that happened. But the circumstances at least present the question. And I think it at least needs to be asked ... right?

We would always assume that any botched patch from Microsoft could only be a mistake. What could Microsoft possibly have to gain from fumbling a patch of a critical CVSS 9.8 vulnerability in their own widely deployed enterprise file sharing server? At the very least it's significant reputational damage. The tech press is now comparing this SharePoint fiasco to the similar 2021 Exchange Server debacle that's widely viewed as a catastrophe.

But now we learn that the flawed patch didn't really come from Microsoft – at least not directly. The bad patch actually came from China, apparently subject only to some low-level oversight.

And then we learn that Microsoft has decided to change that development process to move it away from China. I hate that China and the U.S. are entering into a cyber cold war. But when Chinese state-sponsored attackers are actively attacking U.S. assets there's no denying the fact. And we know from back-tracking the IP addresses that were found to be attacking Microsoft's OnPrem SharePoint servers, it was those same well-known Chinese state-sponsored attackers who jumped on this vulnerability with a vengeance.

There's one other aspect of this that's been missed in all the reporting. That's to note that the fact that the first attack on SharePoint servers was detected on July 7th, the day before July's Patch Tuesday, does not mean that July 7th was the first day of any attack. We've talked about this many times before and we've seen it in practice. The optimal strategy for anyone who's in possession of an unpatched critical 0-day remote code execution exploit is to use that unique advantage with extreme care so as to remain off the radar and prevent the raising of any alarm for as long as possible. You want to carefully choose your targets, remain quiet, and infiltrate the most valuable networks first, before the world wakes up to the fact that on-premise SharePoint servers can be remotely compromised.

The implementation of this strategy suggests that widespread exploitation of the flaw – which would have quickly become evident – may have been deliberately held back until just the day before the Patch Tuesday release. At which point it was unleashed with full automation so as to penetrate as many remaining SharePoint servers as possible just before the patch was made available. What we now know is that Chinese developers working for Microsoft would have been informed of this shortly after May's Pwn2Own competition. And now even Microsoft appears to be uncertain of where their loyalties lie.

And now we also know that the patch didn't completely work. Whether or not this occurred deliberately in this instance, it seems the height of recklessness for Microsoft to be outsourcing its software development to China while China is actively–and successfully–attacking the same software systems it's developing for Microsoft. What's wrong with this picture? Microsoft appears to have reached a similar conclusion and has said that they'll be moving this activity elsewhere.

Russia's attacks on foreign embassies

Microsoft's Threat intelligence group posted a report detailing one way Russia has arranged to intercept and monitor the Internet traffic of the foreign embassies operating within its borders. It was so diabolical that I wanted to share it with our listeners:

Russian ISPs all have SORM – the System for Operative Investigative Activities – installed on premises. This gives the Russian government tapping and interception access to any of the ISP's customers. But wait, all communications are encrypted and authenticated, right? That's what Russia needed to somehow get around.

What Microsoft discovered has been going on for at least the last year. The company attributed the attacks to a group it tracks as Secret Blizzard and is also known as Turla. Previous reporting has linked the group to Center 16 of the Russian FSB intelligence agency, which manages most of the FSB's signals intelligence units. So that makes sense.

The group first selects specific targets and redirects them to an ISP captive portal. That portal explains that they need to update their Kaspersky antivirus. The alleged A/V update package actually installs a new root certificate into the victim's computer along with a malware strain known as ApolloShadow. The malware relaxes the victim's firewalls while the new root certificate legitimizes malicious traffic.

From that point on, Russia is able to freely impersonate any remote site the compromised target may visit. They perform an Adversary in the Middle attack, synthesizing a certificate on the fly for the target to obtain fully unencrypted and visible plain-text traffic. Anyone using an SSL/TLS-style VPN, whose server certificates chain down to standard local roots will have all of network traffic decrypted and inspected.

I hope that embassy IT staff are routinely checking for the appearance of any "extra" certs in their charge's root stores since otherwise this would be a tricky attack to catch.

Microsoft didn't say which embassies Turla attacked, but taking into account that Turla uses a "fake Kaspersky update", it may be Russian-friendly countries from Africa, the Middle East, and Latin America that still use software that's been largely banned from official government use across most Western democracies.

"Dropbox Passwords" manager ending service in October.
I was unaware that Dropbox offered their own password manager. But if any of our listeners might have ever used it, inertia being what it is, they might still be. So I wanted to mention that Dropbox Passwords will be discontinued this coming October 28th. Time to switch!

Meredith Whittaker threatens to leave another country
The Signal Foundation's president Meredith Whittaker has been pushed to once again threaten to withdraw all availability of Signal, this time from Australia. She recently proclaimed that Signal would leave Australia if the government attempted to force it to backdoor its encryption or demand encrypted user data. As we know, she has voiced similar threats to pull Signal from other countries that explored encryption backdoor. This has included France, Sweden, and the UK. And as we noted last week, the European Union's newest head plans to once again push forward on legislation this October. As was noted by last week's coverage, the EU is now planning to leave the encryption itself alone and to, instead, perform its surveillance outside of the encrypted channel, so before data enters and after it exits. Since this might not involve Signal, which accepts incoming data from the underlying OS and asks for its display, I wonder what Signal's position would be in that case.

And, of course, an equally interesting question would be what would Apple's position be, since this would make the design of iOS complicit in turning everyone's iPhone into known surveillance devices. Everything we know about Apple suggests that they would never be willing to turn their iDevices into state surveillance tools. Some sort of reckoning appears to be on the horizon.

In the present case of the Signal uproar, the publication "Information Age" added a bit of background, writing:

> *Laws enabling government access to encrypted private messaging platforms would make Signal’s Australian operations a “gangrenous foot” that would have to be cut off by shutting down local operations, the non-profit's president has warned. Ongoing demands from the likes of ASIO – whose director Mike Burgess has been trying for more than five years to get more power to monitor encrypted messages – have maintained friction between the two communities that has yet to be resolved.*
>
> *Citing the importance of human rights and secure communications as key privacy rights, Signal president Meredith Whittaker told The Australian that “for many people private communication is the difference between life and death.” Even if it were technically possible to snoop on Signal messages – which it is not, due to the platform’s zero knowledge encryption design – she warned that Australian laws mandating access via engineered ‘back doors’ would risk user security worldwide.*
>
> *With “millions” of Australians using Signal, Whittaker said withdrawing from the country would “would hurt the people who rely on us”, but added that she would not hesitate because “if you let the gangrene spread, you poison the body.” Among the users affected by such a move would be the government itself, which – despite police bans on use of the apps – has allowed Signal and its disappearing messages to be used by Home Affairs and other agencies since COVID began. A recent review of 22 Australian government agencies by the Office of the Australian Information Commissioner (OAIC) found widespread use of secure messaging apps even though many lacked appropriate policies for security and transparency.*
>
> *Individuals grilled over their use of Signal include Foreign Affairs Minister Penny Wong and Burgess himself, even as he continues to agitate for access to apps he says are go-to platforms for extremists and “aggressive and experienced” spies targeting Australia.*
>
> *Whittaker’s comments come after reports the government – whose Encryption Act stops short of requiring backdoors – has been intensifying pressure on Signal amidst an escalating campaign to strengthen investigation, interrogation and other powers.*
>
> *The focus on Signal is notable given that it has only 40 million users worldwide – a fraction of WhatsApp’s 2.5 billion, WeChat’s 1.37 billion, and Messenger’s 1.36 billion – and accounts for just 0.85 per cent of the US messaging app market last year. Yet its user base skews towards government executives, journalists, whistleblowers, and other highly security aware individuals attracted to perceptions that it offers higher security that can’t be compromised by court orders.*
>
> *Concern about laws compromising that security have grown so much that media outlet The Guardian recently tapped the University of Cambridge to develop an open source tool enabling end-to-end secure messaging for whistleblowers inside its own news app.*

