MasterCard DNS Error Went Unnoticed for Years

January 22, 2025 43 Comments

The payment card giant **MasterCard** just fixed a glaring error in its domain name server settings that could have allowed anyone to intercept or divert Internet traffic for the company by registering an unused domain name. The misconfiguration persisted for nearly five years until a security researcher spent $300 to register the domain and prevent it from being grabbed by cybercriminals.

```
└─# dig +tcp @dns1.mastercard.com az.mastercard.com

; <<>> DiG 9.19.17-2~kali1-Kali <<>> +tcp @dns1.mastercard.com az.mastercard.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45077
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 5, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: 6d51066062f6102a13bff6c8678149d366a3aabb89779394 (good)
;; QUESTION SECTION:
;az.mastercard.com.             IN      A

;; AUTHORITY SECTION:
az.mastercard.com.      3600    IN      NS      a1-29.akam.net.
az.mastercard.com.      3600    IN      NS      a7-67.akam.net.
az.mastercard.com.      3600    IN      NS      a22-65.akam.ne.
az.mastercard.com.      3600    IN      NS      a26-66.akam.net.
az.mastercard.com.      3600    IN      NS      a9-64.akam.net.

;; Query time: 92 msec
;; SERVER: 216.119.218.53#53(dns1.mastercard.com) (TCP)
;; WHEN: Fri Jan 10 11:24:51 EST 2025
;; MSG SIZE  rcvd: 191
```

A DNS lookup on the domain az.mastercard.com on Jan. 14, 2025 shows the mistyped domain name a22-65.akam.ne.

From June 30, 2020 until January 14, 2025, one of the core Internet servers that MasterCard uses to direct traffic for portions of the mastercard.com network was misnamed. MasterCard.com relies on five shared Domain Name System (DNS) servers at the Internet infrastructure provider **Akamai** [DNS acts as a kind of Internet phone book, by translating website names to numeric Internet addresses that are easier for computers to manage].

All of the Akamai DNS server names that MasterCard uses are supposed to end in “akam.net” but one of them was misconfigured to rely on the domain “**akam.ne**.”

This tiny but potentially critical typo was discovered recently by **Philippe Caturegli**, founder of the security consultancy Seralys. Caturegli said he guessed that nobody had yet registered the domain akam.ne, which is under the purview of the top-level domain authority for the West Africa nation of Niger.

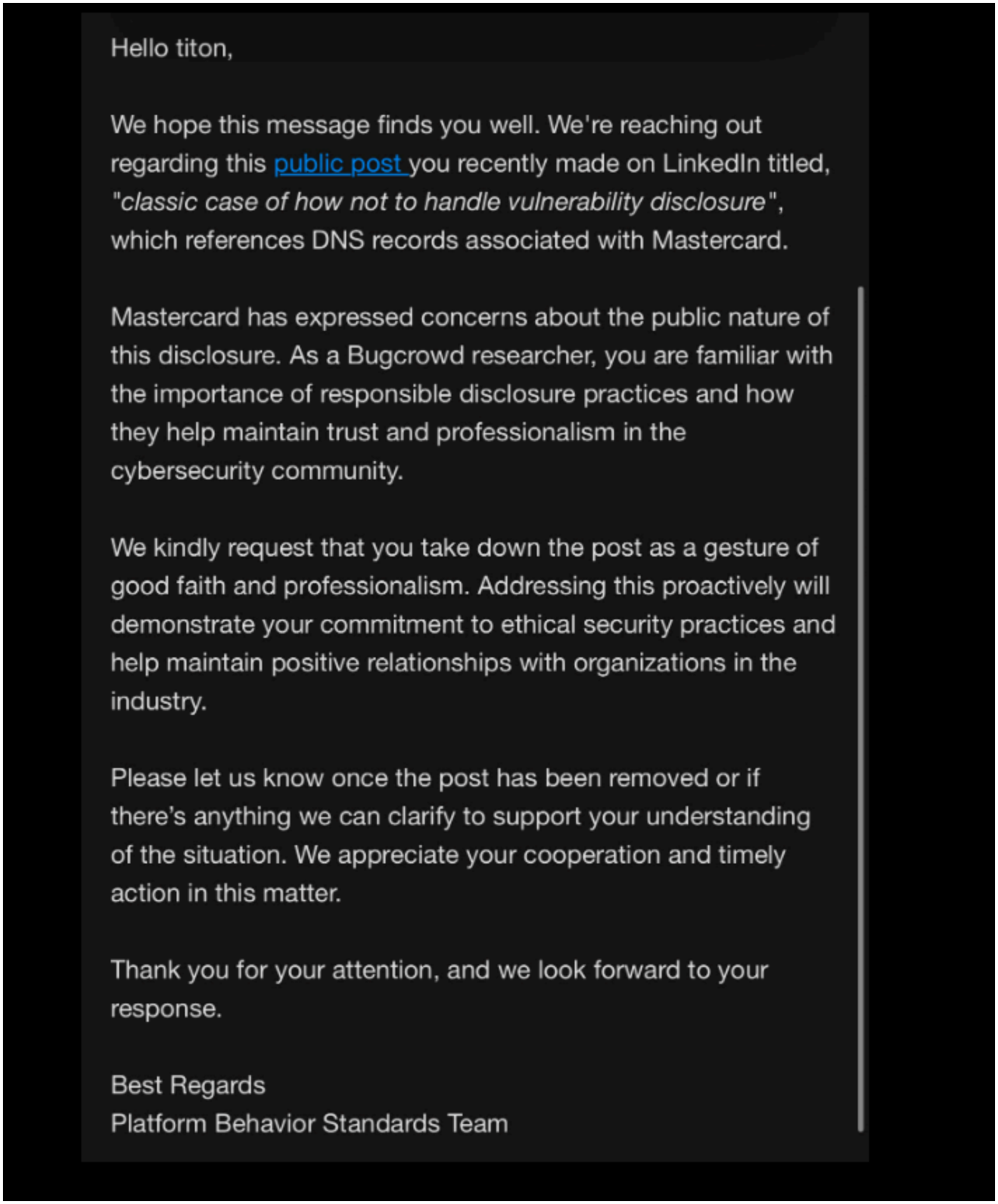
Caturegli said it took $300 and nearly three months of waiting to secure the domain with the registry in Niger. After enabling a DNS server on akam.ne, he noticed hundreds of thousands of DNS requests hitting his server each day from locations around the globe. Apparently, MasterCard wasn’t the only organization that had fat-fingered a DNS entry to include “akam.ne,” but they were by far the largest.

Had he enabled an email server on his new domain akam.ne, Caturegli likely would have received wayward emails directed toward mastercard.com or other affected domains. If he’d abused his access, he probably could have obtained website encryption certificates (SSL/TLS certs) that were authorized to accept and relay web traffic for affected websites. He may even have been able to passively receive Microsoft Windows authentication credentials from employee computers at affected companies.

But the researcher said he didn't attempt to do any of that. Instead, he alerted MasterCard that the domain was theirs if they wanted it, copying this author on his notifications. A few hours later, MasterCard acknowledged the mistake, but said there was never any real threat to the security of its operations.

"We have looked into the matter and there was not a risk to our systems," a MasterCard spokesperson wrote. "This typo has now been corrected."

Meanwhile, Caturegli received a request submitted through **Bugcrowd**, a program that offers financial rewards and recognition to security researchers who find flaws and work privately with the affected vendor to fix them. The message suggested his public disclosure of the MasterCard DNS error via a post on LinkedIn (after he'd secured the akam.ne domain) was not aligned with ethical security practices, and passed on a request from MasterCard to have the post removed.



MasterCard's request to Caturegli, a.k.a. "Titon" on infosec.exchange.

Caturegli said while he does have an account on Bugcrowd, he has never submitted anything through the Bugcrowd program, and that he reported this issue directly to MasterCard.

"I did not disclose this issue through Bugcrowd," Caturegli wrote in reply. "Before making any public disclosure, I ensured that the affected domain was registered to prevent exploitation, mitigating any risk to

MasterCard or its customers. This action, which we took at our own expense, demonstrates our commitment to ethical security practices and responsible disclosure."

Most organizations have at least two authoritative domain name servers, but some handle so many DNS requests that they need to spread the load over additional DNS server domains. In MasterCard's case, that number is five, so it stands to reason that if an attacker managed to seize control over just one of those domains they would only be able to see about one-fifth of the overall DNS requests coming in.

But Caturegli said the reality is that many Internet users are relying at least to some degree on public traffic forwarders or DNS resolvers like **Cloudflare** and **Google**.

"So all we need is for one of these resolvers to query our name server and cache the result," Caturegli said. By setting their DNS server records with a long TTL or "Time To Live" — a setting that can adjust the lifespan of data packets on a network — an attacker's poisoned instructions for the target domain can be propagated by large cloud providers.