It is interesting that the Australian government is targeting Signal. I wonder whether they might be deliberately aiming at a smaller fish first to see whether they can get capitulation from them, then use that to climb the ladder to larger targets saying *“Well, Signal did it for us, so why can’t you, too?”* One problem is that it seems clear that Signal is never going to do it for them. The other is that politicians have no understanding of the technology. The entire industry keeps telling them “no” and they keep insisting that the industry is just being stubborn and just doesn’t want to do it. They assume they can ask for any feature they might want and the techies will figure out how to deliver it.

In the case of Signal, they may be failing to appreciate that Signal's entire existence surrounds their refusal to capitulate. Meredith's repeated clear and well-publicized refusals to compromise Signal's integrity is of significant marketing value for Signal.

Given the well publicized moves that the EU may soon be making, I'd be surprised if Australia increases its pressure. I expect the world will be waiting and watching the EU. I know we will be!

YouTube deploys age-estimation heuristics

I gave this next piece the title *"YouTube deploys age-estimation heuristics"*. We've spoken about heuristic solutions in the past. I generally dislike them because they're inherently fuzzy rules of thumb that don't always do what we intend. But there are times when they're all that's available. Last week the official YouTube blog posted under the headline *"Extending our built-in protections to more teens on YouTube"* with the subhead *"We're extending our existing built-in protections to more US teens on YouTube, using machine learning age estimation."* Here's what they wanted the world to know:

> *People come to YouTube to learn and be entertained. This is true even for the youngest audiences, and it's why we remain laser focused on making sure they have a safe and age appropriate experience. Over 10 years ago we launched YouTube Kids, and 4 years ago implemented supervised accounts for pre-teens and teens.*
>
> *Back in February, we shared that we would soon introduce technology that would distinguish between younger viewers and adults to help provide the best and most age appropriate experiences and protections. Over the next few weeks, we'll begin to roll out machine learning to a small set of users in the US to estimate their age, so that teens are treated as teens and adults as adults. We'll closely monitor this before we roll it out more widely. This technology will allow us to infer a user's age and then use that signal, regardless of the birthday in the account, to deliver our age-appropriate product experiences and protections. We've used this approach in other markets for some time, where it is working well. We are now bringing it to the US, and as we make progress we'll roll it out in other markets. We will closely monitor the user experience, and partner with Creators to ensure that the entire ecosystem benefits from this update. Here's how it works:*
>
> *We will use AI to interpret a variety of signals that help us to determine whether a user is over or under 18. These signals include the types of videos a user is searching for, the categories of videos they have watched in the past, or the longevity of the account.*
>
> *When the system identifies a teen user, we'll automatically apply our age-appropriate experiences and protections, including:*
>
> - *disabling personalized advertising*
> - *turning on digital wellbeing tools*
> - *adding safeguards to recommendations, including limiting repetitive views of some kinds of content*
>
> *If the system incorrectly estimates a user to be under 18, they will have the option to verify that they are 18 or over, such as using a credit card or a government ID. We will only allow users who have either been inferred or verified as over 18 to view age-restricted content that may be inappropriate for younger users.*

So, until we obtain proper online age verification solutions, heuristics are the best that can be done and they are the responsible thing to do. I think it's reasonable for YouTube to examine a user's viewing history and if they clearly appear to be a younger viewer, modify the platform to better suit that viewer. And they also offer a path for challenging that decision.

Private key signing for chrome extension developers

Google has rolled out an optional feature they're calling *"Verified CRX Upload."* We've talked about the danger presented by the compromise of high-profile extension developer accounts. If bad guys are able to somehow get into a developer's account, until now nothing would prevent them from malicious modifying the extension, uploading it to the Chrome Extension Store, and causing all instances of Chrome to update and begin using the malicious code.

Now, Google allows developers to create a 2048-bit RSA private/public key pair and to provide the public key to Google for use in verifying the signature of any Chrome Extension that's subsequently offered by the developer.

Google's instructions to developers make very clear that they must not, in any way, store their private key in any of their Google assets. It should never be uploaded. And, in fact they provide the OpenSSL one-liner to generate the key pair in a console session outside of any browser:

```
openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out privatekey.pem
```

Once the public key has been provided to Google, no Chrome extension that's not properly signed by its matching private key will be accepted for publication. So this is a very clear and clean facility to add another layer of authentication to the process. The onus in on the developer to not misplace their private key, as well as to keep it out of the hands of any attackers. So it should really be kept securely offline somewhere. Google's instructions say:

> - *Don't upload the private key to any public repository or other place*
> - *Don't store your private key in your Google Account. This means someone with access to the Developer Dashboard through your Google Account could publish on your behalf.*
> - *Consider storing your private key securely using a keystore like PKCS#12 or Java Keystore*
>
> - *Warning: Don't lose your private key; otherwise, you must reach out to CWS support, and replacement can take up to one week.*

So this is terrific. It's minimal, sufficient and bulletproof. There's no need for any certificate rigmarole since the authenticated developer is creating the key pair and uploading it to Google in their account where it cannot be changed once it's been set. It's a perfect free and lightweight solution.

A Domain Registrar on the ropes

Through the past 20 years we've looked at many instances where a Certificate Authority was repeatedly found, documented and proven to be acting irresponsibly – either by design or through carelessness. In those instances, when that behavior did not change, those certificate signers had their signing privileges revoked and their businesses were effectively ended. It’s a privilege to be able to charge people for a digital signature and with that privilege comes the responsibility to do so properly.

There’s another somewhat related privilege that the Internet offers, which is the privilege to charge people for domain names they wish to use and to have those domain names registered with the Internet’s DNS servers so that traffic addressed to those domains will be able to find its way to the registrant’s domain-based servers and services.

I don’t recall that we’ve ever encountered a story of misconduct on the part of a domain name registrar where their continued right to register domain names – and charge a nice fee for the privilege – was close to being lost. Today we have such a story.