"With a long TTL, we may reroute a LOT more than just 1/5 of the traffic," he said.

The researcher said he'd hoped that the credit card giant might thank him, or at least offer to cover the cost of buying the domain.

"We obviously disagree with this assessment," Caturegli wrote in a follow-up post on LinkedIn regarding MasterCard's public statement. "But we'll let you judge— here are some of the DNS lookups we recorded before reporting the issue."

```
sqlite> select source_ip,domain,type  from dns_query_log where domain like "%mastercard.com";
141.101.70.214|authnz360.heracles.prod.westeurope.az.mastercard.com|NS
172.69.193.220|heracles.prod.eastus.az.mastercard.com|CNAME
172.69.21.100|ausoutheast.az.mastercard.com|A
172.69.145.39|az.az.mastercard.com|A
172.68.153.32|az.az.mastercard.com|A
172.69.145.39|apigw.stage.beta.eastus.az.az.mastercard.com|A
172.68.153.32|az.az.mastercard.com|A
172.68.153.32|heracles.heracles.az.mastercard.com|A
94.23.164.164|heracles.prod.eastus.az.mastercard.com|A
172.70.120.40|westus.az.mastercard.com|A
172.70.120.40|heracles.prod.aueast.az.mastercard.com|A
172.68.173.112|prod.authnz360.heracles.prod.eastus.az.mastercard.com|AAAA
172.69.193.220|westus.az.mastercard.com|A
172.69.193.220|apigw.prod.westus.az.mastercard.com|A
172.70.161.98|apigw.prod.westus.az.mastercard.com|NS
172.68.168.102|apigw.dev.beta.work.eastus.az.mastercard.com|AAAA
141.101.70.90|eastus.az.mastercard.com|A
172.71.5.53|apigw.prod.australiaeast.az.mastercard.com|A
172.71.5.53|apigw.prod.australiaeast.az.mastercard.com|A
141.101.70.90|westeurope.az.mastercard.com|A
138.246.253.248|az.mastercard.com|NS
138.246.253.248|az.mastercard.com|None
138.246.253.248|az.mastercard.com|SOA
138.246.253.248|az.mastercard.com|MX
138.246.253.248|az.mastercard.com|AAAA
138.246.253.248|az.mastercard.com|TXT
138.246.253.248|az.mastercard.com|CAA
138.246.253.248|az.mastercard.com|A
172.70.113.174|prod.az.mastercard.com|A
172.71.189.44|eastus.az.mastercard.com|A
```

Caturegli posted this screenshot of MasterCard domains that were potentially at risk from the misconfigured domain.

As the screenshot above shows, the misconfigured DNS server Caturegli found involved the MasterCard subdomain **az.mastercard.com**. It is not clear exactly how this subdomain is used by MasterCard, however their naming conventions suggest the domains correspond to production servers at Microsoft's **Azure** cloud service. Caturegli said the domains all resolve to Internet addresses at Microsoft.

"Don't be like Mastercard," Caturegli concluded in his LinkedIn post. "Don't dismiss risk, and don't let your marketing team handle security disclosures."

One final note: The domain akam.ne has been registered previously — in December 2016 by someone using the email address um-i-delo@yandex.ru. The Russian search giant Yandex reports this user account belongs to an "Ivan I." from Moscow. Passive DNS records from DomainTools.com show that between 2016 and 2018 the domain was connected to an Internet server in Germany, and that the domain was left to expire in 2018.

This is interesting given a comment on Caturegli's LinkedIn post from an ex-Cloudflare employee who linked to a report he co-authored on a similar typo domain apparently registered in 2017 for organizations that may have mistyped their AWS DNS server as "**awsdns-06.ne**" instead of "**awsdns-06.net**." DomainTools reports that this typo domain also was registered to a Yandex user (playlotto@yandex.ru), and was hosted at the same German ISP — Team Internet (AS61969).

This entry was posted on Wednesday 22nd of January 2025 10:24 AM

A LITTLE SUNSHINE | HOW TO BREAK INTO SECURITY

AKAM.NE AKAM.NET AKAMAI AWSDNS-06.NE AZ.MASTERCARD.COM AZURE BUGCROWD CLOUDFLARE GOOGLE MASTERCARD PHILIPPE CATUREGLI SERALYS

43 thoughts on “MasterCard DNS Error Went Unnoticed for Years”

Jordan

January 22, 2025

Im baffled at Mastercard’s response, to be so dimissive and seeminly quite hostile is a strange response from such a large entity.

Miah

-

January 22, 2025

Not really. They pointed out that the emperor wasn’t wearing any clothes, and the emperor responded accordingly. Large corporations are not friendly, they are definitely not your friend, and if you bother them they will squash you.

Jordan

-

January 23, 2025

You would have thought in this day and age, someone at Mastercard should have said it might be a good idea even just to reimburse the cost of the domain, send a generic thank you for reporting and then action it as they please (in this case, dismiss it), that’s more where I was coming from, but I totally see your point!

Wannabe Techguy

-

January 22, 2025

I’m not an IT guy and even I know the response is common. I’m baffled that you’re baffled.

Jordan

-

January 23, 2025

More so they wouldn’t even reimburse the cost of the domain as a small token, which you would hope would be the minimum they would do, even if they choose to do nothing with the vulnerability.

J

-

January 22, 2025

I once reported a flaw in their SmartData service where a credit card user could approve their own transactions simply by using the browser developer tools to enable the `Approved` checkbox.
They complained about me to our credit card administrator and asked why I was poking around.
Thankfully, my manager quite reasonably gave them a dismissive answer.
They did eventually fix the issue

Jordan

-

January 23, 2025

It’s quite clear that they either have the wrong attitude toward cybersecurity or, the wrong people addressing and responding to reported issues.

Victor

-

January 23, 2025

Not strange really, that’s how a lot of large companies respond when they get caught doing something wrong. It makes you considee what else is Mastercard trying to hide.

The_Skeptic

-

January 23, 2025

I’m not. I’ve seen it before from any number of organizations. When an insular company discovers and fixes their own internal problems, they can control the story. It usually means no one is the wiser outside the company. Even when there’s mandatory disclosure they usually bury the disclosure as deep as possible in filings.

When a 3rd party discovers a problem the corproration can’t control the story so the immediate reaction is nearly always hostile to bully those they can into silence. It’s all fun and games till adverse research disclosures affect stock price or job status for management. Financial corporations like MC, Visa, and the like are not anyone’s friends. They have no morals other than survival. Survival means making money. They lash out at anyone that threatens their lifeblood.

It takes a conscious effort and cultural shifts to make corporations behave in a social, non-darwinistic manner. Most c-suite executives are as morally bankrupt as the corporations they run. That’s why there are laws in place to manage the relationship between security researchers and large entities with tremendous resources at their disposal.

Alyx

January 22, 2025

> DomainTools reports that this typo domain also was registered to a Yandex user (playlotto@yandex.ru), and was hosted at the same German ISP — Team Internet (AS61969).

Team Internet (AS61969) is running ParkingCrew. So this is probably not related to any of the yandex users.

Former TI employee

January 22, 2025

> […] was hosted at the same German ISP — Team Internet (AS61969).

This is just a Domain Parking vendor. There is no malware hosted, but a lot of ads. You point your domains there and get money for the delivered ads.

I would interpret the situation that someone just leveraged the typo to earn money, but not actively doing any harm.

Alyx

-

January 22, 2025

I mean, these domains are not really high (browser) traffic domains.
Feels more like they got automatically re-registered once they expired.

Many companies do that, hoping there are still back links generating traffic or even that the domain might be worth something.

Darrin

-

January 22, 2025

I wonder if people realize this. Even though the names returned may not mean anything to the average person and would never be browsed to, these could (and judging by the name, some are) API gateways. Look up what APIs are and how dangerous this could have been. Each credit card transaction is performed ultimately by an API call that is sent to one of these servers. This information includes, for instance all the info needed to authorize a transaction. Account info. The back end things you never see. Those transaction/authorization codes? The client (store, website, you) sends the request to authorize a charge. If successful, a return packet is sent including the authorization code. This opened MC up for Man-in-the-middle (MiTM) attacks. This could have been a huge attack and MasterCard should have acknowledged instead of attempting to downplay it.

r.saulpa

January 22, 2025

2023 Net Profit at Mastercard was over $11 billion. Data from Statista.

ren

January 22, 2025

“”MasterCard acknowledged the mistake, but said there was never any real threat to the security of its operations.

“We have looked into the matter and there was not a risk to our systems,” a MasterCard spokesperson wrote. “This typo has now been corrected.””””

Lol

NKT

January 22, 2025

So it was exploited for a couple of years, then abandoned! Then rediscovered 6 years later.