Last Wednesday, the publication “Domain Name Wire” posted some news under their headline: *“ICANN sends breach notice to domain registrar Webnic”* and the subhead: *“Domain industry overseer [that would be ICANN] says domain registrar is lax when investigating and responding to DNS abuse complaints.”* Here’s how the story as told by Domain Name Wire goes:

> *ICANN has sent a breach notice to Web Commerce Communications Limited dba WebNic.cc, a fairly large domain name registrar in Asia. WebNic has about 500,000 .com domain names under management in addition to domains in other extensions. ICANN says the registrar is not complying with Section 3.18.2 of the registrar accreditation agreement, which addresses DNS abuse mitigation.*
>
> *The organization said Webnic failed to follow appropriate steps when receiving DNS abuse complaints. ICANN’s notice said:*
>
> > *ICANN has observed a concerning pattern regarding DNS Abuse mitigation requirements in cases involving WebNic. In multiple instances reviewed by ICANN Contractual Compliance, actionable evidence of DNS Abuse was provided to the Registrar through abuse reports. However, mitigation actions were repeatedly delayed and, in some instances, only taken until after the abuse reporter escalated the matter by submitting a complaint to ICANN. The Registrar frequently issued repeated requests for evidence to abuse reporters – even when the original reports appeared actionable – and failed to fully consider information or clarifications provided by the abuse reporter, ICANN or otherwise reasonably accessible to the Registrar. In other cases, the Registrar requested evidence from the abuse reporters that did not appear to be relevant to the reported activity, causing additional delays.*
>
> *ICANN said the registrar frequently responds to ICANN Contractual Compliance notifications on the last day of the deadline or after it has passed, and those responses are incomplete. Additionally, ICANN says the registrar is not displaying information on its website that is required, including:*
>
> - *The details of the Registrar’s deletion and auto-renewal policies.*
> - *The Registrar’s renewal and redemption/restore fees.*
> - *The methods used to deliver pre- and post-expiration notifications.*
> - *The name and positions of the Registrar’s officers and the name of the ultimate parent entity.*

> *ICANN Compliance has been contacting the registrar about issues since at least February of this year. Finally, WebNic has until August 19 to cure the violations or ICANN will begin the termination process.*

Once again, this just makes me shake my head. More than 500,000 .COM domains in addition of many others. That enterprise is probably generating at least $10 to $15 million dollars per year, for basically just setting up an e-Commerce website, taking registration information and maintaining accounts. And apparently, just as we've seen several times in the past with the Certificate Authority business, the owners and managers appear to lose sight of the fact that this ability to print money is a privilege and not a right. And it's a privilege that can be withdrawn and lost.

This made me curious to know what these WebNic people had and had not done. So I tracked down the notification that ICANN had sent to WebNic. And once again we see that ICANN is falling all over themselves to give these apparent cretins every chance and opportunity to save their own skins. The notice that I found indicated that it had been sent on July 29th, and transmitted via electronic mail, facsimile and courier.

Here's what ICANN sent with the title: *"RE: NOTICE OF BREACH OF REGISTRAR ACCREDITATION AGREEMENT"*

> *Please be advised that as of 29 July 2025, Web Commerce Communications Limited dba WebNic.cc ("WebNic" or "Registrar") is in breach of its 2013 Registrar Accreditation Agreement with the Internet Corporation for Assigned Names and Numbers ("ICANN") dated 25 October 2023 ("RAA"). This breach results from WebNic's failure to comply with Section 3.18.2 of its RAA concerning Domain Name System ("DNS") Abuse mitigation.*

Under "Additional Concerns" it then lists those website documentation issues that were mentioned in the news report. The notice also states that *"the ICANN logo on WebNic's website does not appear to conform with the requirements in the Logo License Specification of the RAA."* The the notice gets to some interesting bits, writing: *"To cure the breach, WebNic must take the following actions by 19 August 2025, 21 days from the date of this letter"*. So that's exactly two weeks from today. Here are the steps that ICANN requires of WebNic by that deadline:

> 1. *Explain all steps the Registrar took to reasonably investigate and reach a determination regarding the use of the domain names us-ledger[.]com, uni-stores-info[.]com, tronlink[.]trading, tronink[.]net, theuni-swap[.]com, thebalan-er[.]com, raydiumx[.]org, kodiak-finance[.]org, app-uni-infos[.]com, and keplr-apps[.]net for DNS Abuse before and after being contacted by ICANN Contractual Compliance regarding these cases. The explanation must include evidence of each step taken and the date each step was taken.*
>
> 2. *Explain why the evidence that the Registrar possessed regarding the use of the domain names listed in item #1 at the time the Registrar investigated the initial abuse reports submitted by the reporters, was deemed insufficient to compel WebNic to reasonably investigate and determine whether the domain names were being used for the specific type of DNS Abuse reported, if applicable.*

> 3. *Explain the process the Registrar has implemented to enable WebNic to fully and promptly assess and act on reports of DNS Abuse in the terms prescribed by Section 3.18 of the RAA. This description must include:*
>
>   a. *Each step of the process and the date the step was implemented.*
>   b. *The target response and mitigation timelines at each stage of the process, and how unnecessary delays are prevented and tracked.*
>   c. *The criteria that the Registrar will generally use for evaluating the sufficiency and relevance of evidence submitted in DNS Abuse reports.*
>   d. *An explanation of how, and how often, the Registrar will monitor and measure the effectiveness of this process to ensure continued compliance with DNS Abuse mitigation requirements.*
>
> 4. *Provide a link to the location on the Registrar's website where WebNic displays the following information:*
>
>   a. *Its renewal and redemption/restore fees.*
>   b. *A description of the methods used to deliver the Registrar's renewal notifications.*
>   c. *The Registrar's deletion and auto-renewal policies.*
>   d. *The names and positions of the Registrar's officers.*
>   e. *The name of the Registrar's ultimate parent entity.*
>   f. *The correct ICANN logo in accordance with the Logo License Specification of the RAA; or remove the ICANN logo from WebNic's website.*
>
> 5. *Provide evidence that the Registrar's registration agreement includes a link to the fees and descriptions referenced in items 4.a and 4.b above.*
>
> 6. *Provide the remediation measures the Registrar has implemented, including the dates of implementation, to ensure that WebNic provides full and timely responses to ICANN Contractual Compliance matters.*
>
> *If WebNic fails to timely cure the violations explained in this Notice of Breach and provide the information requested by 19 August 2025, ICANN may commence the RAA termination process.*

In other words, we have finally run out of patience with you. You have exactly three weeks to explain your past flagrant lack of compliance with the agreement under which you are being allowed to print money, to bring yourself into full compliance and to prove it. If you once again fail to heed these warnings, as you repeatedly have all year, you will find that all of the domains you've had the privilege of renting to your customers will cease to function. They will be de-registered from the Internet's DNS and you can deal with the fallout from that. Have a nice day.

There was also an attachment to this which was interesting. It was titled *"Failure to comply with DNS Abuse mitigation requirements"* and it read:

> *Section 3.18.2 of the RAA requires registrars to take prompt mitigation actions when they reasonably determine that a registered domain name sponsored by the relevant registrar is being used for DNS Abuse which, for the purposes of the RAA, is defined as malware, botnets, phishing, pharming, and spam (when spam serves as a delivery mechanism for the other four forms of DNS Abuse) as those terms are defined in Section 2.1 of SAC115. The Registrar did*

> *not demonstrate compliance with these requirements with respect to the reports addressed in the compliance cases in the chronologies below.*
>
> [We then have that paragraph that was originally cited in the article, which said:]
>
> *Furthermore, ICANN has observed a concerning pattern regarding DNS Abuse mitigation requirements in cases involving WebNic. In multiple instances reviewed by ICANN Contractual Compliance, actionable evidence of DNS Abuse was provided to the Registrar through abuse reports. However, mitigation actions were repeatedly delayed and, in some instances, only taken after the abuse reporter escalated the matter by submitting a complaint to ICANN.*
>
> *The Registrar frequently issued repeated requests for evidence to abuse reporters - even when the original reports appeared actionable - and failed to fully consider information or clarifications provided by the abuse reporter, ICANN or otherwise reasonably accessible to the Registrar. In other cases, the Registrar requested evidence from the abuse reporters that did not appear to be relevant to the reported activity, causing additional delays. This pattern was observed in multiple cases beyond those referenced in this Notice of Breach, including compliance cases 01425212, 01432829, 01336064, and 01439634.*
>
> *On 25 July 2025, the Registrar informed ICANN Contractual Compliance that WebNic had implemented certain improvements to its DNS Abuse mitigation processes as of 11 June 2025. However, a review of case records and communications after 11 June 2025 demonstrates that the Registrar remains out of compliance.*
>
> *The Registrar has also developed a pattern of responding to ICANN Contractual Compliance notifications either on the last day of the specified deadline or after it has passed, often providing incomplete responses and causing further delays and escalations.*
>
> *Moreover, ICANN continues to receive new complaints exhibiting similar allegations and patterns of noncompliance, involving a large number of domain names registered with WebNic.*
>
> *This ongoing behavior constitutes repeated violations of Section 3.18.2 of the RAA and facilitates the prolonged exposure of DNS Abuse to potential victims.*
>
> *CHRONOLOGIES*
>
> *In the compliance cases detailed in the chronologies below, ICANN notified the Registrar of the violations, including the relevant ICANN policies, agreements and processes.*
>
> *Each communication requested the evidence, information and actions needed from WebNic to become compliant. Each subsequent communication to the compliance notifications constituted an additional attempt by ICANN to obtain evidence of compliance from the Registrar. The telephone call details below describe further attempts from ICANN to communicate to the Registrar the details of the cases, and to make an ICANN Contractual Compliance staff member available to address any questions in order to assist WebNic in becoming compliant. All efforts were unsuccessful.*

So the bottom line is that bad guys are using this Asian domain name registrar to establish domain names that are being used for various malicious purposes. And when the abuse of these domain names – with ample evidence – is brought to this Registrar’s attention they just blow it off. Eventually, those reporting the abusive domain names – probably well known and respected security organizations – decided that they need to involve ICANN.

At this point we see the same sort of falling all over themselves attempts from ICANN to not abuse their ultimate power that we've repeatedly seen from the CA/Browser forum members who really don't want to put a certificate authority out of business, but they're really left with no alternative. Here, ICANN is giving these WebNic.cc guys every possible chance to save themselves and to not be kicked off of the gravy train.

I went over to their website at https://www.webnic.cc/ and it looks **fantastic!**. It's got every bell and whistle you could ever want. Stuff is sliding in from off stage, and fading in and out and spinning around as I scroll. There are photos of happy people working and children playing in the sun. Life is grand and everything looks great. But apparently that's all just surface glitz created by some fancy web designer and a bunch of JavaScript. We know that underneath this fancy façade this registrar is behaving so irresponsibly that they may soon be out of business.

This, of course, begs the question: What then happens to all of their hundreds of thousands of customers who were seduced by the glitzy website into entrusting their cherished domains to this registrar?

ICANN has a procedure for handling that. ICANN asks around among the other domain registrars in good standing to determine who would like to take over, in this case WebNic's, domains and customers. ICANN appoints what's known as a "gaining registrar" to take over the affected domain names. There's even an acronym for this: BTAT stands for Bulk Transfer After Termination. All of the terminating registrar's domains are assigned to the gaining registrar with the current domain registrants not needing to take any action. ICANN then notifies the domain holders via email and public announcement. And, importantly, the current domain holder's rights are retained. Their domain registrations remain valid with expiration dates and other settings preserved and the new registrar honoring the remaining registration term. And existing registrants are given the option to transfer their domain elsewhere if they prefer.

It's a mess, but it's the best that can be done under the circumstances. It's difficult to imagine that these guys are not going to come up with some face saving attempt to hold onto their registrant status. Anyone would be crazy to let it go ... but stranger things have happened.

TP-Link tells customers to ditch faulty routers

If any of our listeners might still have an old TP-Link Archer C50 router in service, it's well past time to say goodbye. Not only are those routers now End-of-Life, but they unfortunately shipped with hardcoded static encryption keys in their firmware – and there's now a CVE for it: 2025-6982. There doesn't appear to be any remotely exploitable flaw, but the encryption key used to protect the router's configuration, which contains the admin credentials, Wi-Fi passwords and other internal settings can be trivially decrypted. The encryption is just DES using ECB – Electronic Code Book – cipher, which was never very strong. Again, not an emergency. But much newer routers offer much better security and more state of the art features. Routers are one of those things that it makes sense to replace every five years or so.

Listener Feedback

Before we examine specific listener feedback I wanted to note that many listeners said they were now going to give the Brave browser another try and many others asked rhetorically "what took you so long, Gibson?" Some said they had looked at it in the past and not been impressed, but that in looking at it again it looked great. The guiding philosophy behind Brave appears to even more closely match our listeners' than Firefox. Whereas Firefox is mostly just the alternative to Chrome, Brave is truly on a mission to offer the most privacy enforcement possible. It may be that privacy on the Internet is a lost cause, but why not choose Brave over the others when there's no down-side cost?

Aaron Shaffer

> *Steve, You seem to be entirely unaware of Apple's state ID program for Apple Wallet. Several states already have it deployed. A digital version of my Ohio driver's license has been in my wallet for the last year for example. The state of Ohio also has a free app that someone else can use for me to tap my phone to their phone to verify age from that digital ID. Correct me if I'm wrong, but it seems that all we need is some kind of API call to do the same validation for websites. Thank you for all your good work. I've been a listener since Episode 1. /Aaron*

Aaron was completely correct in concluding that I had not been keeping up with the state of smartphone wallets and existing efforts. So I spent some time since seeing his note looking into what's been going on in that space.

In California as in Ohio, we have a digital drivers license program. It goes by the abbreviation mDL for "Mobile Drivers License". There's a California DMV Wallet app for both Apple and Android phones, and it offers a system known as "TruAge".

I installed the apps under both platforms – into my iPhone and into that $39 Samsung A15 smartphone I had just purchased for Android – and I configured it. The app setup was quick and easy. The apps required me to show them the front and back of my California driver's license, and to then pose for facial recognition while it brightly illuminated the screen in various colors which were reflected off my smiling face.

Once that was done, the apps were satisfied and I had effectively installed a biometrically locked digital driver's license into my phones. Next up was figuring out what "TruAge" was all about.

The TruAge system was developed by NACS – the National Association of Convenience Stores – together with a nonprofit entity known as Conexxus. Conexxus is a retail focused technology standards developer. Together, NACS and Conexxus developed the "TruAge" technology for the retail convenience store industry to support the purchase of age-restricted consumables such as alcohol and tobacco. In bragging about TrueAge, they explain: *"TruAge verifies only age, not identity. It does not store name, address, eye color, etc.—unlike many legacy ID scanners that may capture over 30 personal fields. The encrypted token cannot be linked back to you, and data is not sold or shared."*

However, unfortunately, the *"cannot be linked back to you"* portion is not entirely true. I was immediately suspicious when I saw that the token presented was described as a single-use, encrypted composite consisting of the presenter's driver's license number (whoops!), the issuing state, the license expiration date and the presenter's date of birth. And, sure enough, the "ca.gov" FAQ page says, answering the question *"What happens to the data you do capture?"*:

“TruAge encrypts your data points and then protects them even further by creating anonymous tokens. These anonymous tokens cannot be traced back to you without legal authorization from a court-issued subpoena. Neither retailers nor cashiers retain any of the extracted information.”