Mike Wolfe

January 22, 2025

Doing the right thing is never wrong, though the response from Mastercard was poor. If it had been my decision, I would have sent a ‘thank you’ with a Platinum Mastercard that had at least a $300 credit balance to help offset any expenses. A huge callout to Philippe Caturegli on behalf of security practitioners everywhere.

Vinod Patel

January 22, 2025

It’s a shame that Mastercard haven’t compensated for the good deed for the time and costs for the Good Samaritan deeds that

I also think that the UK’s BT should not have stopped the open community using Yellow Pages to reference to addressing IP as many of you experienced folks may remember! And when devices were ypmaster and ypslave in SunOS and similar BSD Unix variations. master and slave are also not used for obvious reasons. We’ll done @krebsonsecurity

RichG

January 22, 2025

Very Poor Response by Mastercard, as if it was from someone who didn’t understand or care. If I was Mastercard I would have sent a gracious note with a $300 reimbursement card for the registration, and

another card with a thank-you for their time and trouble over Mastercard's error.

Al M End

January 22, 2025

Let's see if I have this right: Akamai has no auditing process to determine if a routing goes to a non-responding (dead letter) address? Not trying to absolve MC of this oversight; in 1980s Cuckoo's Egg was written to describe how a team of German hackers had made their way into Defense Dept. mainframes, discovered in a sub-dollar accounting error and confirmed via a network of pagers that alerted Cliff Stol (the author) to intrusion/attempts.

I feel the new climate (political and otherwise) will be fewer and fewer mea culpas and more and more threatening lawsuits or FBI action if you don't take that defamatory LinkedIn post down.

Benji Wiebe

-

January 22, 2025

It's not Akamai's fault. They could check their clients' NS settings as a courtesy but it's not their responsibility nor is it in their control.

Geoff Zub

-

January 22, 2025

But as a security policy they should probably register possible typo squating domains and this is a pretty obvious one… It's a reasonably low cost method of protection.

John Locke

-

January 22, 2025

it was Russian hackers not German. they were using a German satellite. he was using it as a proxy. and selling the information to the KBG

Wannabe Techguy

-

January 22, 2025

Well there have already been many lawsuits and FBI action has been going on for decades I think. It doesn't matter who is in office.

Dave

January 22, 2025

Didn't MasterCard pay a couple billion for a security company called Recorded Future lately?

Dennis

January 22, 2025

What else are you guys expecting from a credit card company?

DomainDanger

January 22, 2025

This was clearly and issue, and good that it's sorted now (at least for Mastercard, but I'm sure many others who have that typo are still unresolved). Dangling domains have a big risk.

I think there are a few parts of the article that would be better rephrased or have further clarity.

“Had he enabled an email server on his new domain akam.ne, Caturegli likely would have received wayward emails directed toward mastercard.com or other affected domains.”
I think this sentence is incredibly misleading, if someone reads ’emails directed toward mastercard.com’ they will be thinking ‘@mastercard.com’ not the subdomain az.mastercard.com. It doesn’t look like az.mastercard.com has ever had an MX record itself, so there’s been no historical use of people even emailing @az.mastercard.com.

Additionally, minor technical point – ‘Had he enabled an email server on his new domain akam.ne’ that would not be the steps to intercept any incoming emails destined to @az.mastercard.com (or any other host within the az.mastercard.com zone). Sure he would have to run an MX server somewhere, but the important part is he would have to intentionally create MX records in the az.mastercard.com zone (that he hosts on a22-65.akam.ne.), which point to this other MX server. It’s not simply hosting an email server ‘on his new domain’.

“He may even have been able to passively receive Microsoft Windows authentication credentials from employee computers at affected companies.”
I think the chance that Mastercard created an ADDS forest or domain using an FQDN within the az.mastercard.com zone is extremely slim. Sure, Active Directory is used heavily in Windows environments – but not only would they need to be running Windows Virtual Machines in those environments that are domain joined, they’d also need to create a new AD domain within that zone. It appears they are using cloud-native approaches for these Azure resources like web apps, application gateways etc.

There absolutely is a risk to what Caturegli found – but I think there are better examples to give, like maybe investigating what services are actually run on those hosts, and the fact that if he were to place resource records in the zone for those labels (or use some wildcards), he could of course be the recipient to a lot of traffic destined for those web apps and application gateways. With a cursory look, it appears things are appropriately firewalled to prevent external inbound traffic.

ronw

January 22, 2025

If “there was not a risk to our systems”, then why did Mastercard care about the LinkedIn post and want it taken down? That seems like saying “It’s not a problem, but don’t talk about the thing we say is not a problem”.