So, it’s true that in a retail convenience store setting TruAge will be far more privacy preserving than the traditional requirement of revealing a driver’s license which discloses the individual’s entire identity with their name, home address, exact date of birth, and more in the clear. But, unfortunately, TruAge also fails the *“minimal information sharing”* test when the only thing being required is a proof of biological age.

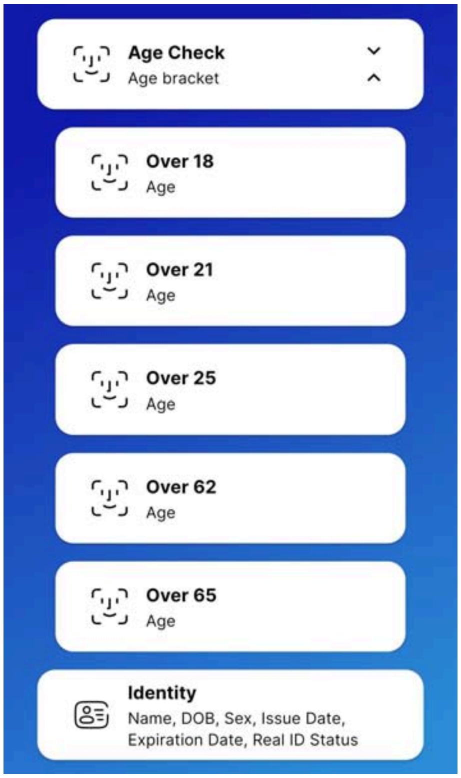
However, less than three months ago, this past May 15th, the NACS association proudly published a press release with the headline: *“TruAge’s Technology Named the De Facto Standard for Digital Age Verification”* with the subhead: *“The World Wide Web Consortium has incorporated TruAge’s underlying technology into its new Verifiable Credentials.”*

That suggests that at least some aspects of the TruAge verification system will be coming soon to a browser near us. Here’s what they wrote:

> *TruAge, the innovative, universally accepted age-verification system that makes it easier to more accurately verify an adult customer’s age when purchasing age-restricted products, and its core-technology have been incorporated into the latest W3C Verified Credentials, Verifiable Credentials 2.0, that were introduced today.*
>
> *The World Wide Web Consortium (W3C) is an international council created in 1994 to create and publish web standards to ensure the growth and development of the web.*
>
> *The new W3C Verified Credentials, which were ratified in late April by its governing body, are a comprehensive update to web standards and affirm that TruAge technology is the centralized standard for digital personhood, making TruAge the accepted standard for all applications that involve age verification.*
>
> *Paul Ziv, TruAge’s vice president of technology and operations said: “TruAge was developed to address strong consumer interest in using a trusted and reliable digital ID that combined consumer privacy and ease of use with the potential for mass retail integration—and it has delivered on that promise. It is very gratifying that W3C agrees with our vision and solution.”*
>
> *Verifiable credentials are increasingly important as communications and commerce continues to go digital, because they can contain all the same information as physical credentials, similar to driver’s licenses and other identification cards. Importantly, by adding technologies such as digital signatures, verifiable credentials can be tamper-proof and seen as more trusted than their physical counterparts.*
>
> *TruAge scans all U.S. driver’s licenses and is also incorporated into the State of California’s mobile driver’s license (mDL) and digital wallet. The W3C announcement makes TruAge the de facto standard for age verification that could be incorporated into all relevant code for pertinent products developed by companies including Microsoft and Apple.*
>
> *While Verifiable Credentials 2.0 was approved to improve the ease of expressing digital credentials, there also were several privacy-preserving goals that were important; both of these objectives are central to the core of TruAge.*

The article continues to elaborate and congratulate itself at some length. And it does again assert that *“It also provides admissible proof-of-age verification appended to retailers’ transaction logs that can be unlocked under subpoena and submitted as evidence.”*

Because TruAge explicitly and deliberately binds the credentialed user’s identity into their age assertion, it does ***not*** do what we want for general purpose online age assertion. So we’re left with the question of how much of TruAge’s over-identification is actually part of the W3C’s new Verifiable Credentials 2.0 specification. Since things like driver’s license number and issuing state are explicitly U.S. identifiers, and the W3C’s specifications need to be global and country-agnostic, I assume that what the W3C may have inherited from TruAge is just its broad single use encrypted token technology without there being any requirement for what’s encrypted within that token.



Aaron started me looking into this with his mention of Ohio. But Ohio and California are not alone. The U.S. states currently offering some form of smartphone wallet storable digital drivers licenses are: Arizona, California, Colorado, Delaware, Georgia, Hawaii, Iowa, Louisiana, Maryland, Mississippi, Missouri, New York, Ohio, Utah and Puerto Rico. Additionally, Montana, New Jersey, Pennsylvania and Texas have pending mobile drivers license legislation underway and 10 other states plus Washington DC have announced their intentions to adopt mobile drivers licenses.

At the moment it’s unclear how all of this is going to shake out and fit together. But, for what it’s worth, my experience with setting things up in California was surprisingly quick, easy and streamlined. I now have iOS and Android apps in my phones that are able to scan a website’s QR code to, in some fashion, assert my full identity if I wish, or just whether I’m above a given age. And while we know that the TruAge system is asserting more than just our ages, it’s still early days and my guess is that the W3C will wind up with a minimal information disclosure solution.

Before we leave this topic I should also mention that, as I had hoped, Yubico’s Stina Ehrensvard is all over this subject. Last Wednesday she sent me a note which read: *“Hi Steve, Hope all is well. Please find our white paper on age verification at internet scale.”* She attached a short 5-page position paper authored by the SIROS Foundation. It’s titled: *“Deployability First: Making Age Verification Work at Internet Scale”* it has the subhead: *“A Position Paper for the 2025 Joint W3C/IAB Workshop on Age-Based Content Restrictions”*. We couldn’t ask for anything more on-point than that. And Stina is the founder of the SIROS foundation. She’s putting the money she made from first founding Yubico to very good use. And, Leo, I know you know Stina as well as I do. God help anyone who stands in her way! She has a way of obtaining the results she’s after. With Stina on the case, the world’s needs for online privacy-respecting age-based content restrictions are in the best possible hands. And as Yubico’s founder, she earned her sway.

So I was certainly uninformed when I recently commented that nothing was happening on the age verification front. A great deal is happening and the best possible people are at work on this problem.

In the meantime, I looked for any sort of TruAge demo site but I was unable to find anything. It appears that TruAge is something of a closed ecosystem for retailers. And that’s just as well, since it’s not sufficiently privacy-enforcing.

Sci-Fi

I wanted to take a moment to say that Andy Weir's second novel, "Artemis" is, in a word, wonderful. The synopsis I saw of it being about some sort of lunar heist doesn't begin to do it justice. I'm at 60%, and the book is pure pleasure. It occurs to me that Andy is very good at creating anti-heroes. Project Hail Mary's Dr. Grace was certainly no one's hero, and neither is Artemis' Jasmine. But if you consider the words "Science" and "Fiction" you would be hard pressed to find any book that better satisfied those terms. There are no neural implants, super-human augmentation, anti-gravity repellor rays or trans-dimensional space folding utilizing energy tapped and funneled down from the 12th dimension. There's none of that. What there is, however, is a very satisfying entirely plausible story penned by someone who is very comfortable with actual science and who writes very enjoyable prose. At 60% of the way through, I am fully engaged, on pins and needles, cannot wait to get back to it, and I have no idea what's going to happen next.

Chinese Participation in MAPP

https://nattothoughts.substack.com/p/when-privileged-access-falls-into

This week, I want to share what I feel is a very fair and balanced assessment of the consequences of the unfortunate, but nevertheless very real, geo-political tensions that have been growing between the U.S. and China, and the consequences of China's longstanding early access to Microsoft's serious security vulnerabilities.

What I want to share was posted to the Natto Thoughts Substack last Thursday in the wake of the SharePoint-driven global network breaches. Natto Thoughts describe themselves, writing:

> *Natto Thoughts explores the intersection of culture, technology, and security, with stories, analysis and insights into the humans of the information age—whether decision-makers, criminals, or ordinary users. We probe the language, culture, institutions, political systems, and unwritten social rules that constrain and inspire their actions.*
>
> *Natto is a sticky Japanese fermented soybean dish with an acquired taste. Fermented foods are slow foods. It helps keep your microbiome—that complex ecosystem that helps you digest— healthy. Like natto, our thoughts have had time to "ferment." We are a group of experts with decades of experience in geopolitical analysis and cyber threat intelligence between us. We do research in a variety of European and Asian languages.*

Last Thursday, having "fermented" on this for some time, they posted under the headline: *"When Privileged Access Falls into the Wrong Hands: Chinese Companies in Microsoft's MAPP Program."* And they added the subhead: *"Chinese companies face conflicting pressures between MAPP's non-disclosure requirements and domestic policies that incentivize or mandate vulnerability disclosure to the state."* Since we've touched on the Chinese government's disclosure requirements for their Chinese enterprises, and since it is so relevant today, having read what these guys have to say, I felt that this audience needed to hear it, too:

> *On July 25, 2025, Bloomberg reported that Microsoft is investigating whether a leak from its Microsoft Active Protections Program (MAPP) allowed Chinese hackers to exploit a SharePoint vulnerability before a patch was released. Microsoft attributed the campaign – dubbed "ToolShell" after the custom remote access trojan used – to three China-linked threat actors: Linen Typhoon, Violet Typhoon, and Storm-2603. The attackers reportedly compromised over 400 organizations worldwide, including the U.S. National Nuclear Security Administration.*
>
> *Launched in 2008, MAPP is designed to reduce the time between the discovery of a vulnerability and the deployment of patches. By giving trusted security vendors early access to technical details about upcoming patches, Microsoft enables them to release protections (such as antivirus signatures and intrusion detection rules) in sync with its monthly updates. The program, however, relies on strict compliance with non-disclosure agreements and the secure handling of pre-release data.*
>
> *Concerns about some Chinese companies violating MAPP requirements are longstanding. In 2012, Microsoft removed Chinese company Hangzhou DPTech Technologies Co., Ltd. from the program for violating its nondisclosure agreement (NDA). According to Bloomberg, in 2021, Microsoft suspected that at least two other Chinese MAPP partners leaked details of unpatched Exchange server vulnerabilities, enabling a global cyber espionage campaign linked to the Chinese threat group Hafnium.*

The Microsoft Exchange hack affected tens of thousands of servers, including systems at the European Banking Authority and the Norwegian Parliament, and was met with global condemnation. Although Microsoft said it would review MAPP following the incident, it remains unclear whether any reforms were implemented, or whether a leak was ever confirmed. In light of the SharePoint case, today's piece examines how MAPP operates, the risks posed by Chinese firms in the program, and which companies are currently involved.

The core purpose of MAPP is to minimize the window of risk between patch rollout and deployment. Simply releasing a patch doesn't mean systems are protected: many organizations delay patching, and attackers often exploit known vulnerabilities during this lag. By giving trusted vendors early access to vulnerability details, Microsoft ensures they can build and distribute detection signatures and other defensive measures in advance, so these protections are already active when the patch is published. Without MAPP, vendors would only begin creating protections after public disclosure, leaving many systems globally, including in China, exposed for critical hours or days.

To participate in MAPP, security vendors must meet criteria that demonstrate their ability to protect a broad customer base. Applicants must be willing to sign a non-disclosure agreement, commit to coordinated vulnerability disclosure practices, share threat information, and actively create in-house security protections such as signatures or indicators of compromise based on Microsoft's data. Microsoft retains discretion over admission and may suspend or expel members who fail to meet participation standards.

According to the MAPP website, members are divided into three tiers based on the amount of time they receive vulnerability information before public release and other criteria: Entry (24 hours in advance), ANS (up to 5 days in advance), and Validate (invite-only, focused on testing detection guidance). However, recently admitted MAPP partners and recognized experts have observed that Microsoft may provide critical vulnerability and threat intelligence as early as two weeks prior to public disclosure. Criteria for determining the criticality which warrants such early releases and to whom the intelligence flows is unclear.

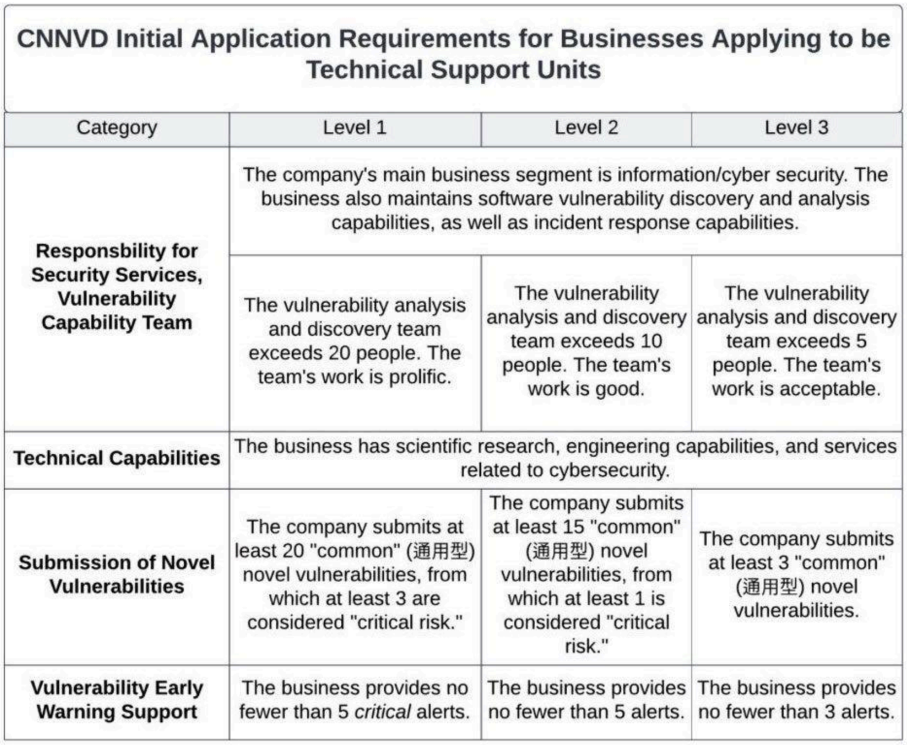
Chinese companies operating within MAPP present a unique risk due to national regulations mandating the disclosure of vulnerabilities to the state. In September 2021, China implemented the Regulations on the Management of Network Product Security Vulnerabilities (RMSV), which require any organization doing business in China to report newly discovered 0-day vulnerabilities to government authorities within 48 hours. This gives Chinese state agencies early access to high-impact vulnerabilities – often before patches are available.