Timo

-

January 23, 2025

In other words: “you can’t proof anything 100% certain and our lawyers will handle the rest so piss off now that we made the cheapest possible fix”

Joshua

January 22, 2025

https://www.recordedfuture.com/press-releases/mastercard-finalizes-acquisition-recorded-future

Physician heal thy self!

Tyler P

January 22, 2025

Reminds me of the Seinfeld episode where Kramer gets all the calls for MOVIEFONE.

JasonR

January 22, 2025

I don’t understand why companies don’t enable DNSSEC in their domains. Mastercard.com does not. There are many advantages, but this should be a requirement for all certificate issues to verify DNS look-ups for all zones that do have DNSSEC enable. This would then prevent a typo such as this from allowing a certificate to be issued by a typo-squatting DNS admin.

I suspect in most cases speed and operational uptime is more important than security.

J Miller

January 22, 2025

Well, the researcher did sit on the registration error for 3 weeks while waiting for his .ne domain name purchase to go through – that’s 3 more weeks of leaving the vulvnerability untouched for what reason? He should have contacted Mastercard or Akamai immediately upon discovering the issue so that it could have been resolved quickly.
So, I don’t see any altruism here and he’s out $300 for his own experiment. I may have done the same but I wouldn’t then expect Mastercard to thank me.

DoubleA

-

January 23, 2025

Noticing the error is one thing; having the evidence that the error was actually exploitable is another thing entirely. He had the ability to provide details to MasterCard that were credible enough for them to address the issue, despite their poor reception of the report.

Some Person

January 22, 2025

Maybe you should ask bugcrowd how much they got for emailing you on behalf of Mastercard. If you ask me Mastercard should not have dismissed your approach, compensated you for the domain name and approached you themselves if they wanted your LinkedIn post removed. Good on you for calling this out.

G.Scott H.

January 22, 2025

Please correct me if I am wrong. Is not the case usually that a frequently mistyped domain is purchased by the owner of the correctly typed name? They do this to protect their customers and their reputation.
So it should have been Akamai interested in claiming the akam.ne domain, the the mistyped version of their akam.net domain. Mastercard should not take ownership of the typo domain since other Akamai customers seem to make the same typo and are affected in the same way.
Mastercard has responded badly. The researcher should have also approached Akamai and offered them the domain instead.
Overall, better than a malefactor owning the domain.

JasonR

-

January 22, 2025

Stupid practice. I may or may not have worked at employer(s) who bought dozens of typo domains, plus derogatory domains, e.g. companyxyzsucks.com, companyxyz-sucks.com etc. Pointless as there are dozens if not hundreds of permutations derogatory and typo domains. Secure the main brand in all the large TLDs and move on.

vb

January 22, 2025

Mastercard's response is similar to "We have investigated ourselves and found no wrongdoing" – used by governments and corporations around the world.

iS

January 22, 2025

"No good deed goes unpunished". I'm a firm believer of this lately…sigh.

Thanks, Brian. Btw have you heard of the other prominent researcher/blogger Dancho Danchev? Seems like he just disappeared.

Greg Choules

January 23, 2025

How many other zones out there are using "akam.ne" in error? A couple of thoughts occur to me:
1) If this is a common mistake, might it be that (at some point in the past) Akamai themselves mistakenly advised customers to use that name, no-one checked and it ended up in zone data?
2) Akamai *could* have foreseen that "akam.ne" is a possible typo of "akam.net" and that, given ".ne" *does* exist, it had the potential to cause havoc if gone unchecked, so should have registered that name themselves.
Just my 2p

Zach

January 23, 2025

It's also interesting that Bugcrowd implied after mitigation of the vulnerability ethically posting about it was in ethical… In my mind that means they are suggesting they were mad they didn't get any money

SH

January 23, 2025

Ah Mastercard. Beside of the already mentioned lack of DNSSEC usage, they also do not configure a CAA record.
Also if you integrate with them you can have your mtls client certificate from any public CA and mastercard leaves it in the dark if they pin on some property or if they just accept any client cert in the end. At a glance it doesn't feel like they implement a lot of best practice.

cybercdh

January 23, 2025

Shameless plug, I wrote a tool a while ago to detect this kind of thing
https://github.com/cybercdh/nsfckup