Microsoft itself acknowledged the implications of this policy in its 2022 Digital Defense Report, noting that "this new regulation might enable elements in the Chinese government to stockpile reported vulnerabilities toward weaponizing them."

While the RMSV serves as the primary legal pathway for the state to acquire 0-days, it is not the only mechanism. In 2023, cybersecurity analysts Dakota Cary and Kristin Del Rosso uncovered a parallel, more opaque process involving the China National Vulnerability Database of Information Security (CNNVD), which is overseen by the Ministry of State Security (MSS). Under this framework, Chinese cybersecurity firms voluntarily partner with CNNVD to report vulnerabilities, ***in exchange for financial compensation and prestige.*** *These firms, known as technical support units (TSUs), are stratified into three tiers based on the number of vulnerabilities they submit each year. Tier 1 TSUs must submit at least 20 "common" vulnerabilities annually, including a minimum of 3 classified as "critical risk."*

Yikes. I imagine that everyone listening appreciates how traditional Chinese culture could factor into both the financial compensation and the prestige aspects of this, and how these minimal annual submission requirements to achieve and maintain Tier status would tend to introduce unhealthy incentives.

China's CNNVD Handbook provides a requirements chart for the three participation tiers:



CNNVD Initial Application Requirements for Businesses Applying to be Technical Support Units

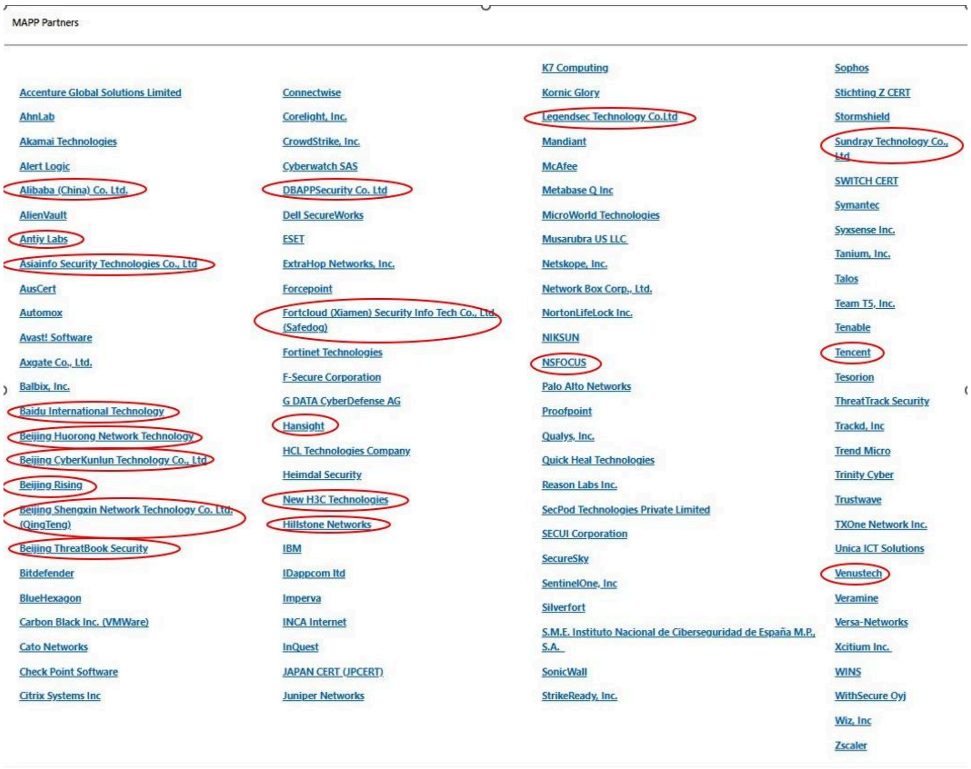
Category	Level 1	Level 2	Level 3
Responsbility for Security Services, Vulnerability Capability Team	The company's main business segment is information/cyber security. The business also maintains software vulnerability discovery and analysis capabilities, as well as incident response capabilities.		
	The vulnerability analysis and discovery team exceeds 20 people. The team's work is prolific.	The vulnerability analysis and discovery team exceeds 10 people. The team's work is good.	The vulnerability analysis and discovery team exceeds 5 people. The team's work is acceptable.
Technical Capabilities	The business has scientific research, engineering capabilities, and services related to cybersecurity.		
Submission of Novel Vulnerabilities	The company submits at least 20 "common" (通用型) novel vulnerabilities, from which at least 3 are considered "critical risk."	The company submits at least 15 "common" (通用型) novel vulnerabilities, from which at least 1 is considered "critical risk."	The company submits at least 3 "common" (通用型) novel vulnerabilities.
Vulnerability Early Warning Support	The business provides no fewer than 5 *critical* alerts.	The business provides no fewer than 5 alerts.	The business provides no fewer than 3 alerts.

Requirements for companies applying to join the CNNVD's Technical Support Units. Source: CNNVD Handbook, Translation by Dakota Cary

As early as 2017, the U.S. threat intelligence firm Recorded Future demonstrated that vulnerabilities reported to CNNVD are assessed by China's Ministry of State Security for their potential use in intelligence operations. As of this writing, 38 companies are classified as Tier 1 contributors to CNNVD, 61 as Tier 2, and 247 as Tier 3. Of these, ten Tier 1 companies, one Tier 2, and one Tier 3 company are currently Microsoft MAPP members.

In addition to providing new vulnerabilities to the CNNVD, these Technical Support Units are also required to provide "vulnerability early warning support" to the Ministry of State Security: at least 5 "critical alerts" annually for Tiers 1 and 2, and at least 3 for Tier 3. As cybersecurity and tech companies, many of these TSUs likely provide this early warning support by reporting newly observed attacks on their customers or systems. Nothing other than Microsoft's non-disclosure agreement precludes TSUs from sharing MAPP data with CNNVD, which may view such submissions as fulfilling this vulnerability early warning support requirement.

Our analysis of the MAPP main page via the Wayback Machine shows that the number of Chinese companies listed in MAPP increased from thirteen in December of 2018 (the earliest available snapshot) to 19 out of a total of 104 member companies globally as of this writing. China thus has the largest national representation after the US.



MAPP Partners

Accenture Global Solutions Limited
AhnLab
Akamai Technologies
Alert Logic
Alibaba (China) Co. Ltd.
AlienVault
Antiy Labs
Asiainfo Security Technologies Co., Ltd
AusCert
Automox
Avast! Software
Axgate Co., Ltd.
Balbix, Inc.
Baidu International Technology
Beijing Huorong Network Technology
Beijing CyberKunlun Technology Co., Ltd
Beijing Rising
Beijing Shengxin Network Technology Co. Ltd. (QingTeng)
Beijing ThreatBook Security
Bitdefender
BlueHexagon
Carbon Black Inc. (VMWare)
Cato Networks
Check Point Software
Citrix Systems Inc

Connectwise
Corelight, Inc.
CrowdStrike, Inc.
Cyberwatch SAS
DBAPPSecurity Co. Ltd
Dell SecureWorks
ESET
ExtraHop Networks, Inc.
Forcepoint
Fortcloud (Xiamen) Security Info Tech Co., Ltd. (Safedog)
Fortinet Technologies
F-Secure Corporation
G DATA CyberDefense AG
Hansight
HCL Technologies Company
Heimdal Security
New H3C Technologies
Hillstone Networks
IBM
IDappcom ltd
Imperva
INCA Internet
InQuest
JAPAN CERT (JPCERT)
Juniper Networks

K7 Computing
Kornic Glory
Legendsec Technology Co.Ltd
Mandiant
McAfee
Metabase Q Inc
MicroWorld Technologies
Musarubra US LLC
Netskope, Inc.
Network Box Corp., Ltd.
NortonLifeLock Inc.
NIKSUN
NSFOCUS
Palo Alto Networks
Proofpoint
Qualys, Inc.
Quick Heal Technologies
Reason Labs Inc.
SecPod Technologies Private Limited
SECUI Corporation
SecureSky
SentinelOne, Inc
Silverfort
S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A.
SonicWall
StrikeReady, Inc.

Sophos
Stichting Z CERT
Stormshield
Sundray Technology Co., Ltd
SWITCH CERT
Symantec
Syxsense Inc.
Tanium, Inc.
Talos
Team T5, Inc.
Tenable
Tencent
Tesorion
ThreatTrack Security
Trackd, Inc
Trend Micro
Trinity Cyber
Trustwave
TXOne Network Inc.
Unica ICT Solutions
Venustech
Veramine
Versa-Networks
Xcitium Inc.
WINS
WithSecure Oyj
Wiz, Inc
Zscaler

Since 2018, several Chinese companies have appeared and disappeared from the MAPP list. Companies that have since disappeared include Beijing Leadsec, Huawei, and Neusoft (removed between December 2018 and November 2019), Qihoo 360 (between November 2019 and October 2020), Hangzhou H3C Technology (between December 2021 and October 2022), and Sangfor (between October 2022 and September 2023).

The reasons for a company's removal from the MAPP list are not always clear. In the case of Huawei and Qihoo 360, the timing aligns with their addition to the U.S. Entity List in 2019 and 2020, respectively. For others, we could not locate any public explanation from Microsoft, unlike the 2012 public notice from the Microsoft Security Response Center regarding DPTech's removal for violating MAPP's NDA requirements.

Of the 19 Chinese companies currently participating in MAPP, 12 are classified as CNNVD TSUs. Based on previous research into their vulnerability submissions to Microsoft's bug bounty program, Tier 1 TSUs such as Tencent, Cyber Kunlun, Sangfor, QiAnXin, and Venustech operate dedicated labs – with varying levels of focus – on identifying vulnerabilities in Microsoft software products.

It is also possible that individuals working at MAPP companies in China individually decide to pass along or sell such information to offensive teams. With access to valuable information and a clear market of buyers, insider risk at MAPP partners themselves cannot be ruled out.

Regardless of the specific mechanism for information diffusion, it is clear that China's incentives for reporting such vulnerabilities – both economic and reputational, as companies seek to meet CNNVD quotas and maintain TSU status for potential business opportunities – create an environment which incentivizes abuse.

> *Vulnerabilities reported to the Ministry of State Security-run CNNVD may be evaluated for potential operational use before being disclosed to the public. Chinese APT groups are known for their speed and coordination in exploiting such vulnerabilities. According to advisories from multiple national cybersecurity agencies and threat intelligence firms, groups such as APT40 and APT41 have exploited vulnerabilities within hours of public disclosure. Chinese APTs are also effective at sharing exploits across groups. Once a vulnerability has been successfully weaponized, it often circulates rapidly among operators.*
>
> *Both of these dynamics were on display during the 2021 Microsoft Exchange campaign. On February 23rd, 2021, MAPP distributed proof-of-concept (POC) code to its members so they could engineer detections. Five days later, mass exploitation of the vulnerabilities with similar code to that distributed via MAPP blanketed the web. According to threat intelligence firm ESET, exploitation began with the China-linked threat group Tick and was quickly followed by other China-linked groups, including LuckyMouse, Calypso and the Winnti Group. Microsoft made patches publicly available for customers shortly thereafter on March 2, 2021–seven days after distributing POC code to MAPP members.*
>
> *A similar pattern recently emerged with the exploitation of the SharePoint vulnerabilities first disclosed at Pwn2Own Berlin in May. The winning submission was reported to Microsoft shortly after the event. As per standard MAPP procedures, Microsoft distributed vulnerability details to selected partners up to two weeks before the public patch, scheduled for July 8th. Yet CrowdStrike observed exploitation as early as July 7, again suggesting that threat groups may have gained access to vulnerability details before protections were made widely available. Microsoft attributed the activity to no fewer than three China-linked groups on July 22.*
>
> *Microsoft's stated mission is to "empower every person and every organization on the planet to achieve more." In line with this mission – and given Microsoft's strong global presence, including a vast user base in China – initiatives like MAPP play a critical role in protecting users from malicious actors. However, such programs require strong safeguards and clear accountability, and ensuring full compliance can be difficult. In unique contexts such as China's centralized vulnerability disclosure system, the inclusion of Chinese companies warrants special scrutiny, especially those participating in domestic programs that incentivize reporting vulnerabilities to the state.*

And this report concludes:

> *Unfortunately for Microsoft's user base in China, the government incentivizes behavior which* ***should*** *jeopardize the continuing participation of legitimately defensive companies in MAPP.*
>
> *It is the role of the PRC government to enforce laws on companies operating within its jurisdiction and responding to its policies. In consideration of Microsoft's pursuit of adequate defense and support of its users, and in line with the company's mission statement, it may be appropriate for Microsoft to temporarily suspend PRC-based companies from MAPP pending an investigation by the PRC government into the potential violation of Microsoft's NDA with local companies.*
>
> *Microsoft has the systemic importance to request such an investigation, as the behavior clearly jeopardizes the safe operation of Critical Information Infrastructure under the PRC Cyber Security Law.*

Given all of the facts that these guys lay out, and the future – if not the past – potential for the rapid abuse of a critical global flaw in widespread Microsoft networking systems, I sincerely hope Microsoft is seriously reconsidering the trusting relationship they have long enjoyed with China's security firms.

If, paraphrasing Kahn, we **were** all one big happy planet, then I'd say that Microsoft's historical position makes sense. Why not share these discovered vulnerabilities before they are patched and remediated? But the sad truth is, tensions are escalating and there doesn't appear to be any reasonable end in sight.

Given that U.S intelligence agencies have firmly concluded that U.S. interests are under constant cyberattack from Chinese threat actor groups which are being actively sponsored by the People's Republic of China, how can it possibly remain rational for Microsoft to be willfully providing Chinese researchers – and indirectly the Chinese government – the very means to attack us, perhaps devastatingly?